111-028-4335
MOTC-IOT-110-MEB005

小客車租賃業數位轉型發展計畫-商業模式設計與數位轉型推動實務之專案管理及監督審驗

交通部運輸研究所

中華民國 111 年 3 月

111-028-4335
MOTC-IOT-110-MEB005

小客車租賃業數位轉型發展計畫-商業模式設計與數位轉型推動實務之專案管理及監督審驗

著者：黃啟倡、林良泰、林威延、李英弘、李舒媛、
陳其華、史習平

交通部運輸研究所

中華民國 111 年 3 月

小客車租賃業數位轉型發展計畫-商業模式設計與數位轉型推動實務之

專案管理及監督審驗

著　　者：黃啟倡、林良泰、林威延、李英弘、李舒媛、 陳其華、史習平
出版機關：交通部運輸研究所
地　　址：105004 臺北市松山區敦化北路 240 號
網　　址：www.iot.gov.tw (中文版＞數位典藏＞本所出版品)
電　　話：(02)2349-6789
出版年月：中華民國 111 年 3 月
印 刷 者：全凱數位資訊有限公司
版(刷)次冊數：初版一刷 15 冊
本書同時登載於交通部運輸研究所網站
定　　價：非賣品

著作財產權人：中華民國（代表機關：交通部運輸研究所）
本著作保留所有權利，欲利用本著作全部或部分內容者，須徵求交通部運輸研究所書面授權。

交通部運輸研究所合作研究計畫出版品摘要表

<table>
<tr><td colspan="4">出版品名稱：小客車租賃業數位轉型發展計畫-商業模式設計與數位轉型推動實務之專案管理及監督審驗</td></tr>
<tr><td>國際標準書號（或叢刊號）</td><td>政府出版品統一編號</td><td>運輸研究所出版品編號
111-028-4335</td><td>計畫編號
110-MEB005</td></tr>
<tr><td>本所主辦單位：運輸經營管理組
主管：陳其華
計畫主持人：陳其華
研究人員：史習平
聯絡電話：(02)23496839
傳真號碼：(02)25450431</td><td colspan="2">合作研究單位：逢甲大學
計畫主持人：黃啟倡
研究人員：林良泰、林威延、李英弘、李舒媛
地址：臺中市西屯區文華路 100 號
聯絡電話：(04)24517250#6640</td><td>研究期間
自110年2月

至110年12月</td></tr>
<tr><td colspan="4">關鍵詞：專案管理、小客車租賃業、策略研擬、監督審驗</td></tr>
<tr><td colspan="4">摘要：
為提升小客車租賃業數位化能力，並改善小客車租賃產業營運環境與整體交通環境，本所辦理「小客車租賃業數位轉型發展計畫-商業模式設計與數位轉型推動實務」。希望透過本計畫之專案管理，進行各方溝通與協調，定期召開會議，追蹤主計畫執行與系統開發進度，確保主計畫能夠如期、如質地完成，以降低風險發生機率，並透過監督審驗機制，針對系統進行實際測試，包含：功能性測試與驗證、安全性驗證、壓力測試與易用性測試等，並研提相關系統意見，以做為後續系統平台精進之參考，並進一步確認系統開發項目符合計畫需求，俾利後續推廣應用。</td></tr>
<tr><td>出版日期</td><td>頁數</td><td>定價</td><td>本 出 版 品 取 得 方 式</td></tr>
<tr><td>111 年 3 月</td><td>438</td><td>非賣品</td><td>凡屬機密性出版品均不對外公開。普通性出版品，公營、公益機關團體及學校可函洽本所免費贈閱；私人及私營機關團體可按定價價購。</td></tr>
<tr><td colspan="4">備註：1.本研究之結論與建議不代表交通部之意見。
2.本研究係使用行政院國家科學技術發展基金經費辦理。</td></tr>
</table>

PUBLICATION ABSTRACTS OF RESEARCH PROJECTS
INSTITUTE OF TRANSPORTATION
MINISTRY OF TRANSPORTATION AND COMMUNICATIONS

TITLE: Development Project for the Digital Transformation of the Car Rental Industry – Project Management and Supervision of business model design and digital transformation to promote practice

ISBN(OR ISSN)	GOVERNMENT PUBLICATIONS NUMBER	IOT SERIAL NUMBER	PROJECT NUMBER
		111-028-4335	110-MEB005

DIVISION: Operations and Management Division
DIVISION DIRECTOR: Chi-Hwa Chen
PRINCIPAL INVESTIGATOR: Chi-Hwa Chen
PROJECT STAFF: Hsi-Ping Shih
PHONE:886-2-23496839
FAX:886-2-25450431

PROJECT PERIOD
FROM February 2021
TO December 2021

RESEARCH AGENCY: Feng Chia University
PRINCIPAL INVESTIGATOR: Chi-Chuang Huang
PROJECT STAFF: Liang-Tay Lin, Wei-Yen Lin, Ying-Hong Li, Shu-Yuan Li
ADDRESS: No. 100, Wenhwa Rd., Seatwen, Taichung, Taiwan 40724, R.O.C.
PHONE: (04)24517250#6640

KEY WORDS: Project Management, Car-Rental, Strategy Discussion, Supervision

ABSTRACT:

To enhance the digitization capability and improve the operation and overall transportation environment of the car rental industry, we carried out the "Development Project for the Digital Transformation of the Car Rental Industry -business model design and digital transformation facilitating practice". It was hoped that through the project management of this study, communication and coordination between all parties could be carried out, regularly tracking development progress to ensure that the system construction could be completed with a certain quality and on time, as well as in compliance with relevant laws and regulations. And to reduce the probability of risk. Through the supervision and verification mechanism, the system platform was test, including functional testing and verification, security verification, stress testing and usability testing, and advices providing, as a reference for subsequent system platform improvement, and further confirmation of the system The development project meets the needs of the plan and benefits the follow-up promotion and application.

DATE OF PUBLICATION	NUMBER OF PAGES	PRICE
March 2022	438	Not For Sale

1.The views expressed in this publication are not necessarily those of the Ministry of Transportation and Communications.
2.The budget of this research project is contributed by National Science and Technology Development Fund.

目錄

表目錄 V
圖目錄 VII
第一章 緒論 1
1.1 計畫背景 1
1.2 計畫目的 1
1.3 計畫內容 2
第二章 文獻回顧 7
2.1 智慧租車及營運 7
2.2 專案管理及監督審驗 8
2.3 文獻評析 19
第三章 專案管理及監督審驗 21
3.1 專案管理 21
3.1.1 專案進度控管 21
3.1.2 辦理事項列管追蹤 33
3.1.3 知識諮詢成果 35
3.1.4 風險控管 55
3.1.5 各階段風險與管控措施 58
3.1.6 本案實際發生風險及管控情況 62
3.2 系統測試與驗證 66
3.2.1 系統測試範圍 66
3.2.1.1 智慧租車共通平台 66
3.2.1.2 新智慧租車平台 68
3.2.2 系統測試與認證 71
3.2.2.1 智慧租車共通平台 71
3.2.2.2 新智慧租車平台 94
3.3 監督審驗 159
3.3.1 品質監督審驗工作與流程 159

3.3.2 第三方獨立驗證與認證 171
第四章 結論與建議 199
4.1 結論 199
4.2 建議 200
參考文獻 201
附件一 期中審查意見回覆表 203
附件二 期末審查意見回覆表 207
附件三 PWA 頁面驗證(PWA Scan report by Lighthouse) 213
附件四 弱點掃描 231
附件五 易用性測試 341
附件六 符合性驗證相關截圖 347
附件七 期末審查簡報 387

表目錄

表 2.1-1 國內外小客車租賃業之營運模式比較 7
表 3.1-1 會議綜整表 22
表 3.1-2 本計畫之專管任務 32
表 3.1-3 會議結論辦理情形管考 33
表 3.1-4 服務建議書之專管建議 35
表 3.1-5 評估圖示與情形對照表 36
表 3.1-6 期初發表會簡報與企劃書之專管建議追蹤表 36
表 3.1-7 小客車租賃業者招募相關文件之專管建議追蹤表 37
表 3.1-8 深度訪談計畫之專管建議追蹤表 43
表 3.1-9 其他資料之專管建議追蹤表 47
表 3.1-10 系統(含金流)相關文件之專管建議追蹤表 50
表 3.1-11 本計畫採用之風險矩陣與等級 56
表 3.1-12 風險等級與機率 58
表 3.1-13 本專案風險因子一覽表 58
表 3.1-14 招募進度檢核表 64
表 3.2-1 智慧租車共通平台系統-服務端定義、名稱與網址對照表 67
表 3.2-2 新智慧租車平台-服務端定義、名稱與網址對照表 68
表 3.2-3 測試所需軟體工具 72
表 3.2-4 測試評估缺失等級說明 95
表 3.2-5 測試評估缺失等級表-平台與車商作業端 95
表 3.2-6 測試評估缺失等級表-行動門市端 97
表 3.2-7 測試評估缺失等級表-附駕司機 98
表 3.2-8 測試評估缺失等級表-消費者端 98
表 3.2-9 使用性問題嚴重程度分級標準 138
表 3.2-10 情境一：消費者租車(自駕) 139
表 3.2-11 情境二：消費者取車(自駕)、門市人員核銷 139
表 3.2-12 情境三：消費者租車(附駕)、司機接單執行代駕 140

表 3.2-13 情境四：平台管理人員查看訂單狀態、車商主管派車並上架車輛 140
表 3.2-14 SUS 評分方式說明 141
表 3.2-15 受測者填寫結果 142
表 3.2-16 CarU 前台(PWA/Web)反饋紀錄表 143
表 3.2-17 行動門市 app 反饋紀錄表 146
表 3.2-18 附駕司機 app 反饋紀錄表 147
表 3.2-19 CarU 後台反饋紀錄表 147
表 3.2-20 新智慧租車反饋紀錄表 147
表 3.3-1 因應品質管理要求的文件審查項目 159
表 3.3-2 評估等級表 168
表 3.3-3 第三方監督審驗問題表 170
表 3.3-4 測試設置說明表 172
表 3.3-5 測試物件說明表 173
表 3.3-6 驗證測試執行人員表 175
表 3.3-7 新智慧租車平台系統驗證查檢表 176
表 3.3-8 第一年期-新智慧租車平台認證期程表 193
表 3.3-9 第二年期-小客車租賃服務整合旅遊生態系平台認證期程表 196

圖目錄

圖 1.2.1 數位轉型推動計畫與本計畫對應之工作項目 2
圖 2.2.1 歐盟授權獨立驗證構之子系統驗證作業流程 12
圖 2.2.2 德國聯邦鐵路獨立驗證與認證體系 13
圖 2.2.3 歐盟授權獨立驗證構之子系統驗證作業流程 14
圖 2.2.4 政府、特許機構及驗證與認證機構之三方工作關係圖 15
圖 2.3.1 小客車租賃業數位轉型發展計畫專案管理概念圖 20
圖 3.1.1 風險之 ALARP 圖 55
圖 3.1.2 本計畫風險控管方法及流程圖 57
圖 3.2.1 智慧租車共通平台整合旅遊生態系平台整體架構圖 66
圖 3.2.2 漢名 1201 所提交之文件清單 70
圖 3.2.3 智慧租車共通平台-點選圖片後無法正常檢視圖片 72
圖 3.2.4 智慧租車應用服務(消費者)-無法修改會員資料 73
圖 3.2.5 智慧租車應用服務(消費者)-設定資訊有兩個變更密碼 73
圖 3.2.6 智慧租車應用服務(消費者)-交易資訊圖片無法正常顯示 74
圖 3.2.7 智慧租車應用服務(車商)-交易資訊圖片無法正常顯示 74
圖 3.2.8 ZAP Scanning Report-後台片段截圖 76
圖 3.2.9 ZAP Scanning Report-前台片段截圖-part 1 76
圖 3.2.10 ZAP Scanning Report-前台片段截圖-part 2 77
圖 3.2.11 金流測試截圖-輸入訂單測試資料 78
圖 3.2.12 金流測試截圖-選擇租用車輛 79
圖 3.2.13 金流測試截圖-確認預約車輛 80
圖 3.2.14 金流測試截圖-金流頁面跳轉前頁 80
圖 3.2.15 金流測試截圖-付款方式輸入頁 81
圖 3.2.16 金流測試截圖-填寫完付款方式後的確認訊息框 82
圖 3.2.17 金流測試截圖-OPT 簡訊驗證碼輸入頁面 82
圖 3.2.18 金流測試截圖-OPT 簡訊驗證碼接收結果 83
圖 3.2.19 金流測試截圖-交易資料傳輸頁面 83

圖 3.2.20 金流測試截圖-交易完成頁面(金流端) 84
圖 3.2.21 金流測試截圖-交易完成 84
圖 3.2.22 金流測試截圖-交易完成頁面(使用者端) 85
圖 3.2.23 金流測試截圖-交易查看頁面(使用者端) 86
圖 3.2.24 金流測試截圖-交易查看頁面(平台端) 87
圖 3.2.25 金流測試截圖-交易訂單取消頁面(使用者端) 88
圖 3.2.26 金流測試截圖-交易訂單確認頁面(使用者端) 89
圖 3.2.27 金流測試截圖-交易訂單完成確認頁面(使用者端) 89
圖 3.2.28 金流測試截圖-交易訂單取消確認頁面(平台端) 90
圖 3.2.29 金流測試截圖-測試訂單資料頁(使用者端) 91
圖 3.2.30 金流測試截圖-輸入錯誤的卡號資訊測試交易(使用者端) 91
圖 3.2.31 金流測試截圖-交易失敗顯示資訊(綠界頁面) 92
圖 3.2.32 金流測試截圖-交易失敗顯示資訊(使用者端) 92
圖 3.2.33 金流測試截圖-交易失敗後顯示之訂單資訊(使用者端) 93
圖 3.2.34 金流測試截圖-交易記錄於平台端的顯示 94
圖 3.2.35 [T-C-01] 車商管理-email 無法留白 99
圖 3.2.36 [T-C-02] 營運統計表-無報表下載功能 99
圖 3.2.37 [T-C-03] 站點管理-GPS 定位異常 100
圖 3.2.38 [T-C-03] 站點管理-定位問題導致站點地圖資訊失準 101
圖 3.2.39 [T-C-03] 站點管理-站點地圖「處理」功能操作異常 101
圖 3.2.40 [T-C-03] 站點管理-「說明」功能顯示異常 101
圖 3.2.41 [T-C-04] 車輛管理-輸入欄位沒有檢查格式 102
圖 3.2.42 [T-C-04] 車輛管理-資料顯示異常 102
圖 3.2.43 [T-C-04] 車輛管理-資料刪除回饋顯示異常 103
圖 3.2.44 [T-C-05] 駕駛管理-資料刪除回饋顯示異常 103
圖 3.2.45 [T-C-05] 駕駛管理-站點資料顯示功能異常 104
圖 3.2.46 [T-C-06] 員工管理-不同車商使用同帳號的回饋訊息 104
圖 3.2.47 [T-C-06] 員工管理-密碼資料非強制輸入 105
圖 3.2.48 [T-C-06] 員工管理-密碼留白所遭遇的錯誤畫面 105

圖 3.2.49 [T-C-06] 員工管理-員工管理頁面顯示資訊改善建議 105
圖 3.2.50 [T-C-07] 車商價格管理-車型資料操作疑似誤設計 106
圖 3.2.51 [T-C-08] 站點價格管理-顯示資訊與車商價格管理相同 107
圖 3.2.52 [T-C-09] 內附項目管理-新增功能操作異常 107
圖 3.2.53 [T-C-10] 上架管理-上架功能操作異常 108
圖 3.2.54 [T-C-10] 上架管理-上架功能檢視限制與顯示異常 108
圖 3.2.55 [T-C-10] 上架管理-無上架進度檢視相關資訊 109
圖 3.2.56 [T-C-10] 上架管理-上架後 CarU 端顯示過濾器異常 109
圖 3.2.57 [T-C-11] 訂單管理-訂單判斷與顯示邏輯疑似異常 110
圖 3.2.58 [T-C-11] 訂單管理-訂單狀態顯示異常(如已還車，但顯示未派車等) 110
圖 3.2.59 [T-U-01] 登入-使用 Google 帳號登入顯示異常 111
圖 3.2.60 [T-U-02] 車輛搜尋-資訊顯示相關修正建議 112
圖 3.2.61 [T-U-03] 購物車與購買-購物車資訊在金流交易取消後會消失 112
圖 3.2.62 [T-U-03] 購物車與購買-於金流交易取消後，優惠券呈現已兌換 .. 113
圖 3.2.63 [T-U-03] 購物車與購買-待修正議題 113
圖 3.2.64 [T-U-04] 金流交易-操作未成功，平台依舊顯示訂單確認。 114
圖 3.2.65 [T-U-05] 檢視訂單-完成金流交易卻顯示訂單為付款失敗-part 1 ... 114
圖 3.2.66 [T-U-05] 檢視訂單-完成金流交易卻顯示訂單為付款失敗-part 2 ... 115
圖 3.2.67 [T-U-05] 檢視訂單-照片上傳未正常顯示於管理頁面，前後台訂單編號資訊未同步 115
圖 3.2.68 [T-U-05] 檢視訂單-管理端如果取消訂單，使用者端狀態不會更新；系統端的時戳有誤 116
圖 3.2.69 CarU 後台存取錯誤訊息 116
圖 3.2.70 透過 Line 軟體開啟行動門市頁面，顯示相機載入失敗 117
圖 3.2.71 消費者於附駕司機頁面，需另外選附駕駛才行。 117
圖 3.2.72 PWA 檢測結果-消費者端 118
圖 3.2.73 PWA 檢測結果-行動門市端 119
圖 3.2.74 PWA 檢測結果-附駕司機端 119

圖 3.2.75 弱點掃描概要-CarU 平台 121
圖 3.2.76 弱點掃描概要-新智慧租車平台 121
圖 3.2.77 弱點掃描概要-行動門市 122
圖 3.2.78 弱點掃描概要-附駕司機 122
圖 3.2.79 弱點掃描概要-API 主機 123
圖 3.2.80 系統平台 SSL 憑證效期 123
圖 3.2.81 系統平台 API 檢測-取得商品 ID-1 124
圖 3.2.82 系統平台 API 檢測-取得商品 ID-2 125
圖 3.2.83 系統平台 API 檢測-取得商品詳細資訊 125
圖 3.2.84 系統平台 API 檢測-根據租車期間查詢該商品價格.. 126
圖 3.2.85 系統平台 API 檢測-訂購商品並取得核銷 QRcode 126
圖 3.2.86 系統平台 API 檢測-變更整筆或部分訂單狀態 127
圖 3.2.87 系統平台 API 檢測-消費者上傳租還車照片 127
圖 3.2.88 系統平台 API 檢測-查詢訂單內容 128
圖 3.2.89 透過修改 URL 取得/修改/其他車商的資料-1 128
圖 3.2.90 透過修改 URL 取得/修改/其他車商的資料-2 129
圖 3.2.91 透過修改 URL 取得/修改/其他車商的資料-3 129
圖 3.2.92 透過修改 URL 取得/修改/其他車商的資料-4 130
圖 3.2.93 壓力測試-CarU 平台 133
圖 3.2.94 壓力測試-新智慧租車平台 134
圖 3.2.95 壓力測試-行動門市 135
圖 3.2.96 壓力測試-附駕司機 136
圖 3.2.97 註冊-無先行提示密碼設定限制；手機格式錯誤仍可註冊成功 150
圖 3.2.98 搜尋商品-進階搜尋中已勾選的項目未顯示在搜尋畫面中 150
圖 3.2.99 訂購商品-按「立即訂購」的邏輯是直接進行付款，不需再按「預定」 151
圖 3.2.100 填寫取還車日期-不知道要選擇下方日曆的日期因而重複點選日期欄位 152
圖 3.2.101 勾選加購服務-取消勾選框內仍有打勾殘影 152

圖 3.2.102 取還車照片紀錄-上傳速度過慢且無上傳中之提示 153
圖 3.2.103 我的訂單-我的訂單通常會在主選單內，而非藏於第二層選單中 153
圖 3.2.104 我的訂單-訂單無 QRcode 之查找提示 153
圖 3.2.105 行動人員核銷-核銷後左下方的按鈕顯示「掃得很重」 154
圖 3.2.106 附駕司機核銷-開始任務後無執行中任務，且找不到結束任務功能 154
圖 3.2.107 後台訂單管理-訂單狀態與付款狀態資訊不一致 155
圖 3.2.108 控制台-數字的呈現方式應與通用性之按鈕設計有所區別 155
圖 3.2.109 車輛管理-手機版頁面無法顯示已建立之內容 155
圖 3.2.110 新增駕駛資料-不同的儲存按鈕令使用者感到困惑 156
圖 3.2.111 上架管理-使用者不清楚上架流程，車輛總數小於上架及庫存數 156
圖 3.2.112 訂單管理-系統顯示「已還車」卻仍可進行派車 157
圖 3.2.113 訂單管理-空租訂單卻顯示「代駕開始」 157
圖 3.2.114 訂單管理-過濾時間之功能不明顯 158
圖 3.3.1 IV&V 評估方法與目的 161
圖 3.3.2 現地見證/稽核流程 165
圖 3.3.3 軟體生命週期、相關產出報告與因應之測試 167
圖 3.3.4 符合性認證流程圖 168
圖 3.3.5 認證作業流程 169
圖 3.3.6 Google Chrome 瀏覽器版本確認圖 173
圖 3.3.7 新智慧租車共通平台登入畫面 173
圖 3.3.8 附駕司機 PWA 登入畫面 174
圖 3.3.9 行動門市 PWA 登入畫面 174
圖 3.3.10 Taiwan CarU 電商平台登入畫面 174
圖 3.3.11 消費者 WebSite 登入畫面 175
圖 3.3.12 第一年期-新智慧租車平台認證甘特圖 194
圖 3.3.13 第二年期-小客車租賃服務整合旅遊生態系平台認證甘特圖 197

第一章 緒論

1.1 計畫背景

隨著科技的發展，資訊的進步，大型專案為現今臺灣發展時常面臨的推動作法，因此為使計畫執行達一定品質，以往會透過專案管理團隊的協助，提升整體計畫執行的質與量。在此背景下，交通行動服務 (Mobility as a Service, MaaS) 的概念廣受各國探討，因此為提供生活便利性、提供多元商機，租賃小客車在整體交通運輸服務上，扮演串起民眾行動需求的重要角色。為積極輔導小客車租賃業數位轉型，交通部向行政院國家科學技術發展基金管理會提送補助計畫申請，並結合經濟部技術處現有技術資產，共同發展符合臺灣適地性之「智慧租車平台服務」大型建置專案，期能藉由新科技與智慧化服務的導入，強化整體交通行動服務網絡以及提升國內小客車租賃相關產業衍生產值，增加整體產業的競爭力，提供民眾更優質的服務體驗。

因此，為使上述服務平台能有效推廣與執行，有必要透過第三方專案管理團隊進行計畫品質監督與審驗，以系統測試、文件審查及多面相的專業技術諮詢，提升計畫的執行品質與降低若干之風險。

1.2 計畫目的

為確保「小客車租賃業數位轉型發展計畫-商業模式設計與數位轉型推動實務」系統規劃建置、既有相關技術持續發展、服務推廣、營運模式、策略研擬等之完善，並有效掌握成果品質，符合專案設定服務水準，爰辦理本計畫，藉由具專案管理及監督審驗能力之專案管理廠商，辦理計畫之「專案管理」及「獨立驗證與認證」工作，以期達成專案管理品質之提升、建置案品質之監控查核、審查作業效率之提高，及確保相關系統之建置、產品服務之推廣，得以符合需求且具永續性。亦針對「小客車租賃業數位轉型發展計畫-商業模式設計與數位轉型推動實務」相關工作項目，擬定本計畫應執行之專案管理、專業知識諮詢、獨立監督審驗等工作項目，如圖 1.2.1 所示。

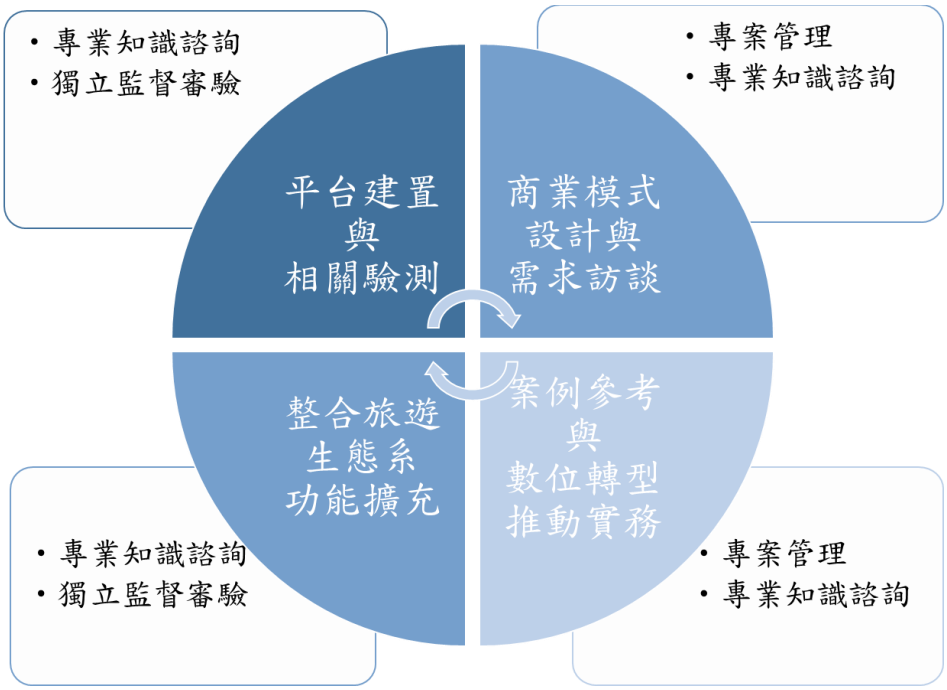


圖 1.2.1 數位轉型推動計畫與本計畫對應之工作項目

1.3 計畫內容

本計畫主責監督與審驗「小客車租賃業數位轉型發展計畫-商業模式設計與數位轉型推動實務」(簡稱主計畫)系統規劃建置、服務推廣、營運模式、策略研擬等項目，而本計畫須完成之三個主要工作項目，包含「專案管理服務」、「專業知識諮詢」與「獨立監督審驗」。

由於智慧租車平台系統為一個大平台，在專案執行上除了軟體開發外，亦需解決眾多小客車租賃業者的需求與問題。在有限的時間與資源下，面對業者需求(一千多家小客貨車租賃業者在數位化轉型的過程中，勢必會衍生許多問題與需求)，在專案執行上會面臨到資源配置的問題、風險評估與控管(不理想與不可忍受之風險擬定對應之處理方法。針對軟體部分，及早發現軟體問題，並快速解決，以避免軟體瑕疵之擴大)、系統功能設計與規劃的取捨、系統的功能性測試與驗證(確保建置案軟體之設計，具有產品功能發揮)、軟體使用者介面的評估等問題，勢必需要有專業團隊負責專案進度管控、品質管理與風險控管、系統測試與驗證、監督審驗與專業知識諮詢，以確保此專案在執行上能夠有預期的成果與品質。結合產官學的眾人智慧達到提供明確的工作範疇、里程碑與交付標的、系統分析設計與測試、系統上線與驗收等各階段確認問題與驗證之專業技術諮詢服務，並釐清責任歸屬。

本計畫每週定期追蹤主計畫執行狀況、每兩週定期與主計畫廠商召開工作會議與相關討論會議。除此之外，亦須提供專業知識諮詢服務，針對主計畫提出之規劃構想與實際產出文件之差異，研提相關意見與建議，並於主計畫建置之系統實際上線前，進行實際驗測，確保後續營運團隊、小客車租賃業者、使用者能正常且順利使用，且須確保主計畫撰寫之相關技術文件品質符合需求，未來能順利授權相關開發成果與文件。

以下為本計畫兩年期應執行之工作項目，如下所述：

1. 第1年期須協助「小客車租賃業數位轉型發展計畫-商業模式設計與數位轉型推動實務(1/2)」(以下簡稱主計畫)之「專案管理服務」、「專業知識諮詢」與「獨立監督審驗」。

(1) 專案管理服務

A. 追蹤管控主計畫執行過程之相關問題與議題。

B. 協助辦理分項二「智慧租車服務營運規劃與推動實務」子項一「商業模式設計與數位轉型推動實務」之採購、期中審查、期末審查、經費支用查核(依科技部補助專題研究計畫經費處理原則)等行政作業。

C. 協助督導辦理與彙整「小客車租賃業數位轉型發展計畫(1/1)」期末報告，俾利函送行政院國家科學技術發展基金管理會辦理結案事宜。

D. 提出分項二「智慧租車服務營運規劃與推動實務」子項一「商業模式設計與數位轉型推動實務」之風險控管計畫，針對 R2(不理想)與 R3(不可忍受)之風險擬定對應之處理方法，逐月滾動檢討風險控管計畫。

E. 參與主計畫相關會議，並針對計畫執行團隊所規劃之數位轉型輔導、創新服務方案規劃、行銷推廣活動、營運模式及相關策略等，協助進行審驗，並研提相關建議與評估業者及使用者接受度。

(2) 專業知識諮詢

協助督導主計畫之推動，提供明確的工作範疇、里程碑與交付標

的、系統分析設計與測試、系統上線與驗收等各階段確認問題與驗證之專業技術諮詢服務，並釐清責任歸屬。透過專業諮詢服務，提供進度管控與完工報告，確保各團隊計畫執行成效。

(3) 獨立監督審驗

A. 就主計畫期初建置可做為推動數位轉型之平台，提出系統相關功能測試(應含網站功能測試、壓力測試、資安測試等)及 API 測試計畫，據此執行並詳實記錄測試過程及結果，彙整缺失紀錄、產出測試報告並提出相關建議，以確認系統符合需求，且正常運作。前述之測試需求，需先與數位轉型推動計畫得標廠商約定好之期限內進行測試，以避免系統測試損壞之風險。

B. 透過協助審查主計畫於執行過程中，依據其契約等相關文件規範，所交付之各項文件 (如系統設計規格書、系統整合測試計畫書、期中與期末報告書、內部整合測試報告、壓力測試報告、資安測試報告、標準 API 技術文件、後臺管理操作手冊、系統維運操作手冊、使用手冊等)與系統，並於指定之期限內研提相關審查意見。

C. 前述相關紀錄文件、審查意見、測試報告等，需於指定之期限內完成，並交付電子檔。

D. 其他辦理專案管理及監督審驗等相關臨時交辦事項。

2. 第2年期須協助「小客車租賃業數位轉型發展計畫－商業模式設計與數位轉型推動實務(2/2)」(以下簡稱第二期主計畫)之「專案管理服務」、「專業知識諮詢」與「獨立監督審驗」。

(1) 專案管理服務

A. 追蹤管控數位轉型發展計畫執行過程之相關問題與議題。

B. 協助辦理第二期主計畫之採購、期中審查、期末審查、經費支用查核(依科技部補助專題研究計畫經費處理原則)等行政作業。

C. 提出第二期主計畫之風險控管計畫，針對 R2(不理想)與 R3(不可忍受)之風險，擬定對應之處理方法，並逐月滾動檢討風險控管計

畫。

D. 參與第二期數位轉型推動計畫相關會議，並針對主計畫所規劃之數位轉型輔導、創新服務方案規劃、行銷推廣活動、營運模式及相關策略等，協助進行審驗，並研提相關建議與評估業者及使用者接受度。

(2) 專業知識諮詢

協助督導小客車租賃業整合旅遊生態系之工作，提供明確的工作範疇、里程碑與交付標的、系統分析設計與測試、系統上線與驗收等各階段確認問題與驗證之專業技術諮詢服務，並釐清責任歸屬。透過專業諮詢服務，提供進度管控與完工報告，確保各團隊計畫執行成效。

(3) 獨立監督審驗

A. 針對第二期數位轉型推動計畫建置之「小客車租賃服務整合旅遊生態系平台」，提出系統相關功能測試(應含網站功能測試、壓力測試、資安測試等)及 API 驗測計畫，據此執行並詳實記錄測試過程及結果，彙整缺失紀錄、產出測試報告並提出相關建議，以確認系統符合需求，且正常運作。前述之測試需求，需先與平台開發團隊約定好之期限內進行測試，以避免系統測試損壞之風險。

B. 透過協助審查數位轉型發展計畫於執行過程中，依據其契約等相關文件規範，所交付之各項文件 (如系統設計規格書、系統整合測試計畫書、期中與期末報告書、內部整合測試報告、壓力測試報告、資安測試報告、標準 API 技術文件、後臺管理操作手冊、系統維運操作手冊、使用手冊等)與系統，並於指定之期限內研提相關審查意見。

C. 前述相關紀錄文件、審查意見、測試報告等，並於運研所指定之期限內完成，並交付電子檔。

D. 其他辦理專案管理及監督審驗等相關臨時交辦事項。

第二章　文獻回顧

2.1 智慧租車及營運

小客車租賃業定義為可同時提供車輛租用及駕駛人代駕服務，但是不能執行計程車客運業之相關服務內容。該業務之計費以時租或日租為主，其租用服務最小時間單位為一小時，目前國內除了和運租車(iRent)規模較大且完整之外，其他業者普遍規模較小，而且資訊化程度不足(以紙本作業為大宗)。依據交通部 106 年小客貨車租賃業營運狀況調查資料顯示，國內小客貨車租賃業者計有 1,755 家(157,228 輛車)，其中短租車例假日平均出租率僅為 37.5%，平常日更是低於 30%；可見車輛的閒置與空車率過高，造成營運上的困境。因此，若能提升車輛出租率，得以創造營收之空間。然而，經資料統計車輛數在 20 輛以下的業者佔 72.1%，可見中小企業林立且大部分數位化程度皆不足，缺乏完善之資料收集與彙整的方式，進而無法實現資料分析與加值應用；加上使用者的運輸需求多元化，最終導致資訊整合的速度較慢，無法及時滿足使用者的需求，並因應市場的快速變化做戰略調整，而降低競爭力。

除了瞭解上述國內小客車租賃業者之需求與痛點外，亦針對未來建置商於建置智慧租車平台，綜整國內外較具知名度之小客車租賃業者或是相關代理平台之營運範圍與營運模式如表 2.1-1 所示。

表 2.1-1 國內外小客車租賃業之營運模式比較

	格上租車	和運租車	gogoout	Expedia	Renatlcars
總部	臺灣	臺灣	臺灣	美國	英國
營運範圍	臺灣	臺灣	臺灣、美國	美國	180 個國家
服務模式	租車/包車	租車/包車	租車	租車	租車
付款方式	至租車地繳款/線上付款	線上付款	線上付款	線上付款	線上付款
站點數	約 50 個	約 50 個	約 9,000 個	-	約 46,000 個
平台特性	獨立運作	獨立運作	租車代理平台	租車代理平台	租車代理平台
合作平台	N/A	N/A	N/A	Trivago、Hotels.com	Booking、agoda

(資料來源：團隊自行整理)

而 2018 年消費性電子產品展覽會(CES)展上提出交通行動即服務(Mobility as a Service, MaaS)後，成為各國爭相研究之重點，而 MaaS 的本質以人為本的服務，

透過各種交通資源的取得與管理，以滿足不同使用者的需求。「小客車租賃業數位轉型發展計畫」的主要目標為輔導小客車租賃業數位轉型，其關鍵媒介為「智慧租車平台服務」；以大平台的方式，讓租賃業者於平台上架車輛(即提供線上租賃服務)，讓使用者可以透過平台適時適地選擇適合的業者與車輛(例如透過人工智慧的方式推薦車輛、預約制、動態價格等方式進行媒合)，進而達到小客車出租率的提升；同時讓使用者行的方便，在提高幸福感的同時，也提升了業者的競爭力。

除了大平台便民使用外，若能適時搭配交通部觀光局推廣之觀光圈在地組織，打造具特色的區域旅遊，並與當地食、宿、遊、購商家合作，對於明年度主計畫於中臺灣推動食宿郵購一站式旅運平台，將更有效益。若能由建置商所建置之租車平台，搭配阿里山、中彰、雲嘉南等觀光圈，及近乎全臺灣均可使用的臺灣好玩卡，將對於後續旅遊相關服務推廣事半功倍。

2.2 專案管理及監督審驗

本計畫名稱為「小客車租賃業數位轉型發展計畫-商業模式設計與數位轉型推動實務之專案管理及監督審驗(1/2)」，目的在於對「小客車租賃業數位轉型發展計畫-商業模式設計與數位轉型推動實務(1/2)」專案項下計劃進行專案管理，確保該計畫依照業主的預算及契約時間，交付符合業主需求之專案成果。

歷史上許多重大計畫就已經透過專案管理，協助其達成計畫目的，例如：巴拿馬運河、人類登陸月球及商用軟體開發等等。而這些計畫的共通之處，是它們皆為暫時性(Temporary)的工作，即計畫必須在預定的時間宣告完成，並非無止盡的進行，因此衍生出專案管理的需求。

目前我國大多數重要公共工程，有獨立專管單位的設計，委託民間單位進行專案管理，如高雄輕軌工程、桃園捷運綠線、桃園會展中心等，政府機關透過委託的專案管理或專業營建管理（PCM）協助機關確認需求、協助施工團隊之遴選、專案規劃、監控設計品質與進度、預算審核等管理與監控任務。

專案管理者應具備專業背景及經驗，可以協助計畫提高成功機會、風險即時應對、平衡專案的各種影響因素。相反地，若計畫未執行專案管理，或專案管理者缺乏相關專業背景，可能造成計畫成果錯過期限、品質低落、利害關係人的不滿等狀況。

當專案管理者由第三方擔任，可進一步成為業主、建置廠商、顧問專家之溝通媒介，提高專案溝通順暢度，同時在專案品質管理方面，專管團隊與業主、建

置廠商建立三級品管機制，透過三方的層層檢驗，確保計畫成果符合預期。

本計畫之專案管理及監督審驗，係確保主計畫依照業主的預算及契約時程內，交付符合業主需求之專案成果，除透過相關會議參與、議題討論外，更導入第三方獨立驗證單位，使整體專案執行品質獲公平公正單位確認，相關綜整本計畫所獲效益如後。

1. 提升第二年專案管理服務
   (1) 統整第一年專管經驗，於計畫第二年的專案管理章程中，針對第一年待改善之專管項目，並提出完善之專案章程，供業主單位、建置廠商、專案管理單位三方之參照依據，以提升第二年計畫管理品質。
   (2) 扮演建置計畫團隊、顧問專家之溝通媒介，提高專案溝通順暢度。
   (3) 監控試營運階段之系統問題，透過即時調整建置計畫各階段之執行進度，以確保系統問題順利解決，使建置計畫能順利如期如質完成。
   (4) 追蹤建置計畫團隊回報之使用者需求與改善意見，據此協助調整相關系統改善時程與項目，以控制並減少系統發展過程中的變動性，使建置案能順利如期如質完成。
2. 專業之技術團隊與諮詢服務
   (1) 會同專家學者審查建置計畫各階段之各項交付產品及成果，並提供審查意見及建議，以縮短文件及系統的審查時間。
   (2) 透過技術會議與審議，確保建置計畫所開發之軟體可因應未來科技技術發展、業務衍生需求、設計品質及產品需求等，發揮功能、安全、實用、效能、擴充、維護、移植、創新等效益。
3. 嚴謹之品質管理
   (1) 建立專業測試團隊，並與業主、建置廠商及專案管理單位密切互動，確保測試流程之落實。
   (2) 監督建置案廠商運用測試工具與壓力測試工具，審驗建置廠商之測試計畫與測試報告，以加速測試工作之進行。
   (3) 有效追蹤試營運及正式營運期間之問題之解決與改善，以避免軟體瑕疵之擴大或使用者無法順利使用之情事。
   (4) 以「早期發現、快速改善」為方法，達「減緩風險、專案成功」之目的。
4. IV&V 之起源與功能

   獨立驗證與認證(Independent Verification and Validation, IV&V)之基本概

念是藉由一個公正獨立的第三方單位或組織，針對一個系統發展的各個階段採用一系列方法與技術進行驗證，並對成果進行認證，用以確認系統的品質、安全與功能。IV&V 觀念於 1970 年代首次被提出，起因為美國陸軍發展愛國者反飛彈系統時，為能有效降低軍事開發的高度失敗風險之特性，於是透過建立計畫、方法、工具、技術發展及驗收準則等流程，有效的提高研發成功率與產品可靠度。發展至今，其觀念與機制已廣泛運用於軟體開發、航太科技與軍事工業上。而近年有關大型的基礎公共建設建置(如：軌道系統工業)亦開始導入 IV&V 機制來確保其可靠性與安全性。

一般而言，IV&V 執行單位需具備三要件，分別為：技術獨立、管理獨立及財政獨立。技術獨立係指 IV&V 執行單位之執行人員不應介入系統開發;且不得對於系統開發過程中有任何偏見及提供任何主觀建議；管理獨立則是代表 IV&V 執行單位需為獨立管理單位，有其義務及權利指出系統開發過程中所發現的異常，且不必受制任何其他單位之管理限制；財政獨立則是確保 IV&V 執行單位不因經濟上的壓力而產生非公正/公平之 IV&V 結果報告。為能確保 IV&V 執行單位能滿足上述條件，常見透過第三方機構執行 IV&V 來達到公平客觀的目的。此外，透過第三方機構執行 IV&V，亦可藉由外部管理的角度，來消除主觀意識所造成的盲點，並可以外部管理的手段，來強制改善系統存在的錯誤或缺點。

驗證的主要精神及概念係確保系統開發過程中，各子系統或模組之測試與分析符合規範之要求，並應同時確認現階段之產出結果與前一階段產出結果具有系統一致性。其工作項目包含：需求分析、設計分析、軟體分析及驗證試驗等。而認證的主要精神及概念係針對系統發展結果的認證，藉以確保系統最終產品的規格和功能，符合設計的概念與規範要求，屬於成果監督管理的概念。

透過第三方公正單位執行 IV&V，一方面可避免因原系統開發者的主觀意識造成的認知偏差，並可降低因其內部考量因素(如：成本、進度等)而降低或疏忽對品質的要求。此情況之發生可視為系統開發者內部政策考量優先於技術面考量。針對此現象，透過第三方公正單位執行 IV&V 可將政策上之關注降到最低。此外，美國太空總署的 IV&V 執行單位於報告中說明透過第三方公正單位執行 IV&V 之優點包含有：

(1) 可有更佳的軟體/系統執行成果。

(2) 提升軟體可靠度的使用信心。

(3) 設計規範可合乎相關法令。

(4) 可建立程式的接受標準。

(5) 計畫發展過程更加透明。

(6) 提供更好的決策準則。

(7) 提供第二個專業技術來源選擇。

(8) 降低維護成本。

(9) 減少操作上的變更頻率。

Arthur, J. D 指出透過第三方公正單位執行 IV&V 對系統開發具有以下之優點：

(1) 可對系統提供一個客觀之評估。

(2) 可用另外一個觀點對系統進行分析。

(3) 確保發展階段之正確性和妥當性。

(4) 可改善設計瑕疵。

總結來說，透過第三方公正單位執行 IV&V 可確保系統開發在整個系統生命週期中達到不同階段的安全、品質與功能等需求，並可帶來其他附加價值。

5. IV&V 之發展方式與現況

IV&V 的發展方式可區分為自行發展(In-House Development)、商業發展(Commerical Development)與政府發展(Government Development)。相關說明如下。

(1) 自行發展：

於組織內部自行成立 IV&V 部門，並專責對組織內部的計畫執行 IV&V，其運作、管理及資源與經費需具有獨立性的維持。自行發展模式通常僅有規模龐大的組織，才有其能力與需求，例如美國太空總署的 IV&V 部門。

(2) 商業發展：

為一 IV&V 專業組織透過商業經營的型態，接受委託執行 IV&V。此發展模式常見於具產品或系統自我發展能力且具有足夠經濟規模的市場。

(3) 政府發展：

因政府法令制度規範的需求，由政府成立或與民間機構合作發展的

IV&V 組織，常見於在某些特定產業領域，例如：歐洲國家針對軌道工業系統所發展的 IV&V 組織。

而對於將 IV&V 機制應用於政府開發專案建設，目前最被廣為運用之領域為軌道工業系統的安全驗證與認證之領域，包含：歐盟/歐洲國家及日本等地區，皆已推動軌道工業系統相關的驗證與認證，說明如下：

A. 歐盟之鐵路獨立驗證與認證制度

由歐盟 15 國代表所組成之歐洲高速鐵路整合委員會，針對歐洲高速鐵路系統之交互運轉性，訂定交互運轉技術規範(European Association for Railway Interoperability, TSIS)，並依此建立歐盟各國高速鐵路系統交互運轉的各項條件。而歐盟各國需聘請獨立機構來驗證該國之高速鐵路系統確能符合 TSIS 之要求。圖 2.2.1 為歐盟授權獨立驗證構之子系統驗證作業流程。

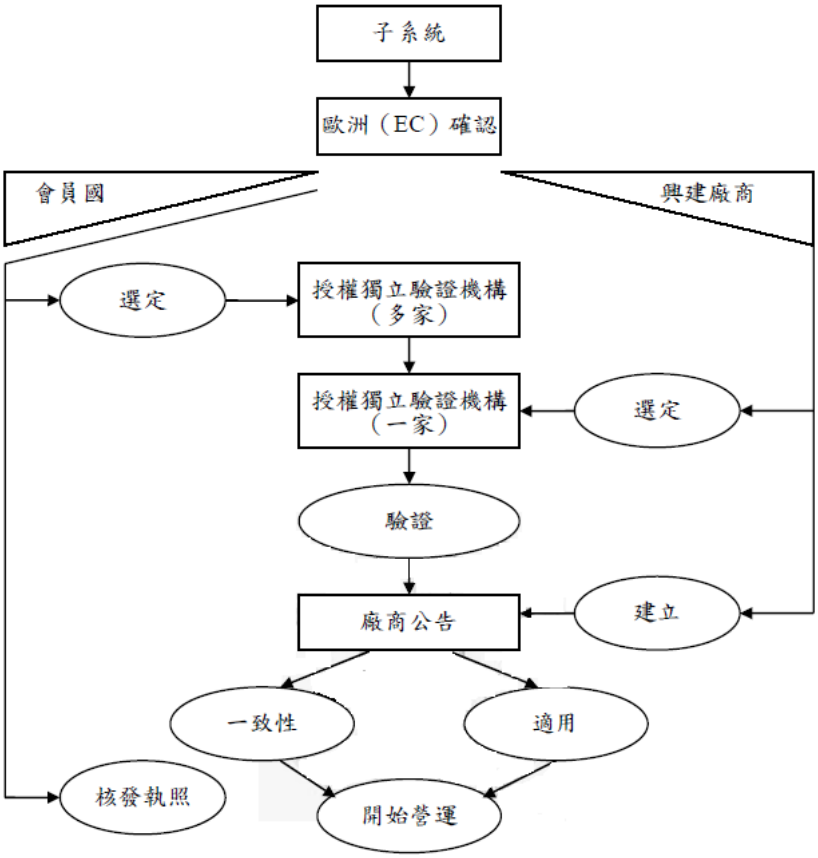


圖 2.2.1 歐盟授權獨立驗證構之子系統驗證作業流程

B. 德國聯邦鐵路之獨立驗證與認證機制

德國聯邦鐵路局於 1994 年成立，隸屬於德國聯邦交通部，為德國鐵路事務之主管機關，執行技術監督並可授權經其認可之獨立驗證機構，從事文件審查、評估與測試等工作。此外，聯邦鐵路局人員依法可於任何時間內對承包高之車輛或設施執行驗證與認證作業。圖 2.2.2 為德國聯邦鐵路獨立驗證與認證體系。

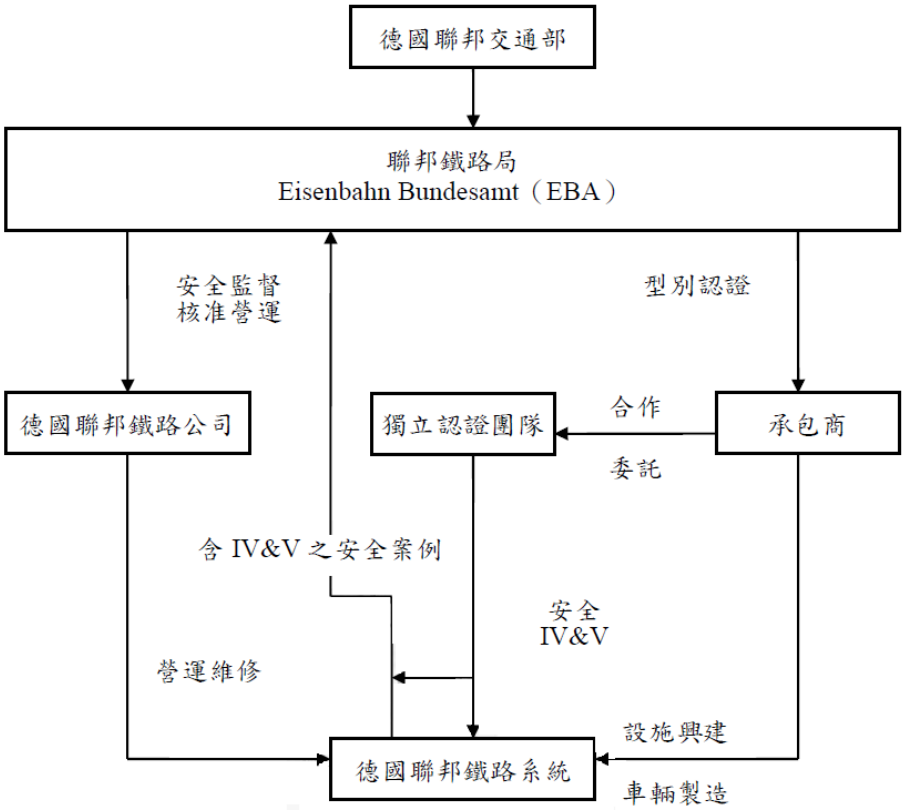


圖 2.2.2 德國聯邦鐵路獨立驗證與認證體系

C. 日本鐵路獨立驗證與認證制度

日本鐵道之 IV&V 系統由鐵道綜合技術研究所制定(如圖 2.2.3)，特許機構於建置期間需遵守該制定之標準。建置過程中無需執行細部驗證與認證工作，僅需於特定時間點進行驗證與認證，以確保確實達到所制定之標準，為日本鐵道獨立驗證與認證體系。

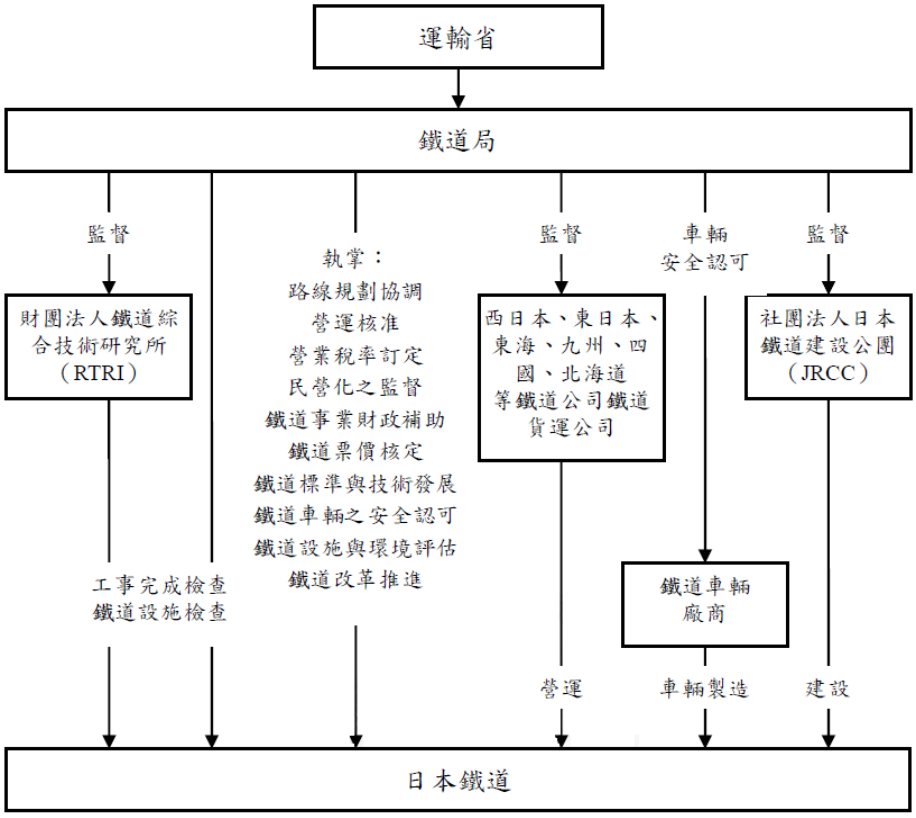


圖 2.2.3 歐盟授權獨立驗證構之子系統驗證作業流程

除了軌道工程因具法源依據而明確要求 IV&V 機制外，近年亦有相關政府單位考量專案建置或後續營運的複雜性、安全性及風險程度，於專案計畫內要求導入 IV&V，相關國內外案例說明如下。

(a) 英國 塞芬二橋

塞芬二橋為一跨港灣橋，其總長約 5.1 公里，其工程包含建置一跨距長約 465 公尺之斜張橋及增設聯絡道路。英國政府要求特許機構建立 IV&V 團隊並導入其機制，其團隊成員及監督工作包含：

i. 聯絡道路增設工程需經由政府所指定之獨立審查團隊，進行道路設計及監造工作。

ii. 橋梁由承包商所委託之獨立審查團隊，負責設計之審核及核準。

iii. 全案之合約由政府所指定之顧問團隊為代表管理監督。

(b) 希臘安提利翁大橋

希臘安提利翁大橋之興建主要為連接佩樂波尼斯與希臘西北方。考量此橋樑工程興建時所需的技術複雜度，希臘政府要求特許機構需有經

政府機關核準之獨立工程顧問公司執行 IV&V，進行監督管理、審查並核準其設計文件、品質計畫、品質手冊及所有品質管制文件。IV&團隊及監督工作包含：

i. 監督工程進度。

ii. 稽查審核所有品保及品管步驟之執行。

iii. 永久性工程、設計與規範之審查。

iv. 工程符合時簽發審查證明書。

v. 適時簽發里程碑完成及付款證明書、簽發完工證明書、

vi. 監督承包商、政府及承貸銀行團之每月合約進度及其財務狀態報告。

(c) 交通部高速公路局-民間參與高速公路電子收費系統建置及營運

交通部高速公路局(以下簡稱高公局)要求此計畫之特許公司聘請經為高公局核許之獨立驗證與認證機構，依契約之要求負責驗證與認證特許公司對計畫契約要求相關責任，而後再依查核的結果提送獨立報告予高公局審查，作為專案成果審查依據。其契約三方工作關係及相關之作業型與作業關係如圖 2.2.4。

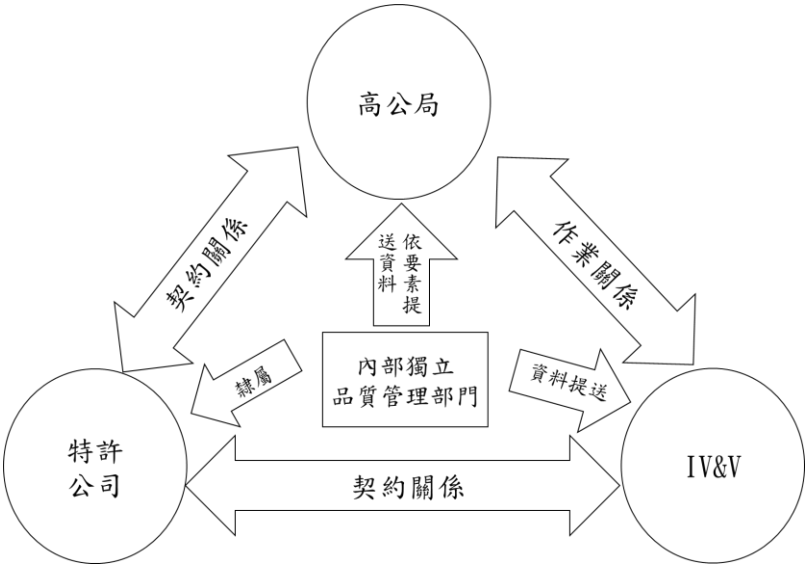


圖 2.2.4 政府、特許機構及驗證與認證機構之三方工作關係圖

6. IV&V 對軟體系統平台開發之作用

軟體系統平台開發首重於系統的完整性、可靠性及操作環境的友善性，且能確實滿足需求端的要求，並具備相對應的安全機制。然而在開發的過程中，常見因未於開發初期即時發現系統相關缺陷，導致軟體系統平台於開發完成後，仍無法正確執行需求功能或產生安全漏洞，此時若要進行修正，往往需要花費更多的時間及經費。圖 2.3.5 為軟體系統平台開發於不同階段發現缺陷需進行修正時所需的相對成本費用，當軟體系統平台的缺陷越早發現，其所需的修正的相關費用越低(Dabney & Barber, 2003)。

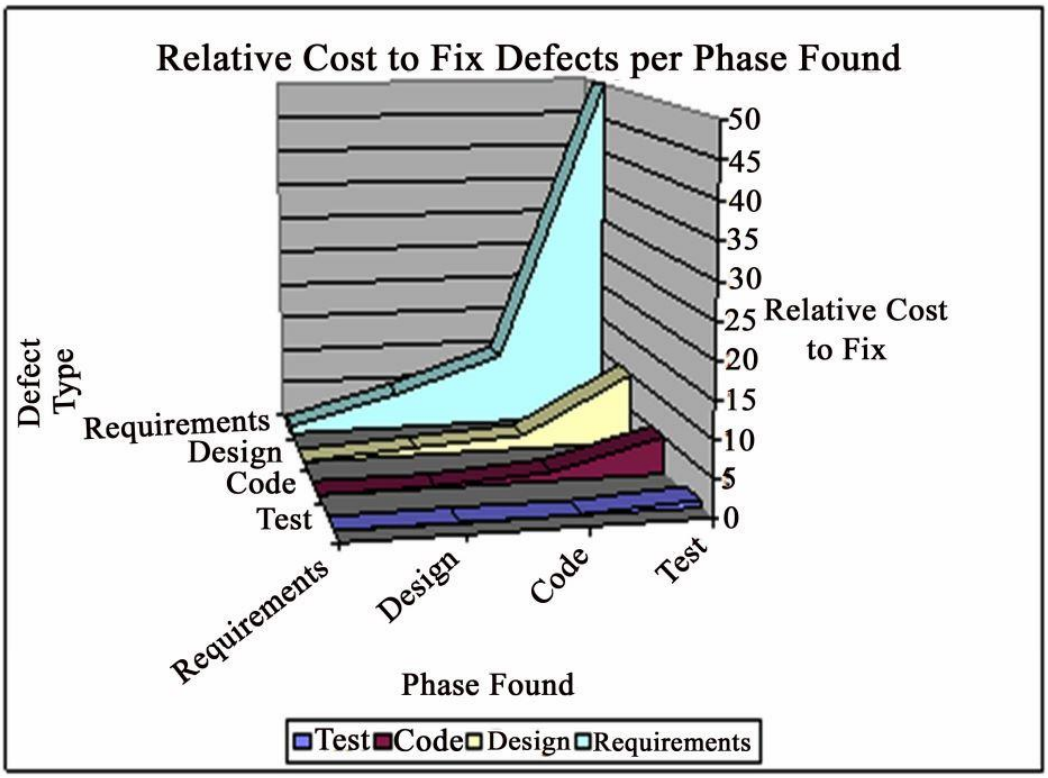


圖 2.3.5 不同開發週期下，軟體系統平台缺陷修正所需的相對成本

於軟體系統平台開發初期即導入 IV&V，可早期發現相關缺陷，並即時進行修正。美國國防部(Department of Defense, DoD)及食品藥品監督管理局(Food and Drug Administration, FDA)為確保軟體系統平台開發承包商能達到規格要求並滿足相關安全性，要求承包商需導入 IV&V 機制(Charles & Turner, 2004)。而由相關研究結果顯示，導入 IV&V 確實能早期發現軟體系統之缺陷，可有效降低開發成本及產出相對穩定可靠的軟體系統平台(Rahamn, et al., 2018, Akella & Rao, 2011, Easterbrook, 1996)。

Arthur, et al. (1999) 透過二組不同獨立團隊同時開發一軟體系統平台，其中一組團隊導入 IV&V 並進行相互比較，由圖 2.3.6 可得知，導入 IV&V 之團隊在需求(Requirements)及設計(HLD 及 LLD)階段發現的缺陷數量遠多於未導入 IV&V 之團隊，而在程式設計及測試(Code/UT 及 I&T)階段，未導入 IV&V 之團隊發現的缺陷數量則多於導入 IV&V 之團隊。整體而言，導入 IV&V 之團隊發現之缺陷數量多於未導入 IV&V 之團隊。然而，比較缺陷改善所需的時間，導入 IV&V 之團隊所需花費的時間，低於未導入 IV&V 之團隊所需花費的時間，如圖 2.3.7 及 2.3.8 所示。圖 2.3.9 為系統軟體開發完後的性能測試結果比較，可看到導入 IV&V 之團隊所建置的軟體系統平台，測試通過項目數遠高於未通過項目數；反之，未導入 IV&V 之團隊未通過的測試項目數，多於通過項目數。此結果代表導入 IV&V 之團隊所建置的軟體系統平台具有較佳的穩定度。

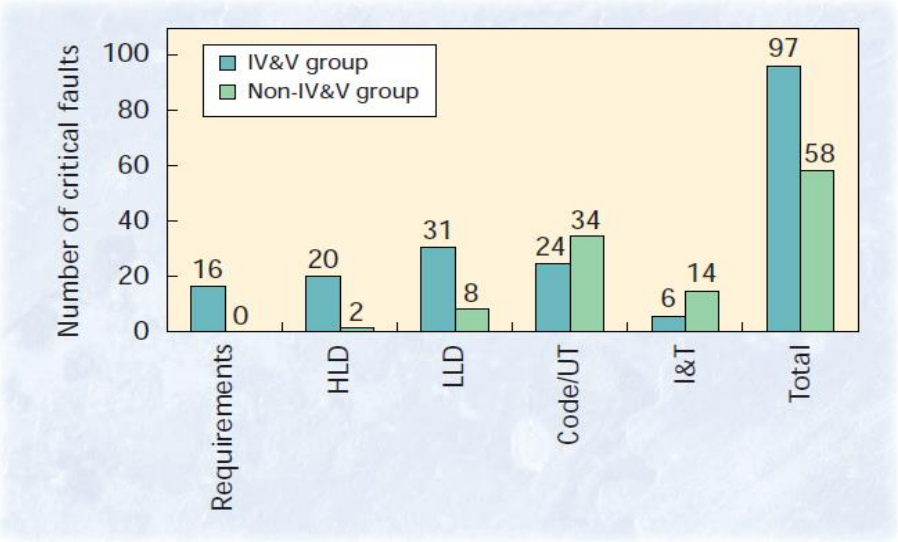


圖 2.3.6 軟體系統平台各階段缺陷數量比較

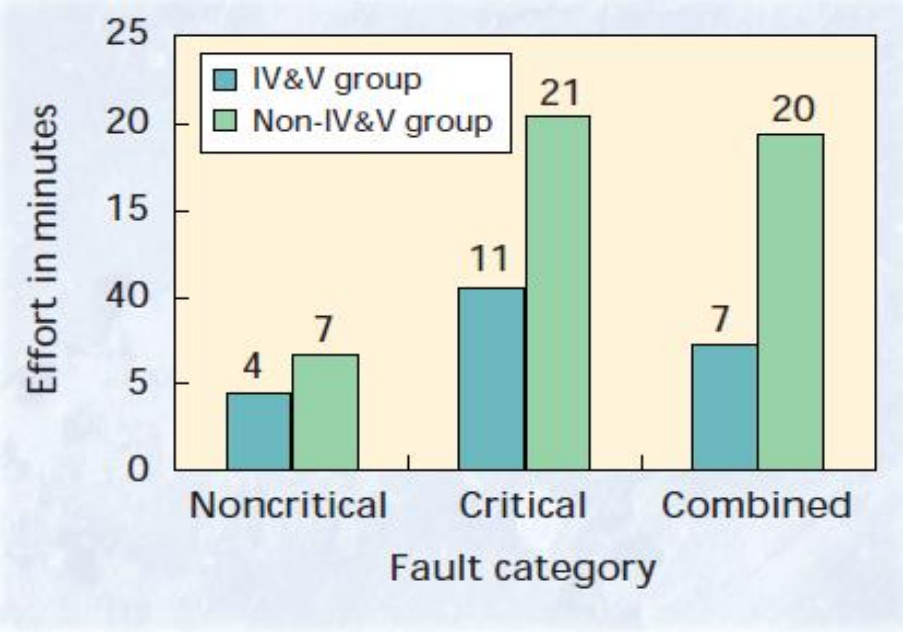


圖 2.3.7 軟體系統平台缺陷改善時間比較

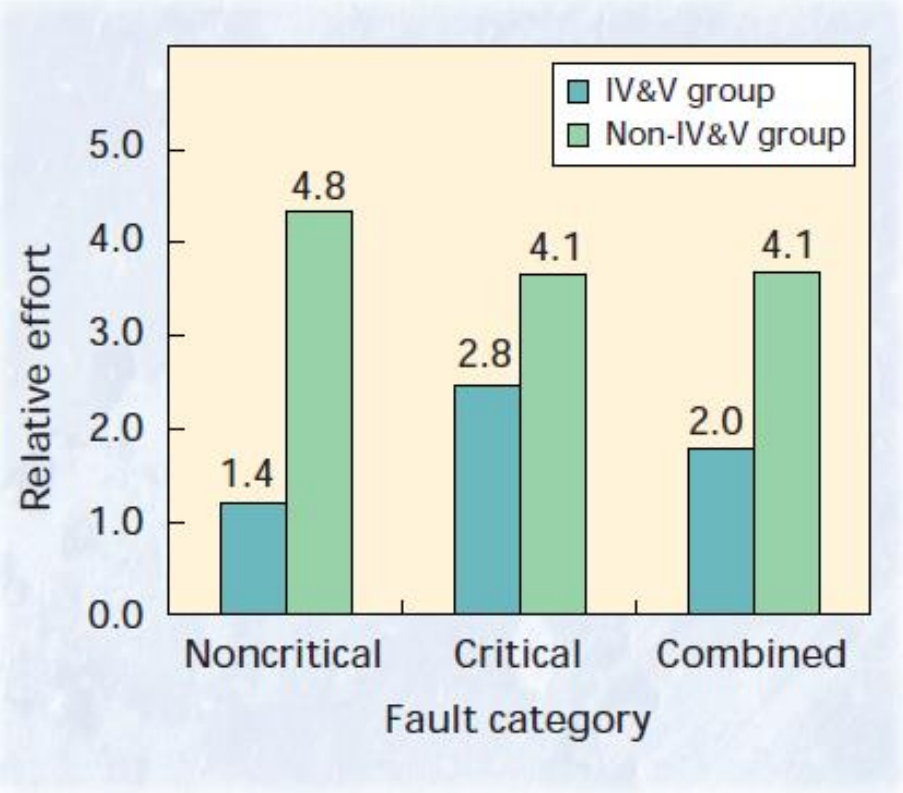


圖 2.3.8 軟體系統平台單一缺陷平均改善時間比較

Test class	Number of tests	Group 1 (IV&V) Passed / Failed	Group 2 Passed / Failed
Duplicate IV&V tests	5	5 / 0	3 / 2
Exceeding weigh limit	4	4 / 0	0 / 4
Exceeding maximum number of interactions	2	2 / 0	1 / 1
Boundary condition tests	5	5 / 0	2 / 3
Input missing or wrong format	5	3 / 2	3 / 2
Input out of bounds	5	5 / 0	0 / 5
Group 1 code particulars	5	5 / 0	0 / 5
Group 2 code particulars	5	4 / 1	2 / 3
Total	36	33 / 3	11 / 25

圖 2.3.9 軟體系統平台測試結果比較

由文獻回顧結果可知，軟體系統平台開發導入 IV&V 可於開發初期發現系統缺陷並即時改善，藉以達到降低金錢及時間成本，並且具有較佳的系統可靠度。

2.3 文獻評析

以目前國內的小客車租賃業市場來說，中小企業林立且大部分數位化程度皆不足，要如何突破此現況的窘境呢？使規模較小之小客車業者也能合作，進而提升整體小客車租賃之使用率，以創造更大的效益。「小客車租賃業數位轉型發展計畫」主要目標為輔導小客車租賃業數位轉型，以「智慧租車平台服務」之平台小規模之客車租賃業者，於平台即時顯示出使用者指定時段目前尚可接受承租之車輛，使用者透過該平台能夠選擇適合的業者與車輛，期望以往於連續假期出遊前，使用者較無完整資訊需自行詢問租車業者是否尚有車輛可供出租之窘境，可以獲得改善，並透過平台的價格與合約透明化功能，也能提升使用者之權益，進而使小客車出租率的提升。

另有關 IV&V 觀念與機制已逐漸被推廣應用於公共建設計畫的管理監督查核。特別是針對具先進、系統複雜、風險大及安全性要求的領域上，國際間已有建立 IV&V 相關的法令規範，也成立相關組織來發展推動 IV&V 觀念機制。目前國內政府相關單位也逐漸導入 IV&V 機制，如高公局所管之國道電子收費或交本所推動之 MaaS 專案，皆為確保專案達如期、如質、如實之優良品質於公共工程上之案例。

本計畫名稱為「小客車租賃業數位轉型發展計畫-專案管理及監督審驗(1/2)」，目的在於對「小客車租賃業數位轉型發展計畫(1/1)」計畫進行專案管理，藉由第

三方管理者擔任業主、建置計畫團隊、小客車租賃業者以及顧問專家之溝通橋梁，以填補多方溝通與協調中的縫隙，並提高專案溝通之順暢度，在透過第三方專案品質管理，確保產出成果品質時效以交付符合需求之計畫成果，專案管理概念如圖 2.3.1 所示。

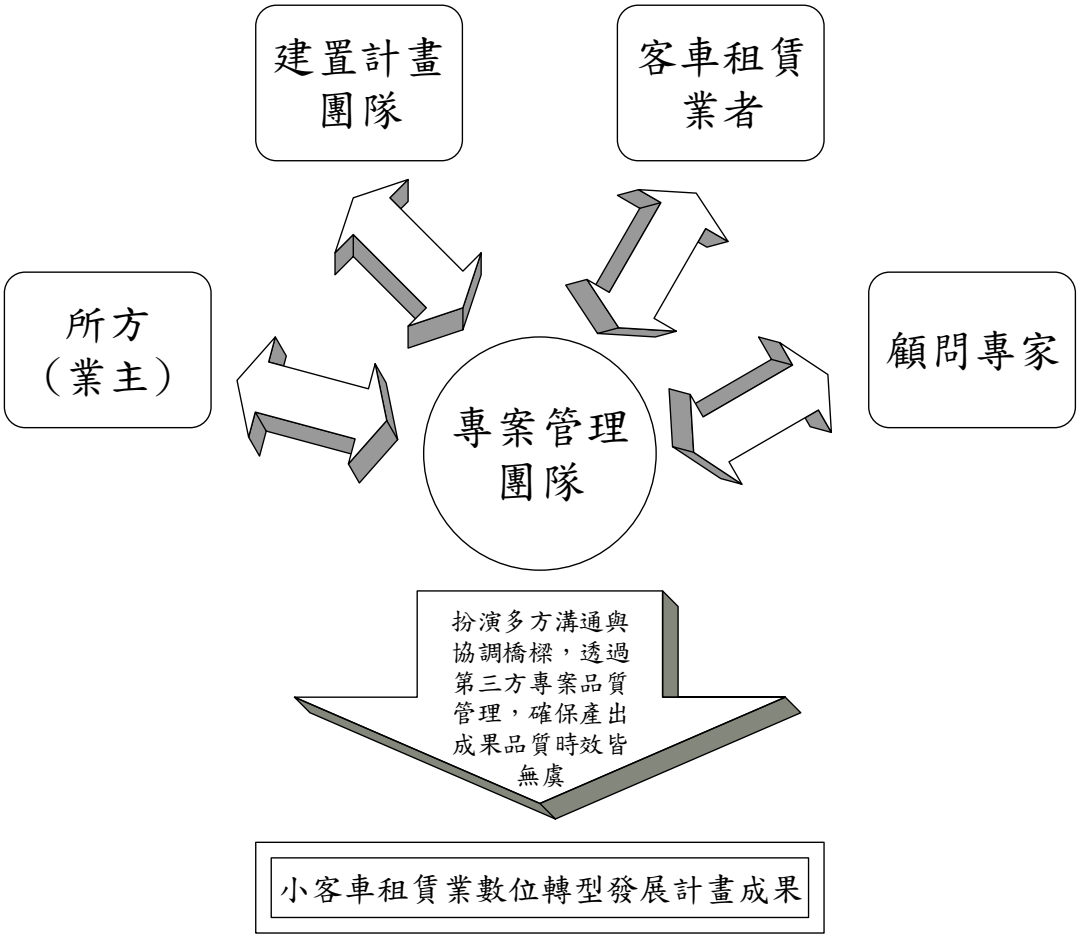


圖 2.3.1 小客車租賃業數位轉型發展計畫專案管理概念圖

第三章　專案管理及監督審驗

3.1 專案管理

本章節針對主計畫之專案執行進度進行控管，並列管追蹤辦理進度，除此之外，亦有相關專業領域人員，可提供知識諮詢服務，以提升專案執行效益，且為避免風險產生，研提相對應之處理措施，以確保主計畫能如期、如質完成。

3.1.1 專案進度控管

本所於 110 年 2 月 26 日開始執行分項二「智慧租車服務營運規劃與推動實務」子項一「商業模式設計與數位轉型推動實務」之招標作業與評選作業，3 月 10 日辦理公開說明會，與會出席單位包括小客車租賃業者、電信業者、科技與資訊相關業者，4 月 19 日召開評選會議，由漢名科技股份有限公司(後簡稱為漢名科技)得標，並於 5 月 6 日完成簽約作業。

4 月 13 日召開本計畫啟動工作會議，討論主計畫各投標廠商所提出之服務建議書內容，是否符合計畫所需，相關建議統整於 3.1.2 節中說明。5 月 11 日與漢名科技召開聯合啟動工作會議，討論計畫後續執行時程與流程規劃。原訂漢名科技須於簽約日(110 年 5 月 6 日)起 30 天內，完成辦理期初發表會，但因受疫情影響，無法辦理相關實體會議，延後至 9 月 23 日，疫情稍緩後，得以辦理相關會議，但總參與人數不得高於 50 人。

5 月 27 日、6 月 17 日、7 月 7 日、7 月 22 日等，約每兩週召開一次聯合工作會議，並邀集交通部路政司、交通部科技顧問室、交通部公路總局等主管機關共同參與，惟因應疫情，亦採取視訊會議方式召開，並且不定期協助召開會議，討論智慧財產權聲明、創新服務等議題。除工作會議外，針對漢名科技之研究主題與重點中明訂須召開以下之相關會議，會同參與，確保漢名科技相關工項是否確實達成。

(1) 期初發表會；
(2) 4 場次產業數位轉型座談會；
(3) 營運人員及平台操作之教育訓練；
(4) 8 場次有助於產業數位轉型暨平台推廣應用之座談會、說明會、論壇、工作坊等。

另為避免後續於系統之智慧財產權移轉與劃分上產生疑慮，亦針對「智慧財產權管理與運用設計專業服務」計畫辦理招標與評審作業，於 7 月 1 日公告招標，7 月 19 日召開評審會議，由博大國際智權股份有限公司(簡稱博大團隊)得標，7

月 27 日完成簽約。

截至 12 月 27 日，已召開 13 場次工作會議，及召開相關座談會、說明會與教育訓練等，綜整如表 3.1-1 所示。

表 3.1-1 會議綜整表

日期	會議名稱	議題	實際出席單位
04.13	工作會議	服務建議書內容討論與優缺點分析	1. 本所 2. 逢甲團隊
05.11	工作會議	1. 系統平台開發與驗測時程 2. 期初發表會規劃 3. 智財權與技術轉移 4. 業者招募 5. 創新服務	1. 本所 2. 漢名科技 3. 逢甲團隊
05.27	工作會議	1. 期初發表會規劃 2. 期初報告工作項目進度 3. 調查分析與創新服務規劃進度 4. 旅遊生態系平台功能規劃	1. 本所 2. 漢名科技 3. 逢甲團隊
06.17	工作會議	1. M3 系統介接 2. 期初報告工作項目進度 3. 租賃車業者招募計畫 4. 產業現況調查與深度訪談 5. 既有智慧財產權 6. 創新服務規劃	1. 科顧室 2. 公路總局 3. 本所 4. 漢名科技 5. 逢甲團隊
07.07	工作會議	7. 介接 M3 系統進度 8. 平台系統功能模組架構 9. 平台收費機制 10. 租賃車業者招募進度 11. 品牌 LOGO 設計 12. 創新服務規劃進度 13. 智慧財產權聲明	1. 科顧室 2. 公路總局 3. 本所 4. 漢名科技 5. 逢甲團隊
07.09	創新保險會議	創新保險	1. 本所 2. 漢名科技 3. 新安東京海上產險 4. 逢甲團隊
07.14	創新服務會議	1. MeN Go 點數納入「生態	1. 高雄市政府交通局

日期	會議名稱	議題	實際出席單位
		系平台」 2. MeN Go 聯名卡 3. 服務模式	2. 高雄捷運股份有限公司 3. 中冠資訊股份有限公司 4. 本所 5. 漢名科技 6. 逢甲團隊
07.16	創新服務會議	1. 創新服務模式適法性 2. 創新服務車資費率 3. 營運計畫書提送申請 4. MeN Go 點數納入「生態系平台」	1. 公路總局 2. 本所 3. 漢名科技 4. 逢甲團隊
07.19	輔導小客車租賃業數位轉型說明暨座談會 (東部、離島)	1. 業者招募說明 2. 計畫及平台功能規範	1. 東部地區與離島之小客車租賃公會與業者 2. 本所 3. 漢名科技 4. 逢甲團隊
07.21	輔導小客車租賃業數位轉型說明暨座談會 (南部)	1. 業者招募說明 2. 計畫及平台功能規範說明	1. 南部地區之小客車租賃公會與業者 2. 本所 3. 漢名科技 4. 逢甲團隊
07.22	工作會議	1. 租賃車業者招募說明會辦理狀況檢討 2. 期初報告內容說明 3. 系統功能模組架構與第三方 API 串接內容 4. 捷運通勤接駁之辦理方向與進度說明 5. 創新保險辦理進度	1. 科顧室 2. 公路總局 3. 本所 4. 漢名科技 5. 逢甲團隊 6. 小客車租賃商業同業公會全國聯合會
07.23	輔導小客車租賃業數位轉型說明暨座談會 (中部)	1. 業者招募說明 2. 計畫及平台功能規範說明	1. 中部地區之小客車租賃公會與業者 2. 本所 3. 漢名科技 4. 逢甲團隊
07.26	輔導小客車租賃業數位轉型說明暨	1. 業者招募說明 2. 計畫及平台功能規範說明	1. 北部地區之小客車租賃公會與業者 2. 本所

日期	會議名稱	議題	實際出席單位
	座談會 (北部)		3. 漢名科技 4. 逢甲團隊
08.04	工作會議	1. 介接 M3 系統進度 2. 業者招募說明會辦理狀況與招募網站修正(含懶人包與 FAQ) 3. 旅遊生態系平台開發進度 4. 捷運通勤接駁之辦理進度 5. 創新保險辦理進度	1. 公路總局 2. 本所 3. 漢名科技 4. 逢甲團隊 5. 博大團隊 6. 小客車租賃商業同業公會全國聯合會
08.12	期初審查會議	期初報告內容審查	1. 本所 2. 漢名科技 3. 逢甲團隊
08.24	工作會議	1. M3 介接進度說明 2. 旅遊生態系平台開發進度說明 3. 輔導業者數量說明 4. 問卷調查、深度訪談與相關調查分析之進度說明 5. 行銷推廣規劃說明 6. 捷運通勤接駁之辦理進度	1. 公路總局 2. 本所 3. 漢名科技 4. 逢甲團隊 5. 博大團隊 6. 小客車租賃商業同業公會全國聯合會
09.02	工作會議	1. 介接 M3 功能之測試說明 2. 招募進度及教育訓練內容與進度規劃說明 3. 輔導業者數位轉型工作內容與時程規劃說明 4. 智慧租車共通平台金流功能之測試計畫說明 5. 旅遊生態系平台需求規劃文件說明 6. 期中報告章節規劃說明	1. 本所 2. 漢名科技 3. 逢甲團隊 4. 博大團隊
09.07	小客車租賃業者教育訓練	小客車租賃業者平台與 APP 之教育訓練	1. 本所 2. 漢名科技 3. 逢甲團隊 4. 小客車租賃業者

日期	會議名稱	議題	實際出席單位
09.09	小客車租賃業者教育訓練	小客車租賃業者平台與 APP 之教育訓練	1. 本所 2. 漢名科技 3. 逢甲團隊 4. 小客車租賃業者
09.16	工作會議	1. 介接 M3 系統功能測試結果說明 2. 智慧租車共通平台功能測試說明 3. 招募與輔導業者數位轉型辦理成果說明 4. 教育訓練與深度訪談成果說明 5. 捷運通勤接駁規劃與調查結果說明	1. 本所 2. 漢名科技 3. 逢甲團隊 4. 小客車租賃商業同業公會全國聯合會 5. 臺灣省小客車租賃商業同業公會 6. 臺北市小客車租賃商業同業公會 7. 新北市小客車租賃商業同業公會 8. 宜蘭縣小客車租賃商業同業公會 9. 桃園市小客車租賃商業同業公會 10. 臺中市小客車租賃商業同業公會 11. 彰化縣小客車租賃商業同業公會 12. 臺南市小客車租賃商業同業公會 13. 高雄市小客車租賃商業同業公會 14. 臺東縣小客車租賃商業同業公會
09.23	期初發表會	1. 計畫分工 2. 系統架構說明 3. 完整平台規劃說明 4. 小客車租賃業者招募計畫說明 5. 現有成果展示	1. 本所 2. 漢名科技 3. 逢甲團隊 4. 小客車租賃商業同業公會全國聯合會 5. 臺灣省小客車租賃商業同業公會 6. 臺北市小客車租賃商業同業公會 7. 新北市小客車租賃

日期	會議名稱	議題	實際出席單位
			商業同業公會 8. 宜蘭縣小客車租賃商業同業公會 9. 桃園市小客車租賃商業同業公會 10. 臺中市小客車租賃商業同業公會 11. 高雄市小客車租賃商業同業公會 12. 花蓮縣小客車租賃商業同業公會 13. 臺東縣小客車租賃商業同業公會
10.05	業者說明會 (宜蘭場)	1. 計畫說明 2. 系統架構說明	1. 本所 2. 漢名科技 3. 逢甲團隊 4. 小客車租賃商業同業公會全國聯合會 5. 宜蘭縣小客車租賃商業同業公會 6. 小客車租賃業者
10.08	工作會議	1. 期中報告工作說明 2. 系統展示規劃說明 3. 專利索引與技術轉移 4. 系統驗測	7. 本所 8. 漢名科技 9. 逢甲團隊 10. 博大團隊
10.13	系統驗測討論會議	系統驗測範圍與應提供之相關技術文件	1. 本所 2. 漢名科技 3. 逢甲團隊
10.18	期中審查會議	期中報告內容審查	1. 審查委員 2. 交通部公路總局 3. 小客車租賃商業同業公會全國聯合會 4. 本所 5. 漢名科技 6. 逢甲團隊
10.21	系統功能展示說明暨意見交流座談會議	1. 系統功能展示說明 2. 聽取小客車租賃公會與業者之相關意見	1. 本所 2. 洪孟楷委員國會辦公室 3. 漢名科技

日期	會議名稱	議題	實際出席單位
			4. 逢甲團隊 5. 小客車租賃商業同業公會全國聯合會 6. 臺北市小客車租賃商業同業公會 7. 新北市小客車租賃商業同業公會 8. 宜蘭縣小客車租賃商業同業公會 9. 桃園市小客車租賃商業同業公會 10. 臺中市小客車租賃商業同業公會 11. 高雄市小客車租賃商業同業公會 12. 臺東縣小客車租賃商業同業公會 13. 新竹縣小客車租賃商業同業公會 14. 臺南市小客車租賃商業同業公會 15. 苗栗縣小客車租賃商業同業公會 16. 小客車租賃業者
10.22	技術文件討論會議	1. 技術文件種類與大綱	1. 漢名科技 2. 逢甲團隊
10.28	工作會議	2. 租車平台+CarU 系統功能說明 3. 系統功能與資策會之差異說明 4. 籌備產業數位轉型暨平台推廣應用相關會議說明 5. 後續工作內容 6. 逢甲團隊請漢名科技配合辦理事項 7. 博大團隊請漢名科技配合辦理事項	3. 本所 4. 漢名科技 5. 逢甲團隊 6. 博大團隊
11.10	業者說明會	1. 計畫說明	1. 本所

日期	會議名稱	議題	實際出席單位
	(臺中場)	2. 系統架構說明 3. 行銷推廣說明	2. 漢名科技 3. 逢甲團隊 4. 小客車租賃商業同業公會全國聯合會 5. 臺中市小客車租賃商業同業公會 6. 彰化縣小客車租賃商業同業公會 7. 臺東縣小客車租賃商業同業公會 8. 小客車租賃業者
11.11	產業座談會 (桃園場)	1. 計畫說明 2. 系統架構說明 3. 行銷推廣說明	1. 本所 2. 漢名科技 3. 逢甲團隊 4. 小客車租賃商業同業公會全國聯合會 5. 桃園市小客車租賃商業同業公會 6. 小客車租賃業者
11.12	工作會議	1. 創新服務之進度與成果說明 2. 系統功能修正說明 3. 商標 Logo 申請進度 4. 逢甲團隊請漢名科技配合辦理事項 5. 逢甲團隊研提系統功能之意見與建議 6. 博大團隊請漢名科技配合辦理事項	1. 本所 2. 漢名科技 3. 逢甲團隊 4. 博大團隊
11.15	產業座談會 (臺北場)	1. 計畫說明 2. 系統架構說明 3. 行銷推廣說明	1. 本所 2. 漢名科技 3. 逢甲團隊 4. 小客車租賃商業同業公會全國聯合會 5. 臺北市小客車租賃商業同業公會 6. 新北市小客車租賃商業同業公會 7. 小客車租賃業者

日期	會議名稱	議題	實際出席單位
11.16	產業座談會 (新竹場)	1. 計畫說明 2. 系統架構說明 3. 行銷推廣說明	1. 本所 2. 漢名科技 3. 逢甲團隊 4. 小客車租賃商業同業公會全國聯合會 5. 新竹縣小客車租賃商業同業公會 6. 苗栗縣小客車租賃商業同業公會 7. 小客車租賃業者
11.19	法令規章之專家學者座談會	1. 小客車租賃業法規 2. 定型化契約 3. 靠行與停車場問題	1. 本所 2. 漢名科技 3. 逢甲團隊 4. 中央警察大學 5. 看見臺灣基金會 6. 淡江大學 7. 交通部路政司 8. 交通部公路總局 9. 行政院消費者保護處 10. 小客車租賃商業同業公會全國聯合會 11. 新北市小客車租賃商業同業公會 12. 臺灣省小客車租賃商業同業公會 13. 臺北市小客車租賃商業同業公會 14. 宜蘭縣小客車租賃商業同業公會 15. 臺中市小客車租賃商業同業公會 16. 彰化縣小客車租賃商業同業公會 17. 臺南市小客車租賃商業同業公會 18. 新竹縣小客車租賃商業同業公會 19. 高雄市小客車租賃

日期	會議名稱	議題	實際出席單位
			商業同業公會 20. 桃園市小客車租賃商業同業公會 21. 小客車租賃業者 22. 中國信託資融股份有限公司 23. 新安東京海上產物保險股份有限公司
11.19	系統驗測討論會議	1. 逢甲團隊請漢名科技配合辦理事項 2. 逢甲團隊研提系統功能與相關技術文件之意見與建議	1. 本所 2. 漢名科技 3. 逢甲團隊
11.23	產業座談會(高雄場)	1. 計畫說明 2. 系統架構說明 3. 行銷推廣說明	1. 本所 2. 漢名科技 3. 小客車租賃商業同業公會全國聯合會 4. 高雄縣小客車租賃商業同業公會 5. 小客車租賃業者
11.23	輔導營運團隊會議(臺中場)	1. 系統架構說明 2. 獲利來源與收費機制說明 3. 創新服務討論 4. 行銷推廣說明	1. 本所 2. 漢名科技 3. 逢甲團隊 4. 臺中市小客車租賃商業同業公會
11.23	系統驗測討論會議	5. 前次(11.19)系統驗測會議辦理情形說明 6. 系統 7. 逢甲團隊請漢名科技配合辦理事項	1. 本所 2. 漢名科技 3. 逢甲團隊
11.25	產業座談會(花蓮場)	1. 計畫說明 2. 系統架構說明 3. 行銷推廣說明	1. 本所 2. 漢名科技 3. 逢甲團隊 4. 小客車租賃商業同業公會全國聯合會 5. 花蓮縣小客車租賃商業同業公會 6. 臺東縣小客車租賃商業同業公會

日期	會議名稱	議題	實際出席單位
			7. 小客車租賃業者
11.25	輔導營運團隊會議(臺北場)	1. 系統架構說明 2. 獲利來源與收費機制說明 3. 創新服務討論 4. 行銷推廣說明	1. 本所 2. 漢名科技 3. 逢甲團隊 4. 小客車租賃商業同業公會全國聯合會
12.10	系統功能展示說明暨意見交流座談會議	1. 系統功能展示說明 2. 聽取小客車租賃公會與業者之相關意見	1. 本所 2. 漢名科技 3. 逢甲團隊 4. 小客車租賃商業同業公會全國聯合會 5. 臺灣省小客車租賃商業同業公會 6. 臺北市小客車租賃商業同業公會 7. 新北市小客車租賃商業同業公會 8. 宜蘭縣小客車租賃商業同業公會 9. 金門縣小客車租賃商業同業公會 10. 桃園市小客車租賃商業同業公會 11. 臺中市小客車租賃商業同業公會 12. 小客車租賃業者
12.13	期末審查會議	期末報告內容審查	1. 審查委員 2. 交通部公路總局 3. 小客車租賃商業同業公會全國聯合會 4. 本所 5. 漢名科技 6. 逢甲團隊 7. 博大團隊

依照漢名科技所提出之工作時程規劃，例如：建置「租車平台」、深度訪談與平台功能規劃、輔導 600 家以上業者數位轉型等工作任務，延伸訂定本計畫專案管理時程，共計 15 項工作任務，截至 12 月 27 日，已完成 15 項工作任務，如表 3.1-2 與所示。

關於表 3.1-2 編號 9「租車平台」相關文件驗測與報告撰寫、編號 14「生態系平台」相關文件檢視，因受漢名科技開發時程影響，故於期末報告結案(12 月 28 日)前方才完成。原訂漢名科技於簽約日 90 天內，完成建置原資策會之「智慧租車共通平台」，並於簽約日 150 天與綠界科技股份有限公司完成金流功能介接，以及信用卡支付功能，與漢名科技確認驗測項目後，進行實際租車流程與驗測，但 10 月 13 日系統驗測討論會議決議，由漢名科技自行完成資策會「智慧租車共通平台」自行驗測，第三方團隊協助驗測漢名科技開發之「新智慧租車共通平台+旅遊生態系平台」，原訂漢名科技於 10 月底提供相關開發成果，11 月 15 日交付相關技術文件，經檢視後，發現開發成果與技術文件中仍有許多缺漏，詳細建議與意見請詳 3.2 節說明。於 11 月 19 日、11 月 23 日進行系統驗測討論，漢名科技亦回覆相關內容修正將於 11 月 30 日提供，本所已於 12 月 27 日前完成系統驗測與報告撰寫。

表 3.1-2 本計畫之專管任務

編號	任務名稱	預定開始日期	預定完成日期	實際開始日期	實際完成日期
1	逐月滾動風險控管計畫	02.26	12.31	03.19	12.27
2	專業知識諮詢	02.26	12.31	04.13	12.27
3	研提「營運規範與收費機制探討與訂定」建議	05.06	07.30	06.15	07.30
4	研提「租賃車業者招募規劃」建議	05.06	07.30	06.15	07.09
5	研提「服務及商業模式設計、需求規劃與市場定位報告」建議	05.06	10.20	09.01	10.19
6	研提「深度訪談與平台功能規劃」建議	06.01	10.29	06.03	06.23
7	研提「績效稽核機制設計」建議	07.01	12.01	09.01	11.29
8	研提「期初報告」建議	07.05	07.30	07.21	07.30
9	「租車平台」相關文件驗測與報告撰寫	07.15	12.31	06.28	12.27
10	研提「行銷推廣規劃」建議	08.04	12.01	09.01	11.29
11	研提「跨產業策略聯盟與創新服務模式規劃與設計」建議	08.04	12.01	09.01	11.29
12	研提「期中報告」建議	09.01	10.19	09.01	10.19
13	研提「經營計劃書」建議	10.01	12.01	11.08	11.29
14	「生態系平台」相關文件檢視	11.01	12.31	11.15	12.27
15	研提「期末報告」建議	11.15	12.17	12.01	12.10

3.1.2 辦理事項列管追蹤

計畫期間已與漢名科技召開多次工作會議，針對工作會議結論辦理情形，進行列管追蹤，因會議結論數量較多，計 125 條，因此簡易綜整分為幾個主要類別，並針對漢名團隊實際辦理情形進行管考，如表 3.1-3 所示。

表 3.1-3 會議結論辦理情形管考

會議結論之類別	管考狀態	數量	備註
系統建置	持續追蹤	1	關於旅遊生態系平台功能，已多次提醒漢名科技儘速完成，但於期末報告審查會議中發現仍未完成相關功能開發，經溝通後，列入其期末審查意見，作為後續驗收是否通過之依據。
	解除列管	20	漢名科技已完成辦理相關內容。
介接 M3 系統	持續追蹤	1	關於駕駛行為與違規紀錄等欄位是否納入 M3 系統介接，已於 6 月份工作會議提出，後續座談會中，小客車租賃業者亦有提出相關建議，惟漢名科技仍未確認是否要將相關資訊納入介接查詢。
	解除列管	9	漢名科技於合約簽訂後，即開始與交通部公路總局與中華電信公司討論 M3 系統介接內容，經多次討論申請單位、申請方式與申請內容後，終完成辦理相關內容。
營運規章/收費機制	解除列管	12	漢名科技已擬定相關營運規章與收費機制，但相關內容仍待營運廠商進行試營運後，方可確認。
契約分包/契約變更/專案管理表/工作月報與原始憑證	解除列管	7	漢名團隊對於函送分包廠商契約、契約變更函、每週更新之專案管理表、每月 10 日前函送上月工作月

會議結論之類別	管考狀態	數量	備註
			報與原始憑證，其文書處理時程與作業上仍尚有待加強。已多次於工作會議提醒，及發文提醒後，漢名科技仍有延遲提供相關文件的狀況產生。
商標申請	解除列管	9	漢名科技於合約簽訂後，即開始討論商標申請樣式與內容，惟法律事務所因對商標樣式持有其他意見，經多次討論與溝通後，漢名科技已完成辦理相關內容。
深度訪談	解除列管	6	漢名科技原採取 1 對 1 深度訪談的方式，但因考量訪談人數稍嫌不足，故經工作會議討論後，改採取座談會方式，但因難確保座談會訪談品質，故後續討論仍採取 1 對 1 深度訪談的方式進行。
期初發表會	解除列管	13	因受疫情影響，期初發表會延宕辦理，相關規劃內容亦根據中央防疫指揮中心之公告，進行滾動式檢討。
業者招募	解除列管	18	原業者招募數量較為不足，經工作會議上討論後，訂定每半個月之 KPI，確保執行進度，漢名科技已順利於計畫結束前招募
創新服務	解除列管	29	創新服務包含保險創新、捷運接駁等創新服務，經多次工作會議討論後，已有基本規劃雛形，下年度可依照相關規劃成果再行辦理。

許多會議結論內容，有延遲完成的狀況產生，經工作會議上多次提醒，並發文要求後，才能取得漢名科技之相關資料，對於行政文書處理成效不彰，建議可訂定相關規範，並納入下年度契約中，以確保得標廠商能確實完成相關內容。

3.1.3 知識諮詢成果

本計畫提供漢名科技於計畫執行階段，相關專業知識諮詢服務，以提升專案執行效益。並偕同曼塔睿科技股份有限公司、臺灣德國萊因技術監護顧問股份有限公司、道勤工程顧問有限公司協助審查與檢視相關文件，提供知識諮詢與審查意見與建議與建議。

分項二子項一計畫評選作業前，檢視投標廠商所提交之服務建議書，並研提服務方案、研究方法等相關建議與洽詢廠商等相關事項，綜整如表 3.1-4 所示，並於 4 月 13 日工作啟動會議上討論相關內容。

表 3.1-4 服務建議書之專管建議

文件	專管意見
服務建議書	1. 建議說明商業模式推行後對於出租率的提升與達標方式？ 2. 參與業者數量超過預算，將採取何種因應措施？ 3. 建議補充說明城郊區消費者租車情境。 4. 建議補充說明智慧租車共通平台規劃與軟硬體規格、維運方式及資安檢測內容。 5. 建議補充說明金流、使用者個資等資安如何進行或維護。 6. 若使用 Taiwan CarU 介接現行的資策會平台，是否有運作難處？預估需花費的成本與時間？ 7. Taiwan CarU 的示意畫面以網頁為主，但使用者在旅運中多數使用 APP，是否補充說明 Taiwan CarU 未來在 APP 上的規劃，以及未來使用者跟租賃業者如何使用本服務，使用情境是否描述說明(單一 APP 或多個 APP？)。 8. 建議補充說明如何輔導 600 家小客車租賃業者轉型及加入請補充說明 P.301 人事費用明細表與 P.297 工作計畫時程表之工作月數為何有落差？平台，並如何提高使用誘因及信任度？ 9. 專案經理是否為本計畫專任人員？是否具備專案管理證照？ 10. 建議補充說明「小客車租賃業經營管理」之相關實務經驗。

以下將針對漢名科技所提出之相關文件與規劃成果研提意見與建議，並於漢名科技完成辦理後，依據辦理情形進行評估，以下羅列評估圖示與情形。

表 3.1-5 評估圖示與情形對照表

圖示	評估情形
O	相關辦理情形，通過評估結果。
X	相關辦理情形，未通過評估結果。
△	相關辦理情形，無法評估其結果，應再商討。

針對漢名科技所規劃之期初發表會簡報與企劃書，已於 5 月 27 日與 6 月 2 日提供相關建議，如表 3.1-6 所示。

表 3.1-6 期初發表會簡報與企劃書之專管建議追蹤表

文件/章節	專管建議	漢名科技辦理情形	評估情形
活動主視覺/標語	建議主視覺應著重在「小客車租賃數位轉型」計畫的主題上，標語「我們租發吧！」做參考。而非於封面秀出 Taiwan CarU，建議 Taiwan CarU 可以鋪陳在後續推動上顯露。	經多次討論，主視覺除顯露「小客車租賃數位轉型」外，亦加上標語。	O
計畫說明	建議先點出一般民眾對於小客車租賃的痛點，讓大家產生共鳴後，再說明本計畫目的，以利民眾快速了解本計畫內容。	遵照辦理。	O
平面配置圖/入口接待處	運輸研究所 12 樓禮堂，階梯是位於舞台左右兩處，請再修正。另外若於 12 樓辦理期初發表會，接待區與報到區設於 1 樓，建議可再行規劃合適方式。	因考量人員前往 12 樓禮堂，較為不便，已將主場地與報到區變更至本所 B1 國際會議廳。	O

針對漢名科技提供之小客車租賃業者招募相關文件與小客車租賃業者招募網站，已於 6 月 15 日、6 月 28 日、7 月 5 日、7 月 9 日進行審查與檢視，綜整相關建議，並追蹤漢名科技辦理情形，給予相對應之管考建議，如下表 3.1-7 所示。

表 3.1-7 小客車租賃業者招募相關文件之專管建議追蹤表

文件/章節	專管建議	漢名科技辦理情形	管考情形
招募進度總表	招募進度總表欄位順序，應該與招募資料表名稱與順序一致。	遵照辦理。招募進度總表係提供給招募人員來掌控進度，因此以欄位精簡化的方式來設計招募進度總表。各資料表索引順序，將依意見調整一致。	O
招募資料表	1. 建議各個欄位都要提供填寫範例，否則回收的格式可能會不一致。 2. 車輛中只有日租價格，如果只租兩個小時，怎麼計算費用？ 3. 是否須調查業者有無提供額外服務，例如：嬰兒車、導航系統等？ 4. 建議資料欄位與參與暨資料使用授權同意書所列之相關欄位一致，並建議可於車輛欄位中加上燃油種類。	1. 遵照辦理。 2. 目前多數業者租車採全日計價，少部分提供半日計價，對於採用時租計價的業者在空租的業務上幾乎沒有。目前平台營運方向亦尚無規劃以時租方式提供空租租車，倘後續有多數業者反應此項需求，屆時會再請業者提供相關計價資訊，並納入平台中。 3. 已將相關配備納入「據點」資料表中。 4. 燃油種類並非屬於消費者選購租車產品之主要因素，爰仍維持不納入；MOU 將會同步修正。	△

文件/章節	專管建議	漢名科技辦理情形	管考情形
	5. 建議駕駛加上年資或駕照發放日期與生日欄位(因先前 M3 介接是採用駕駛身分證與生日欄位來確認)。 6. 因未來可能更新相關資料及檢視資料正確性，建議可增加資料填寫的時間欄位。	5. 遵照辦理，將一併將駕照發放日納入「駕駛」資料表中。 6. 於彙整相關檔案時，將會註記資料蒐集時間。	
招募計畫書	1. 契約 P.281 金流設定管理，包含現金、信用卡、LINE Pay、街口支付、臺灣 Pay、支付寶、超商繳費與虛擬帳號轉帳以及預存作業金扣款等，但招募計畫書中第四點付款方式僅提到信用卡支付。 2. 灰色字體是否為小貨車租賃業範疇？	1. 平台金流設定將優先完成信用卡線上刷卡功能，其他電子支付功能將會陸續與相關業者洽談合作簽約。招募計畫書中將予以補充說明。 2. 是，參考之招募計畫書暫為草稿，已持續補充修改相關內容。	△
產業調查問卷	問卷對象與契約 P.251 的公會組織似有不同？	問卷調查中所列之公會係將省聯會所轄之地區公會一併列出，因此會與契約所列內容稍有不同。	O
招募網站	1. 建議線上問卷開啟返回上一頁的功能。 2. 報名流程中上所列之文件名稱與實際文件名稱不一致。 3. 請依核准版之參與暨資料使用授權同意書，同步修正招募網站。 4. 建議招募網站上可以加入懶人包資訊(如：計畫說明、營運規範、收費機制、誘因機制、退場機制等)，	1. 遵照辦理。 2. 遵照辦理，已修正。 3. 遵照辦理，已更換參與暨資料使用授權同意書。 4. 遵照辦理，已加入相關懶人包資訊。	O

文件/章節	專管建議	漢名科技辦理情形	管考情形
	以利消弭業者疑惑並提升參與意願。 5. 招募網站中部分標題重複，建議可適當移除。 6. 招募網站主要是讓業者可以清楚參加此計畫的主要用意為何，因此建議應說明目前業者之痛點為何？加入本計畫平台可為其帶來哪些好處？計畫將為他們做什麼等比較具說服力的內容。	5. 遵照辦理，已移除重複標題。 6. 遵照辦理，已加入痛點分析。	
計畫說明簡報_1100709	1. P.6 有列出目前的痛點，建議應增加未來本計畫如何解決這些痛點的對應，讓本計畫更具吸引力。 2. 請漢名思考是否需跟業者說明 P.14 系統架構？建議可以多著墨於操作跟介面說明，並建議放大相關 UI 介面，讓業者可清楚檢視。 3. P.23 數位轉型三階段，建議提供預計的期程或是階段轉換的 milestone，讓業者可瞭解計畫期程與時間關聯(階段事件的發生時間點)。 4. 請更正 P.28 招募說明會辦理時程。 5. 建議可以加強說明業者加入計畫之好處與誘因。另考量部分業	1. 將於【計畫推動－數位轉型三階段】一併說明。 2. 遵照辦理。 3. 業者加入期程不一，難以一致化各業者數位轉型期程，分為三階段做為數位轉型推動步驟，讓業者瞭解數位轉型推動過程。整體計畫時程將於【推動時程】一併說明 4. 遵照辦理。 5. 已於【數位轉型平台介紹】中補充相關內容。另因本計畫旨在	O

文件/章節	專管建議	漢名科技辦理情形	管考情形
	者的資訊能力較薄弱，亦可加說明相關服務資源(如平台、app等)。	協助中小型租賃車業者進行數位轉型，爰【計畫推動－數位轉型三階段】便係讓業者瞭解其轉型後之資源。	
業者招募說明簡報_1100709	1. 請移除 P.4 空白頁。 2. 依據契約 4.4.3 小節之二、(一)說明「對租賃車業者最實質之誘因獎項則是由主管機關頒發之獎項及平台回饋之獎勵金，而平台之獎勵金卻是在合作社營運模式中，向各租賃車業者收取之佣金」，上開所指之「獎勵金」是否為簡報 P.5 中交易服務費的車商獎勵 5%？ 3. P.5 平台收費機制，為避免計畫期間所取得之營收，後續處理上較繁瑣，於計畫期間，向小客車租賃業者收取之費用，須全數歸還，因金流所產生之手續費，由計畫支應。 4. 另外請團隊思考看看是否有免費試用的期間，否則交易 25%可能會有偏高的疑慮。 5. 建議將 P.12 小客車租賃業者加入資格調整至 P.5 平台收費機制之	1. 已刪除。 2. 是的。相關回饋於業者獲消費者之費用皆從所收取之交易服務費來做支應。 3. 將遵照契約規定辦理。 4. 針對市面上相應的電商平台，由平台營運商統一做行銷、金流、系統維運等多元管理所訂費用，並無偏離市場費率。 5. 遵照辦理。	O

文件/章節	專管建議	漢名科技辦理情形	管考情形
	後，P.6 報名流程之前。 6. 簡報中僅提及招募部分，未說明業者退場機制與流程。 7. 因部分業者可能沒有email，P.8 強制填寫email，建議可評估採用簡訊、郵件等方式辦理。 8. 依據契約 4.4.3 小節之二、(二)說明「規劃與既有點數平台合作，以平台服務費抽佣之收入向相關業者購置點數，並以點數作為獎勵忠誠 B2C 消費者之機制」，並未於簡報中說明。	6. 退場機制區分為業者自行退出或經平台營運商認定有違相關規定而令其退出。針對退場機制有另行規劃，暫不於招募座談會上說明。 7. 若業者無 email，建議輔導業者於免費網域來申請，倘若有意願進行數位轉型，相關基本資訊仍須讓業者進一步嘗試。 8. 紅利點數機制與功能，將持續開發。	
常見問題_1100730	1. P.2 業者申請退出計畫，建議統一採用書面方式辦理。 2. P.3 前兩個問題，建議可合併，後兩個問題亦同。 3. P.4 中，針對問題 2，業者端系統是否可於指派車輛後，再次更換車輛？另外針對問題 5，以「地點」進行排序，是否係以「距離遠近」為排序依據？	1. 遵照辦理。 2. 遵照辦理。 3. 倘因臨時調度等狀況，有需更換車輛須以同等級的車輛，避免消費糾紛。係以消費者輸入的取車地點之距離遠近為排序依據。 4. 遵照辦理。	O

文件/章節	專管建議	漢名科技辦理情形	管考情形
	4. 建議補充說明業者現有之系統是否能介接本平台，及應如何申請？		

關於漢名科技提出之深度訪談計畫，已於 6 月 3 日進行審查與檢視，並於 6 月 23 日與漢名科技進行訪談演練，綜整相關建議如下表 3.1-8 所示：

表 3.1-8 深度訪談計畫之專管建議追蹤表

章節	專管建議	漢名科技辦理情形	管考情形
訪談對象	工作計劃書中 2.2.4 節說明及表 2.2.2 舉列之各利害關係人，中小型租賃車業者、主管機關、電子商務業者、餐飲業者、旅館業者、觀光景點業者、購物商場業者與其他使用者，並未列入此次深度訪談對象中，後續是否會另行規劃訪談行程及相關訪談作法？	1. 經查各地區公會理事長，其所經營之小客車租賃業即屬中小型規模，爰各地區公會理事長即同時代表中小型租賃車業者做為本次訪談對象。 2. 將以第一線平台使用者及相關業別主管為優先深度訪談對象，考量主管機關雖為平台利害關係人之一，但其優先性不高，惟為了解主管機關數位治理需求，將於本次訪談計畫中一併針對主管機關進行訪談。 3. 訪談計畫所列旅遊資源管理業者其已具備電子商務相關背景，又豐趣科技與臺灣旅圖其具備 B2B2C 或 B2G2C 之營運背景，已確切掌握食宿遊購業者及終端消費者於旅遊電商之實務需求。同時，食宿遊購業之相關公會組織理事長亦具備觀光旅宿營運相關背景，其易掌握其公會食宿遊購業等會員於營運上之實務，因此將其列為受訪對象，亦較具代表性。	O

章節	專管建議	漢名科技辦理情形	管考情形
訪談範圍與大綱	1. 依據契約中服務建議書審查意見處理情形表，是否確實將商業運轉所需之行銷工具、購物車、會員經營、分潤機制、客服諮詢、營運分析、推播公告等功能納入深度訪談調查中？	1. 行銷工具、購物車、會員經營、分潤機制、客服諮詢、營運分析、推播公告等功能，為規劃階段初擬商業運轉所需之功能，暫不將該些功能納入訪談題目，避免有引導回答之意圖，將透過受訪對象實際業務所需及所期望達成之效益做深度訪談，最終將針對訪談內容歸納本平台應具備之功能。	O
	2. 部分問題較為開放(如：「對於平台的招商計畫，有什麼想法或對策？」、「有沒有什麼是我們應該討論，卻沒有談到的？」)，可能使受訪者不易給出有效內容，建議給予較明確的情境（如：對於平台招商計畫的費用，有什麼建議？）。	2. 深度訪談主要是利用訪談者與受訪者之間的口語交談，達到意見交換與建構，藉由訪談的過程與內容，發覺、分析出受訪者的動機、信念、態度、作法與看法等，使問題與答案不經意浮現，爰優先朝大面向問題訪談受訪者，再依循其所回答內容，更深入探討與了解。因此專管團隊之意見，將納入訪談大綱，並依據受訪者之回答，進一步發掘細部答案。	
	3. 受訪對象跨多種角色，建議部分訪談題目可依照受訪對象而定(如：平台服務提供者使用問題 A~C，食宿旅遊業使用問題 D~F)，較能挖掘不同領域之痛點。	3. 遵照辦理。	

章節	專管建議	漢名科技辦理情形	管考情形
	4. 此次深度訪談對象以租車業者及工會等為主，詢問其是否有租車經驗似乎不妥，應以業者或工會角度上，認為過去民眾在租車上有沒有什麼建議或疑慮或是推行業務上有哪些問題及自身的經驗來分享後，再接續詢問後續問題。	4. 遵照辦理。	
	5. 針對小客車租賃業者，可以詢問加入現有各大租車平台的原因為何，找尋小客車平台的niches。 6. 訪談對象有平台業者，因現在已經進入平台世代，業者通常會使用多平台進行通路撒點，建議可以評估平台之間資料串接的意願跟可行性。此外，為避免智慧租車共通平台與民爭利，建議也可訪談目前較具指標性或同性質的廠商(如 yoxi，近期和泰集團之車輛派遣服務)。	5. 遵照辦理，將納入訪談大綱。 6. 關於評估平台之間資料串接的意願跟可行性，將於訪問平台服務提供者對象時，納入訪談大綱。另關於訪談與本計畫平台相仿之具指標性或同性質的廠商，已納入租／叫車平台業者，其他如 yoxi、LINE TAXI 類型之叫車平台屬計程車客運（服務）業，待後續視訪談所需必要性，再考量納入訪談對象。	
其他建議	建議可搭配狩野分析模式歸納訪談結果，較能收斂並發掘核心功能需求，同時避免後續過度開發（不一定須按照傳統狩野分析	遵照辦理。	O

章節	專管建議	漢名科技辦理情形	管考情形
	法使用問卷，亦可於訪談時納入詢問方式，確認該需求之急迫性）。 透過分類，將需求歸納成以下需求，開發之優先次序為：M>O>A>I。 M 基本型需求（Must-be）：顧客對企業提供的產品／服務因素的基本要求。 O 期望型需求（One-dimensional）：顧客的滿意狀況與需求的滿足程度成比例關係的需求。 A 魅力型需求（Attractive）：讓使用者覺得驚喜的功能。如果有，則會讓使用者感到滿意，但沒有也不會因此表現出明顯的不滿。 I 無差異需求（Indifferent）：使用者對這一因素無所謂。 R 不需要（Reverse）：使用者不需要這種功能，甚至對該功能反感。 Q 有疑問（Questionable）：如出現此反饋則可能問題的問法不合理、受測者沒有很好地理解問題，需重新測試。		

每月與漢名科技及相關主管機關召開工作會議討論，並於會前與會上研提相關建議，及針對創新服務-高捷都會接駁第一階段可行性規劃成果與問卷調查、智慧財產權、系統架構等內容綜整如表 3.1-9 所示。

表 3.1-9 其他資料之專管建議追蹤表

文件/章節	專管建議	漢名科技辦理情形	管考情形
創新服務_高捷都會接駁第一階段可行性規劃成果報告	1. 關於捷運接駁附駕租車服務費收入初估方式，因尖峰時段，捷運站至工業區行車時間較長，可能無法於 1 小時服務 2 趟次，而產生超時問題，應如何解決？ 2. 現階段 MeN Go 點數主要提供輔助運具業者，扮演第一哩及最後一哩使用。與多數使用者空車租賃習慣，以整趟旅次使用為主有落差。 3. 假設平均租車時間為 3 小時，是如何取得？ 4. 現行輔助運具折抵車資每趟次以 135 點(元)為上限，但租借小客車空車費率以	1. 1 小時服務 2 趟次為目前依場域現況初估，實際營運若有超時則規劃仍依預約時設定之單程車資收費，不增加乘客支出為原則。 2. 目前 MeN Go 點數供輔助運具乘客使用時並未限定起迄一端需於大眾運輸車站轉乘，亦即並不以第一哩及最後一哩為前提，此與 MaaS 精神一致，即鼓勵民眾可以不需要持有車輛而仍可獲得所需的運輸服務。 3. 依據交通部 109 年民眾日常使用運具狀況調查，高雄市外出民眾平均每一旅次花費時間約為 21 分鐘，其中公(商)務、休閒旅次又較平均時間為長，故本報告租車需求以來回各 0.5 小時，加上洽公辦事或休閒娛樂 2 小時，預估共 3 小時。 4. 依 MeN Go 現行機制，單趟車資超過點數上限之部分則由乘	△

文件/章節	專管建議	漢名科技辦理情形	管考情形
	200(元)/小時估算，表示部分租車時間無法以點數折抵，其費用如何計算與扣除？建議可設定在此 135 點為上限條件下，能夠使用之哩程或時間。 5. 汽車購置成本較高，報告書中假設捷運接駁附駕租車服務每年擴點成長 50%、空車租賃費收入每年成長 30%，是否過於樂觀。 6. 若此租賃車服務平台可納入，可望提升 MeN Go 點數使用率，惟租賃車服務平台相關成本，以現行 MeN Go 收益來看，恐無法支應。 7. 使用族群中，學生族群(國高中生及大一新生)佔多數，但該族群具備駕照的人數有限，請團隊於後續行銷推廣上，需特別注意及思考因應措施。	客自行支付差額，小客車租賃以時計費，故低於 1 小時仍以 1 小時計費，並無部份時間之問題。 5. 南部地區短租車輛出租率平日僅 27.2%、假日僅 37.5%，且本創新服務每日出車量僅佔高雄整體租車供給之一小部分，故以業者既有車輛規模即足以滿足本報告中所假設之成長規模。未來年預估之成長不侷限於高雄，也包括拓展至其他五都甚至全國各縣市。 6. 增加本創新服務對於平台除初期開發相關介面及串接 MeN Go，後續運營並不會增加平台成本，反而能增加收入機會，因此應無成本之疑慮。 7. 遵照辦理。	
創新服務_高捷都會接駁問卷調查	1. 建議先檢視調查目的，根據目的確立調查向度，如：受調者使用大眾運輸交通工	1. 謝謝指教，已補充相關問題。	O

文件/章節	專管建議	漢名科技辦理情形	管考情形
	具頻率（次數、時間…等）、平常使用交通方式（開車、騎車、搭乘大眾交通工具…）、使用捷運接駁服務意願，再依據每個向度發展問卷試題。如此，較能從各個向度間的關係來了解大眾需求及意願等。 2. 應先詢問受調者目前的上班運具使用現況(如：目前多以什麼交通工具前往工業區？從家裡出門到上班地點約需多久時間？每月通勤費用是多少？)之後才可分析其選擇或不選擇租賃車、共乘的可能原因。 3. 建議個人資料中第1、2、5(年齡、性別、email)問項移到最後面再詢問。 4. 問項 13、20「您願意支付的單程車資是多少？」建議可改為「您可以接受的單程車資落在哪個區間？」，避免因答案範圍較廣及易產生離群值，影響分析結果。	2. 謝謝指教，已補充。 3. 謝謝指教，已調整。 4. 考量避免提供金額選項容易選取較低者，因此仍維持採用開方式問答。	
工作會議簡報_智慧財產權聲明	1. 公總 M3 資料不應屬於本所範圍，應移至第三方。 2. API 應可區分 Client 端與 Server 端，其中	1.遵照辦理。 2.遵照辦理。	O

文件/章節	專管建議	漢名科技辦理情形	管考情形
	Client 端之財產權屬於運研所範疇，建議修正繪圖方式，以更清楚描述智慧財產權歸屬。		
工作會議簡報_系統架構	針對漢名科技提出欲將流量分析、族群/行為分析、踩點活動、抽獎活動及以第三方開發成熟之應用服務作為平台部分功能連結。建議未來於系統規劃報告中，應清楚說明第三方應用程式使用緣由與範圍，並將相關申請程序、接洽步驟、使用流程以及數據蒐集分析等相關事項加以註明。	遵照辦理。	O

關於 90 天系統相關文件、150 天金流相關文件，已於 6 月 29 日、7 月 5 日、9 月 15 日、9 月 28 日提供相關建議如表 3.1-10 所示。

表 3.1-10 系統(含金流)相關文件之專管建議追蹤表

文件	專管建議	漢名科技辦理情形	管考情形
測試成果報告	1. 針對平台測試結果 SonarQube 部分，建議提供詳細的 report，而非只有測試結果頁面截圖，這樣後續在有效性上的佐證易遭受質疑。 2. 目前的系統測試報告資料分散，建議應由漢名提供完整報告，資策會報告輔以附件的方式呈現。	遵照辦理。SonarQube 詳細檢測報告，已於 7/5 提供。	O
使用手冊	針對小客車平台流程說明，請描述如何進行車商流程訓練。	遵照辦理。已納入「以智慧租車共通平台推動小客車租賃業數位轉型說明書」中。	O

文件	專管建議	漢名科技辦理情形	管考情形
系統操作	針對目前的平台 https://dealer.caru.com.tw:8086/, 使用者在密碼輸入錯誤後，無正常回饋，建議評估進行修正。	遵照辦理，已修正完畢。	O
其他	1. 因資策會的平台技轉後的實際應用規劃跟目標不明確，希望漢名可以資策會平台導入後，期望讓使用者作什麼操作應用跟預期的成果，提供文件說明，以便專管團隊根據目標去檢視看還有缺少什麼。 2. 建議提供平台預計以何種形式進行「推動數位轉型」作業的說明，例如上線的網站、使用的 APP 以及相關的版次資訊等。 3. 請補充金流測試計畫書文件。	遵照辦理，已納入「以智慧租車共通平台推動小客車租賃業數位轉型說明書」中。	O
APP 架設_v1	1. App 上架資訊中的開發者應為漢名科技。 2. app 不同身分使用顏色來區分，在操作上容易搞混，建議可以在 icon 上簡易設計，或是導入文字做區分。	1. 漢曜科技為漢名科技過去登記之公司名字，暫不影響計畫推動。預計於 8 月底前完成開發者名稱變更。 2. 遵照辦理，刻正設計 Taiwan CarU 品牌 Logo 中，後續將依據該 Logo 主視覺來延伸設計 icon，並於定案後修正 app icon。	O
其他	請針對資策會原建置系統與漢名建置系統，提供差異對照表。	1. 原先採用 Oracle DB，目前在 AWS 採用 AWS RDS SQL Server。 2. PORT 更新	O

文件	專管建議	漢名科技辦理情形	管考情形
		(1) API 連線資訊：https://網址名稱:8080/SmartRentalServer (2) Socket 連線資訊：https://網址名稱:8081 (3) 租車平台：https://網址名稱:8086/ 3. 原先無「測試計畫書」及「測試成果報告」，此為新增內容。 4. 原先無上架「IOS-App store」及「Android- Google Play」，此為新增內容。 5. 原先無架設平台說明書，此為新增內容。 6. 已更新原先授權的文件（如設計規格書、（使用手冊）。	
(信用卡支付)使用手冊_v2	請確認收費是否正確及目前平台是否有儲存相關交易紀錄？(例如：交易時間、交易金額等)，從流程上看來似乎只是介接，若日後有相關的交易疑慮，是由綠界提供相關資訊嗎？另外相關交易紀錄是否能在平台端上檢視，避免有心人士繪製造假的示意圖以假亂真。	系統儲存交易代碼、交易時間、交易金額及交易紀錄；詳細資訊可由綠界廠商管理後台提供詳細資訊，綠界廠商管理後台(測試用)連結如下： https://vendor-stage.ecpay.com.tw/User/LogOn_Step1 帳密： stagetest1234/test1234 統一編號：53538851	O

文件	專管建議	漢名科技辦理情形	管考情形
技術手冊	1. 請於補充說明金流清分方式，例如： (1) 銀行是直接撥款到平台，再由平台清分？ (2) 銀行撥款到綠界，由綠界清分？ (3) 銀行直接撥款到各車商？ 2. 收費的部分是否有提供月報相關文件？並請確認是由綠界提供或是由漢名自行建立。 3. 11 月中應該還有 Line pay 第三方支付的部分，亦請補充於文件說明中。 4. 金流串接沿用第三方支付提供的 API，使用上應無問題，惟請補充說明相關配套措施(例如：交易成功跟失敗，車商端要如何確認)。 5. 使用手冊中，圖 3-7 交易失敗的畫面，建議應以 APP 的操作畫面為主(應以 APP 樣版呈現，而非 WEB 樣板)。 6. 部分敏感資訊(例如：特店編號、HashKey、HashIV)，建議不要以明文方式呈現，可以透過模糊處理方式呈現。 7. 建議使用手冊應考量營運商端、車商端在金流驗證上所需之相關流程，較為完善。	1. 遵照辦理，金流清分的方式，主要由銀行撥款到綠界後，再由綠界清分給合作廠商，如設計規格書第 2-2 頁。 2. 詳細報表功能由綠界廠商管理後台提供。 3. 本次提供的為信用卡交易的技術及操範圍，將於此意見填報於期中報告書中。 4. 本系統後台於訂單管理功能，顯示訂單狀態停留在『取得訂單』，無法進入『未派車』狀態，搭配綠界廠商管理後台的信用卡收單交易明細查詢，查詢交易失敗原因。 5. 圖 3-7 就是 APP 上消費者會看見的畫面。以目前設計的交易流程，若交易失敗就會跳轉回到付款頁面，顯示交易失敗。 6. 遵照辦理，已模糊與隱蔽。 7. 金流主要使用角色為消費者，對營運商及車商端來說只有交易成功或失敗，等體金流驗	O

文件	專管建議	漢名科技辦理情形	管考情形
		證在綠界科技端,非本系統端,本系統主要提供相對應 API 所需資訊,故建議無須修正寫法。	
(信用卡支付)使用手冊_v3	建議使用手冊應考量營運商端、車商端在金流驗證上所需之相關流程，較為完善。因目前平台並無紀錄單一車商金流總收費，未來可能是由車商自行統計應收金額，若此金額與綠界撥款金額不一致，可能導致收費爭議。建議應制定相對應的帳務稽核程序，並有文件清楚描述相關的金流統計、撥款統計範圍(例如前月的 26~該月的 25 日)、撥款日以及相關手續費等說明，可放在使用手冊或是營運規章中，以便未來帳務稽核時使用。	後續整體的完整金流會放於旅遊生態系服務平台上,智慧租車共通平台僅提供派車等其他租還車及派遣等業務功能。將補充於整體平台業者加入使用條款中，以利加入之小客車租賃業者遵循。	O
	預約車輛，以錯誤之信用卡資料進行測試(卡號：4311-9522-2222-3333、安全碼：333、有效期限輸入 11/22)。顯示付款失敗後，返回使用者的操作頁面(App)，卻顯示信用卡交易完成。再跳轉回訂單畫面後，卻變成 VIOS 1.5 的車款。 測試功能與紀錄均正常，惟付款失敗後，返回使用者的操作頁面(App)，會跳回信用卡交易完成的頁面，可能會誤導使用者的	已完成修改。	O

文件	專管建議	漢名科技辦理情形	管考情形
	操作，建議修正。		

3.1.4 風險控管

本計畫係針對「智慧租車服務營運規劃與推動實務」計畫中之子計畫「商業模式設計與數位轉型推動實務」進行專案管理，針對該案擬定計畫風險控管計畫。本計畫所採用之風險控管辦法，即依據風險強度大小，訂定出風險門檻值，而就風險衡量值的可接受值分三類風險區域，超出風險門檻值上限者為不可忍受風險區域，低於風險門檻值下限者，為可忽視風險區域，介於上、下限者，為合理務實降低風險區域(as low as reasonably practicable, ALARP)，也就是風險尚可接受或是可控制的情況如風險之 ALARP 圖(ALARP carrot diagram)所示。

當風險屬於不可忍受風險區域時，則代表該風險無法受到一般大眾接受，或是超過政府法定標準，因此，則必須採取降低風險的必要措施，值到風險值降至門檻上限值以下；若風險屬於合理務實降低風險區域，可以考量風險降低措施所需要的成本和降低風險所帶來的效益，當經過評估後，且執行符合經濟效益時，則應儘可能採行降低風險的措施。若風險屬於可忽視風險區域，則可無區採用任何措施降低風險。

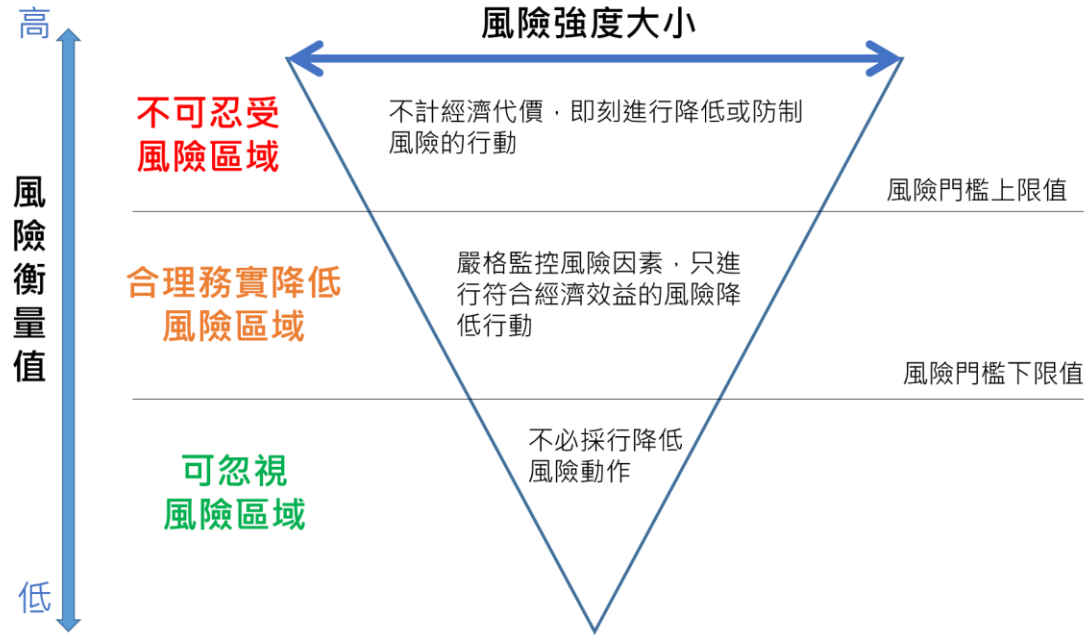


圖 3.1.1 風險之 ALARP 圖

本計畫採用之風險評量方式即建立風險矩陣，以風險發生頻率為橫軸、事故嚴重性為縱軸，進而區分風險等級進行分析，然而風險等級則分為 4 級，分別為：不可忍受風險區域(R1)、不理想風險區域(R2)、可忍受風險區域(R3)及可忽視風險區域(R4)。

子計畫「商業模式設計與數位轉型推動實務」第二期數位轉型推動計畫中，包含採購、期中審查、期末審查、經費支用查核在內的行政作業，提供專案管理服務，同時也針對計畫執行團隊所規劃之數位轉型輔導、創新服務方案規劃、行銷推廣活動、營運模式及相關策略等，協助進行審驗，並研提相關建議與評估業者及使用者接受度，故風險控管擬包括「專案執行作業」及「策略審驗」兩部份。

本計畫針對上述這項行政作業及策略進行風險辨別，找出各風險因子，並依據專案每個月實際執行進度與預期進度差異做為頻率/機率指標，而各風險因子對於專案之重要程度，做為嚴重度指標，帶入風險矩陣中進行風險評量，找出風險等級，再針對該風險屬於不理想(R2)及可忍受(R3)者進行處置，本計畫所採用之風險矩陣及風險等級，如表 3.1-11 所示。

表 3.1-11 本計畫採用之風險矩陣與等級

		頻率/機率(執行進度)				
		>=0%	0%~-5%	-5%~-10%	-10%~-15%	>-15%
重要程度	非常重要	R4	R2	R1	R1	R1
	重要	R4	R3	R2	R1	R1
	普通	R4	R3	R2	R2	R1
	不重要	R4	R3	R3	R2	R2
	非常不重要	R4	R4	R3	R3	R2

所採用之風險控管方法及流程，如圖 3.1.2 所示。本計畫主要依據子計畫「商業模式設計與數位轉型推動實務」所繳交之進度報告進行風險評量及控管，對於討論會議中發現之風險態樣進行評量作業；經評量作業的風險因子，若屬於 R1 等級，則須立即改善，則通知機關並請負責廠商一週內改善，並提交改善報告及進行複核，直到該風險等級低於 R1 等級止；若風險等級屬於 R2 或 R3 者，則依據該風險因子對應工項進行成本效益評估，若有立即改善之必要，亦請廠商一週內改善，若無立即改善必要，則提出改善建議做法，通知廠商於次月或是限期改善；若風險等級為 R4 者，則針對各風險因子所屬工項進行追蹤，若有面臨執行問題，則可提供專案諮詢。

針對可能面臨之風險，均可提供專業諮詢，讓專案執行過程能夠順利，而各項專案諮詢內容，均做為紀錄，提供後續專案執行，或是後續專案及研究參考，為必要之回饋機制。

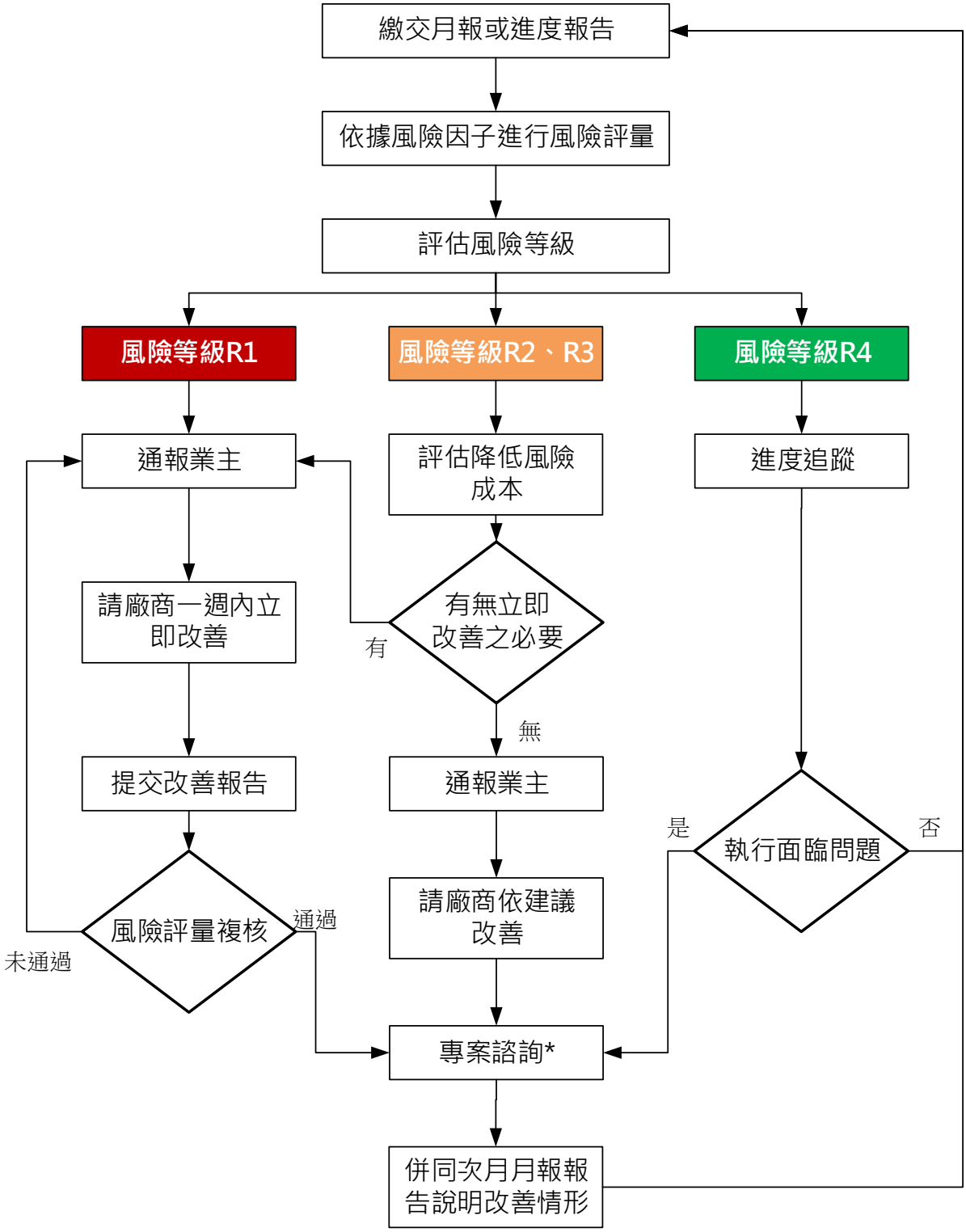


圖 3.1.2 本計畫風險控管方法及流程圖

對於風險等級屬於 R2(不理想)與 R3(不可忍受)時，本計畫另擬定對應之處理方，係因風險等級屬 R2、R3 時，採用降低風險成本方式辦理，則須檢視該風險因子屬於嚴重度可減輕，或者是可減緩發生頻(機)率，再採後續風險移轉作法。例如，若某風險因子屬於重要且發生頻率為-5%~-10%時，則會採用降低發生頻率之作法，將發生頻率降為 0%~-5%，讓風險等級將 R2 降為 R3，如表 3.1-12 所示。

表 3.1-12 風險等級與機率

評估因素/風險等級		頻率/機率(執行進度)				
		>=0%	0%~-5%	-5%~-10%	-10%~-15%	>-15%
重要程度	非常重要	R4	R2	R1	R1	R1
	重要	R4	R3 ← R2		R1	R1
	普通	R4	R3	R2	R2	R1
	不重要	R4	R3	R3	R2	R2
	非常不重要	R4	R4	R3	R3	R2

3.1.5 各階段風險與管控措施

本計畫針對專案籌備、開發到應用等階段，各階段可能遭遇不同程度之風險，提出可能面臨之風險，據此，本計畫將標的專案分為：遴選與競標風險、專案執行風險、系統開發與整合風險、財務風險、營運風險、資安風險及其他不可控制風險七大項。此七大項風險類別中，各個風險因子如表 3.1-13 所示。

表 3.1-13 本專案風險因子一覽表

風險類別	風險因子
遴選與競標風險	備標規範缺漏、廠商遴選時程延宕、簽約及議約期程延宕
專案執行風險	未如期交付開發成果、未如實登載計畫執行
系統開發與整合風險	技術轉移失敗及不完全、轉型推廣量能不足、數據資料無法介接、與現存其他機關系統無法整合
財務風險	開發財務不足、促銷推廣所需財源無法支應
營運風險	平台數據接收遺失、法源規範不足
資安風險	硬體或平台受損、資料遭竊取或遭他人使用
其他不可控制風險	其他不可抗力風險

依據上述列出各類別中的風險因子，本計畫就各風險因子所代表之意涵與定

義，說明如下：

1. 遴選與競標風險
   (1) 備標規範缺漏：指在備標期間，相關規範無法依據實際需求完整制定，使得投標時程受影響。
   (2) 廠商遴選時程延宕：在投標過程中，受廠商提出疑義，使得標案另須檢視，使得廠商遴選時程延宕。
   (3) 簽約及議約期程延宕：完成投標作業後，優先議約廠商對於價金或合約另有疑慮，或是無法進入得標條件，使得期程延宕。
2. 專案執行風險
   (1) 未如期交付開發成果：意指受監理之廠商，未依合約規範如期交付開發成果。
   (2) 未如實登載計畫執行：指執行專案廠商，依合約規定交付開發成果後，內容與合約登載不符。
3. 系統開發與整合風險
   (1) 技術轉移失敗及不完全：意指平台系統開發時，開發之系統內容無法符合使用者需求，或者是無法整合其他必須介接之系統，使得系統功能不足。
   (2) 轉型推廣量能不足：協助使用業者進行數位轉型，無法依原規劃進行推廣，使得受轉型使用業者家數未達標準，或是該產業部分業者無法接受轉型之內容，使得推廣時間延長。
   (3) 數據資料無法介接：所需資料因開發技術不足，無法接收所需資料，或者是接收筆數及欄位不完全。
   (4) 與現存其他機關系統無法整合：因系統需整合他機關其它系統，以進行數據分析或商轉事宜，卻因其它機關或與其廠商契約協定內容或其他考量之故，無法完成整合事宜，導致後續開發時程延後或無法完成履約事宜。
4. 財務風險
   (1) 開發財務不足：系統開發所需經費不足，使得部分開發功能無法使用，卻未有相對預算經費支援之情事。
   (2) 擴充或維護財務不足：有系統擴充需求、系統保養維護之需求，卻未有相對預算經費支援之情事。

(3) 促銷推廣所需財源無法支應：輔導轉型或者是受轉型使用業者，所需支付之經費無法支應，而無法進行促銷及推廣作業。

5. 營運風險

(1) 平台數據接收遺失：平台營運期間，系統無法接受數據，或者使用者介面出現錯誤，致使營運中斷。

(2) 法源規範不足：對於受監督專管專案，在執行期間或是平台營運期間，因法源規範不足，使得專案或營運中斷，或產生糾紛。

(3) 業者加入、退出衍生事務及成本：推廣期間，因業者加入或退出，所衍生之人事、系統修改、行銷推廣等額外資源投入之情事。

6. 資安風險

(1) 硬體或平台受損：硬體或平台受不當使用或防護不足之故，使得設備無法使用或資料受損之情形。

(2) 資料遭竊取或遭他人使用：因資料傳輸未妥善設定，使得所蒐集之資料遺失、遭他人冒用或竊取之情形，致使資料外洩或損失。

7. 其他不可抗力風險

其他不可抗力風險：其他無法預期且無法歸咎於執行合約雙方之風險。

上述各類風險因子，在不同的階段下，各個風險因子均會對於專案造成若干影響，因此在界定完成各風險之意涵，完成風險辨識後，即可進一步針對風險採取進一步的措施。針對計畫本身尚無足夠資料或是文獻支持進行重要程度及發生機率之評量門檻，因此僅依據此些風險因子對於本專管專案造成之影響進行評量，再找出其風險等級，以便進行風險管理。各類別之風險因子之重要程度。以下說明各風險評量：

1. 遴選與競標風險:此類別主要評量各因子對於廠商遴選及競標是否造成影響，因此，對於備標規範缺漏風險，可能會影響後續履約或是在備標期間造成廠商疑慮，因此其重要程度屬於「重要」，其餘兩項對於招標期程延宕，係依據採購法規定辦理，因此重要程度為「普通」。然而，由於各專案之獨特性，並非每位承辦人員或是監辦人員能完全掌握規範內容是否遺漏，因此發生機率為 5~10%。

2. 專案執行風險:對於得標(履約)廠商未如實登載計畫執行進度，將會失去專案監管之依據，造成專案缺失及損失，因此屬於「重要」程度，但專案執行能透過管理之方法進行管控，因此發生機率較低，反觀未如期交付開發成果，

契約中已明定相關罰則，且能進行相關監管作業，因此重要程度屬「普通」，但發生機率較未如實登載高。

3. 系統開發與整合風險：由於本專案之主體屬資訊技術之整合，相關技術若未成功移轉或是移轉不完全，都將造成成果及進度嚴重影響，因此屬「非常重要」程度，但發生機率偏低；此外，轉型推廣量能不足以及數據資料無法介接，就目前資訊技術而言應屬可以克服，因此重要程度為「普通」，但發生機率較高。與其他現存機關系統無法整合情形，亦屬發生機率普通的風險，但在不影響系統功能運作之情形下，其重要程度為「普通」。鑒於專案屬於推廣期間，將可能面臨系統儲存、備份或運作量能不足之情形，屬於資料蒐集及業者加入期間，重要程度屬「重要」，發生機率中等。
4. 財務風險：開發財務不足會導致專案無法如期交付期末報告，會影響整體專案執行，因此，此風險屬於「重要」層級；擴充或維護財務不足是系統運作期間可能面臨之風險，可透過事前規劃或是增列下一年度預算方式，因此嚴重程度為「普通」，屬低發生機率；此外，促銷推廣所需財源無法支應，仍可透過其他方式進行推廣，因此重要程度僅屬「普通」，但都屬低發生機率。
5. 營運風險：平台數據接收遺失發生機率較高，若數據接收遺失，將會影響後續分析事宜，因此屬「重要」層級；另對於法源規範不足部分，可透過修法或是行政命令補正，雖然發生機率偏高，但是嚴重程度屬「普通」。在推廣期間，業者加入、退出所衍生事務及成本將會累績，原列入專案事項中，但可能會出現額外的事務及其衍生的成本，因此重要程度屬「不重要」，且發生機率低。
6. 資安風險：無論是硬體或平台受損或是資料遭竊取或遭他人使用皆屬重要資安事件，屬「重要」層級事件，若承辦廠商稍有不慎將可能發生，因此發生機率也是偏高。
7. 其他不可抗力風險：其他不可抗力風險發生機率偏低，且重要程度對於本專案而言，屬「不重要」程度。

3.1.6 本案實際發生風險及管控情況

其次對於上述風險評量結果，研擬相關作為，進行風險迴避或是轉移，讓其發生機率降低，或是對於其發生的嚴重程度降低，因此對於各風險因子進行風險控制作為，以下就本案各類工作執行過程中，針對風險控制方法說明如下。

1. 遴選與競標風險

(1) 備標規範缺漏：依據採購法巨額採購相關辦法，進行廠商特定條件以及規範書審訂，降低重要/嚴重程度及發生機率。本項工作執行過程中無出現風險。

(2) 廠商遴選時程延宕：備標過程文件及規範說明，尤以廠商資格條件擬定說明，並於廠商提出疑義時儘快精準回復，降低發生機率。本項工作執行過程中，因受經濟部委由資策會開發建置「智慧租車共通平台」技術移轉給本所之時程延宕影響，該部於 109 年 10 月 28 日完成期末報告審查，遲至 110 年 2 月 26 日方才完成技術授權移轉置本所，致使遴選廠商時程延宕。

(3) 簽約及議約期程延宕：依採購法相關規定，制定底價或議約條件，且逐項先行擬定說明，降低發生機率。本項工作執行過程中無出現風險。

2. 專案執行風險：

(1) 未如期交付開發成果：每月定期與建置單位，以及相關關係單位(如交通部公路總局、公會等)進行工作會議討論，透過進度報告確認執行進度，並制定預期罰責，透過本計畫訂定之風險控制流程(R2)進行追蹤，降低重要/嚴重程度。

建置商於開發過程中，邀請「中華民國小客車租賃商業同業公會全國聯合會」列席工作會議，聽取產業端對於該系統的期許及看法，適時納入公會的意見，以使該系統未來能更順利的推廣及使用。但全聯會，認為該系統應以前期資策會所建置的平台進行推廣營運即可，無需再額外開發旅遊生態系之平台，應將此經費運用於小客車租賃業者端的推廣上。而開發旅遊生態系平台為契約工作項目，造成全國聯合會對於此計畫不支持，甚至提出「建置商有分化公會之疑慮」，致使原計畫 KPI (須納入 600 家業者加入此平台，並需有 10,000 筆人車路數據資料，且提升出租率 3%)，進度無法順利推廣。因此，進行以下風險控管措施：

(a) 請建置商前往拜訪全聯會，進一步磋商取得共識。

(b) 積極辦理平台推廣說明會，並逐一聯繫業者邀請加入平台。

(c) 選擇較積極配合的地區公會、業者，進一步洽談推廣細節。以此將可促使 KPI (10,000 筆人車路數據資料，且提升出租率 3%。)能夠有效提升。目前選擇臺中公會進行積極推廣。

依照上述相關風險管控措施，由建置商先行與臺中公會洽談相關招募與合作事宜，截至 11 月 26 日已有 628 家小客車租賃業者參與「小客車租賃業數位轉型發展計畫」，並積極請業者協助完成 10,000 筆人車路數據資料。另外亦請建置商多次拜訪全聯會，於商談達成共識後，全聯會表示願意協助與支持建置商完成相關工作項目，如招募業者加入平台、辦理業者座談會與產業說明會等，並願意由全聯會輔導業者籌組營運團隊，以期接手後續平台營運業務。

(2) 未如實登載計畫執行：透過定期工作會議確認執行內容，要求須定時更新執行進度於專案管理平台，並於 line 群組中回報工作狀況與困難，即時解決問題，而計畫執行期間隨時依進度執行情況進行審視與追蹤，降低重要/嚴重程度。過程中，建置商若延誤預排進度 2~3 天，我方會即時聯繫建置商之計畫經理及主持人，要求需儘速趕上進度，並通知延誤情況，在計劃執行過程中，皆有適時補上，進度執行上之風險皆獲得控制。

3. 系統開發與整合風險：

(1) 技術轉移失敗及不完全：於建置商研擬相關技術項目關聯架構後，建置商需列出關鍵技術及移轉做法，供團隊成員進行檢視。並要求每次需求訪談需製作紀錄，並且將會議結論及作法陳報備查，亦由博大團隊協助確認相關技術授權之關係，確保日後技術授權之權利義務之釐清。

(2) 轉型推廣量能不足：依據建置商之工作執行計畫書、合約規劃推廣家數，分批(比例)進行檢核，並依據檢核點條件。其中，分批(比例進行檢核)可依據時間進行規劃，除透過月報檢核累加推廣家數外，亦可於推廣期間，透過工作會議方式，將檢核時間點縮短為每半個月一次，以妥善掌握推廣情形。由於計畫執行初期，建置商與全聯會尚未取的共識，致使建置商於招募業者數量在接近檢核點時(10 月底)尚有落差，為避免致轉型推廣量能不足之風險產生，本案於相關工作會議中研提以下招募進度，建置商透過召開說明會、個別公會訪談等方式，終使招募情況得以如期達

到契約要求。

表 3.1-14 招募進度檢核表

檢核日期	9/30	10/15	10/30	11/15	11/26
契約要求家數	100	-	-	-	600
逢甲建議家數	150	300	450	600	-
漢名實際家數	238	395	497	628	628

(3) 數據資料無法介接：本計畫於 12 月 1 日起進行系統測試，包含針對功能測試、資料確認、使用者體驗等方式進行測試，並記錄相關測試過程及缺失判定，再將結果交由建置商進行後續修正，確保資料的完整度。並同時告知測試結果，要求建置商於期限內完成，並追蹤其修改進度，避免產生資料不完整及無法介接之風險發生。

(4) 與現存其他機關系統無法整合：本計畫於 12 月 1 日起進行系統測試，包含針對功能測試、資料確認、使用者體驗等方式進行測試，並記錄相關測試過程及缺失判定，再將結果交由建置商進行後續修正，確保資料的完整度。並同時告知測試結果，要求建置商於期限內完成，並追蹤其修改進度，避免與現存其他機關系統無法整之風險發生。

(5) 系統儲存、備份或運作量能不足：針對建置商所開發之系統及預估使用量，本案依此確認儲存空間是否足夠，備份計畫是否合適，確認現階段無系統儲存、備份或運作量能不足之風險，並要求建置商需定期檢視系統運作量能，適時調整儲存及備份計畫。

4. 財務風險：

(1) 開發財務不足：於定期工作會議時，留意開發進度，並定期檢視建置商之核銷憑證，確認其投入開發資源情況。本項工作執行過程中無出現風險。

(2) 擴充或維護財務不足：於期中報告時，確認系統開發及維護(保固)情況，該系統目前皆以建置商服務建議書及契約要求執行，無額外擴充及維護財務投入。

(6) 促銷推廣所需財源無法支應：建置商與中華民國小客車租賃商業同業公會全國聯合會取得共識後，該項工作由全聯會協助執行，過程中已透過招開說明會、個別公會訪談等方式，使招募情況得以如期達到契約要求。

5. 營運風險：

(1) 平台數據接收遺失：請得標廠商提出資料備份機制，以確保數據儲存遺失。亦請廠商於營運期間，每日追蹤資料筆數及內容，若當日出現數據資料落差，應於指定期間完成修復。並要求將相關計畫撰寫成文件，由本案協助檢視，減少日後風險發生。

(2) 法源規範不足：請得標廠商就法律或規範面，於期中期間提出研究成果，並列出建議解決辦法。而對於受到較低法律位階之規定限制者，可優先討論修改或調整辦法，減少營運過程受到法令或規範限制之項目。建置商已透過召開專家學者座談會的方式，邀請相關單位進行與談，從中得出適用法規，避免產生適用法源不足之風險。

(3) 業者加入、退出衍生事務及成本：推廣期間當業者加入時，需造冊(或透過資料庫)並進行管理，定期確認業者營運是否面臨困難，避免業者逕行退出造成衍生退出之事務；加入業者意見及對系統的滿意度，可透過定期問卷於系統中請業者填答並反映，每季或是每半年詢問並統計，以對此進行改善，讓此風險發生機率降低。

6. 資安風險：

(1) 硬體或平台受損：請建置商提出資料備份機制，以確保數據儲存遺失，接著，硬體或平台需定期進行檢視或是掃毒作業，並留意作業平台重大安全更新，並進行系統或韌體升級，避免硬體受損或是中毒情形出現。並要求將相關計畫撰寫成文件，由本案協助檢視，且須在營運前取得資安規範認證，減少日後風險發生。

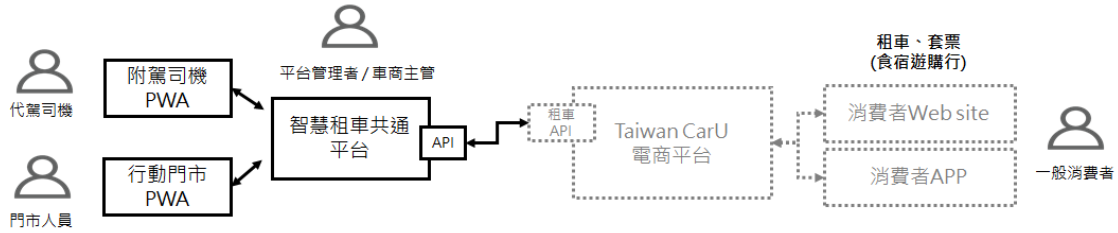
(2) 資料遭竊取或遭他人使用：儲存空間伺服器置放地點應進行人員管制，並定期進行掃毒及漏洞掃瞄作業，確保資料能妥善保存。此外，資料控管應具名，或做帳號管理，以確保資料不被他人使用並要求將相關計畫撰寫成文件，由本案協助檢視，減少日後風險發生。

其他不可抗力風險：由於小客車租賃數位平台建置目的主要係輔導小客車租賃業者數位轉型，且提高其商業應用，因此建置過程中不僅牽涉建置商、系統介接單位、專管單位等，尚牽涉小客車租賃業者及公會的參與及認同。建置初期確實發生建置商與全聯會之溝通落差，致使平台推廣進度無法順利推行，將此出現的風險，透過建置商與全聯會的多次溝通與居中協調、舉辦多次說明會等方式，已獲得解決。

3.2 系統測試與驗證

3.2.1 系統測試範圍

本計畫在執行初期係檢視及測試漢名科技所提供之「智慧租車共通平台」(即原資策會開發平台，漢名科技亦於簽約日 90 天內建置)，隨著計畫執行時的滾動式調整，漢名科技針對「智慧租車共通平台」進行系統優化與改版，提出一全新系統架構，以「新智慧租車平台」搭配「旅遊生態系平台」來提供更完善的服務，系統架構圖，請參閱圖 3.2.1。因此，在期中報告前，主要檢視與測試「智慧租車共通平台」，而在期末報告改為以滿足小客車租賃功能為主的「新智慧租車平台」與「旅遊生態系平台(亦可稱為 Taiwan CarU 電商平台，簡稱 CarU 平台)」部分功能(兩平台後簡稱新智慧租車平台)。



（資料來源：漢名_新智慧租車平台_設計規格書）

圖 3.2.1 智慧租車共通平台整合旅遊生態系平台整體架構圖

3.2.1.1 智慧租車共通平台

依據漢名科技於簽約日 90 天內所建置之「智慧租車共通平台系統」，整體程式可以區分為以下結構，如下表 3.2-1 所示。整個系統網站皆為 Web Service，可分為前台與後台，前台部分經手機 App 程式透過 Webview 方式包裝成為手機端應用程式，包含消費者、車商與駕駛，其服務架構都在同一個伺服器上，透過網頁的不同服務類型(即 URL)來進行區別；後台部分為營運團隊與租賃業者可登入的網站，主要為智慧租車共通平台，用於車輛、訂單管理等功能。

表 3.2-1 智慧租車共通平台系統-服務端定義、名稱與網址對照表

服務端定義	平台名稱	網址
前台-SmartRental	智慧租車應用服務(消費者)	https://dealer.caru.com.tw/web/
前台-SmartRental	智慧租車應用服務(車商)	https://dealer.caru.com.tw/store/
前台-SmartRental	智慧租車應用服務(駕駛)	https://dealer.caru.com.tw/drive/
後台-SmartRentalServer	智慧租車共通平台	https://dealer.caru.com.tw:8086

(資料來源：本計畫自行整理)

針對「90 天交付系統相關文件-系統彙整報告附件」進行資料的檢視，除了檢視合理性外，亦會評估資料是否有缺失，為靜態驗證階段。透過文件的審查與確認判斷系統是否有無缺失(Defects)，並初步評估系統是否適用於運作環境(Operational situation)。經檢視漢名科技於 7 月 16 日所提交的資料檔案，共有 15 個檔案，羅列如下：

1. 設計規格書_v3.docx
2. 設計規格書_附件_v1.docx
3. 設計規格書-M3 擴充_v3.docx
4. 使用手冊-平台_v1.docx
5. 使用手冊-平台 M3_v1.docx
6. 使用手冊-使用者 APP_v1.doc
7. 使用手冊-車商及駕駛 APP_v1.doc
8. 壓力負載測試成果報告_v3.docx
9. 資安檢測-前台-SmartRental_Issues.pdf
10. 資安檢測-前台-SmartRental_Overview.pdf
11. 資安檢測-後台-SmartRentalServer_Issues_0702.pdf
12. 資安檢測-後台-SmartRentalServer_Measures_0702.pdf
13. 資安檢測-後台-SmartRentalServer_Overview_0702.pdf
14. 資安檢測_OWASP ZAP_0626.html
15. 架設平台說明書_v1.docx

其中文件編號 1~3 為系統設計規格書，因系統功能範圍為先前資策會團隊所規劃設計，因此未進行修正；文件編號 4~7 為使用手冊，其中文件編號 4，內文引用到錯誤的編號(i.e., 章節 5)，文件編號 6 跟 7 均為使用手冊，惟內文前段提到運行環境與安裝程序，最後才是軟體的操作流程與畫面，文件目標可能非一般

使用者,建議漢名科技將安裝相關流程移至文件編號 15 併同架設資料一起說明。文件編號 8~14 為系統壓力檢測相關流程與資安檢測資料，相關描述細節請見 3.2.2.1 節。

以上歸納目前所取得之相關資料，漢名科技在取得智慧租車共通平台並完成初步系統上架後，依循前開發團隊的相關經驗，自主執行相關測試，後續將由本所檢視其資料合理性與正確性，另針對後續新增之金流功能，亦於 3.2.2.1 節中詳細說明相關檢測結果。

3.2.1.2 新智慧租車平台

依據漢名科技所提出之新智慧租車平台，整體架構如表 3.2-2 所示。系統以 Web Service 為主，可分為前台(使用者端)與後台(管理者端)，前台部分經手機瀏覽器以漸進式網路應用程式(Progressive Web Apps, PWA)架構提供服務，包含消費者(APP 於第二年提供)、行動門市(即車商)與附駕司機，其整體服務架構由兩個系統平台協助進行，透過 API 來進行資料的傳遞與整合；後台部分為營運團隊與租賃業者可登入的網站，主要測試以新智慧租車平台進行小客車租賃的服務流程，從車商建立、服務站點與車輛上架等管理面操作，到消費者透過 CarU 平台進行租車，下訂後經由測試金流交易，並完成取車跟核銷之相關流程。

表 3.2-2 新智慧租車平台-服務端定義、名稱與網址對照表

服務端定義	平台名稱	網址
新智慧租車 後台	新智慧租車平台 (車商管理頁面)	https://dealer2.caru.com.tw/administrator/
新智慧租車 前台(PWA)	新智慧租車平台 (行動門市)	https://store.caru.com.tw/
新智慧租車 前台(PWA)	新智慧租車平台 (附駕司機)	https://driver.caru.com.tw/
CarU 後台	旅遊生態系平台 (管理頁面)	https://test-caru.welcometw.com/admin
CarU 前台(PWA)	旅遊生態系平台 (消費者)	https://test-caru.welcometw.com

(資料來源：本計畫自行整理)

於 11 月 15 號陸續收到漢名科技所提供之新智慧租車平台與 CarU 平台文件，羅列如下：

新智慧租車平台文件, 2021-11-15

1. 漢名平台_需求規格書_20211114.docx
2. 漢名平台_設計規格書（補 M3）_20211116.docx
3. 漢名平台_API 規格書_20211114.docx
4. 漢名平台_測試計畫書_20211114.docx
5. 漢名平台_使用手冊_20211114.docx

旅遊生態系平台文件, 2021-11-22

1. CarU 測試計畫書及測試成果_v1.docx
2. CarU 系統安裝說明_v1.doc
3. CarU 前台使用手冊_v1.doc
4. CarU 後台使用手冊_v1.docx
5. CarU 需求規格書_v1.docx
6. CarU 設計規格書_v1.docx
7. CarU 系統功能情境測試腳本_v1118.xlsx

根據上述文件內容，初步提供相關改善建議如下：

關於需求規格書的部分：

1. 新智慧租車平台文件缺乏第一年執行改版之相關論述，即與資策會功能差異之對照表，而 CarU 平台文件則建議相關功能需求可以引用訪談相關成果來說明為何新增或更動相關功能，以便完善說明需求規格訂定方式。
2. 兩個平台間之使用者與操作角色建議要定義好並說明清楚，還有系統架構部分，目前新智慧租車平台若無搭配 CarU 平台，是無法 work，應在需求說明書上註明其偶合關係。
3. 通常需求規格書上會定義使用者端與管理端的作業流程，目前 CarU 平台有使用者端的描述，但是沒有管理端的說明(如資料上架、報表跟相關核銷資料下載等)，請補充。

關於設計規格書的部分：

1. 建議補充新智慧租車平台與 CarU 平台之資料庫 ER-model 關聯圖。
2. CarU 平台文件缺少系統架構的描述說明(可以跟新智慧租車平台重疊說明，但是文件單一性應該不能少，或是兩系統整合成一份文件)。
3. 新智慧租車平台跟 CarU 平台缺少使用者介面設計說明(小客車部分只有首頁截圖)。

4. CarU 平台針對 API 部分缺乏與新智慧租車平台互動的內容，並且缺少執行方式的描述(如 URL, POST or GET 等)，目前僅有系統使用的 4 隻 API，未來隨著系統的擴充理應持續新增。
5. CarU 平台系統流程第二張圖有異常，無法正常閱讀。
6. 建議兩個系統平台都要提供 user flow 的相關定義(例如不同使用者角色定義於系統平台的 use case，操作功能與相對應軟體)、另外針對系統平台的設計方法與工具應給予初步描述(如使用什麼語言，前後端軟體、資料庫軟體/版本等)、相關報表設計、例外處理(操作異常的描述等)、資訊安全基本考量描述。

關於測試計畫書的部分：

建議應針對需求規格書或設計規格書裡面提到的功能進行測試，並補充說明測試的操作情境跟軟體平台，以及測試成功跟測試失敗的相關基準描述。

於 11 月 15 日取得上開相關文件後，已於 11 月 19 日及 11 月 23 日與漢名科技進行系統驗測討論，並提供文件與系統修正意見與建議，預計於 11 月 30 日取得漢名科技提供之相關修正內容後，執行系統測試與驗證，而目前將先針對未來驗測流程與驗測重點，於 3.2.2 節中進行說明。

於 12 月 1 日取得漢名科技新上傳的文件，畫面如圖 3.2.2 所示，其目錄檔案清單羅列如下：

圖 3.2.2 漢名 1201 所提交之文件清單

Car U 平台目錄：

1.CarU 測試計畫書及測試成果_v2.docx

2.CarU 系統安裝說明_v2.doc

3.CarU 前台使用手冊_v2.doc
4.CarU 後台使用手冊_v2.docx
5.CarU 需求規格書_v2.docx
6.CarU 設計規格書_v2.docx

新智慧租車平台文件：

1.漢名平台_需求規格書_20211201.docx
2.漢名平台_設計規格書_20211201.docx
3.漢名平台_API 規格書_20211201.docx
4.漢名平台_測試計畫書_20211201.docx
5.漢名平台_使用手冊_20211201.docx

資安文件：

1.CarU_gv3hql.pdf (網站弱點掃描結果，使用 nessus，掃描時間為 2021/11/02)
2.Cay U 壓力測試.docx (使用 loader 進行壓力測試，測試時間為 2021/10/29)
3.資安維護 SLA.docx (資安相關維運規劃描述)

經檢視後，Car U 平台目錄所提供的檔案內容與 11 月 22 日所提供的內容相同(經 word 比對功能、字數、頁數及檔案大小判斷)；新智慧租車平台文件除了「3.漢名平台_API 規格書_20211201.docx」跟「5.漢名平台_使用手冊_20211201.docx」有進行格式調整之外，其餘內容也與上一期相同。針對資安文件部分，網站弱點掃描的內容並無問題，惟測試時使用的軟體版本較舊，離提供測試的軟體版本可能有一段距離(撰寫此文件的描述為 12 月 2 號)；而且測試標的只有針對 CarU，並未針對新智慧租車平台進行測試，本所另外使用工具產生一次完整的掃描結果。壓力測試文件除了有類似問題，針對文件的內容提供僅有一頁，對於測試的細節與標的(URL)並沒有相關說明。建議建置商可以讓報告更臻完整，以增加文件的參考價值。

3.2.2 系統測試與認證

3.2.2.1 智慧租車共通平台

漢名科技於系統測試時，所使用的軟體工具如表 3.2-3，均是採用相當知名的工具，但未說明為何選擇此工具與系統，因此，本所於 110 年 7 月 5 日詢問漢名科技上開問題，於 7 月 16 日漢名科技回覆將納入「以智慧租車共通平台推動小

客車租賃業數位轉型說明書」;於期中報告撰寫前尚未拿到說明書，因此尚不清楚如何讓車商或使用者初步了解系統的操作流程。基於操作流程的初步了解，針對「平台及 app 上架資訊_0624.pptx」所提供的資訊進行簡易功能性測試。

表 3.2-3 測試所需軟體工具

軟體名稱	版本	目的
JMeter	5.3	壓力及穩定性測試工具軟體
Apache ab	2.4.43	壓力及穩定性測試工具軟體
SonarQube	8.7	資安檢測軟體
OWASP ZAP	2.10.0	資安檢測軟體

(資料來源：漢名-智慧租車共通平台測試成果報告書_v3)

1. 智慧租車共通平台簡易功能性測試意見回饋

針對平台 https://dealer.caru.com.tw:8086/, 使用者在密碼輸入錯誤後，無正常回饋，經回報漢名科技後，再次測試，已可正常使用。

(1) 智慧租車共通平台：

在特定操作下可能產生異常行為，如下圖 3.2.3 顯示，點選後無正確的回饋(假設系統找不到圖片，可以顯示其它資訊替代進行操作回饋)。

圖 3.2.3 智慧租車共通平台-點選圖片後無法正常檢視圖片

(2) 智慧租車應用服務(消費者)：

修改會員資訊時，無法成功修改相關資料，顯示的資訊沒有正確的資訊回饋，如圖 3.2.4 顯示；透過手機 APP 操作結果一致。

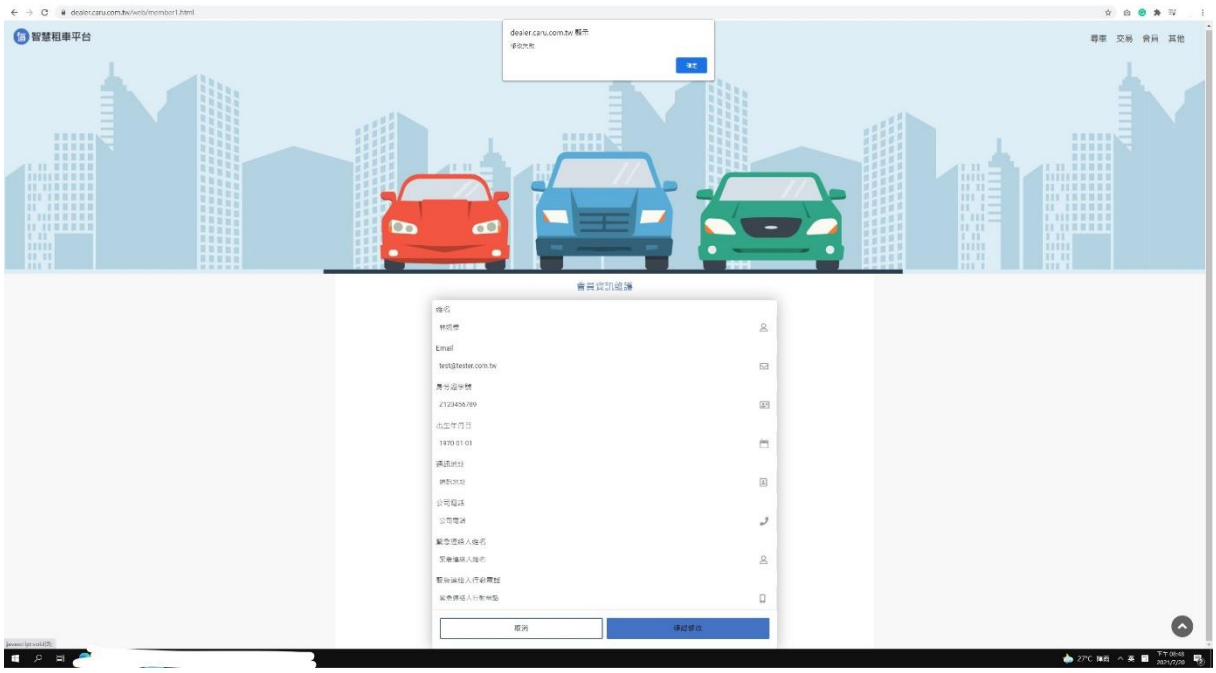


圖 3.2.4 智慧租車應用服務(消費者)-無法修改會員資料

在修改會員資訊時，其設定頁面有兩個變更密碼，為「交易密碼」、「會員帳號密碼」，如圖 3.2.5 顯示，建議兩個按鈕之文字說明或圖示，應有差異；此畫面在手機 APP 中顯示正常。

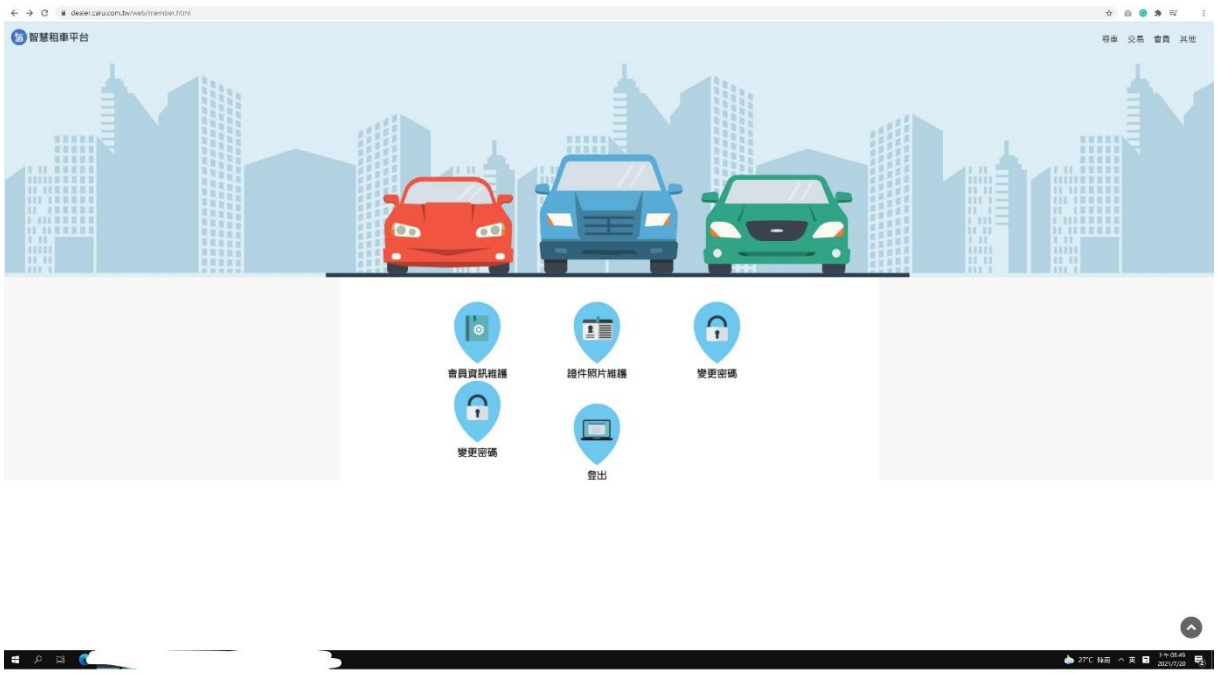


圖 3.2.5 智慧租車應用服務(消費者)-設定資訊有兩個變更密碼

在修改會員資訊時，其交易資訊的圖片顯示異常，如圖 3.2.6 顯示，建議於正式服務上線前應進行修正；此頁面在手機 APP 中一樣為異常顯示。

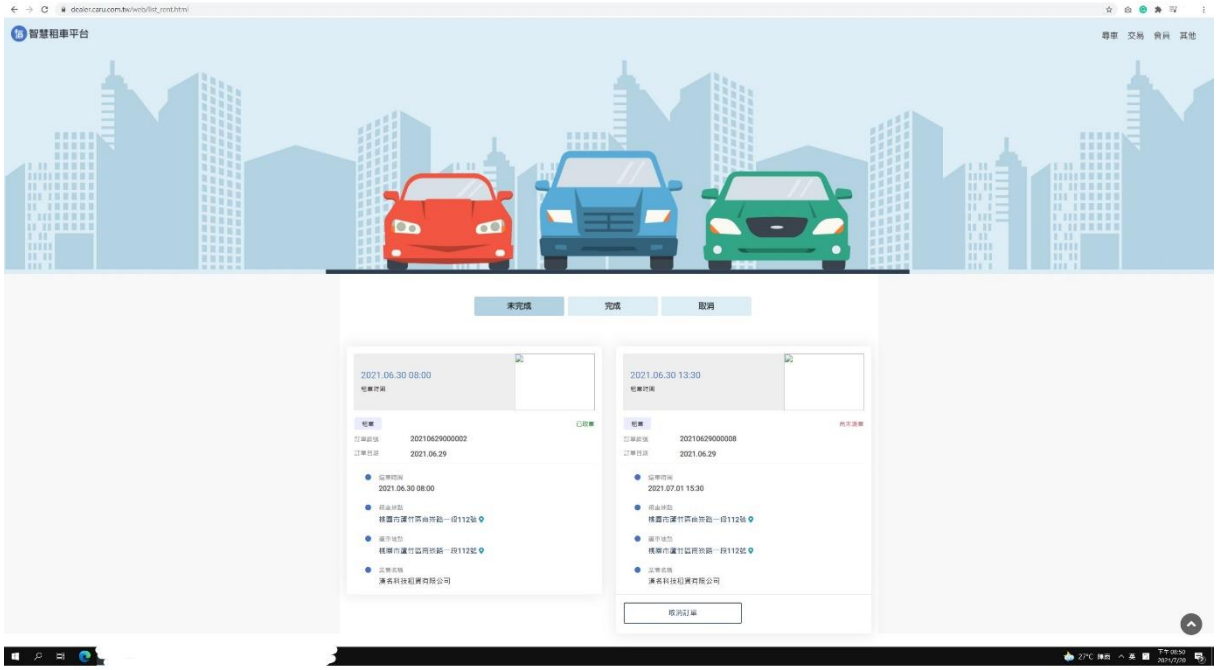


圖 3.2.6 智慧租車應用服務(消費者)-交易資訊圖片無法正常顯示

(3) 智慧租車應用服務(車商)：

於頁面切換時，約有 0.5 秒鐘，查無資料顯示；在手機 APP 端亦同。

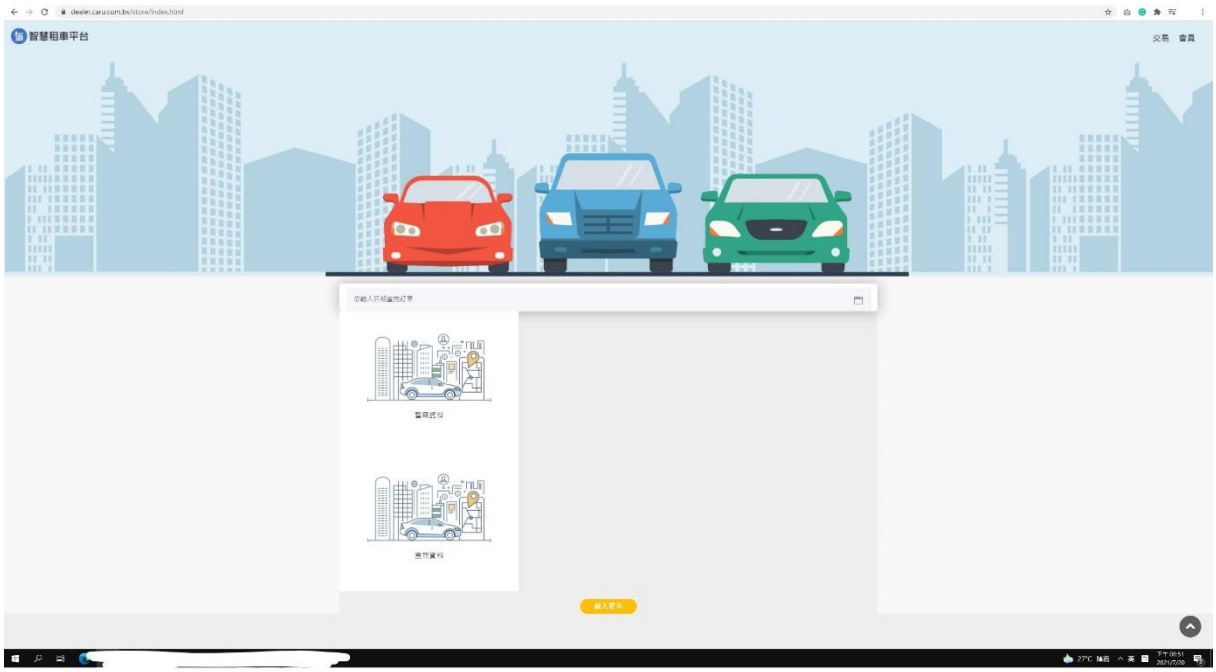


圖 3.2.7 智慧租車應用服務(車商)-交易資訊圖片無法正常顯示

(4) 智慧租車應用服務(駕駛)：

經測試，駕駛端的操作頁面也跟車商有一樣的問題，會有不正常的圖片顯示行為。

2. 智慧租車共通平台測試成果報告意見回饋

(1) 資訊安全相關議題：

報告書中的 SonarQube 測試結果係以截圖方式呈現，但圖片資訊上面沒有相對應的 Project name 跟時間，建議要比照附件資料的呈現方式，於上方顯示 Project name 跟相對應的掃描時間，這樣提供的資訊才具效力。

另一方面，目前 SonarQube 的相關資料沒有看到完整版的 report，易讓人質疑報告的產出方式是否符合標準流程。例如：附件資料「10.資安檢測-前台-SmartRental_Overview.pdf」所產生的數據結果皆為 A，且 Coverage 跟 Duplications 皆為 0%，未找到相關問題，屬於相當罕見之數據結果，但非關鍵因子，應該比照附件資料「13.資安檢測-後台-SmartRentalServer_Overview_0702.pdf」，建議漢名科技再確認是否確實執行掃描。最後，SonarQube 於掃描後，應該可以輸出完整報告，請漢名科技一併提供完整報告，以示資料正確性。

OWASP ZAP 資料呈現無問題，另透過 ZAP 快速掃描標的平台，獲得 Cross-Domain Misconfiguration 等問題的回報(其中前台部分因使用同一架構，所以都有一樣的問題產生，僅列出 web 部分，而 store 與 driver 忽略不顯示)，請參閱圖 3.2.8~圖 3.2.10(詳細內容可以檢視附件電子檔)，請漢名科技檢視是否因平台開發，導致新問題產生，完成的掃描結果已提供本所參考。

ZAP Scanning Report

Summary of Alerts

Generated on 週二, 20 7月 2021 14:39:11

Risk Level	Number of Alerts
High	0
Medium	1
Low	0
Informational	3

Alerts

Name	Risk Level	Number of Instances
Cross-Domain Misconfiguration	Medium	1
Information Disclosure - Suspicious Comments	Informational	2
Timestamp Disclosure - Unix	Informational	373

Alert Detail

Medium (Medium)	Cross-Domain Misconfiguration
Description	Web browser data loading may be possible, due to a Cross Origin Resource Sharing (CORS) misconfiguration on the web server
URL	https://cdnjs.cloudflare.com/ajax/libs/leaflet/1.0.3/leaflet.css
Method	GET
Evidence	Access-Control-Allow-Origin: *
Instances	1
Solution	Ensure that sensitive data is not available in an unauthenticated manner (using IP address white-listing, for instance). Configure the "Access-Control-Allow-Origin" HTTP header to a more restrictive set of domains, or remove all CORS headers entirely, to allow the web browser to enforce the Same Origin Policy (SOP) in a more restrictive manner.
Other information	The CORS misconfiguration on the web server permits cross-domain read requests from arbitrary third party domains, using unauthenticated APIs on this domain. Web browser implementations do not permit arbitrary third parties to read the response from authenticated APIs, however. This reduces the risk somewhat. This misconfiguration could be used by an attacker to access data that is available in an unauthenticated manner, but which uses some other form of security, such as IP address white-listing.
Reference	http://www.hpenterprisesecurity.com/vulncat/en/vulncat/vb/html5_overly_permissive_cors_policy.html
CWE Id	264
WASC Id	14
Source ID	3
Informational (Low)	**Information Disclosure - Suspicious Comments**

圖 3.2.8 ZAP Scanning Report-後台片段截圖

ZAP Scanning Report

Summary of Alerts

Generated on 週二, 20 7月 2021 20:37:05

Risk Level	Number of Alerts
High	0
Medium	4
Low	4
Informational	3

Alerts

Name	Risk Level	Number of Instances
Cross-Domain Misconfiguration	Medium	3
Vulnerable JS Library	Medium	1
X-Frame-Options Header Not Set	Medium	16
Absence of Anti-CSRF Tokens	Low	18
Cross-Domain JavaScript Source File Inclusion	Low	16
Incomplete or No Cache-control Header Set	Low	16
X-Content-Type-Options Header Missing	Low	91
Information Disclosure - Sensitive Information in URL	Informational	13
Information Disclosure - Suspicious Comments	Informational	37
Timestamp Disclosure - Unix	Informational	333

Alert Detail

Medium (Medium)	Cross-Domain Misconfiguration
Description	Web browser data loading may be possible, due to a Cross Origin Resource Sharing (CORS) misconfiguration on the web server
URL	https://cdnjs.cloudflare.com/ajax/libs/hover.css/2.3.1/css/hover-min.css
Method	GET
Evidence	Access-Control-Allow-Origin: *
URL	https://cdnjs.cloudflare.com/ajax/libs/font-awesome/5.11.2/css/all.min.css
Method	GET
Evidence	Access-Control-Allow-Origin: *
Instances	2

圖 3.2.9 ZAP Scanning Report-前台片段截圖-part 1

Medium (Medium)	Vulnerable JS Library
Description	The identified library jquery, version 3.3.1 is vulnerable.
URL	https://dealer.caru.com.tw/web/js/m/common.js
Method	GET
Evidence	/*! jQuery v3.3.1
Instances	1
Solution	Please upgrade to the latest version of jquery.
Other information	CVE-2020-11023 CVE-2020-11022 CVE-2019-11358
Reference	https://blog.jquery.com/2019/04/10/jquery-3-4-0-released/ https://nvd.nist.gov/vuln/detail/CVE-2019-11358 https://github.com/jquery/jquery/commit/753d591aea698e57d6db58c9f722cd0808619b1b https://blog.jquery.com/2020/04/10/jquery-3-5-0-released/
CWE Id	829
Source ID	3

Medium (Medium)	X-Frame-Options Header Not Set
Description	X-Frame-Options header is not included in the HTTP response to protect against 'ClickJacking' attacks.
URL	https://dealer.caru.com.tw/web/register.html?agree=on&idno=ZAP&name=ZAP&password=ZAP&password_again=ZAP&txpwd=ZAP&txpwd_again=ZAP&userName=1
Method	GET
Parameter	X-Frame-Options
URL	https://dealer.caru.com.tw/web/index.html
Method	GET
Parameter	X-Frame-Options
URL	https://dealer.caru.com.tw/web/other_policy.html
Method	GET
Parameter	X-Frame-Options
URL	https://dealer.caru.com.tw/web/register.html?verifyCode=ZAP
Method	GET
Parameter	X-Frame-Options
URL	https://dealer.caru.com.tw/web/login.html
Method	GET
Parameter	X-Frame-Options

圖 3.2.10 ZAP Scanning Report-前台片段截圖-part 2

(2) 壓力測試相關議題：

報告書提到「VV03 測試異常紀錄表」，雖然報告書都是測試通過，建議在附件還是提供該表格，讓資料呈現更完整。

針對測試編號 SCR020 建議提供不同測試腳本，目前有比較 heavy traffic 的情境(2000 個連線做 200 萬次連線，其結果平均為每秒 106 個連線處理、其平均每條連線需 9.4 秒)，所得數據可得知服務處理時間已經超過一般人預期的等待時間。但是這樣的情境在真實世界中是很低的機率才會發生，因此建議加入 light traffic 跟 middle traffice 的測試情境，例如 500 個連線、1000 個連線。

針對測試編號 SCR021 的結果，截圖部分看不出設定上是否有「同時 200 個連線使用者」，建議書面資料的提供應與內文有一致性的對照，或是提供 Jmeter 的測試腳本，才能夠知悉 client 端的傳輸行為；另外描述上說「回應時間小於 3 sec」，但是測試的結果有 CarType/query 跟 Setting/query 兩個測試的平均秒數分別為 4.6 秒跟 4.5 秒，其論述不符合結果，建議調整報告內容的說明；再者，CarType 的 query 會受到資料庫的車種資料筆數影響，換言之，車種資料越多，有可能 query 會越慢(可透過軟體調教或是改變設計等方式做改善)，建議在測試的時候要適當說明一下平台目前車總資料量，如果因為數量的持續上升導致 qeury 時間拉長，可能要評估實際上線後使用者是否能夠在每次 query 時等待這麼長的時間。

針對測試編號 SCR022 部分，同上建議，建議漢名科技可以提供設定頁面的佐證資訊。另外 Users/login 的數據其結果皆為 6ms，從個人電腦到 AWS 的主機端，考量資料傳輸的往返(Round Trip Time, RTT 時間)，在模擬「10 個平台商及 1000 個車商連線」連下，這個數字不太可能為一個定值，建議補充說明測試的網路環境(說明 client/server 的位置，或是提供 ping/traceroute 的截圖)。

針對測試編號 SCR023 部分，同 SCR021 建議實施方式。其中「低於 2sec 即為最佳使用者上線人數」的描述應註明為 500 人的情境。看數據結果於 500 人的時候其 CarType/query, Station/query 的平均秒數皆已經接近 2 秒，倘若站點數量一多，跟使用者人數高於 500，其平均反應時間勢必超過 2 秒。

3. 智慧租車共通平台金流串接功能測試意見回饋

本小節測試執行時間為 9 月 23 日至 9 月 27 日，因手機版 APP 阻擋截圖功能，所以相關操作以網頁版平台 https://dealer.caru.com.tw/web/為主，其相關顯示上只有螢幕大小跟排版(RWD)的差異，其內容一致。

首先輸入測試帳號後，選定測試資料「桃園、蘆竹區、不使用甲租乙還」以進行訂單確認，對金流串接的相關功能結果做檢測與確認。相關測試細項與回饋如下：

(1) 正常操作流程的測試過程與結果

步驟一：輸入訂單測試資料，輸入完成後點選「搜尋」按鈕。

圖 3.2.11 金流測試截圖-輸入訂單測試資料

步驟二：選定租用車輛，以 TOYOTAVIOS 1.5 為測試標的，點選「租車」按鈕。

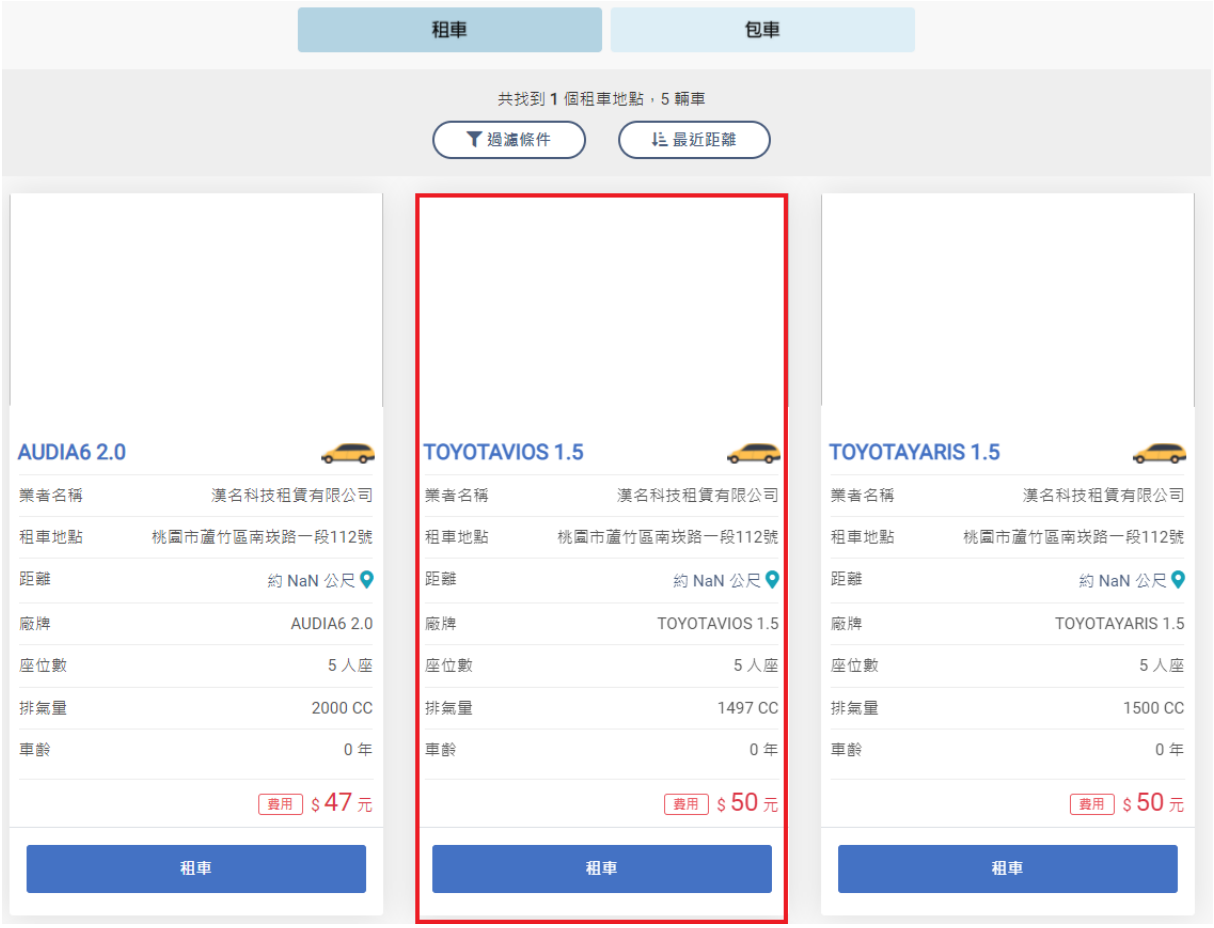


圖 3.2.12 金流測試截圖-選擇租用車輛

步驟三：確認預約車輛，點選「進行付款」按鈕。

圖 3.2.13 金流測試截圖-確認預約車輛

步驟四：頁面跳轉前的等待頁面。

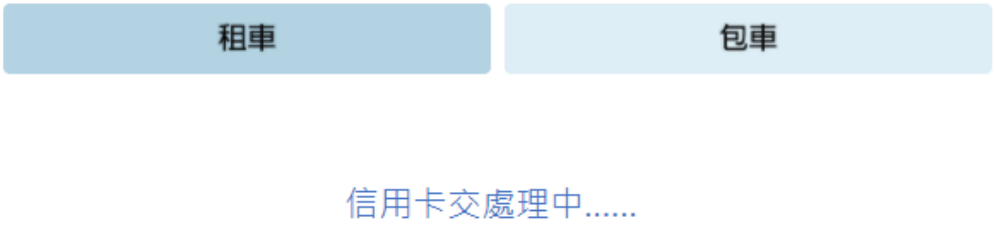


圖 3.2.14 金流測試截圖-金流頁面跳轉前頁

步驟五：確認訂單資訊後輸入付款方式。

圖 3.2.15 金流測試截圖-付款方式輸入頁

步驟六：點選相關確認訊息，測試頁面溫馨提醒「關閉」按鈕與信用卡交易「確定」按鈕。

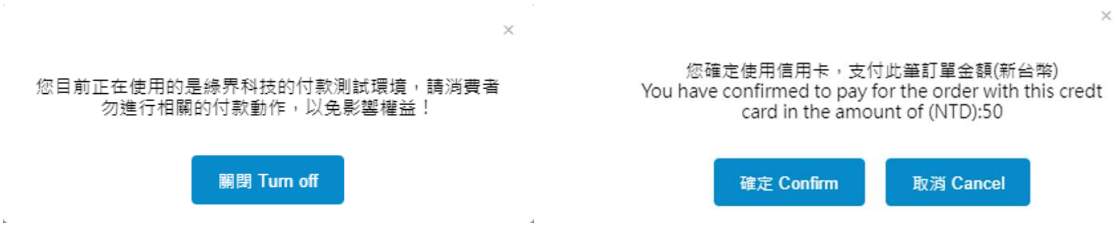


圖 3.2.16 金流測試截圖-填寫完付款方式後的確認訊息框

步驟七：一次性密碼(OTP)簡訊驗證的輸入畫面，根據使用者填入的手機門號，會收到相對應的驗證碼。

圖 3.2.17 金流測試截圖-OPT 簡訊驗證碼輸入頁面

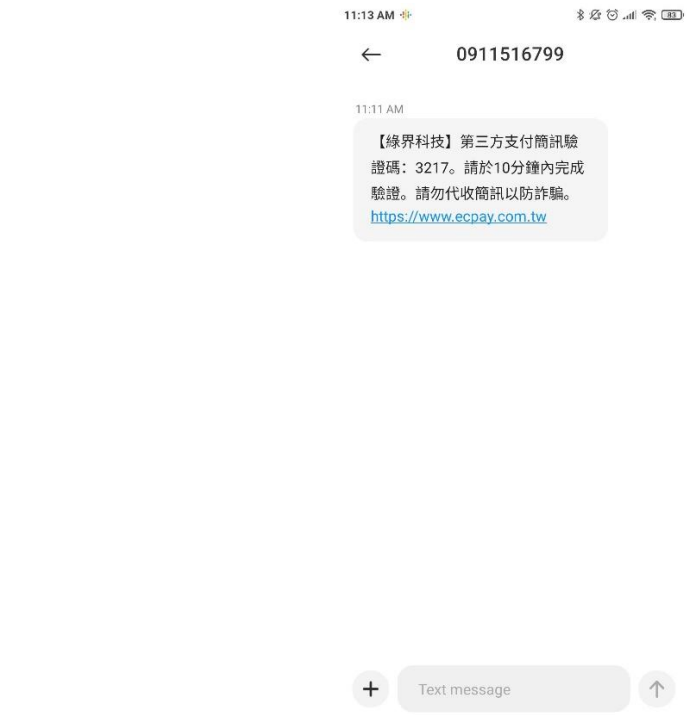


圖 3.2.18 金流測試截圖-OPT 簡訊驗證碼接收結果

步驟八：輸入接收到的 OTP 簡訊驗證碼後，繼續進行交易。

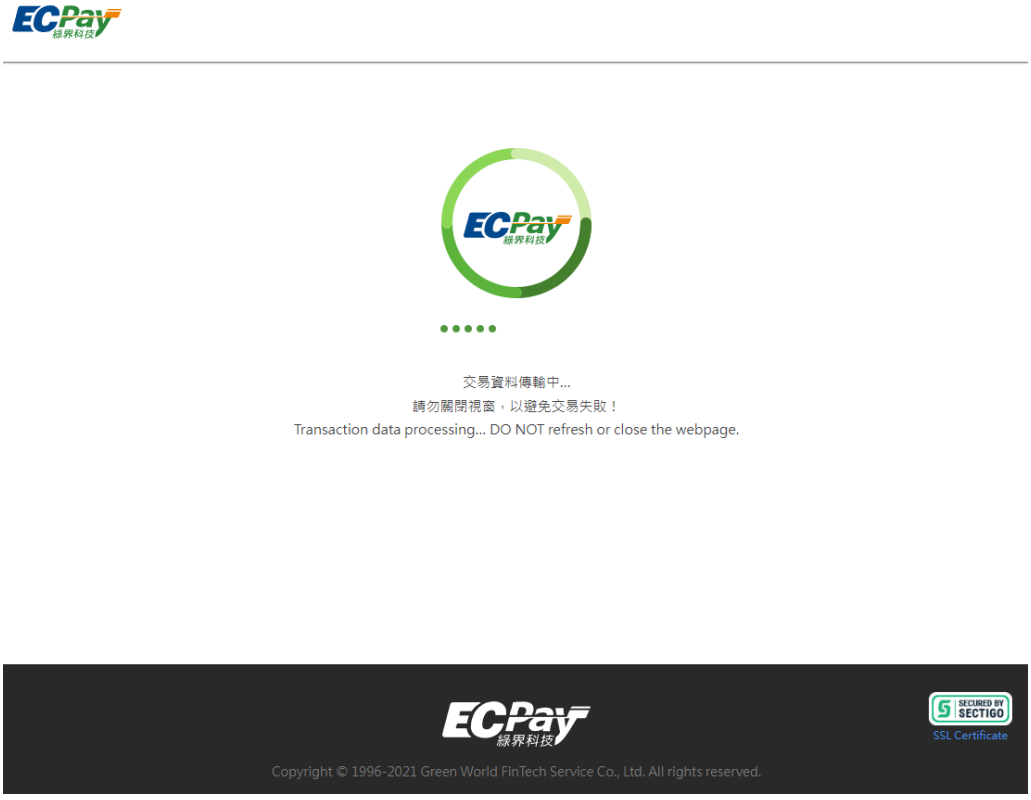


圖 3.2.19 金流測試截圖-交易資料傳輸頁面

步驟九：交易完成後，會看到交易完成的頁面，即可點選「返回商店」按鈕。如果交易過程中有輸入 Email，會同步收到訊息。

圖 3.2.20 金流測試截圖-交易完成頁面(金流端)

圖 3.2.21 金流測試截圖-交易完成

步驟十：於交易完成後檢視交易詳細資料。

圖 3.2.22 金流測試截圖-交易完成頁面(使用者端)

步驟十一：檢視使用者端的交易查看頁面。

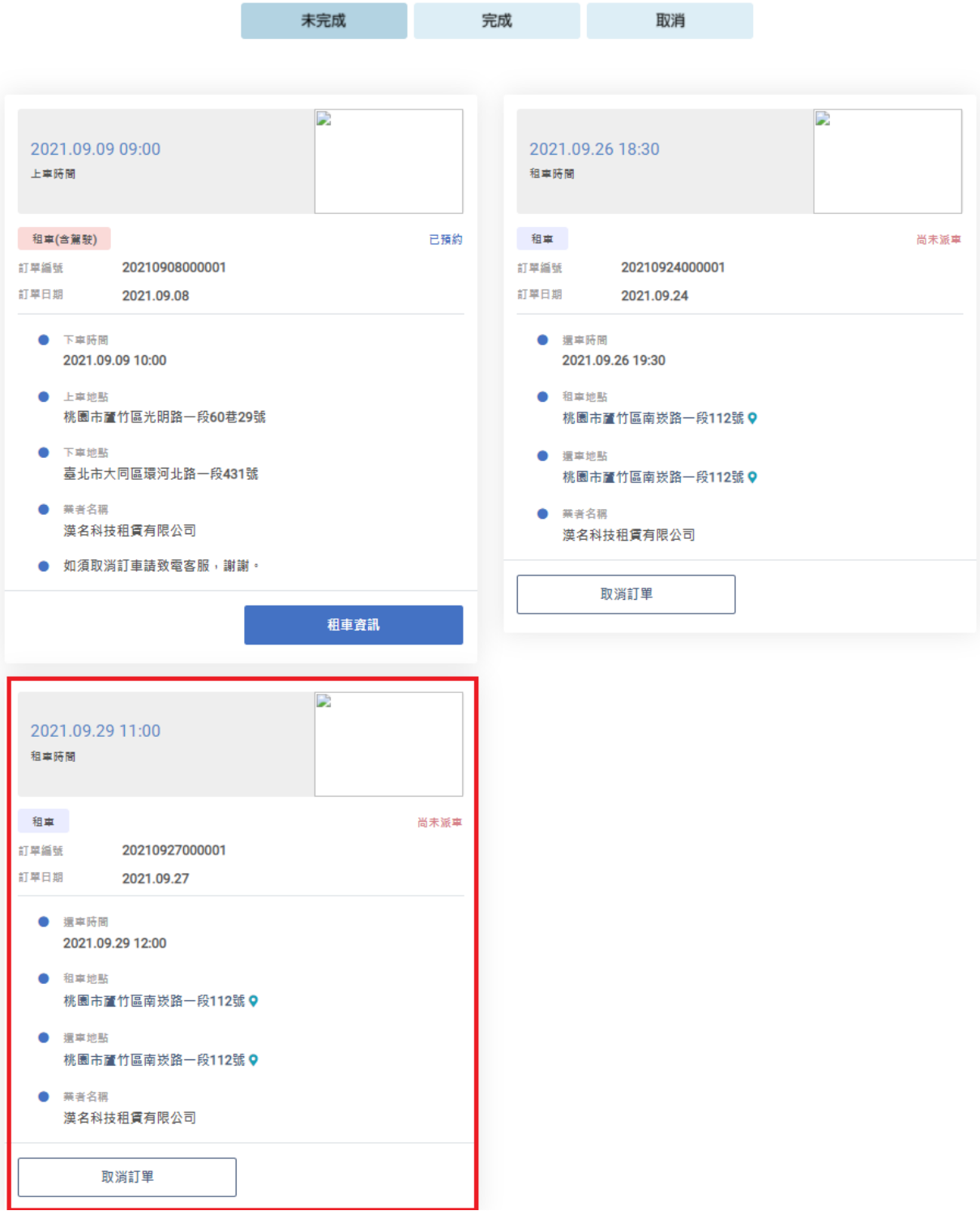


圖 3.2.23 金流測試截圖-交易查看頁面(使用者端)

步驟十二：檢視平台端的訂單管理頁面，檢視該筆交易。

圖 3.2.24 金流測試截圖-交易查看頁面(平台端)

步驟十三：測試交易取消功能，於使用者端上檢視同一筆交易後，點選「訂單取消」按鈕。

圖 3.2.25 金流測試截圖-交易訂單取消頁面(使用者端)

步驟十四：操作頁面有跳出提示，點選「確認取消」按鈕；點選後會看到彈出式視窗告知已經完成取消租車訂單。

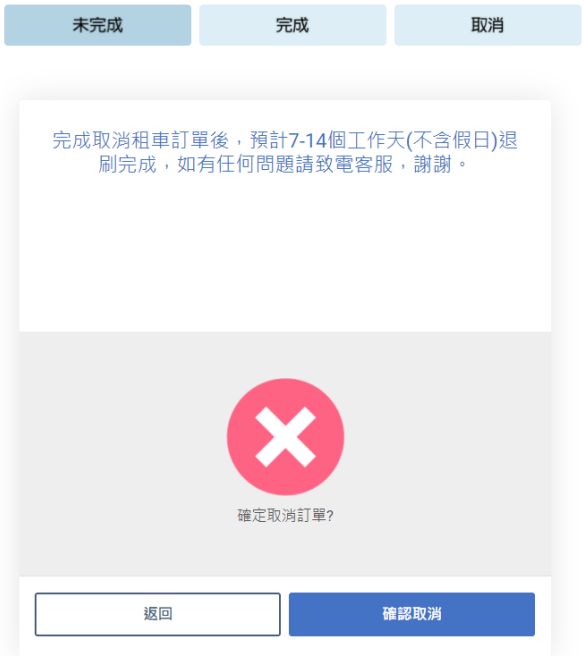


圖 3.2.26 金流測試截圖-交易訂單確認頁面(使用者端)

圖 3.2.27 金流測試截圖-交易訂單完成確認頁面(使用者端)

步驟十五：再次檢視平台該訂單，可以看到訂單取消的資料。

圖 3.2.28 金流測試截圖-交易訂單取消確認頁面(平台端)

經以上十五個步驟測試後，確認金流在基本操作情境下的相關測試功能均屬正常。

(2) 輸入錯誤資料操作流程的測試過程與結果

步驟一：比照先前的測試流程，輸入相關訂單資訊。

圖 3.2.29 金流測試截圖-測試訂單資料頁(使用者端)

步驟二:於信用卡輸入頁面輸入錯誤的資料,卡號:4311-9522-2222-3333、安全碼：333、有效期限輸入 11/22。

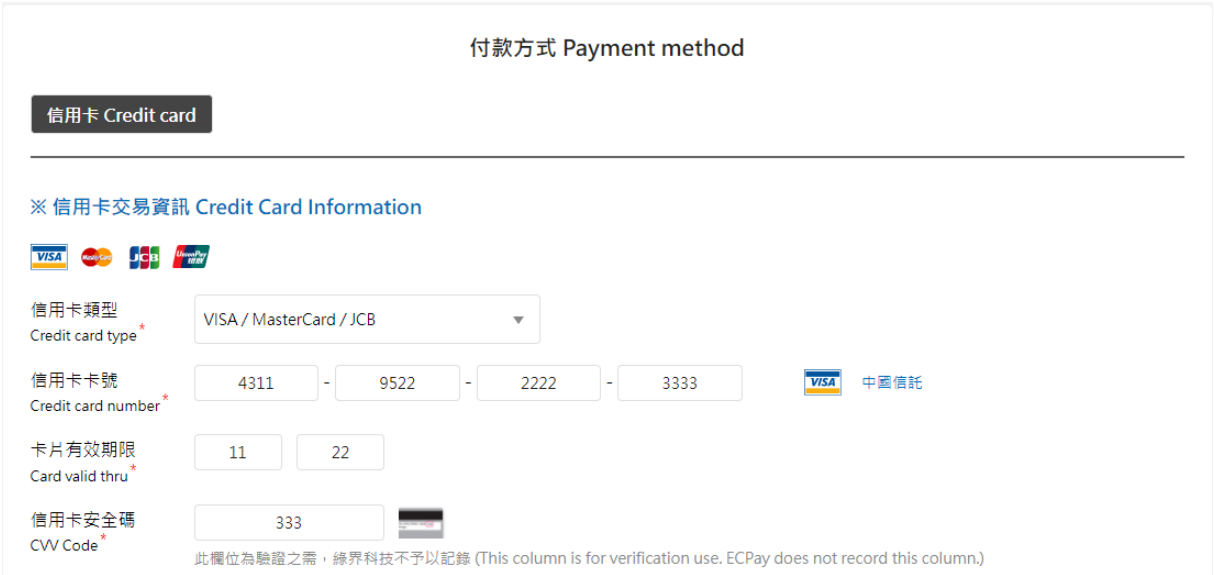


圖 3.2.30 金流測試截圖-輸入錯誤的卡號資訊測試交易(使用者端)

圖 3.2.31 金流測試截圖-交易失敗顯示資訊(綠界頁面)

步驟三：返回使用者的操作頁面(App)，即看到信用卡交易完成。後續再跳轉回訂單畫面，但卻非原訂單車輛，已變更為 VIOS 1.5 的車款。

圖 3.2.32 金流測試截圖-交易失敗顯示資訊(使用者端)

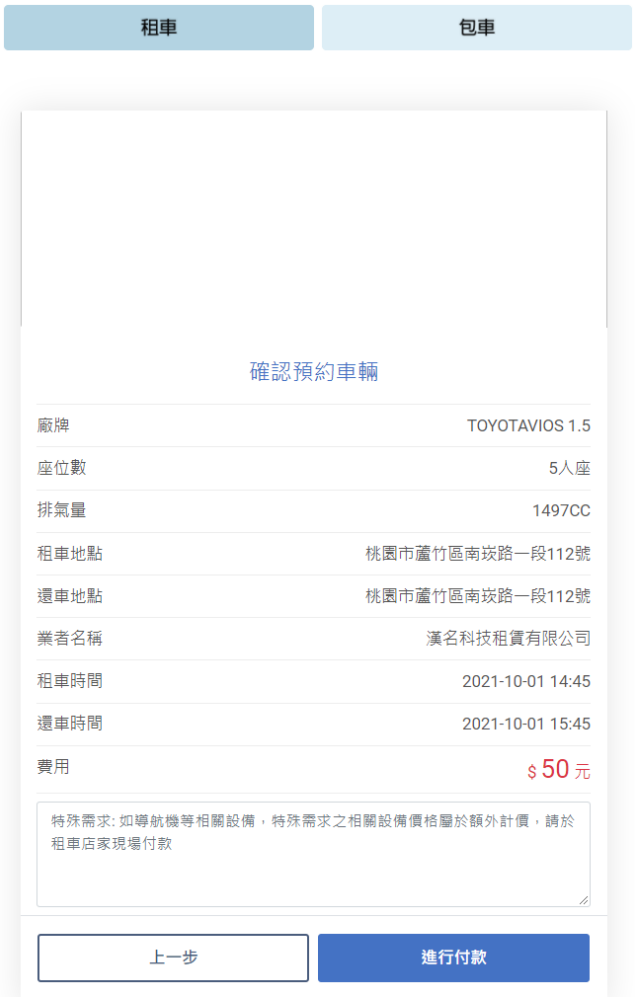


圖 3.2.33 金流測試截圖-交易失敗後顯示之訂單資訊(使用者端)

步驟四：檢視平台的交易資料，可以看到有刷卡失敗的相關記錄存在。

圖 3.2.34 金流測試截圖-交易記錄於平台端的顯示

經以上四步驟的測試後，功能與記錄均屬正常，惟步驟三的流程可能會誤導使用者的操作(圖 3.2.32 點選「上一步」會在跳回 “信用卡交易完成”的頁面，無限循環)，已於 9 月 28 日建議漢名科技進行修正。

3.2.2.2 新智慧租車平台

新智慧租車平台前端操作是以 PWA 為主，因此本計畫後續測試驗證會以功能性測試與驗證(包含系統內部 API 運作)、安全性驗證(軟體弱點偵測與常規資安基礎設定)、壓力測試(軟體基本負載測試)與易用性測試(使用者經驗易用性評估)為主。

測試標準皆需滿足完整性、安全性、可靠性、穩定性等面向，並視測試結果進行項目測試評估分數。平台測試評估分數根據如表 3.2-4 測試評估等級表。缺

失等級由 A 至 D，嚴重程度由高至低，其中缺失等級每高一級別皆包含或不包含上一級別之缺失。若測試中出現任意一次 A 級別將予以測試失敗。

表 3.2-4 測試評估缺失等級說明

等級	標準	測試標準說明	備註
A	重大缺失	功能項目無法運作 嚴重安全性漏洞	測試失敗 系統上線前建議完成修正
B	缺失	功能項與預期不符 安全性漏洞	需立即修正 建議安排適當時機修正
C	錯誤	文字描述易產生誤導，流程操作有高困難度	需改善操作，可安排適當時機修正
D	補強	錯別字、版面異常	可安排適當時機修正

1. 功能性測試與驗證

以實際租車情境流程的進行操作，根據設計規格書、使用手冊所提供的資料，執行相關功能的測試；針對新智慧租車平台所涵蓋的功能進行測試，例如車商管理、車商價格管理、內附項目管理、加購項目管理、站點管理、車輛管理、駕駛管理、員工管理、站點價格管理、上架管理、訂單管理、核銷作業(行動門市)、交車作業(行動門市)、結案作業(行動門市)、核銷作業(行動門市)、開始任務(附駕司機)與結束任務(附駕司機)；消費者端則是使用 CarU 的前台頁面進行車輛搜尋與下訂等交易作業，以滿足本案第一年小客車租賃相關運作需求。每個測試項目在整體測試流程執行下來，至少執行六次測試，部分測試項目在執行過程中遭遇問題導致無法順利進行，有先通報漢名科技進行修正，團隊待問題修正後有再次測試確認。

測試結果請參閱表 3.2-5~表 3.2-8，其中相關備註另提供佐證截圖於表格後逐一說明。**建議漢名科技於系統正式上線運作前，要把評比 A 跟 B 的項目進行修正。**

表 3.2-5 測試評估缺失等級表-平台與車商作業端

項目	成功	失敗	其他	備註
車商管理 (平台端)	✓			[T-C-01]

項目	成功	失敗	其他	備註
				新增車商帳號沒問題，但 email 欄位是強制輸入，有些車商可能沒有 email，建議可以讓該欄位留白。
營運統計表 (平台端)	✓			[T-C-02] 為所有資料的總和，但沒有相關時間資訊跟報表輸出功能。
站點管理	✓			[T-C-03] 新增相關操作沒問題，不過定位功能誤差很大，會影響到其他相關地圖資訊，建議修正，**評比為 C。** 其他操作 icon 跟儲存相同，建議修訂。 站點地圖功能點選「處理」後，操作顯示異常，但是處理功能可能非常規性功能，因此**評比為 D。** 說明按鍵的呈現內容不正確，建議修定，**評比為 D。**
車輛管理	✓			[T-C-04] 新增車輛的車牌、出廠年/月都無輸入格式的檢查，可接受任意長度的字元，怕後續會影響到 M3 的介接，建議修定，**評比為 C。** 針對資料刪除的系統回饋資訊，建議改成人類可讀的描述方式，如資料刪除成功，建議修定，**評比為 D。**
駕駛管理	✓			[T-C-05] 系統端不同車商之間的帳號設計為同一資料表，因此容易發生帳號已經存在的情境，在這個情境發生的時候，站點資料的選擇功能會無法正確顯示資料，因此建議改善，**評比為 C。** 另外，司機在車商的合作方式極可能為多站點彈性服務，但是目前系統功能司機只能配置於單一個站點，在配置上的彈性較差(等於不同服務站點要要多個帳號)。
員工管理	✓			[T-C-06] 跟駕駛管理有相同帳號問題，另外在密碼輸入欄位並非強制欄位，需修定，**評比為 B。**
車商價格管理	✓			[T-C-07] 在編輯功能可以編輯目前表單內沒有的車型，在操作流程跟設計上疑似有誤，建議釐清後安排修正，**評比為 D。**
站點價格管理			✓	[T-C-08] 此功能所呈現的資訊跟車商價格管理一樣，看不出其差異。

項目	成功	失敗	其他	備註
內附項目管理			✓	[T-C-09] 進行新增操作會顯示異常，需修正，**評比為 B。**
加購項目管理			✓	同內附項目管理的描述。
上架管理			✓	[T-C-10] 車輛上架過程中在特定操作下會遇到錯誤，而且操作過程中的系統處理時間很長(數十秒以上)，因此容易讓使用者誤以為系統異常，建議修正跟調整，**評比為 C。** 上架資料不會馬上顯示於 CarU 平台，而且也沒有相關系統回饋資訊可以檢視，如進度查詢、預期上架時間等，建議至少提供一些可檢視進度方式的資料，畢竟特定時間才會批次上架一次，以現今的系統作業時間來說，服務水準是比較慢的，**評比為 C。** 經團隊反覆測試後，某些情況下，車商上架的車種在 CarU 平台經消費者帳號搜尋比對後，數量會不一致，**評比為 A。此問題後續反應給漢名科技後，已完成修正。**
訂單管理			✓	[T-C-11] 訂單判斷與顯示邏輯疑似異常，訂單在取消的狀態，同時也列入租用車輛數的計數，需修正，**評比為 A。** 訂單的各種操作狀態沒有前後關係的檢查，因此可能會發生奇怪的操作組合導致無法有效的檢視訂單正確性，需修訂或改善，**評比為 B。**

表 3.2-6 測試評估缺失等級表-行動門市端

項目	成功	失敗	其他	備註
核銷作業			✓	核銷作業進行時，沒有檢查消費者端的訂單是否是屬於該門市，因為目前的系統架構是每一個門市都一組帳號，導致車商在多個門市之間要如果忘記做帳號切換，或是登入錯誤門市的帳號，就會發生資料流程的議題。需修正，**評比為 A。**
交車作業			✓	流程可順利操作完成，不過輸入的「實際交車車號」，並沒有跟管理平台端的派車進行功能整合上的綁定，需修正，**評比為 B。**
結案作業	✓			流程可順利操作完成，不過訂單上的結案時間有誤，需修正，**評比為 C。**

表 3.2-7 測試評估缺失等級表-附駕司機

項目	成功	失敗	其他	備註
開始任務			✓	問題同行動門市端的核銷描述，可以透過司機的帳號進行核銷作業，且核銷對象沒有檢查其合法性與正確性，後續運行時恐衍生諸多問題，需修正，**評比為 A。**
結束任務	✓			

表 3.2-8 測試評估缺失等級表-消費者端

項目	成功	失敗	其他	備註
登入	✓			[T-U-01] 測試過程中使用 Google 登入有異常，後續再次測試為正常。
車輛搜尋	✓			[T-U-02] 熱門租車資料較多時，建議限縮或以其他方式提供，以免造成資訊版面的誤用，建議修正，**評比為 D。**
購物車與購買		✓		[T-U-03] 購物車資訊於金流交易取消後會不見，呈現購物車為空的狀態，需修正，**評比為 B。** 當下如果有使用優惠券，優惠券也會消失，顯示為已使用，需修正，**評比為 A。**
金流交易			✓	[T-U-04] 購物車所帶的金額跟金流所顯示的金額不同，需修正，**評比為 A。** 金流頁面取消操作，平台端顯示訂單成立，需修正，**評比為 A。** **以上兩點於測試當下，即回報漢名科技，已完成問題修訂。**
檢視訂單			✓	[T-U-05] 下訂後結果檢視訂單為付款失敗，但是有收到交易成功資相關訊息，需修正，**評比為 A。這點於測試當下即回報漢名科技，已完成問題修訂。** 在使用者端有顯示圖片，不過在管理頁面端是空白的，需修正，**評比為 A。** 管理端如果取消訂單，使用者端狀態不會更新，需修正，**評比為 B。**
顯示 QRcode	✓			訂單完成後需等待 5 分鐘後才會顯示 QRcode，建議在交易狀態顯示進行調整；或是於訂單流

項目	成功	失敗	其他	備註
				程中進行提醒跟告知，以免造成消費者的誤會，建議修正，**評比為 C**。

(1) 實際測試相關功能畫面截圖：

針對上述缺失表格所描述，此小節提供對應畫面之截圖與描述。

[T-C-01] 車商管理：email 強制輸入

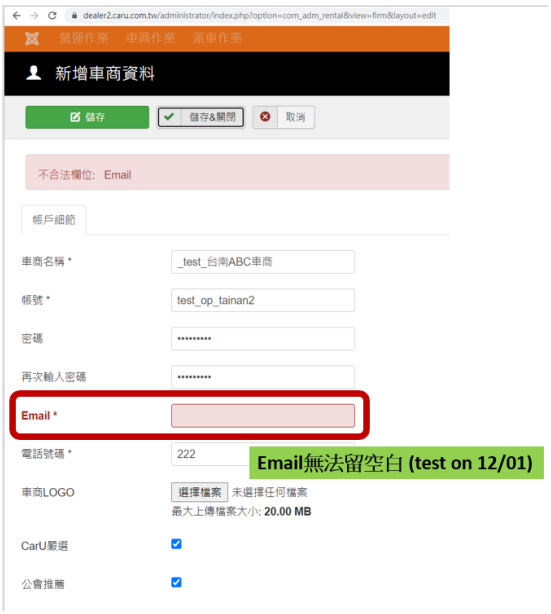


圖 3.2.35 [T-C-01] 車商管理-email 無法留白

[T-C-02] 營運統計表：無報表下載功能，無起訖時間可設定

圖 3.2.36 [T-C-02] 營運統計表-無報表下載功能

[T-C-03] 站點管理：定位異常、站點地圖「處理」、「說明」功能操作異常

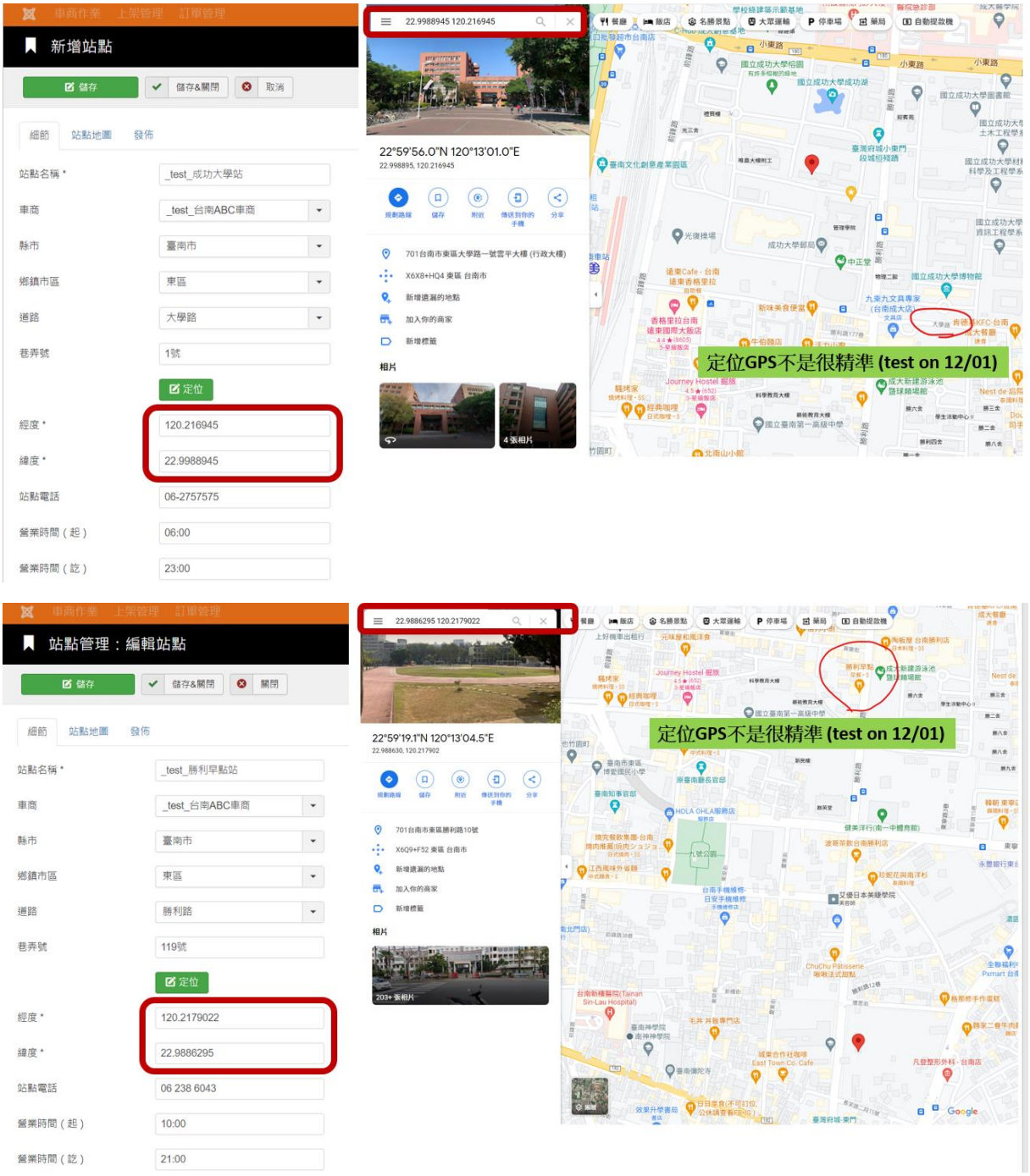


圖 3.2.37 [T-C-03] 站點管理-GPS 定位異常

圖 3.2.38 [T-C-03] 站點管理-定位問題導致站點地圖資訊失準

圖 3.2.39 [T-C-03] 站點管理-站點地圖「處理」功能操作異常

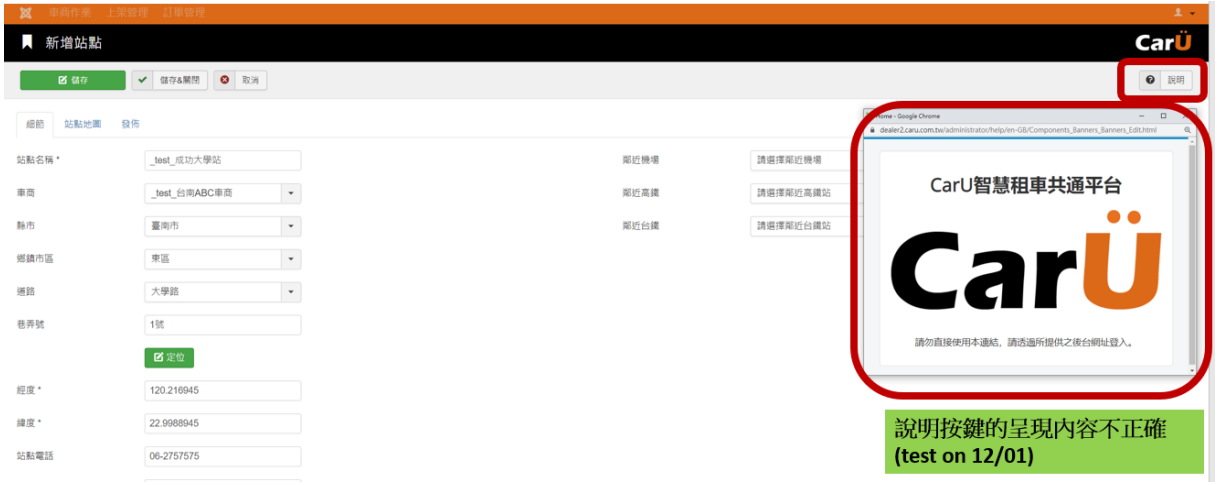


圖 3.2.40 [T-C-03] 站點管理-「說明」功能顯示異常

[T-C-04] 車輛管理：輸入欄位沒有檢查格式、資料刪除回饋顯示異常

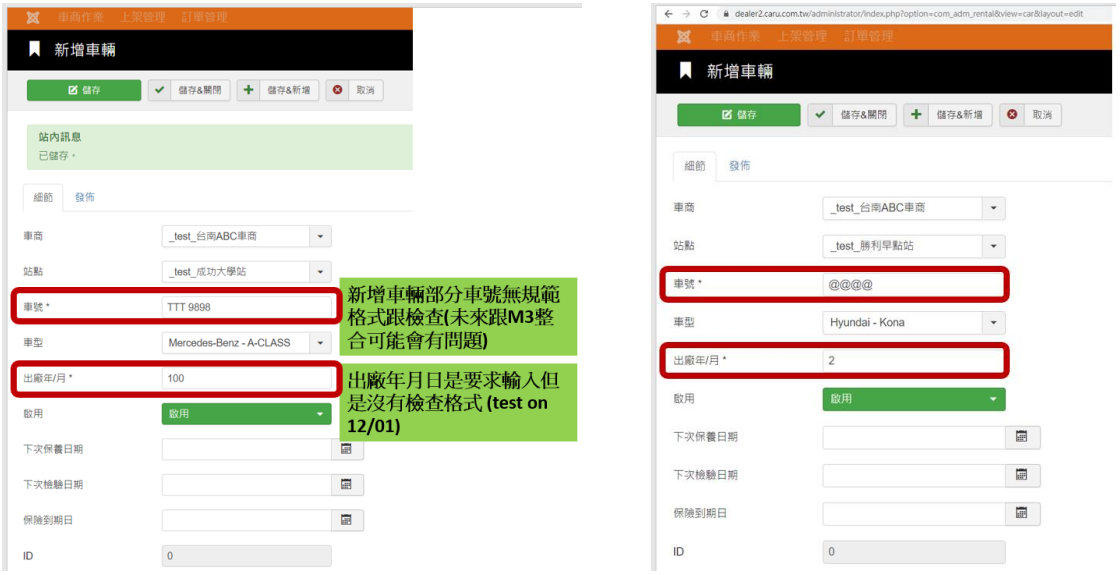


圖 3.2.41 [T-C-04] 車輛管理-輸入欄位沒有檢查格式

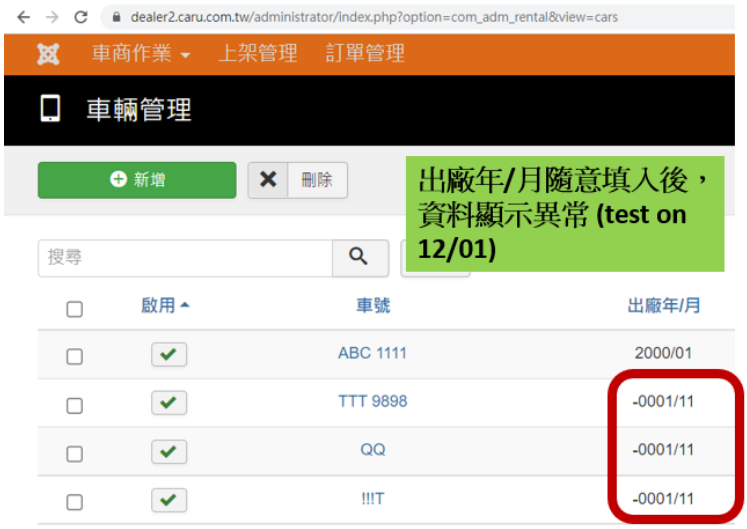


圖 3.2.42 [T-C-04] 車輛管理-資料顯示異常

圖 3.2.43 [T-C-04] 車輛管理-資料刪除回饋顯示異常

[T-C-05] 駕駛管理：重複帳號回饋顯示異常、站點資料顯示功能異常

圖 3.2.44 [T-C-05] 駕駛管理-資料刪除回饋顯示異常

圖 3.2.45 [T-C-05] 駕駛管理-站點資料顯示功能異常

[T-C-06] 員工管理：不同車商同帳號、密碼資料非強制輸入

圖 3.2.46 [T-C-06] 員工管理-不同車商使用同帳號的回饋訊息

圖 3.2.47 [T-C-06] 員工管理-密碼資料非強制輸入

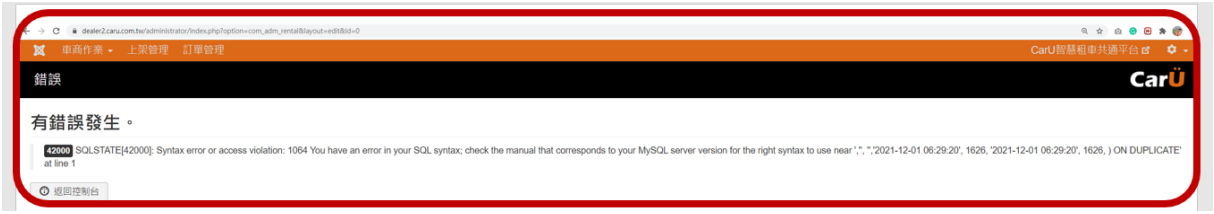


圖 3.2.48 [T-C-06] 員工管理-密碼留白所遭遇的錯誤畫面

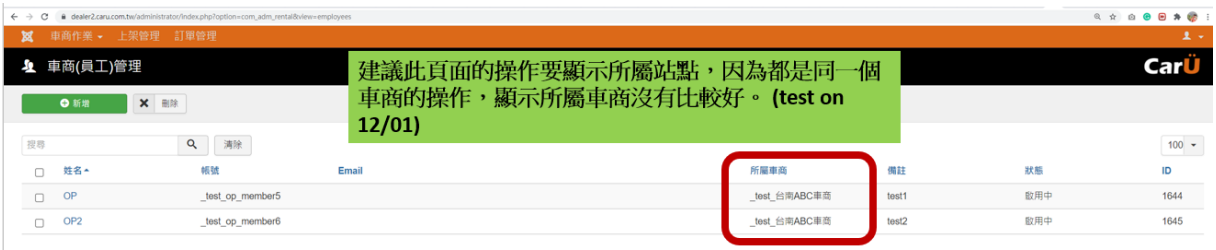


圖 3.2.49 [T-C-06] 員工管理-員工管理頁面顯示資訊改善建議

[T-C-07] 車商價格管理：於已選擇車型內可以改選其他非清單上的車型

圖 3.2.50 [T-C-07] 車商價格管理-車型資料操作疑似誤設計

[T-C-08] 站點價格管理：顯示資訊與車商價格管理相同

圖 3.2.51 [T-C-08] 站點價格管理-顯示資訊與車商價格管理相同

[T-C-09] 內附項目管理：新增功能操作異常

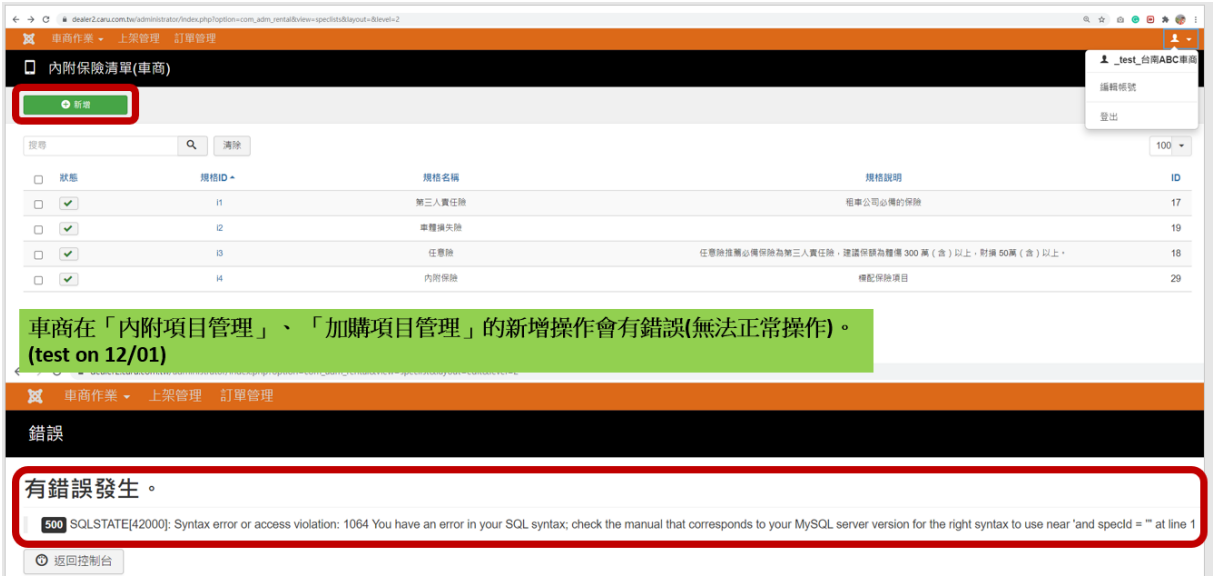


圖 3.2.52 [T-C-09] 內附項目管理-新增功能操作異常

[T-C-10] 上架管理：上架功能操作異常、無相關資料可以做進度檢視

圖 3.2.53 [T-C-10] 上架管理-上架功能操作異常

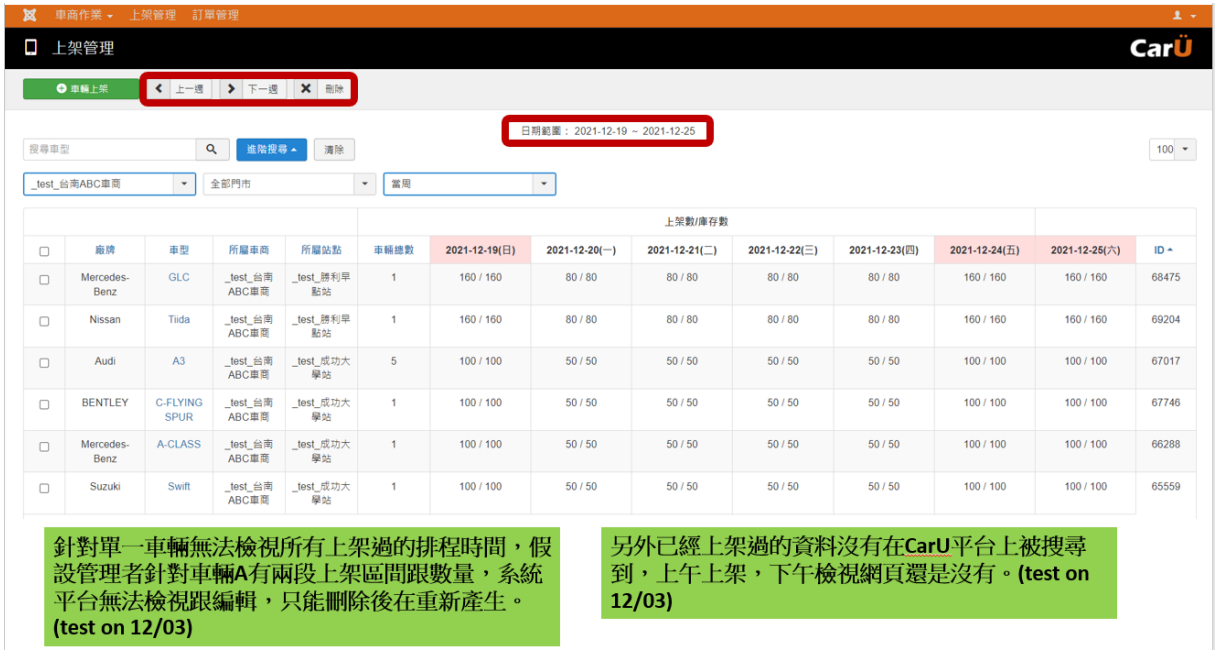


圖 3.2.54 [T-C-10] 上架管理-上架功能檢視限制與顯示異常

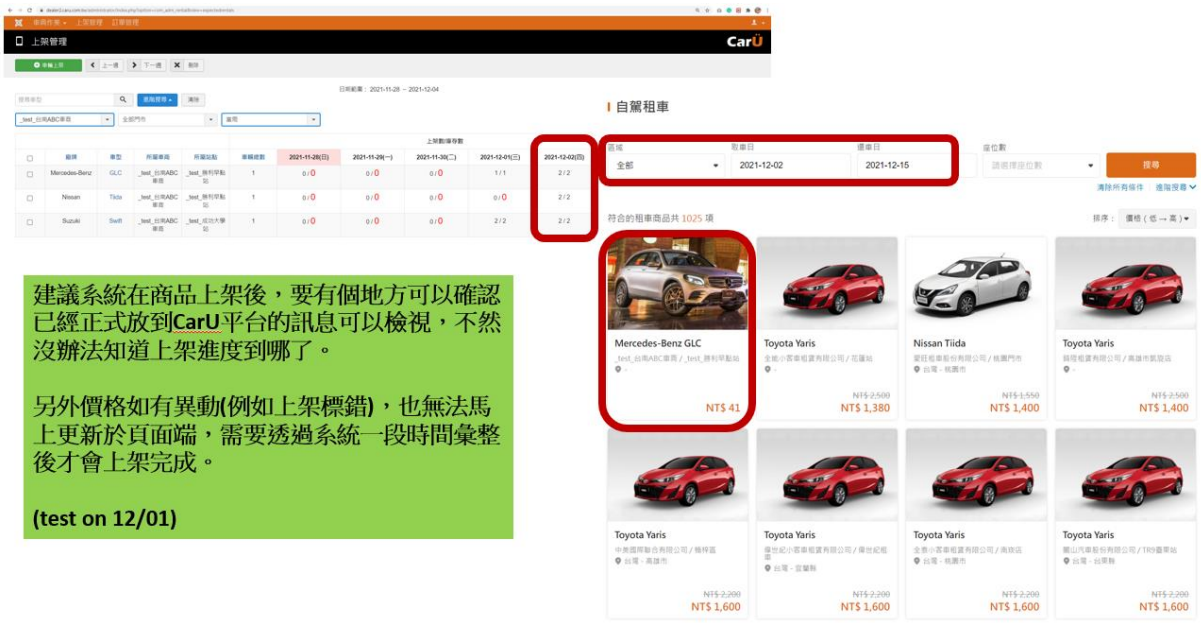


圖 3.2.55 [T-C-10] 上架管理-無上架進度檢視相關資訊

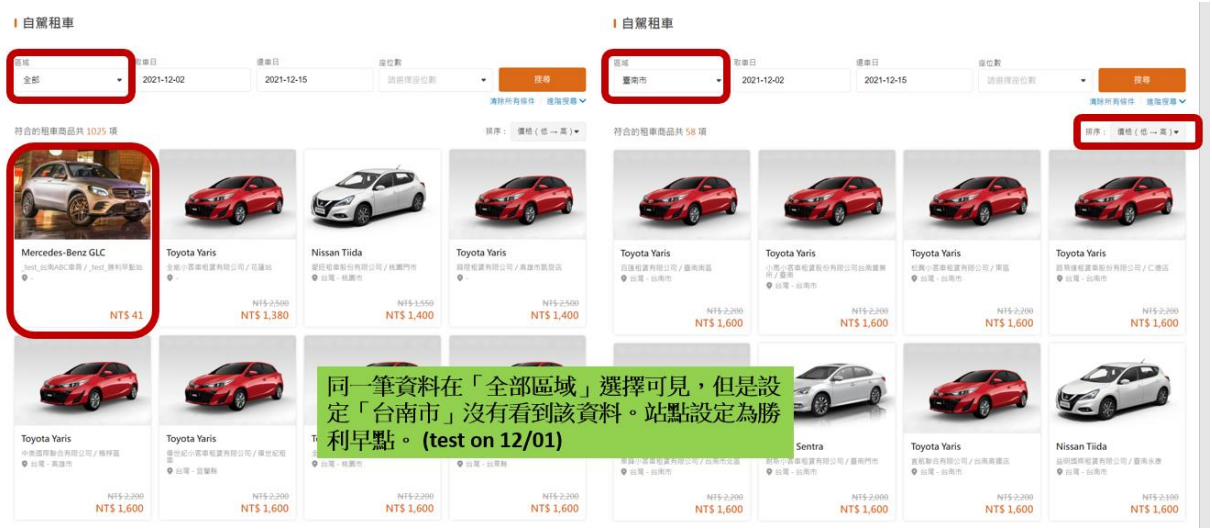


圖 3.2.56 [T-C-10] 上架管理-上架後 CarU 端顯示過濾器異常

[T-C-11] 訂單管理：訂單判斷與顯示邏輯疑似異常

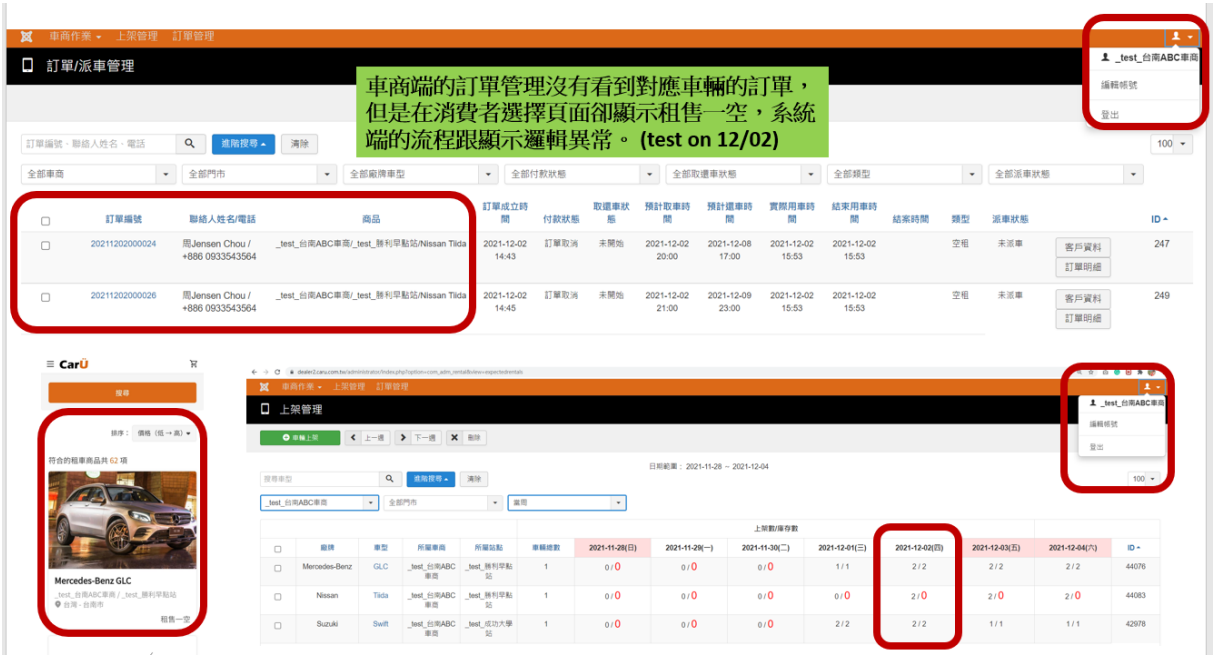


圖 3.2.57 [T-C-11] 訂單管理-訂單判斷與顯示邏輯疑似異常

圖 3.2.58 [T-C-11] 訂單管理-訂單狀態顯示異常(如已還車，但顯示未派車等)

由於此功能的重要性極高，會影響到訂單的資訊顯示與車商的商業運作行為。因此較多說明，目前 CarU 系統的訂單同步是指定一個時間(或是每 *N* 個小時)執行批次同步，因此車商在更改訂單資料後，需等到批次同步後相關資訊才會更新至最新狀態，**因此可能會發生系統之間同步的時間差，導致訂單資訊錯誤的問題發生**。經詢問漢名科技後，目前系統針對訂單的處理邏輯如下：

(1) 如果商品資料異動，會在下一次同步時更新 CarU 端的資料；

(2) 在尚未同步的這段期間，商品仍可以被瀏覽及交易；

(3) 下單時 CarU 端還是會即時跟新租車平台再次確認最新庫存與價格；

(4) 若即時確認當下發現無庫存或價格異動，回報商品資料異動，中止交易；

(5) 若商品異動資料涉及商品描述或主檔規格變動，商品會先下架，需經營運人員審理後上架。

這樣的執行方式，消費者還是會檢視到錯誤的資料，最後沒辦法下訂單，造成時間上的損失，進而導致成本上升，也會大大降低使用者體驗。建議漢名科技應思考有無比較好的改善方式，或是有異動就先下架，然後等時間到再上架，避免消費者看到錯誤的資訊為優先。

[T-U-01] 登入：使用 Google 帳號登入顯示異常(測試期間有發生，現已排除)。

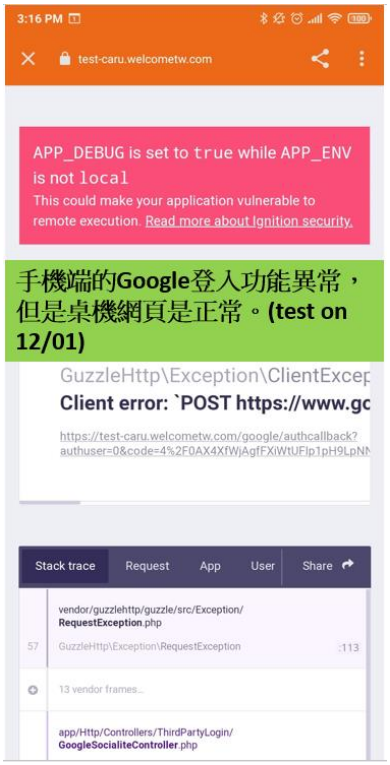


圖 3.2.59 [T-U-01] 登入-使用 Google 帳號登入顯示異常

[T-U-02] 車輛搜尋：資訊顯示相關修正建議

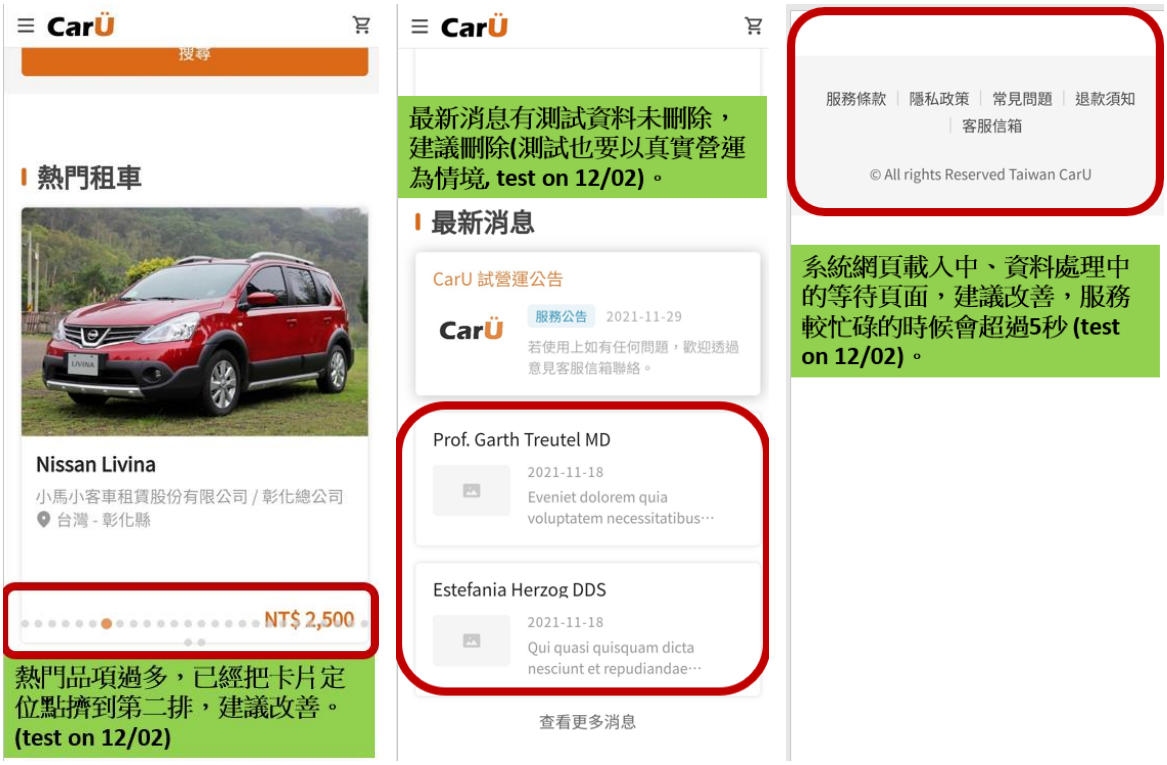


圖 3.2.60 [T-U-02] 車輛搜尋-資訊顯示相關修正建議

[T-U-03] 購物車與購買：購物車資訊在金流取消後會消失，與其他問題

圖 3.2.61 [T-U-03] 購物車與購買-購物車資訊在金流交易取消後會消失

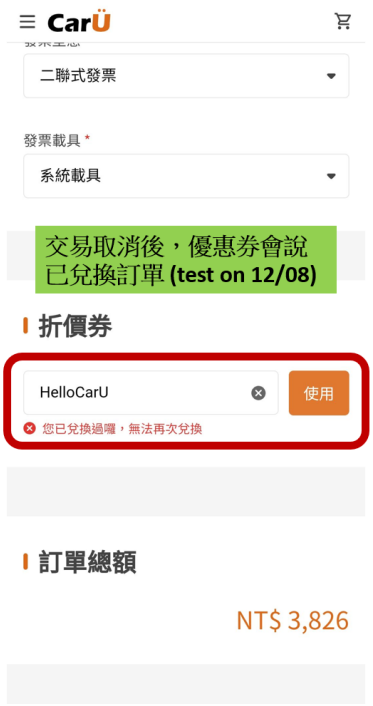


圖 3.2.62 [T-U-03] 購物車與購買-於金流交易取消後，優惠券呈現已兌換

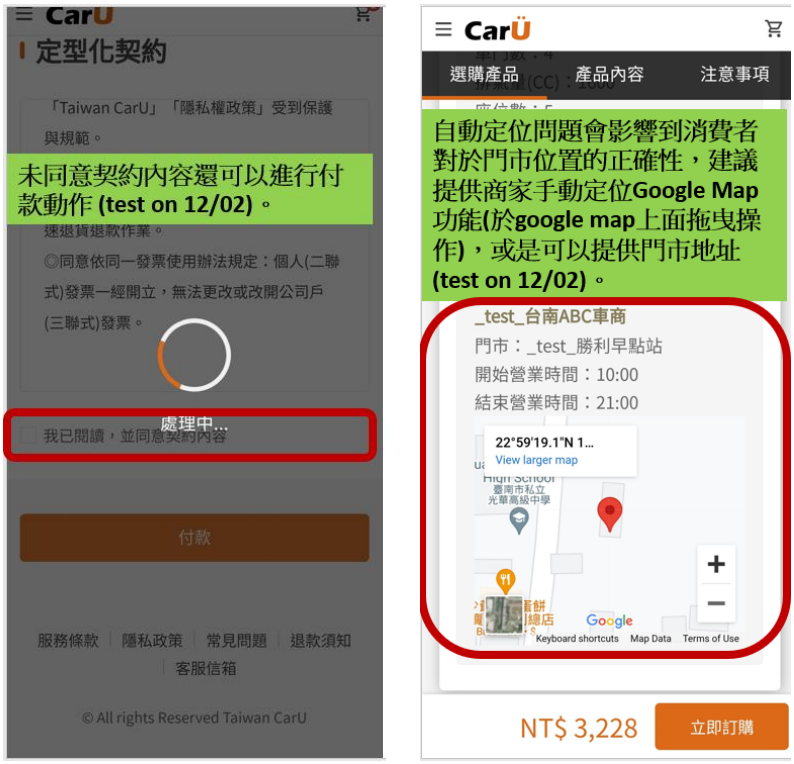


圖 3.2.63 [T-U-03] 購物車與購買-待修正議題

[T-U-04] 金流交易：購物車金流與第三方金流的數字不同，請參閱圖 3.2.61 左一跟左二圖；金流操作未成功，平台端依舊顯示訂單確認。

圖 3.2.64 [T-U-04] 金流交易-操作未成功，平台依舊顯示訂單確認。

[T-U-05] 檢視訂單：下訂後結果檢視訂單為付款失敗，但是有收到交易成功資相關訊息；交易失敗後，優惠券也無法使用。

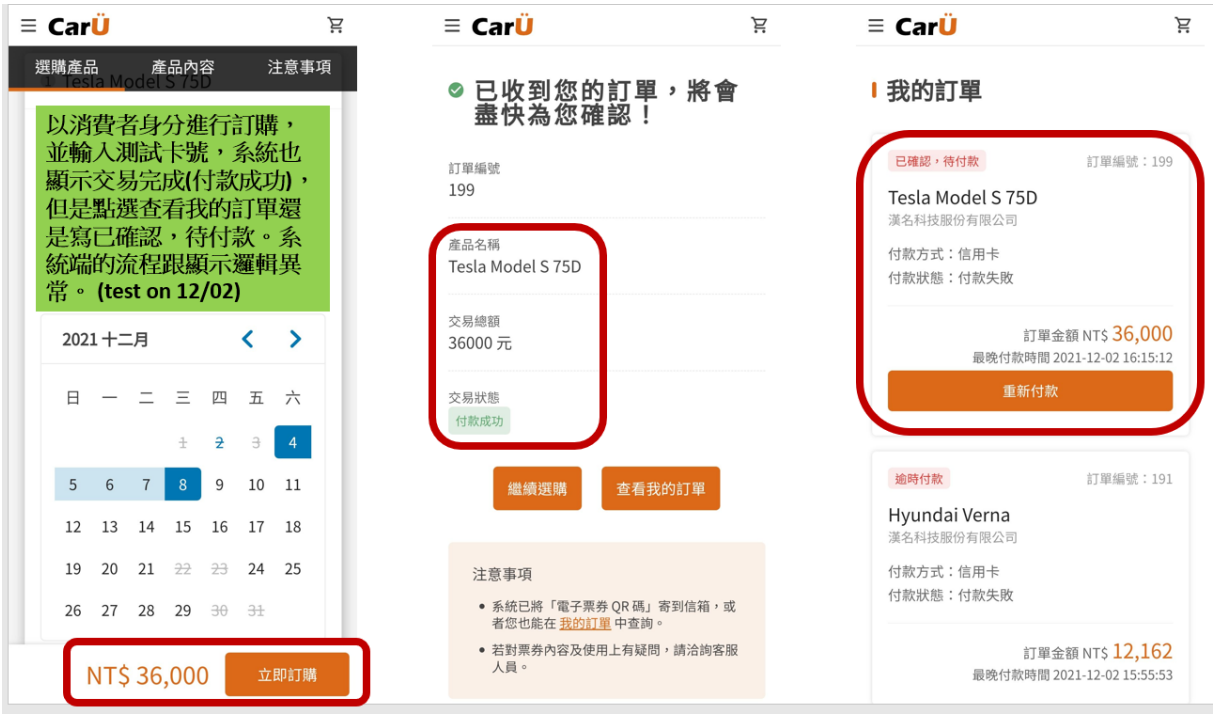


圖 3.2.65 [T-U-05] 檢視訂單-完成金流交易卻顯示訂單為付款失敗-part 1

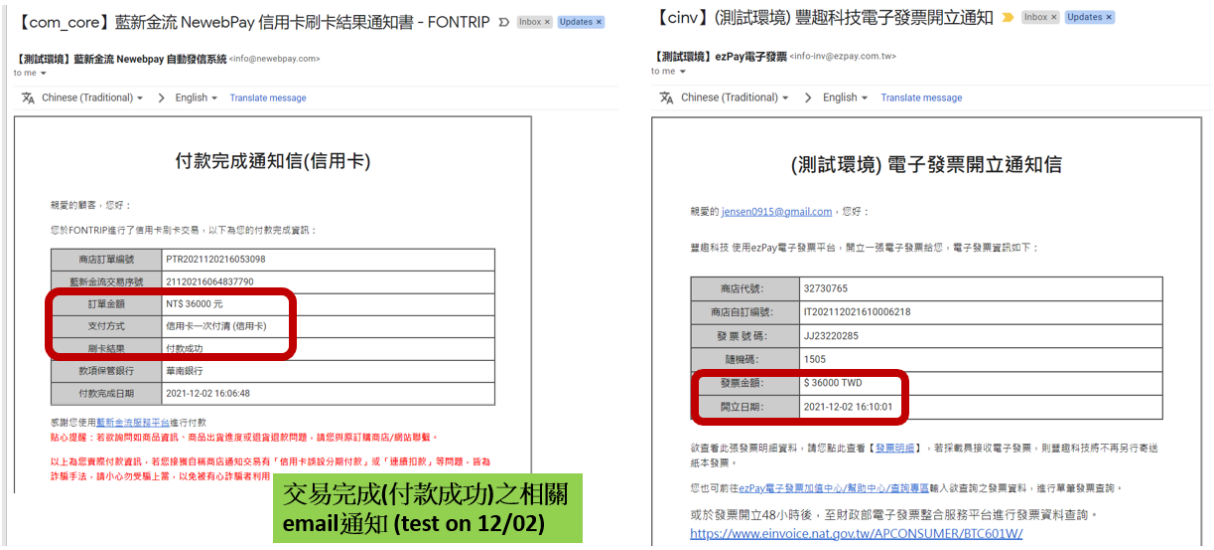


圖 3.2.66 [T-U-05] 檢視訂單-完成金流交易卻顯示訂單為付款失敗-part 2

圖 3.2.67 [T-U-05] 檢視訂單-照片上傳未正常顯示於管理頁面，前後台訂單編號資訊未同步

圖 3.2.68 [T-U-05] 檢視訂單-管理端如果取消訂單，使用者端狀態不會更新；系統端的時戳有誤

其他項目說明：

CarU 系統後台非本次主要測試標的，不過在測試期間會需要登入做資料正確性的檢視，在測試期間發現該平台有無法正常動作的狀態(於 12/06 早上)，如圖 3.2.69 所示，疑似系統廠商沒有確實區分測試環境跟正式環境。

圖 3.2.69 CarU 後台存取錯誤訊息

因 PWA 的相關功能使用需由主流瀏覽器開啟方能正常執行，假設是透過 APP 內建的瀏覽器(如 Line)，會無法開啟相機(如圖 3.2.70 所示)或是取得 GPS 位址，這點可能進行宣導或是教育訓練，以免相關人員在執行上無法順利完成任務。

圖 3.2.70 透過 Line 軟體開啟行動門市頁面，顯示相機載入失敗

消費者於「附駕司機」頁面搜尋車輛後，要下訂時還需要另外勾選「附駕駛」的選項，否則訂單會變成「空租」的屬性，這樣的操作流程容易衍生相關消費糾紛，建議直接綁定並啟用該屬性會比較好，否則金額差很多，如圖 3.2.71 所示。

圖 3.2.71 消費者於附駕司機頁面，需另外選附駕駛才行。

(2) PWA 頁面驗證：

針對 PWA 部分的檢視，團隊使用實際操作與檢測工具 Lighthouse。因工具 report 內容較多，因此僅呈現概要內容的截圖(詳細內容如附件三)。消費者、行動門市與附駕司機皆具備 PWA 功能(差別在於頁面的載入速度跟是否有針對 PWA 做最佳化)，顯示於圖 3.2.72~圖 3.2.74。

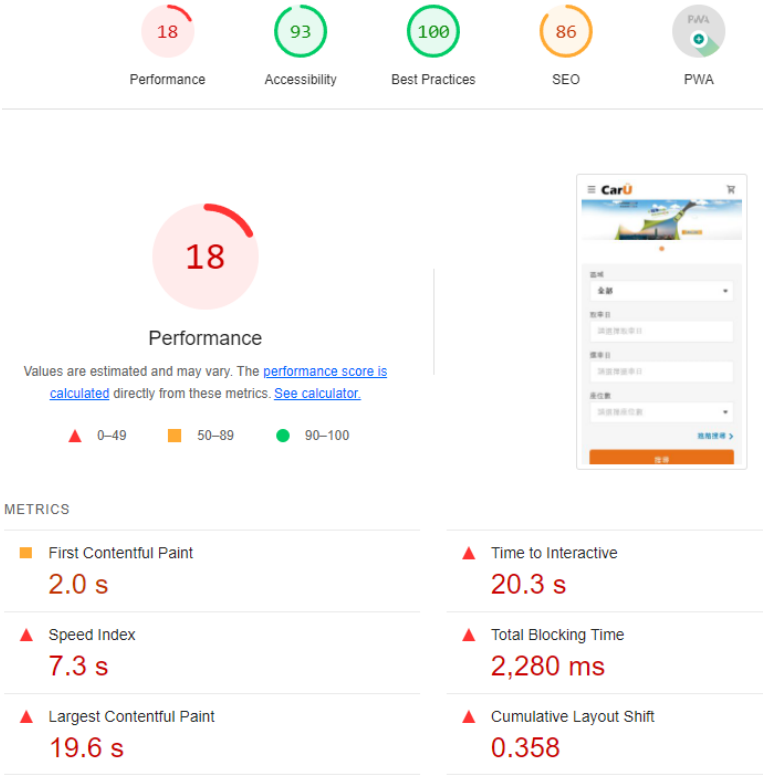


圖 3.2.72 PWA 檢測結果-消費者端

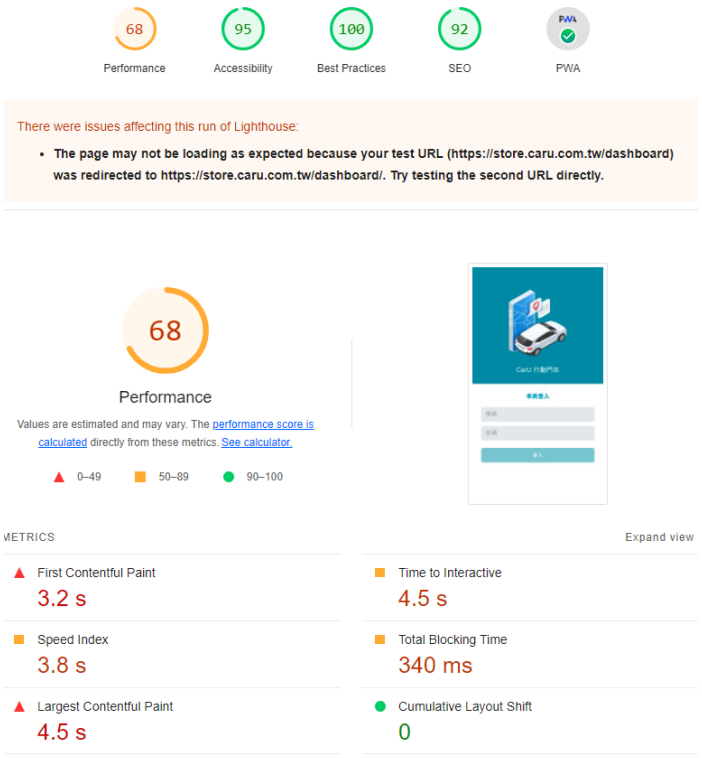


圖 3.2.73 PWA 檢測結果-行動門市端

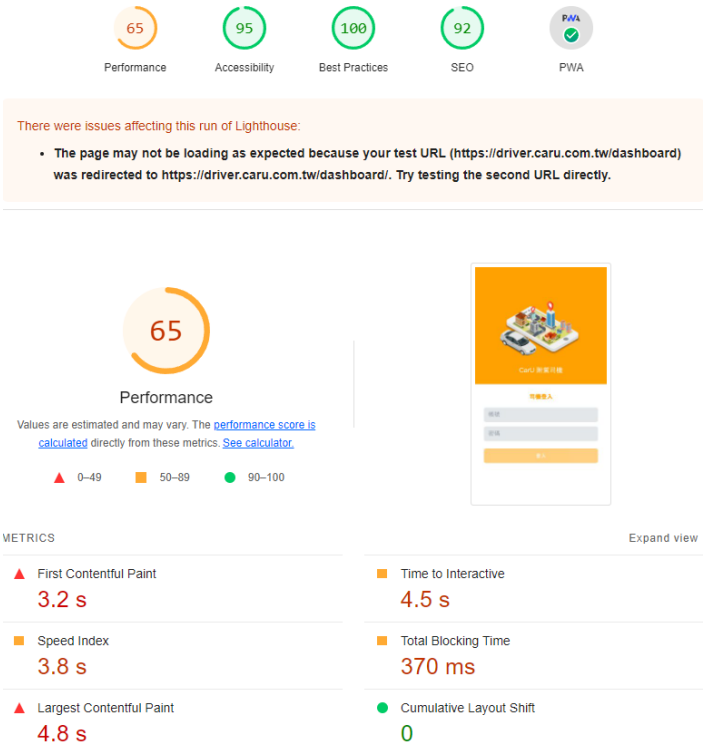


圖 3.2.74 PWA 檢測結果-附駕司機端

(3) 相容性測試：

針對不同瀏覽器與行動裝置的操作跟測試，包含 Chrome、Edge、Firefox、Safari 四大主要瀏覽器與 Android 跟 iOS 手機進行操作後，畫面排版上沒有遇到明顯的操作問題。

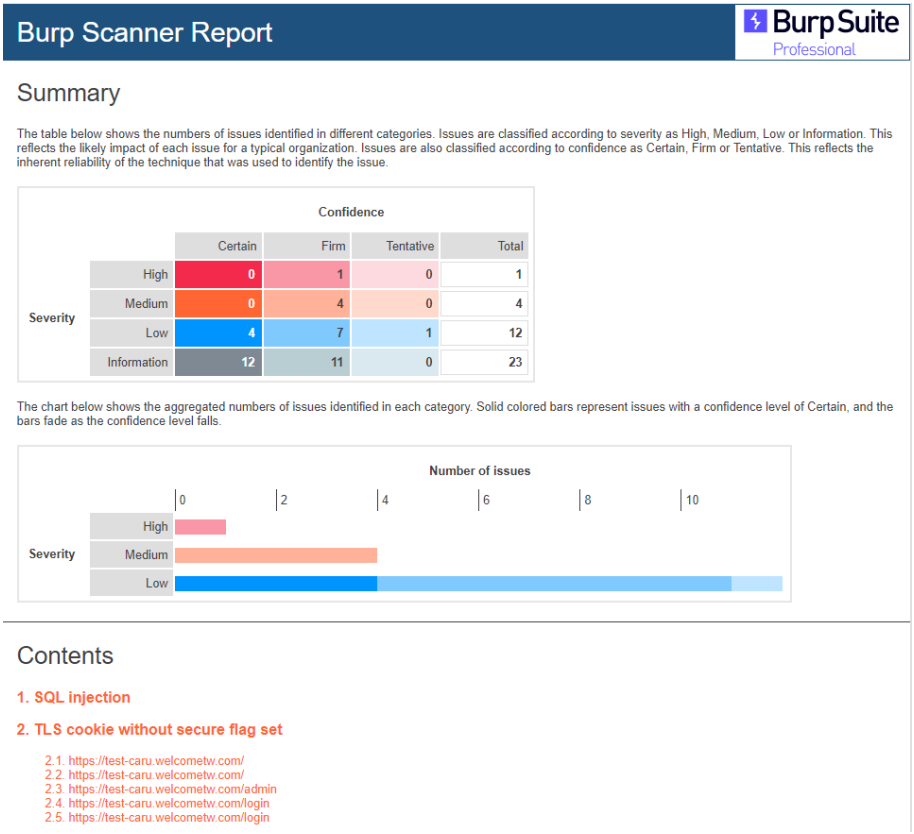
2. 安全性驗證

透過工具軟體進行網站弱點掃描，並提供相關修正建議；並檢視平台內部之 API 運作是否有做到基本防護(如 URL 上任意輸入其他資訊是否可以檢視他人資料)。

(1) 網站弱點掃描：

針對本次弱點掃描，我們團隊選用 Burp 來執行。因工具 report 內容較多，僅擷取概要內容(詳如附件四)，依序為 CarU 平台、新智慧租車平台、行動門市、附駕司機與 API 主機，參閱圖 3.2.75~圖 3.2.79。

除了 CarU 平台有明顯的 SQL injection 問題外(高風險的資安問題，需於正式上線前修正完畢，**評比為 A**)，其他平台皆無明顯的問題。例如 Cross-Domain Misconfiguration (如 Cross-Origin Resource Sharing 設定)、X-Frame-Options Header Not Set、TLS cookie without secure flag set 等都是待系統正式上線前進行正確的設定即可。至於憑證部分初步檢視結果如圖 3.2.80 所示，因 R3 為免費的 SSL 憑證效期較短，較常用於開發跟測試環境，所以才會被檢測工具檢查出來，列出 TLS certificate 的 issue。



Burp Scanner Report

Burp Suite Professional

Summary

The table below shows the numbers of issues identified in different categories. Issues are classified according to severity as High, Medium, Low or Information. This reflects the likely impact of each issue for a typical organization. Issues are also classified according to confidence as Certain, Firm or Tentative. This reflects the inherent reliability of the technique that was used to identify the issue.

Severity	Confidence			
	Certain	Firm	Tentative	Total
High	0	1	0	1
Medium	0	4	0	4
Low	4	7	1	12
Information	12	11	0	23

The chart below shows the aggregated numbers of issues identified in each category. Solid colored bars represent issues with a confidence level of Certain, and the bars fade as the confidence level falls.

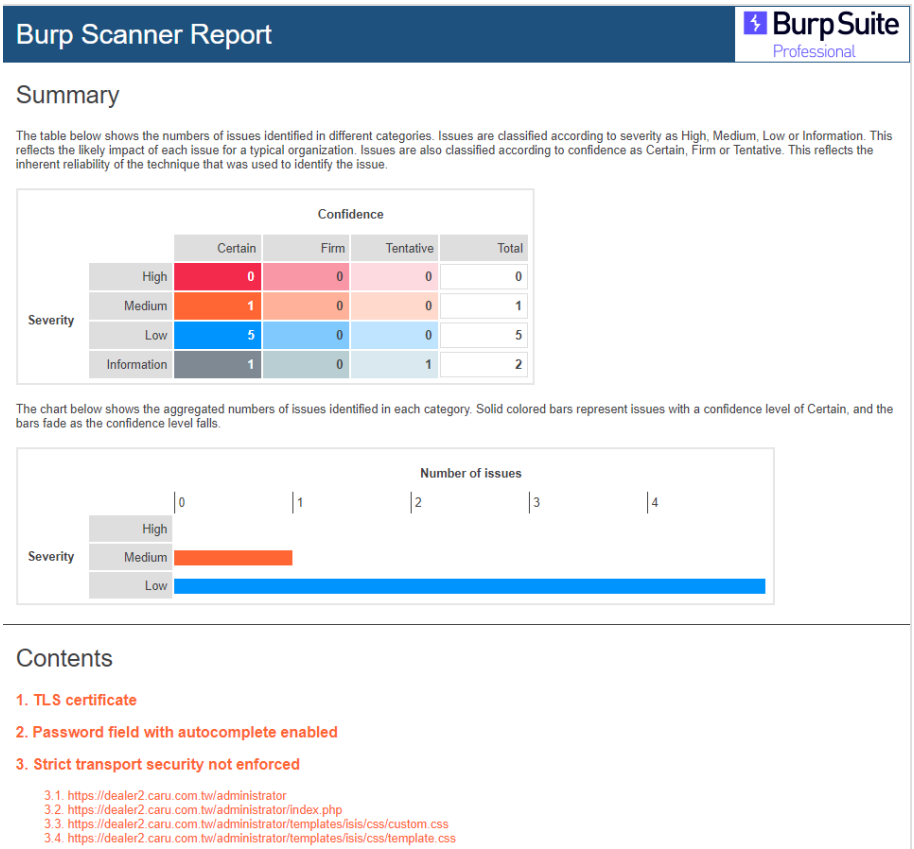
Contents

1. SQL injection

2. TLS cookie without secure flag set

2.1. https://test-caru.welcometw.com/
2.2. https://test-caru.welcometw.com/
2.3. https://test-caru.welcometw.com/admin
2.4. https://test-caru.welcometw.com/login
2.5. https://test-caru.welcometw.com/login

圖 3.2.75 弱點掃描概要-CarU 平台



Burp Scanner Report

Burp Suite Professional

Summary

The table below shows the numbers of issues identified in different categories. Issues are classified according to severity as High, Medium, Low or Information. This reflects the likely impact of each issue for a typical organization. Issues are also classified according to confidence as Certain, Firm or Tentative. This reflects the inherent reliability of the technique that was used to identify the issue.

Severity	Confidence			
	Certain	Firm	Tentative	Total
High	0	0	0	0
Medium	1	0	0	1
Low	5	0	0	5
Information	1	0	1	2

The chart below shows the aggregated numbers of issues identified in each category. Solid colored bars represent issues with a confidence level of Certain, and the bars fade as the confidence level falls.

Contents

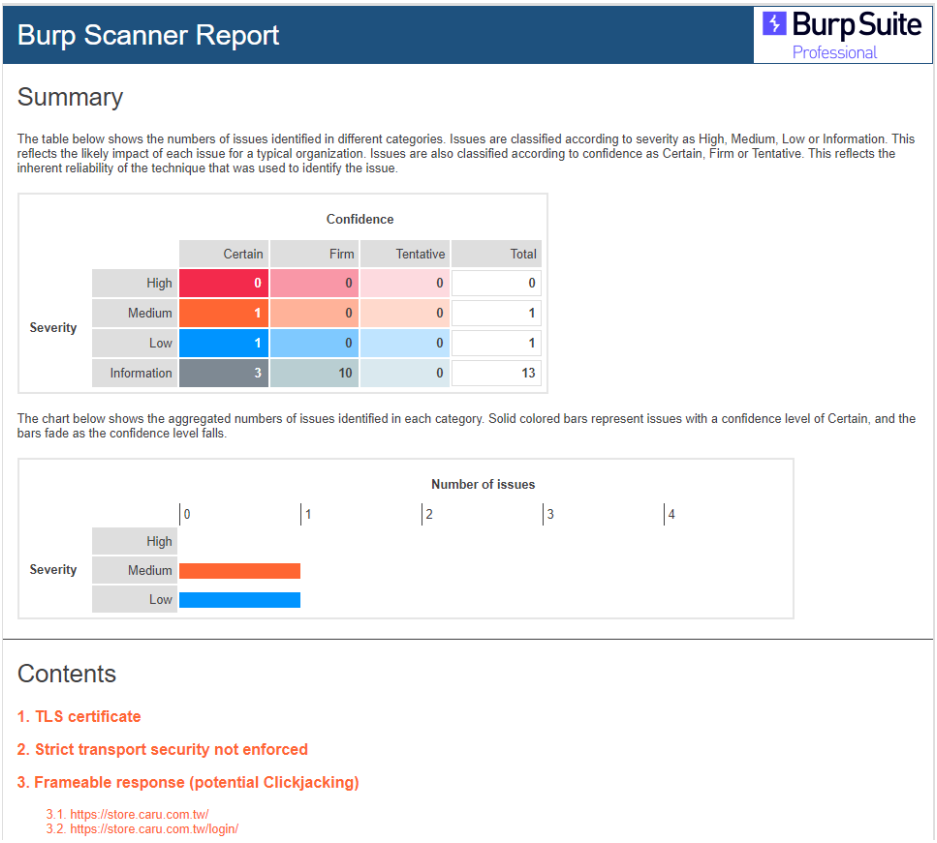
1. TLS certificate

2. Password field with autocomplete enabled

3. Strict transport security not enforced

3.1. https://dealer2.caru.com.tw/administrator
3.2. https://dealer2.caru.com.tw/administrator/index.php
3.3. https://dealer2.caru.com.tw/administrator/templates/isis/css/custom.css
3.4. https://dealer2.caru.com.tw/administrator/templates/isis/css/template.css

圖 3.2.76 弱點掃描概要-新智慧租車平台



Burp Scanner Report

Burp Suite Professional

Summary

The table below shows the numbers of issues identified in different categories. Issues are classified according to severity as High, Medium, Low or Information. This reflects the likely impact of each issue for a typical organization. Issues are also classified according to confidence as Certain, Firm or Tentative. This reflects the inherent reliability of the technique that was used to identify the issue.

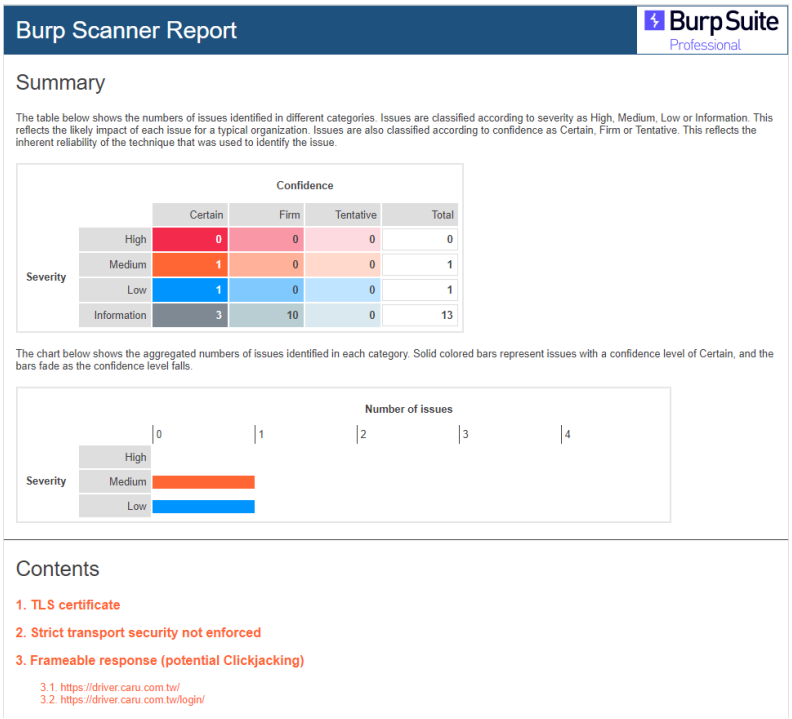
Severity	Confidence			
	Certain	Firm	Tentative	Total
High	0	0	0	0
Medium	1	0	0	1
Low	1	0	0	1
Information	3	10	0	13

The chart below shows the aggregated numbers of issues identified in each category. Solid colored bars represent issues with a confidence level of Certain, and the bars fade as the confidence level falls.

Contents

1. TLS certificate
2. Strict transport security not enforced
3. Frameable response (potential Clickjacking)
3.1. https://store.caru.com.tw/
3.2. https://store.caru.com.tw/login/

圖 3.2.77 弱點掃描概要-行動門市



Burp Scanner Report

Burp Suite Professional

Summary

The table below shows the numbers of issues identified in different categories. Issues are classified according to severity as High, Medium, Low or Information. This reflects the likely impact of each issue for a typical organization. Issues are also classified according to confidence as Certain, Firm or Tentative. This reflects the inherent reliability of the technique that was used to identify the issue.

Severity	Confidence			
	Certain	Firm	Tentative	Total
High	0	0	0	0
Medium	1	0	0	1
Low	1	0	0	1
Information	3	10	0	13

The chart below shows the aggregated numbers of issues identified in each category. Solid colored bars represent issues with a confidence level of Certain, and the bars fade as the confidence level falls.

Contents

1. TLS certificate
2. Strict transport security not enforced
3. Frameable response (potential Clickjacking)
3.1. https://driver.caru.com.tw/
3.2. https://driver.caru.com.tw/login/

圖 3.2.78 弱點掃描概要-附駕司機

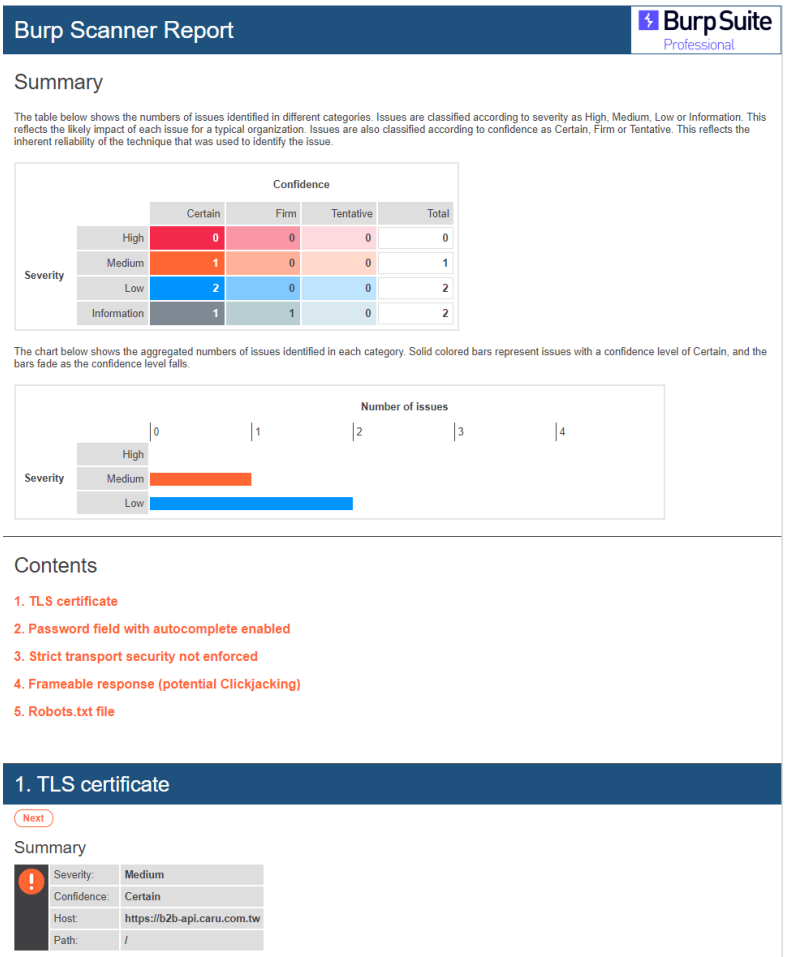


圖 3.2.79 弱點掃描概要-API 主機

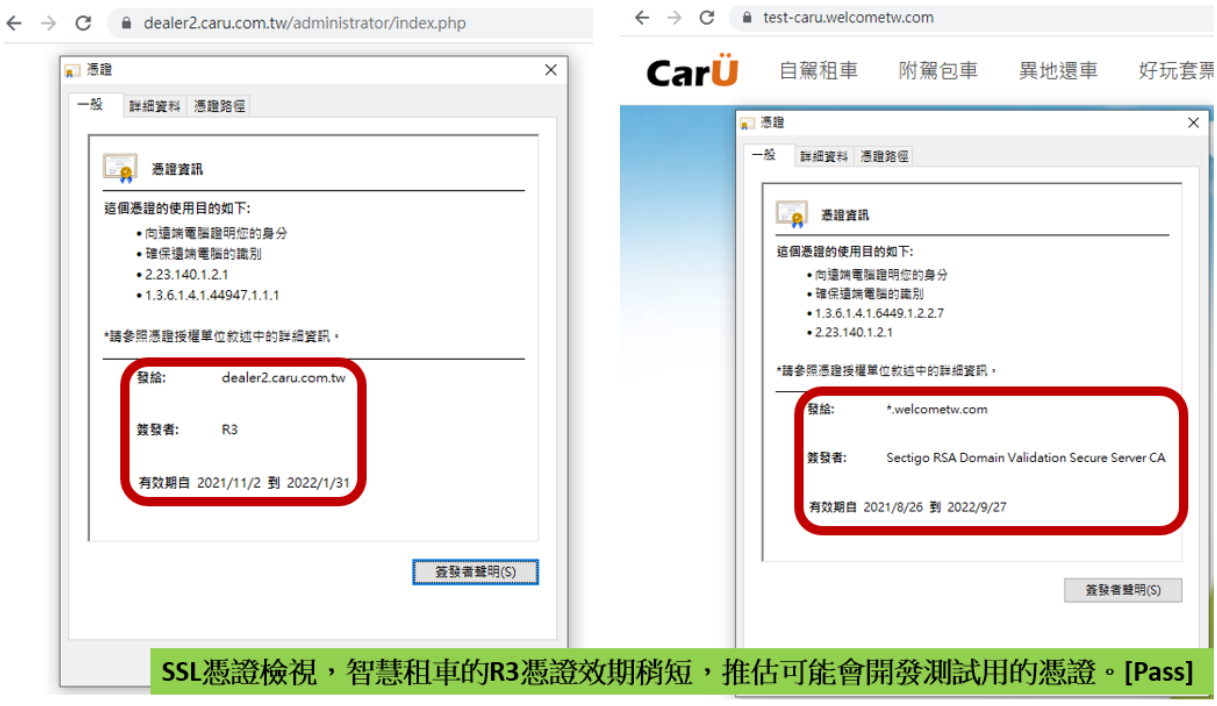


圖 3.2.80 系統平台 SSL 憑證效期

(2) 平台內部 API 測試：

系統內部使用的 API 經測試，共有 8 支 API，在知悉平台帳號密碼下進行相關操作行為，相關截圖請參閱，經測試後主要有三項問題，為 Access-Control-Allow-Methods 欄位未限縮範圍、API Token 未經過驗證，隨意輸入即可進行、未進行欄位格式驗證，易造成 SQL injection 攻擊(在使用者知悉平台帳密時)，經評估後需改善(後續說明也造成系統內部操作安全性問題)，**評比為 A**)。

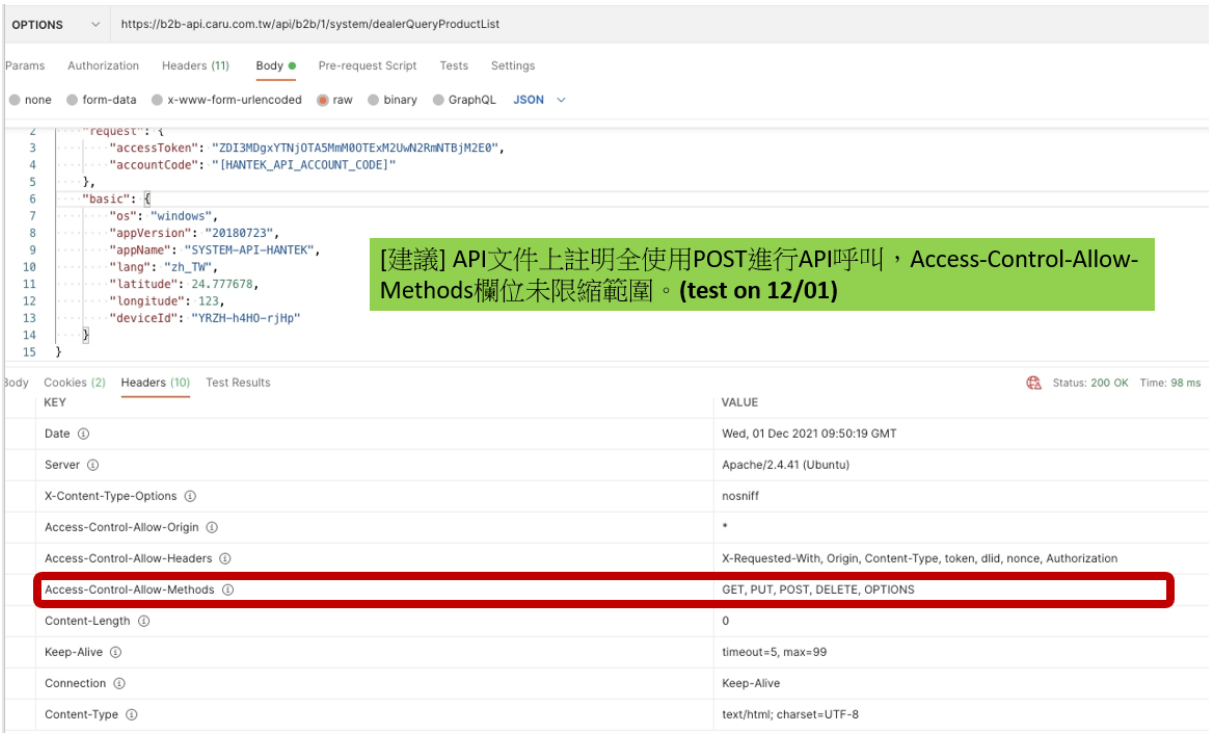


圖 3.2.81 系統平台 API 檢測-取得商品 ID-1

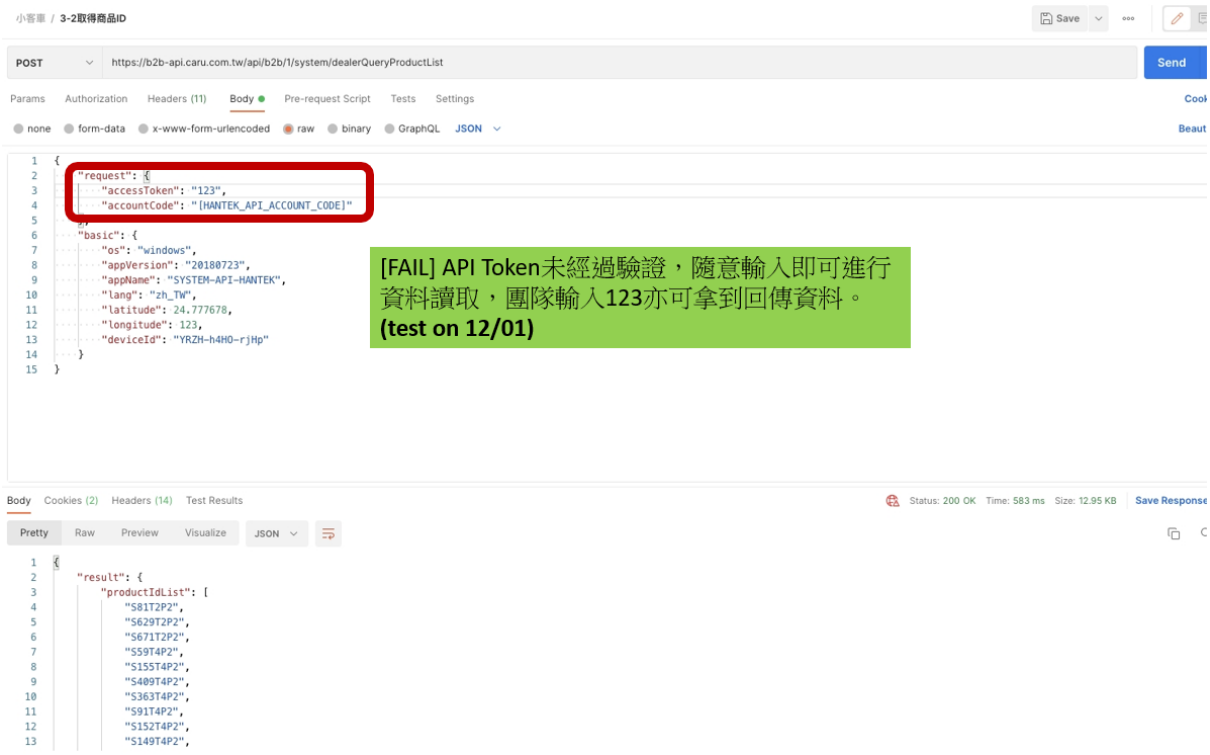


圖 3.2.82 系統平台 API 檢測-取得商品 ID-2

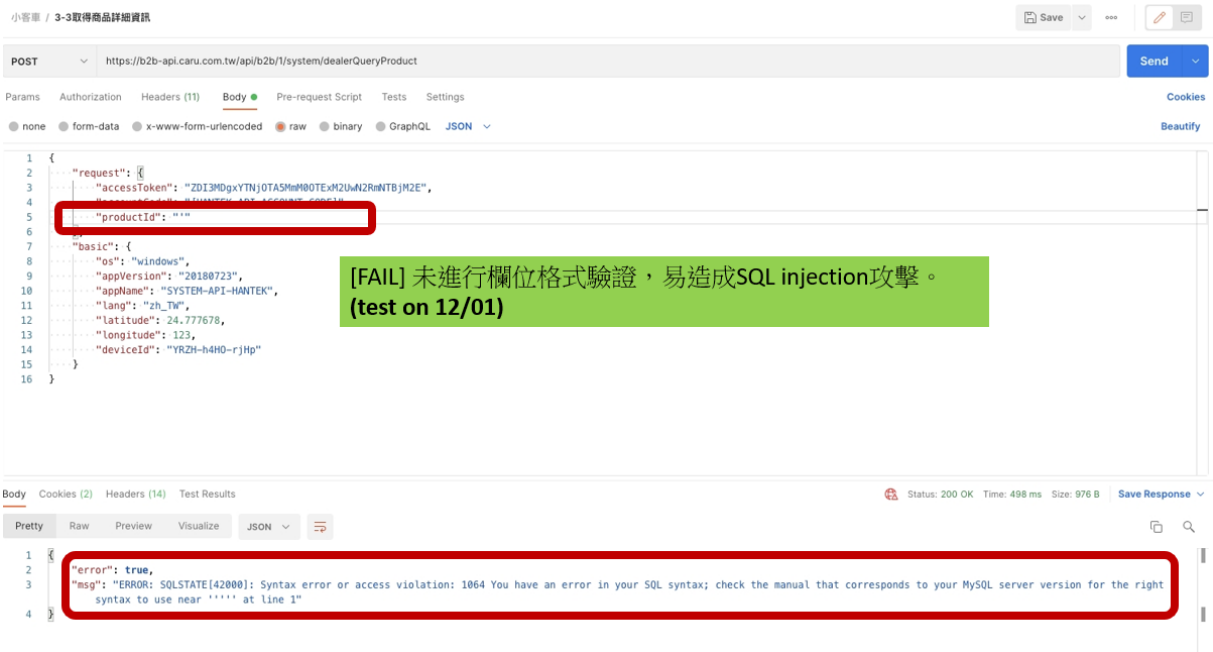


圖 3.2.83 系統平台 API 檢測-取得商品詳細資訊

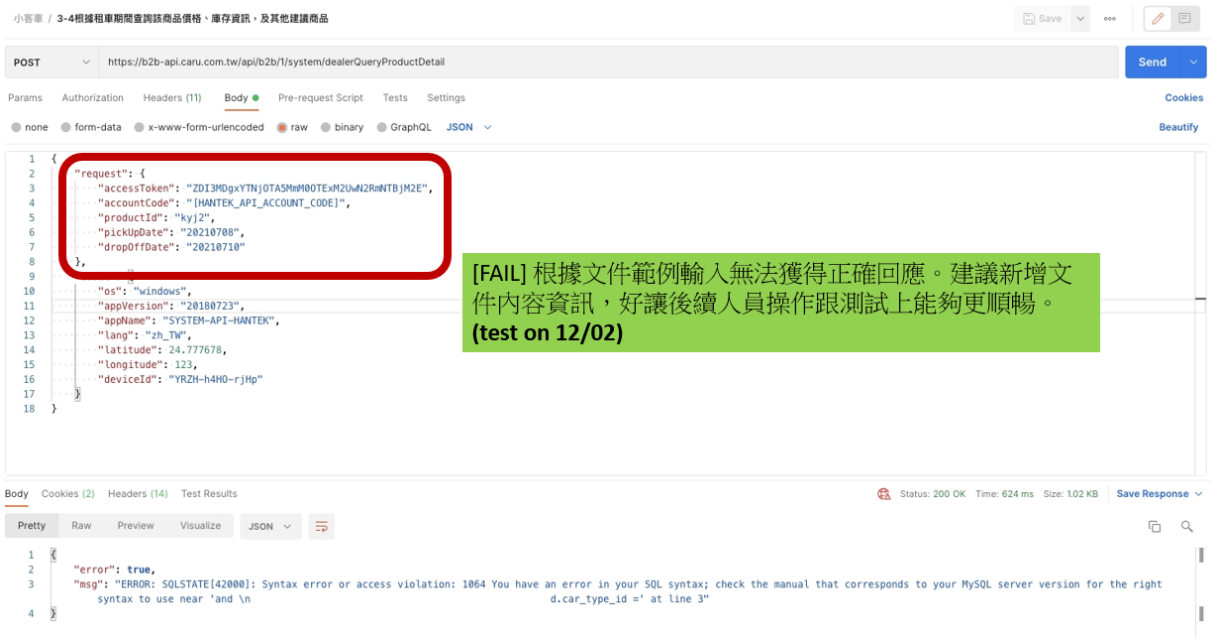


圖 3.2.84 系統平台 API 檢測-根據租車期間查詢該商品價格..

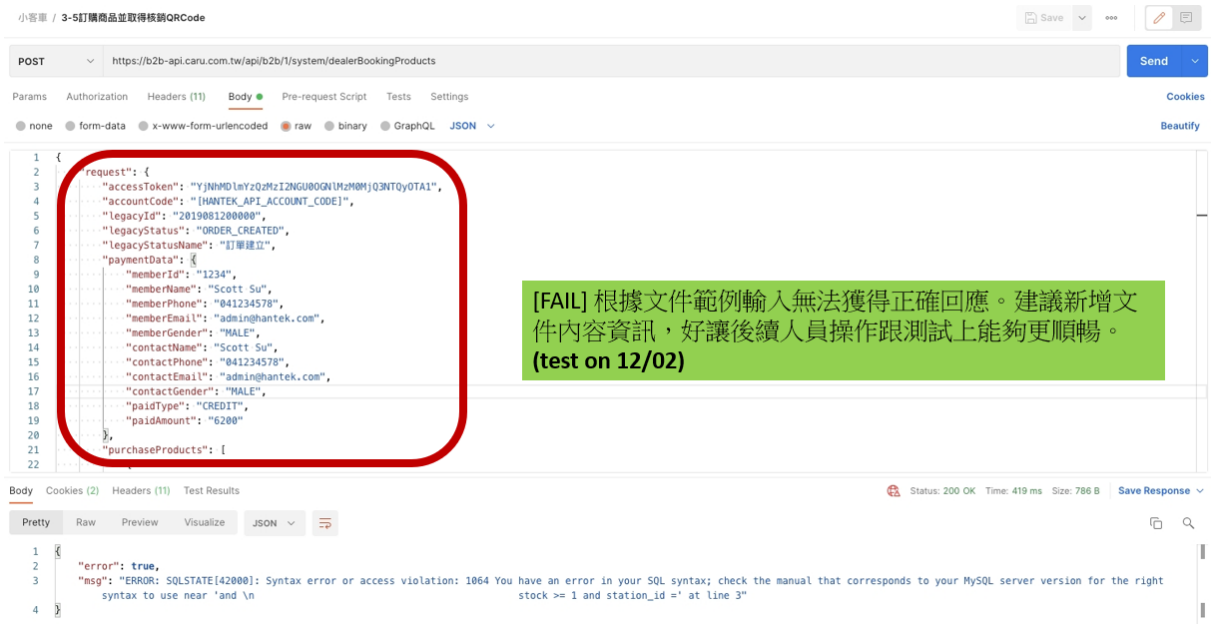


圖 3.2.85 系統平台 API 檢測-訂購商品並取得核銷 QRcode

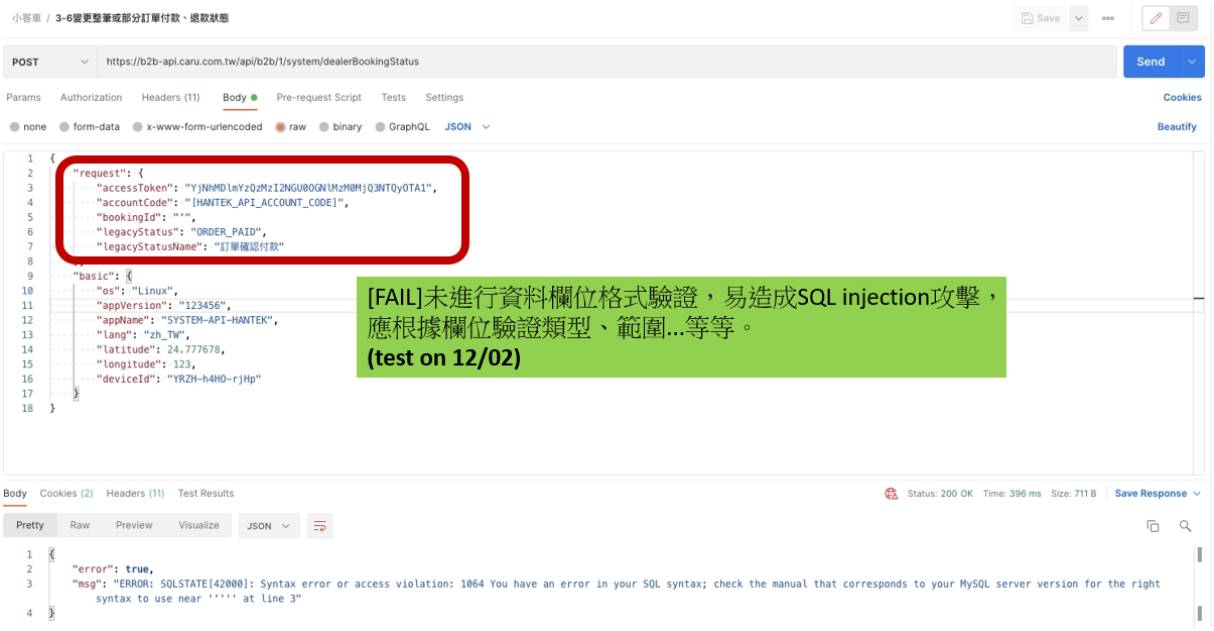


圖 3.2.86 系統平台 API 檢測-變更整筆或部分訂單狀態

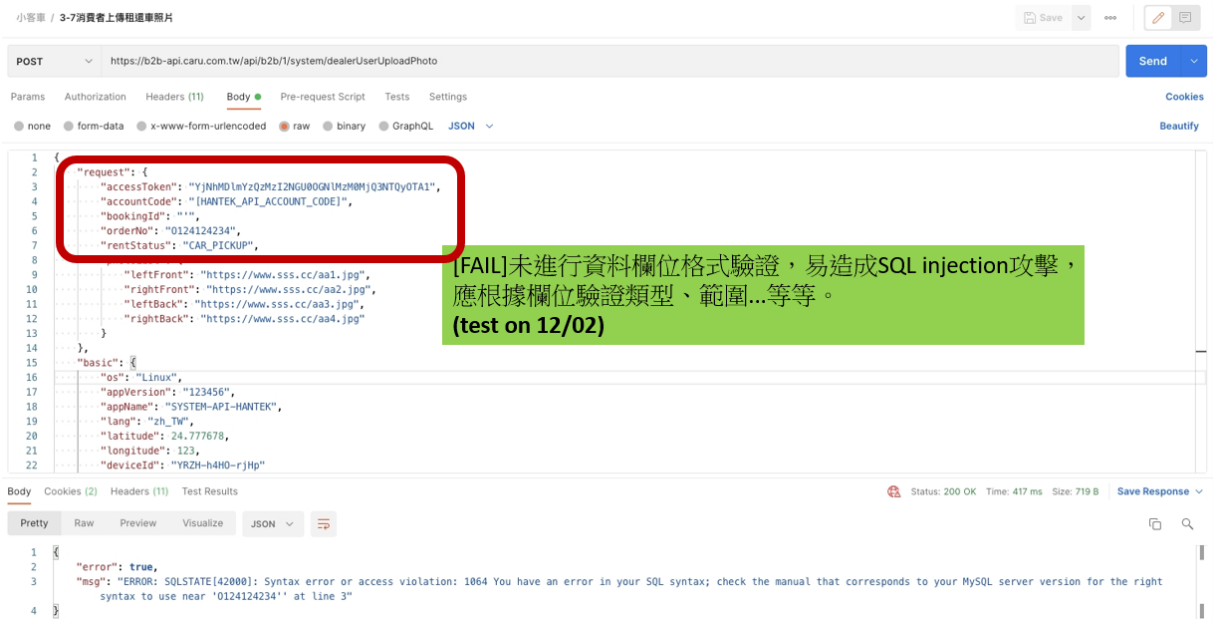


圖 3.2.87 系統平台 API 檢測-消費者上傳租還車照片

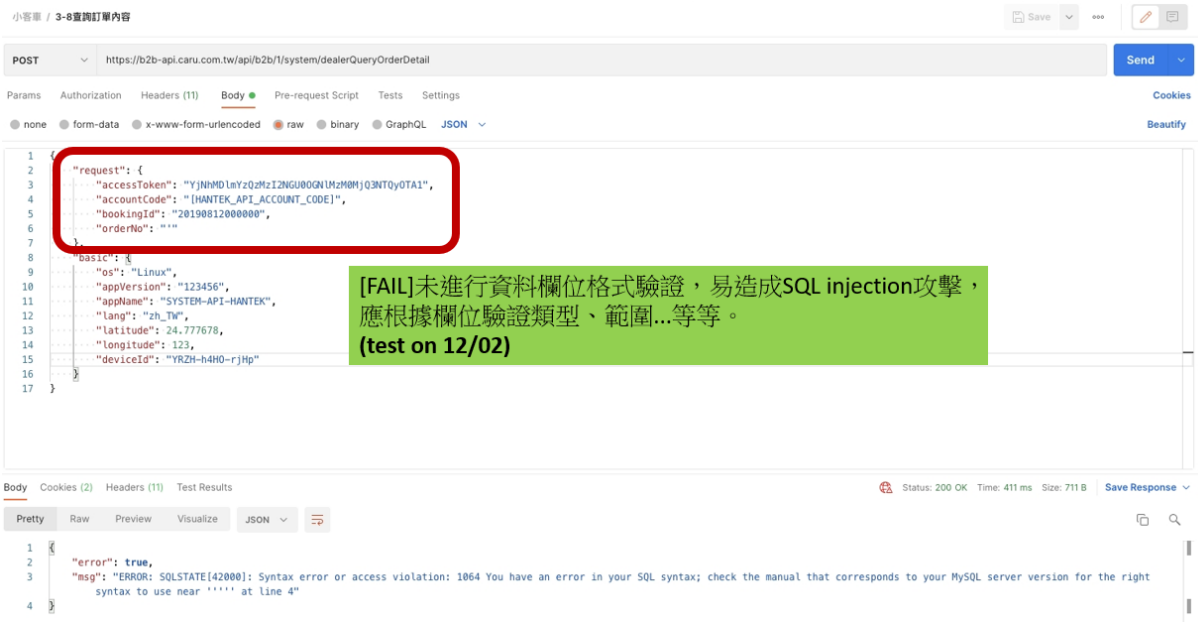


圖 3.2.88 系統平台 API 檢測-查詢訂單內容

因 API 未確實檢查 Token，所以在資料存取上容易有「人為」資安漏洞，經測試，在平台內部一些相關操作，透過 URL 上的資料修改，就可以取得跟編輯其他車商的相關資料，詳細操作範例請參閱圖 3.2.89~圖 3.2.91。

圖 3.2.89 透過修改 URL 取得/修改/其他車商的資料-1

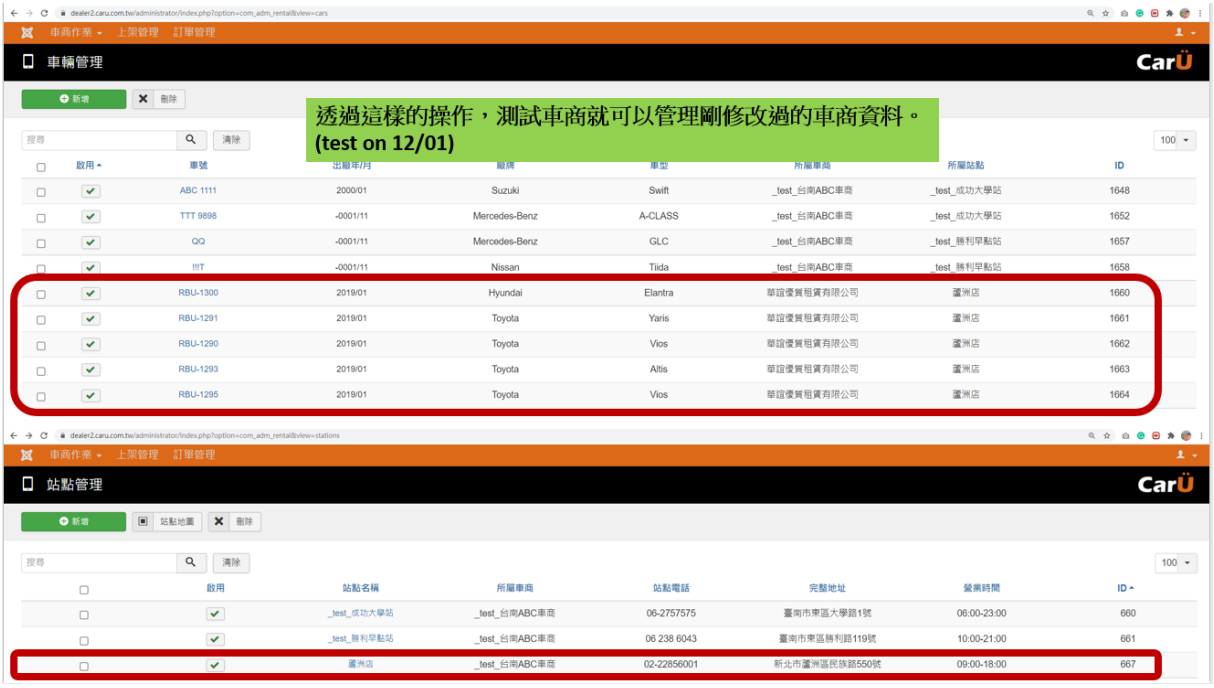
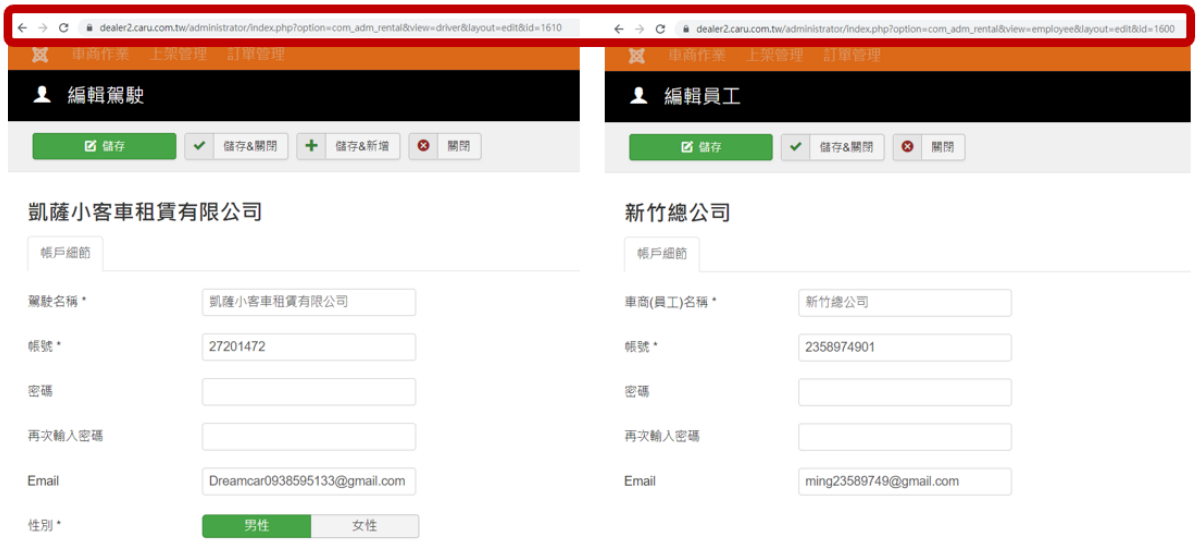


圖 3.2.90 透過修改 URL 取得/修改/其他車商的資料-2



其他資料如「駕駛」跟「員工」都有一樣的問題，可以透過更改URL ID來取得其他資料跟修改。(test on 12/01)

圖 3.2.91 透過修改 URL 取得/修改/其他車商的資料-3

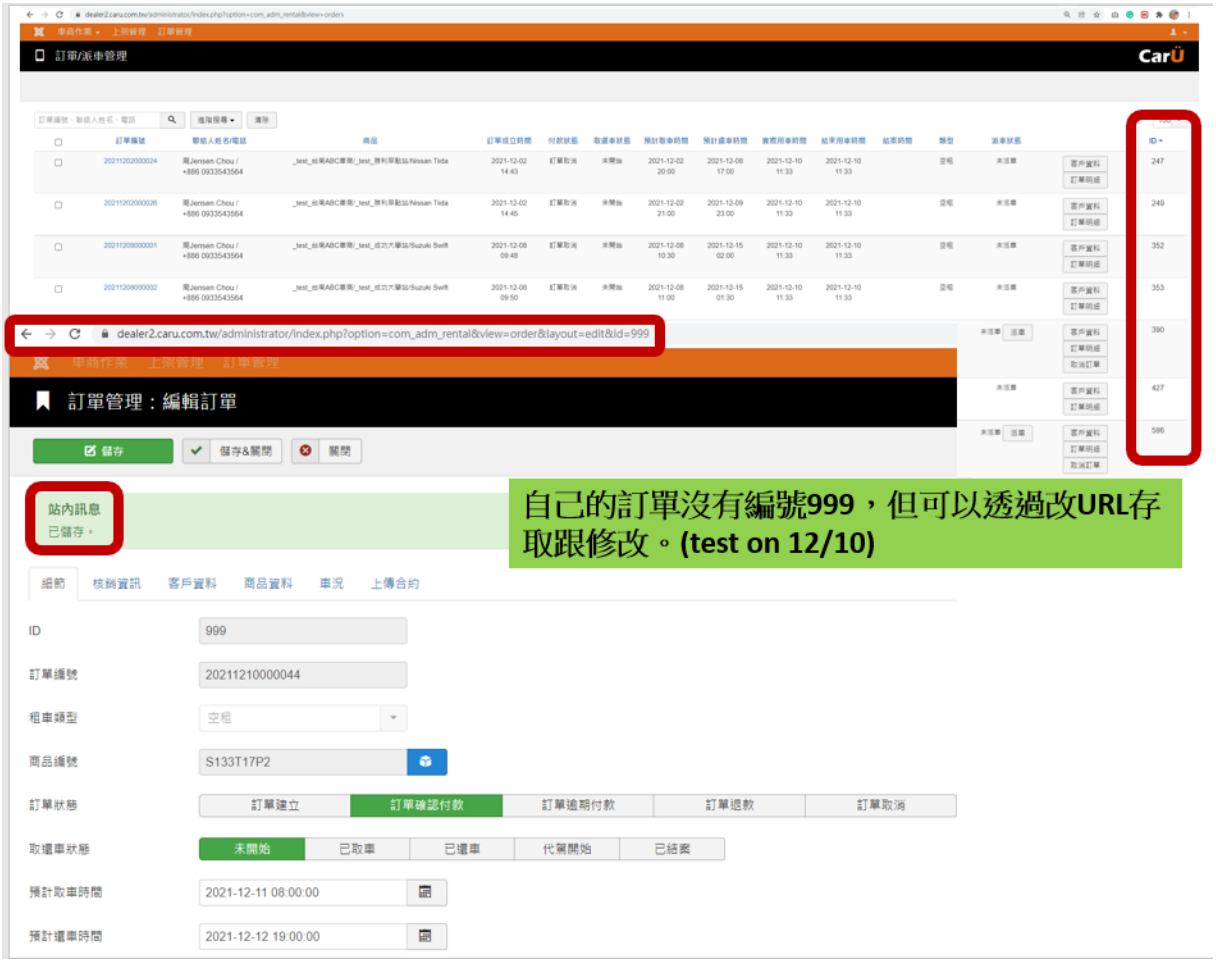


圖 3.2.92 透過修改 URL 取得/修改/其他車商的資料-4

整體改善建議：根據執行相關測試後，功能性與安全性部分提供以下建議給漢名團隊。

- 目前相關操作流程**無前、後關係或權限**的檢查，建議新增檢查點跟對應檢查機制，可以降低大量的錯誤操作。
- 新智慧租車平台上架管理的功能在**非即時性且無相關狀態可檢視**，建議改為即時或是可以有上架狀態的頁面可查詢，以減少車商無法確認資訊所衍生的不安全感。
- 資安問題經檢視有 **SQL injection** 的可能，還有使用者可以透過**修改 URL 檢視跟異動資料、API token 檢查機制無確實動作**，都須於服務上線前完成修訂。SQL injection 部分建議在資料庫查詢的語法要導入物件關聯對映(Object Relational Mapping, ORM)，或是在 Query 的資料內容要特別過濾資料屬性跟類別，排除未經許可的語法；經 URL 檢視與編輯其他車商的資料，此問題建議新增訪問資料時的權限與所有權人的檢查，可以大幅降低不合

規範的操作行為；API token 沒有確實動作，此功能規範為系統內部基本功能，通常是程式的 bug 或是工程師在測試其他功能時，為求方便關閉驗證功能，於系統上線後忘記開啟。建議開發商在使用者接受度測試時(User acceptance testing, UAT)，內部的基礎功能要有個 check list 做逐一反覆測試，已確保功能有確實開啟，不然日後只要軟體有更新版本(如新增功能、系統優化等)，都可能再次發生此問題。

- QRcode 核銷**沒有綁定訂單屬性**(如門市與司機)，導致核銷方無論使用門市或是司機都可以執行，假設是功能特性，建議在操作上有個提醒，以免誤動作。
- 部分功能在**特定操作流程**有問題發生(如取消付款後，購物車的資料會消失)，建議服務上線前要修訂完成。

3. 壓力測試

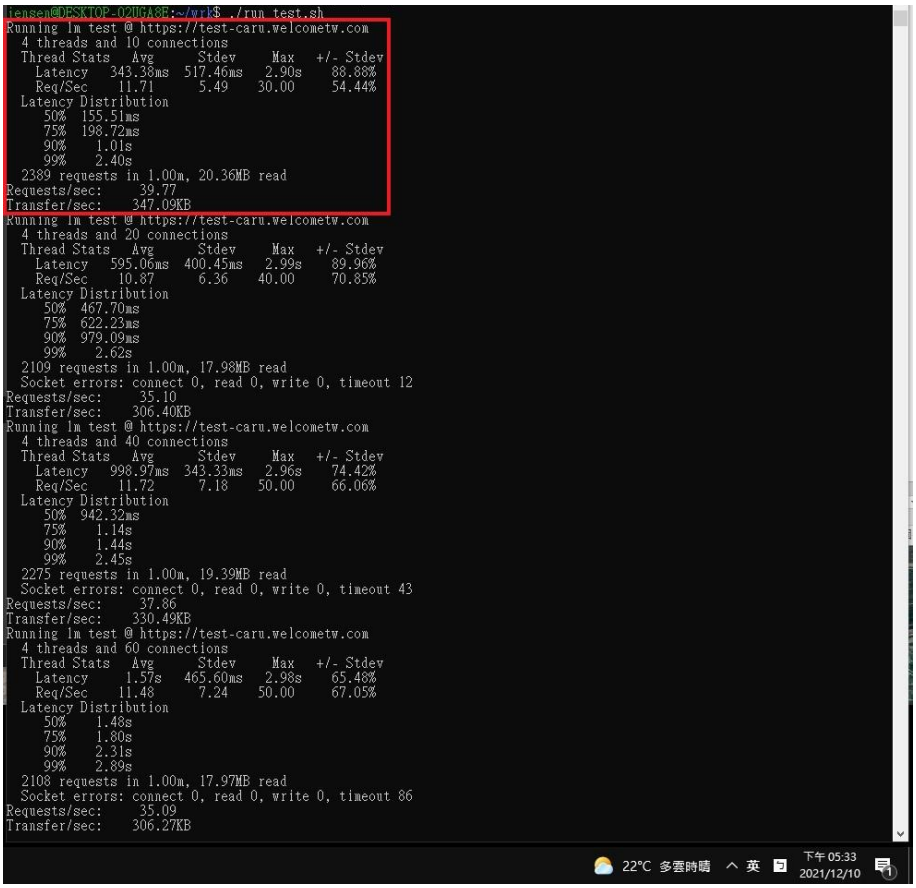
透過工具軟體進行網站基礎負載測試，以適當的 connection request 數量評估系統網站的效能跟穩定性。本次測試選用 wrk，該工具為近期較多人選用的 HTTP benchmarking 測試工具，類似早期使用的 ab (apache bench)或 jmeter。因為 open source 的工具且使用上較容易上手，在 github 上面已經累積至 3 萬多的星星(如同臉書的讚)。

測試標的鎖定在 Web service 的首頁服務，主要測試服務端對於流量尖峰的反應時間，分別為 CarU 平台、新智慧租車平台、行動門市與附駕司機。其測試環境為 AMD Ryzen 5 3600 6-Core Processor 3.59G, 記憶體 32G 的個人電腦，搭配有線網路(至少 100Mbps/sec)，透過 4 個執行緒產生不同連線數 C (測試期間維持開啟的 HTTP 連接總數，分別為 10, 20, 40, 60, 80, 100, 120, 140)，每一筆測試期間為 60 秒。為了保持相關 reports，測試結果以截圖方式呈現於圖 3.2.93~圖 3.2.96。如圖 3.2.93 左上紅框為例，每組測試結果顯示依序為：

- 測試時間與標的，即 1 分鐘跟對應之 URL。
- 測試參數，即執行緒數量跟測試期間維持開啟的連線數量。
- 執行緒的狀態與對應結果(如平均、標準差、最大值、標準差範圍)。
- 延遲統計。
- 每秒連線數統計。
- 延遲分布，其中 50%、75%、90%跟 99%的分佈意為有多少百分比的使用

者(即連線)可以在其延遲時間內收到伺服器的回應，以第一組 75%的 case 即為 0.62 秒。

- 測試期間總共送出的請求數量(request)跟資料讀取量(MB)。
- Socket errors (第二組才有)，主要統計超時(timeout)的數量，即使用者在 3 秒內沒有收到伺服器回應的數量。
- 在這次測試中的每秒請求數。
- 在這次測試中的每秒資料傳輸量。



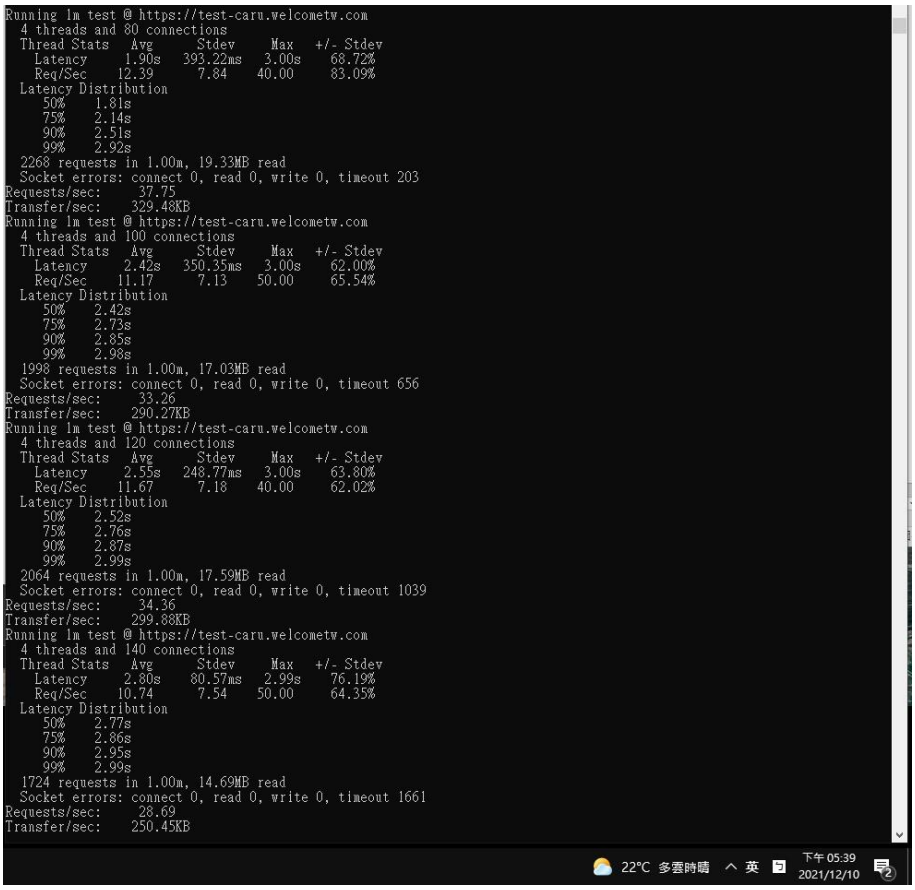
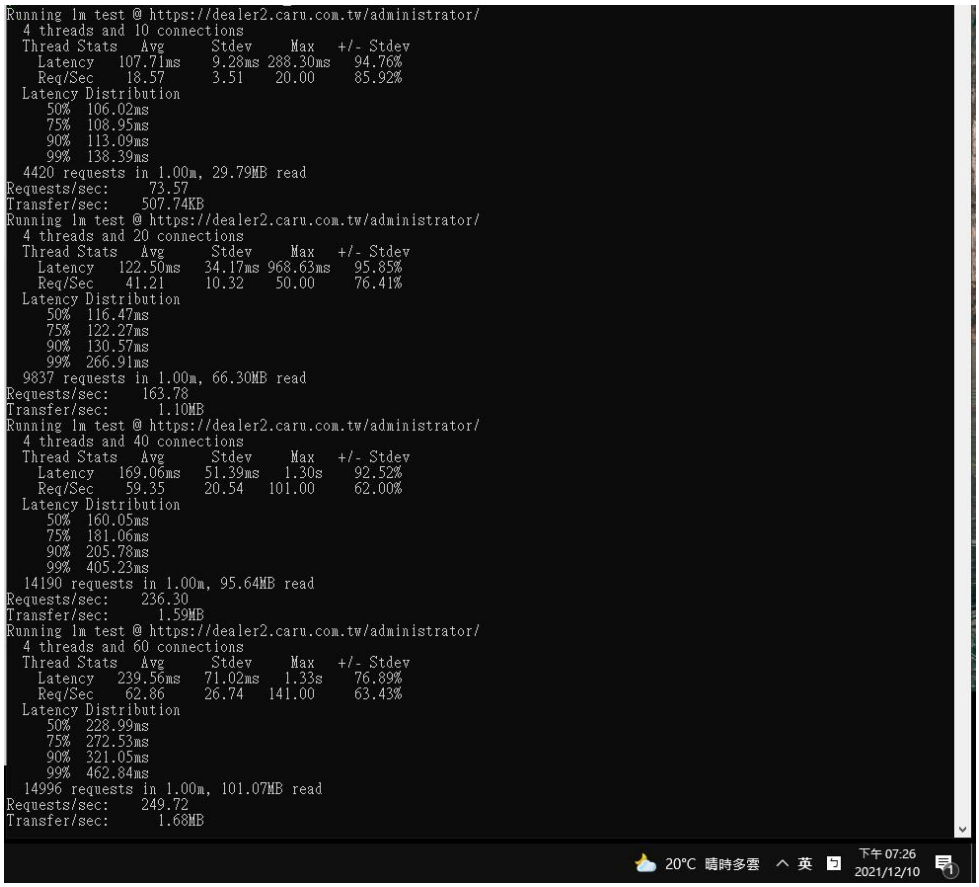


圖 3.2.93 壓力測試-CarU 平台



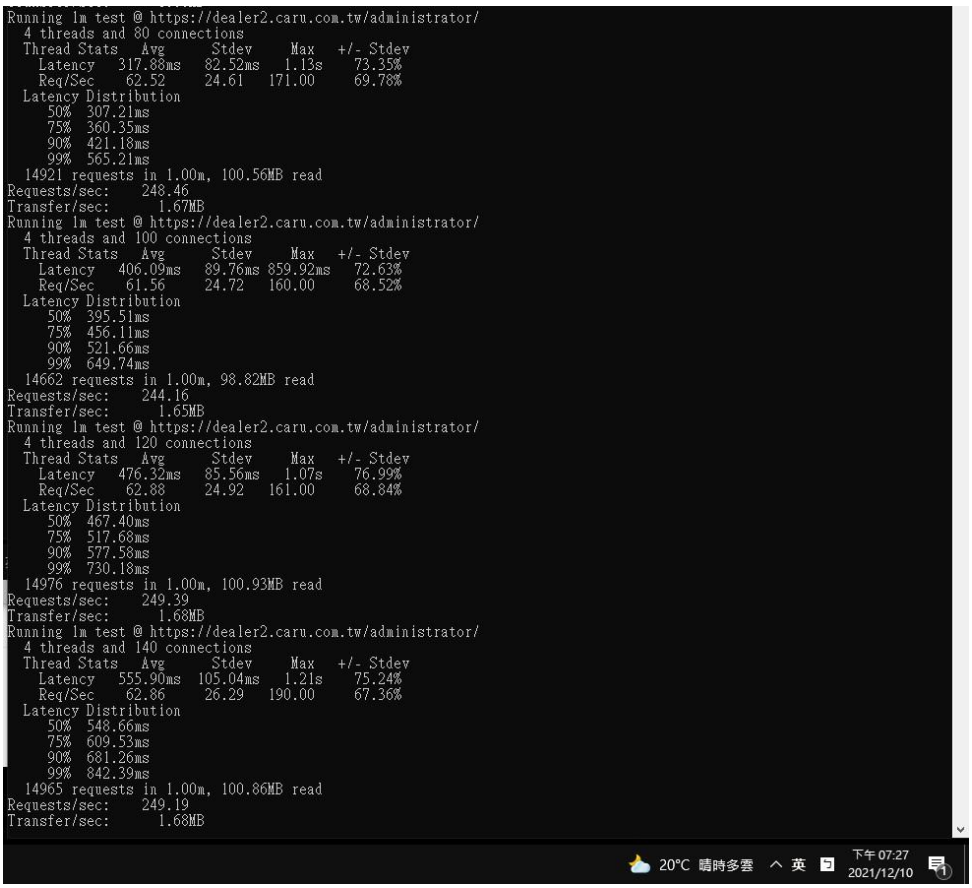
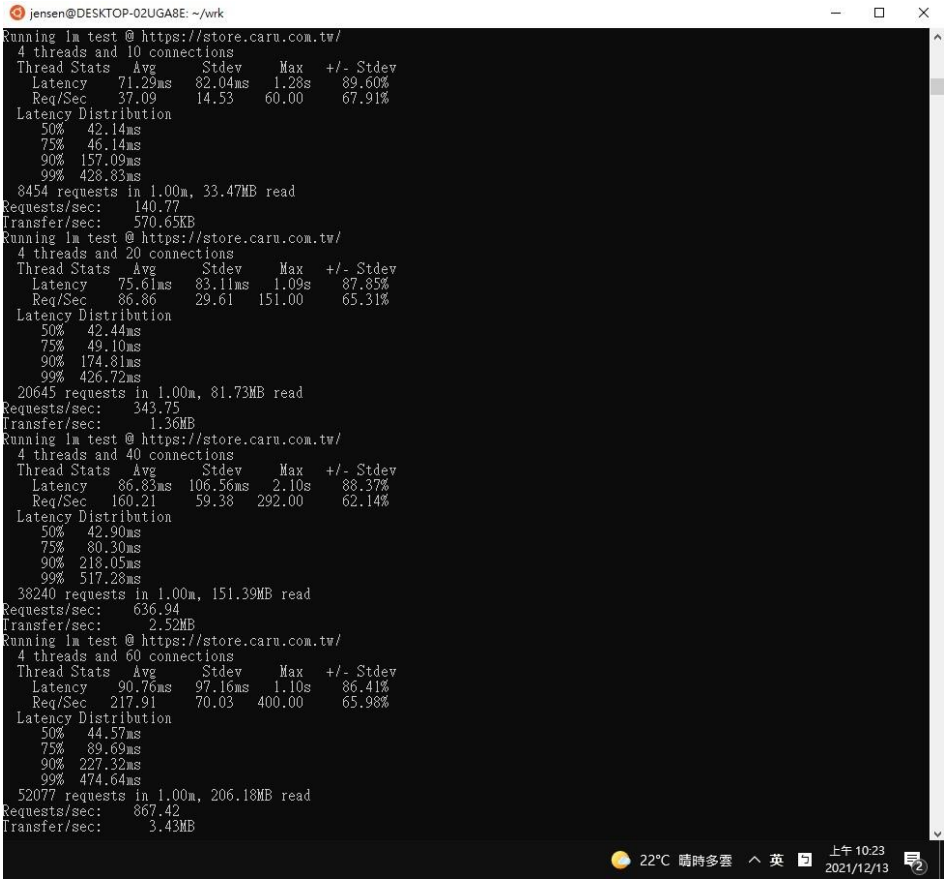


圖 3.2.94 壓力測試-新智慧租車平台



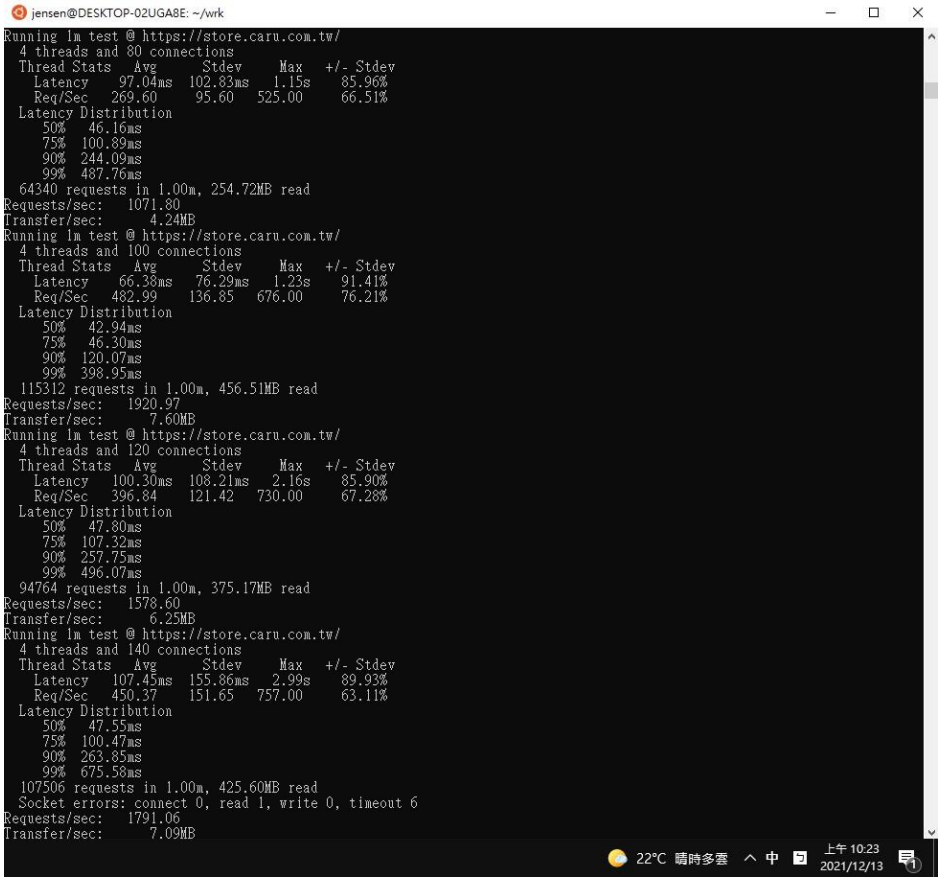
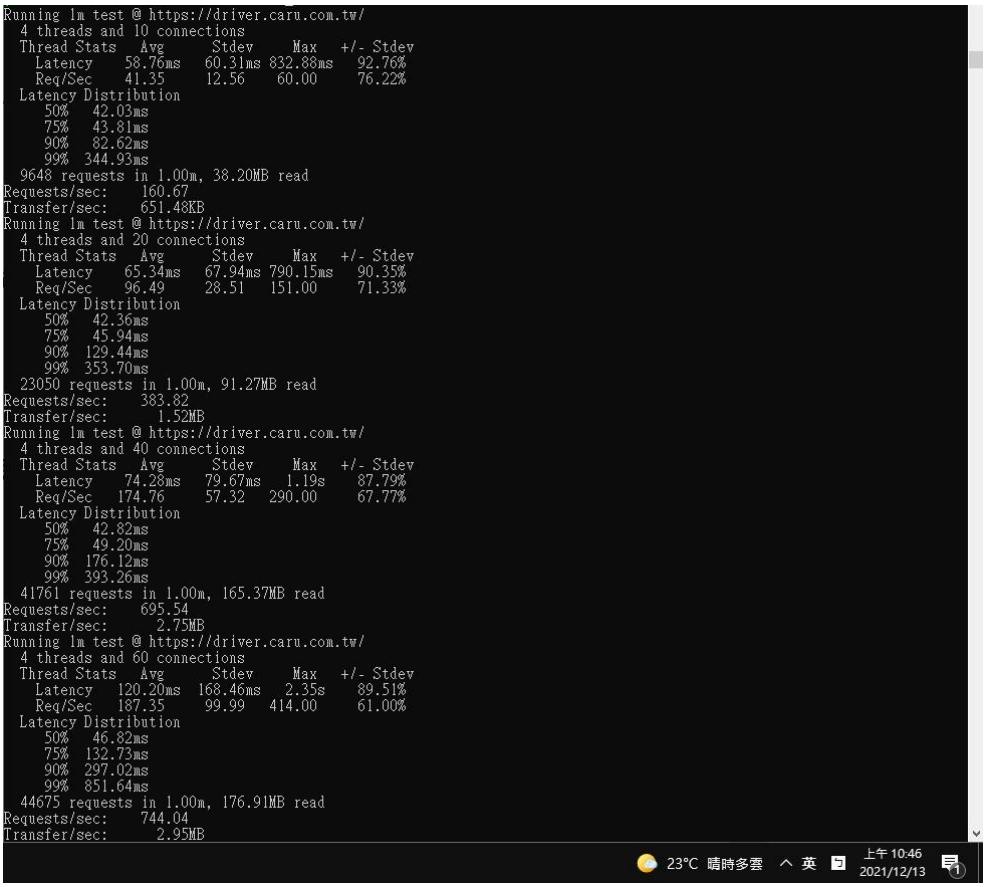


圖 3.2.95 壓力測試-行動門市



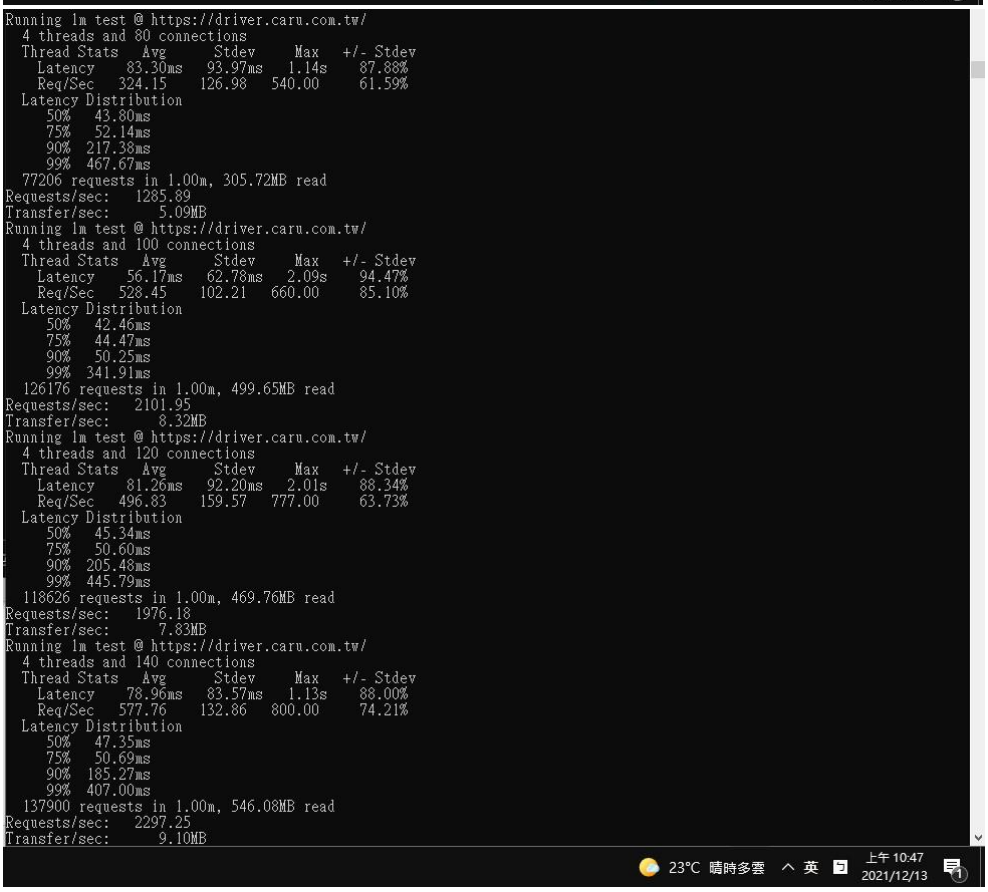


圖 3.2.96 壓力測試-附駕司機

根據測試結果，CarU 平台目前的相關環境配置，大約在每秒鐘有 20 位使用服務的時候，其 90%的使用者可在 1 秒以內收到伺服器的回應。如果超過這個數量可能會明顯的感受到延遲增加，造成不良的使用者體驗；建議未來實際上線運行的時候可以適當增加硬體效能，讓伺服器在處理相關資料時可以減少延遲。其餘三個平台在本次測試中都可以承受其流量負載，無其他顯著問題。

4. 易用性測試

易用性測試並非功能性測試，主要是驗證系統軟體服務的操作流程是否為直覺反應，針對目前系統軟體所提供的常用功能(如租車、核銷等)，透過受測者的操作從旁進行資料的蒐集(如錄製操作者的操作流程)，觀察受測者的行為，記錄並分析受測者行為的感受，綜合相關修正建議進而改善系統軟體服務，使其更佳貼近使用者的操作習慣，進而提高整體易用性。通常一個好的軟體服務會不定期進行易用性測試，以作為軟體流程跟介面的精進修改與調整，透過不斷的修正與調查，提供高品質的系統軟體服務。

本次測試採整合式任務設計，於測試前先擬定目標測試功能(涵蓋小客車租賃服務行位的基本使用功能)，並針對目標測試功能規劃相對應的任務(每項任務須包含目標測試功能)，進而整合成為四項測試情境。受測者需藉由綜合使用各平台功能來完成所指派之任務，任務執行期間測試人員不提供任何操作指示，以判斷該任務之執行是否有效。至於受測者招募數量則參考 Nielsen, et al. (1993)之歸納：若受測者是有類別的，則每個類別至少要有四位；若無，大部分的易用性問題在前六位即可找到。故本次易用性測試共招募十位受測者，其中六位為消費者，四位為車商。消費者主要測試情境一至情境三之內容，而車商主要測試情境四之內容，並同時讓此二類受測者交互操作各介面以利綜合評估。測試情境即任務羅列如下：

一 情境一：消費者租車(自駕)

- 角色：消費者
- 任務：消費者使用手機 PWA/Web 註冊、登入、搜尋、下單、付款
- 使用平台：CarU 前台

二 情境二：消費者取車(自駕)、門市人員核銷

- 角色：消費者、車商門市人員
- 任務：消費者出示 QRcode、門市人員確認訂單狀態並核銷訂單

- 使用平台：CarU 前台、行動門市 app

三　情境三：消費者租車(附駕)、司機接單執行代駕

- 角色：消費者、司機
- 任務：消費者訂購附駕包車、司機核銷訂單並回傳任務執行狀態(開始/結束代駕)
- 使用平台：CarU 前台、附駕司機 app

四　情境四：平台管理人員查看訂單狀態、車商主管派車並上架車輛

- 角色：平台管理人員、車商門市人員
- 任務：查看訂單並派車、上架特定車型每日車輛
- 使用平台：CarU 後台、新智慧租車平台

測試過程中，其中一位車商因年紀較長，不熟悉電腦及手機的操作，故評為測試失敗。測試人員將各項任務的操作流程進行記錄並整理後，製作出「使用性問題嚴重程度分級表」及「受測者反饋紀錄 Log 表」。可同時對照兩表，得知受測者所遇到的問題及其嚴重程度。

(1) 使用性問題嚴重程度分級表

本分級表係用來確認受測者遇到的操作異常嚴重程度；本表之分級是透過**是否成功/失敗、操作順暢度**來判定，由於考量到同一異常事件對不同使用者的阻擋程度不同，故此為受測者提出他認定的判定結果，並綜合測試人員之觀察所得出最終的數據。表 3.2-9 為使用性問題嚴重程度之分級標準。表 3.2-10 至表 3.2-13 則是各情境的使用性問題嚴重程度分級表。

表 3.2-9 使用性問題嚴重程度分級標準

等級	程度描述
1 級-嚴重程度低	使用者能完成任務
2 級-嚴重程度中	完成任務會有困難，有效性、效率皆被影響
3 級-嚴重程度高	會導致任務失敗，沒有其他方法能完成任務

表 3.2-10 情境一：消費者租車(自駕)

受測者/測試任務	註冊帳號並登入	搜尋自駕租車商品	填寫時間、內容	訂購商品	付款
消費者 1	1	2	2	1	1
消費者 2	1	2	2	1	1
消費者 3	1	1	3	1	2
消費者 4	1	1	2	2	1
消費者 5	2	1	2	2	1
消費者 6	2	2	2	2	2
車商 1	1	1	2	1	3
車商 2	1	2	2	2	1
車商 3	2	1	2	2	2

表 3.2-11 情境二：消費者取車(自駕)、門市人員核銷

受測者/測試任務	消費者出示 QRcode	消費者取車拍照上傳	車商核銷
消費者 1	3	2	2
消費者 2	2	3	3
消費者 3	3	1	3
消費者 4	3	1	3
消費者 5	3	2	2
消費者 6	3	1	2
車商 1	2	1	2
車商 2	3	1	1
車商 3	3	3	1
車商 4	測試失敗		

表 3.2-12 情境三：消費者租車(附駕)、司機接單執行代駕

受測者/測試任務	搜尋附駕包車商品	填寫時間、內容	訂購商品	司機核銷	司機開始任務	司機結束任務
消費者 1	2	1	1	1	1	3
消費者 2	2	2	1	1	1	3
消費者 3	1	2	3	1	1	3
消費者 4	1	1	1	3	3	3
消費者 5	3	1	1	1	3	3
消費者 6	3	1	3	1	1	3
車商 3	2	1	3	1	1	3

表 3.2-13 情境四：平台管理人員查看訂單狀態、車商主管派車並上架車輛

受測者/測試任務	查看訂單狀態(CarU 後台)	查看庫存量	上架車輛	查看今日訂單(新智慧租車平台)	進行派車
消費者 1	2	1	3	2	2
消費者 5	1	1	2	2	1
消費者 6	1	1	2	2	1
車商 1	1	1	2	1	1
車商 2	1	1	2	1	1
車商 3	3	1	3	3	3
車商 4	測試失敗				

(2) SUS 易用性量表紀錄

本表透過在受測者操作完所有流程後進行填寫，填寫後按照一固定公式進行換算並得出總分及評級。

題目共有十題，羅列如下：

1. 我想我會經常使用這個產品。
2. 我覺得這個產品過於複雜。
3. 我認為這個產品是簡單好用的。
4. 我想我需要有人協助才能使用這個產品。
5. 我覺得這個產品的功能整合得很好。
6. 我覺得這個產品有很多不一致的地方。
7. 我認為其他人能快速學習使用這個產品。
8. 我覺得使用這個產品很麻煩。
9. 我很有自信地使用這個產品。
10. 我需要學會很多資訊才能使用這個產品。

根據以上題目，以數字 1 到 5 做填答，1 分為非常不同意，5 氛圍非常同意。

SUS 易用性量表詳細評分方式如表 3.2-14 所示。

表 3.2-14 SUS 評分方式說明

評分方式		
項目	**說明**	**分數**
原始分數計算方式	非常不同意	1
	不同意	2
	普通	3
	同意	4
	非常同意	5
奇數正向題計算方式	原始分數-1	
偶數負向題計算方式	5-原始分數	
SUS 總分	(所有題目加權分數相加)*2.5	
SUS 評級	SUS 總分>90	A
	90≧SUS 總分>80	B

評分方式		
項目	**說明**	**分數**
	80≧SUS 總分>70	C
	70≧SUS 總分>60	D
	60≧SUS 總分	E

受測者填寫完畢，經計算後得結果如下表。

表 3.2-15 受測者填寫結果

受測者	**第一題**	**第二題**	**第三題**	**第四題**	**第五題**	**第六題**	**第七題**	**第八題**	**第九題**	**第十題**	**SUS 總分**	**SUS 評級**
Tester 1	2	5	2	3	2	3	2	5	2	1	32.5	E
Tester 2	3	1	4	1	3	4	4	2	5	1	75	C
Tester 3	1	5	1	5	1	5	1	5	4	5	7.5	E
Tester 4	4	2	4	2	3	4	3	2	4	2	65	D
Tester 5	2	2	3	2	1	4	2	2	3	3	45	E
Tester 6	1	4	2	5	2	5	1	4	2	5	12.5	E
Tester 7	5	4	5	1	4	3	4	5	1	4	55	E
Tester 8	5	4	4	4	4	3	4	2	4	2	65	E
Tester 9	3	4	2	5	3	4	2	5	3	2	32.5	E
總體評分及評級											43.3	E

(3) 受測者反饋紀錄 Log 表

本測試也有將所有受測人員反饋之項目(包含操作異常、不順暢、或是建議希望有的操作體驗)進行記錄，作為後續優化之方向參考(如表 3.2-16 所示)。

表 3.2-16 CarU 前台(PWA/Web)反饋紀錄表

受測者	反饋項目
消費者 1	1. 先下單了才發現要註冊並登入。 2. 座位數用數字呈顯比較直覺。 3. 搜尋結果超出頁面卻沒有指示，會找不到。 4. 商品沒有星數作參考。 5. 商品資訊頁面太長，建議分幾頁，或將閱讀重點加粗、換色，以減少單頁需負荷的資訊量。 6. 系統預設先勾選“已同意”定型化契約內容，感受不好。 7. 重複的動作太多，例如：進入商品預約頁面還要再重新填一次預約時間；填完信用卡還要再填一次信箱。 8. 找不到要核銷的 QRcode。 9. 系統連結的拍攝技巧參考網頁僅有文字描述，無法即時從該參考獲得建議。 10. 上傳車況照片之後沒有一個確認機制，不知道已經完成上傳。 11. 勾選進階搜尋選項後，看不到已選擇的過濾項目。 12. 附駕租車搜尋結果頁面沒有顯示駕駛資訊，消費者不知道所租駕駛的長相、年齡和性別等。 13. 附駕租車預訂頁面中仍有「附駕駛」的選項，不知道是否要勾選，勾選了會有兩個駕駛？ 14. 點選「附駕租車」，頁面仍顯示「自駕租車」。 15. 租車平台不太適合用「加入購物車」的說法。 （使用機型為 Xperia 5 ii）
消費者 2	1. 安卓手機沒有將網頁加入主畫面的選項，只能安裝應用程式。 2. 不知道訂單裡有 QRcode，要出示的時候找不到。 3. 車況照片上傳速度過慢，以為沒有上傳成功。若有「正在上傳中」的提示字眼會比較好。 4. 以為改變搜尋條件，下方的搜尋結果就會跟著變，不需要特別按「搜尋」按鈕。 5. 前面已經填寫過要租車的時間，後來又要再輸入一次時已經忘記了。

受測者	反饋項目
	6. 按了「附駕包車」卻還是顯示「自駕租車」的頁面，以為還在舊頁面。 （使用機型為 Sony 1）
消費者 3	1. 填寫日期方式很不直覺。 2. 付款失敗也會有 QRcode，不知道是否需要重新付款。 3. 載入訂單時間過長，要出示 QRcode 時無法載入訂單內容。 4. 按「立即訂購」還要再按一次「預訂」，以為立即訂購就是直接進入付款。 5. 以為「附駕包車」已經含附駕駛的條件，不知道還要再勾選一次「附駕駛」。 6. 網購平台通常在付款完成後，頁面會回到訂單位置。這個平台還要再重新點進「會員資訊」裡的「我的訂單」才找的到。 7. 建議在第一次使用此 app 時可以附有操作小提示。 8. 選「附駕包車」時無法得知駕駛的性別會有疑慮。若顯示簡單的儀容照片（如 Uber eats）會比較安心。 9. 租車時沒有定位服務比較不方便。 （使用機型為 Vivo v17）
消費者 4	1. 熱門租車等的卡片定位點太多。 2. 選擇取車日期後，還車日期的視窗直接跳出，會反應不過來，不知道現在已經要選還車日期。 3. 不懂為何點選「預訂」後還要重複填寫時間。 4. 「到府送車」、「甲租乙還」、「高鐵取車」、「機場取車」等加購服務在勾選處均可以複選，但有些服務無法同時存在。應有勾選某選項後，有些選項不能勾選的機制。 5. 填寫取還車日期和時間時，以為取還車時間按鈕僅是說明左方欄位的日期選擇，故漏選了時間。 6. 註冊時電話號碼沒有打正確格式還是可以通過，下單時才顯示不正確。 7. 已經選過要租用的車輛，才跳出要註冊，註冊後選項就被清除。 8. 付款方式沒有 Apple pay，還要特別輸入卡號很麻煩。 9. 「我的訂單」應該要是主選單的選項，藏在會員資訊裡會找不到。 10. 介面一直把「我要退款」顯示在非常明顯的位置，看起來有些奇怪。 11. 一開始登入進去的畫面沒有顯示是附駕駛還是沒有附駕駛的租車。

受測者	反饋項目
	12. 附駕包車頁面裡還有「附駕駛」的選項，不知道要不要選。 13. 整體使用上算快速。 （使用機型為 Iphone XS）
消費者 5	1. 熱門租車等的卡片定位點過多。 2. 輸入過的資料不會自動記住，比如手機載具條碼。 3. 沒有可以搜尋特定車商商品的篩選功能。 （使用機型為 Iphone 7 plus）
消費者 6	1. 不懂訂單狀態和交易狀態的差異。同時顯示「付款成功」和「已確認，待付款」。 2. 想要退款，卻顯示「退款申請失敗」。 3. 搜尋結果頁面很長卻還有分頁，建議滑到底就直接刷新，或是多幾頁分頁。 4. 清除勾選加購項目後，勾選框仍然會顯示淡淡的打勾殘影，以為沒有清除成功。 5. 不清楚訂單上的「已完成」是甚麼樣的狀態。 6. 推薦熱門租車和最新租車的意義不明，因為消費者並非在熱門租車的地點。 7. 點進商品頁面中沒有不同的車齡、里程數和價格，卻無法直接訂購，還要再按一次「預定」。 8. 使用限制及注意事項內容太冗長，建議改成可展開/收合之按鈕，要看的消費者自行點開來看。 9. 重複選填時間很讓人困惑。 10.「帶入會員資料」太小容易忽略，導致再重填寫一次資料。 11. 已訂購的商品資訊收合起來，不會注意到，且商品名稱為一串代碼，不是車型等等。 12.「我的訂單」應該要在主選單直接看到。 13.「最新消息」分頁裡還有多個分頁，消費者不會想要點那麼多次去看。 （使用機型為 Google Pixel 4a）
車商 1	1. 有些跑車是兩座或四座，但選項只有五座以上。 2. 到府送車沒有填寫地址的欄位。 3. 附駕駛的部分應新增半夜的價格，半夜價格應更高。 （使用 Web）
車商 2	1. 若要續租要上平台預約還是連絡車商？平台上沒有續租的服務。 2. 各車商合約在預定時就要給消費者看到。 3. 訂單總計價格和實際價格有所出入。 4. 消費者不會想要花時間拍照上傳，幾乎都採錄影方式，錄車

受測者	反饋項目
	外及車內做自我保障。 （使用 Web）
車商 3	1. 無法針對指定車商去做搜尋。排序置頂的是否有額外付費？ 2. 平台沒有提供付現功能。 3. 區域選擇只有縣市，但範圍仍然太大，若有縣市底下的行政區選擇會幫助消費者縮短搜尋時間。 4. 提供加購保險服務滿貼心的。 5. 訂購資料每個欄位都強制填寫比較麻煩。 6. 「加入購物車」的說法用在租車平台比較奇怪。 7. 訂單成立後應提示 QRcode 位置。 8. 車輛通過 ETC 平台端怎麼紀錄？ （使用機型為 Samsung note 10 plus）

表 3.2-17 行動門市 app 反饋紀錄表

受測者	反饋項目
消費者 1	1. 核銷的功能位置不明顯，花了比較多時間找。 2. 可連結至駕駛駕照查詢功能不錯。 3. 下排功能鍵太小。 4. 登入進去先顯示核銷畫面比較直覺且快速。 （使用機型為 Xperia 5 ii）
消費者 2	1. 用網頁版掃描時顯示相機無法使用，用 app 才可以。 2. 掃描完左邊的按鈕寫「掃得很重」，不知道是甚麼意思。 3. 有駕照現況查詢很方便。這就表示消費者不用帶駕照嗎？如此是否會有安全疑慮？ （使用機型為 Sony 1）
消費者 4	1. 不清楚「已核銷」和「未開始」同時顯示是甚麼意思。 2. 「今日應取車及還車」之訂單點選了只有該訂單變深色的反應，沒有其他改變，不知道是不是故障沒有反應。 3. 相機無法使用。(網頁版及 PWA 版均無法) 4. 無法使用 QRcode 核銷，想要使用人工核銷卻顯示「無未核銷訂單」。 （使用機型為 Iphone XS）
消費者 5	其他車商的訂單還是可以核銷成功。 （使用機型為 Iphone 7 plus）

表 3.2-18 附駕司機 app 反饋紀錄表

受測者	反饋項目
消費者 1	核銷完頁面顯示無執行中任務，故無法結束任務。 （使用機型為 Xperia 5 ii）
消費者 2	找不到結束任務功能。 （使用機型為 Sony 1）
消費者 3	應該要有保持登入的選項，或車商可核發證件供掃 QRcode 登入。 （使用機型為 Vivo v17）
消費者 4	相機無法使用。(網頁版及 PWA 版均無法) （使用機型為 Iphone XS）
消費者 5	1. 無附駕駛的訂單仍然成功核銷。 2. 核銷完後頁面顯示「無執行中任務」。 （使用機型為 Iphone 7 plus）
消費者 6	無附駕駛的訂單仍然成功核銷。 （使用機型為 Google Pixel 4a）

表 3.2-19 CarU 後台反饋紀錄表

受測者	反饋項目
消費者 1	付款狀態與前台顯示不一致。 （使用 Web）
消費者 6	1. 申請退款後，消費者要如何得知可以取回費用？ 2. 訂單中沒有顯示所選車商。 （使用 Web）

表 3.2-20 新智慧租車反饋紀錄表

受測者	反饋項目
消費者 1	1. 按下「儲存」按鈕以為是「儲存並關閉」，後來才發現沒有關閉。 2. 找「派車」按鈕花了不少時間。 （使用 Web）
消費者 3	1. 最左的縱排和最上的橫排用不同顏色，直覺會以為只是標

受測者	反饋項目
	題，不會知道可以點選。有些不同顏色的按鈕按了卻沒有反應。 2. 不知道可以點選「訂單成立時間」作日期的過濾。且點了兩次才有反應。 3. 現場拍攝的車況照是採用人工審核嗎？若是，是否要等待一段時間？ 4. 現在都有自動辨識車頭車尾的儀器，若導入則可節省拍車況的環節。 （使用 Web）
消費者 5	1. 上架數及庫存數多於車輛數是否不合理？ 2. 邏輯上新訂單會在最上方，但系統顯示在最下方，因此會找不到。 3. 沒有附駕駛的訂單，在取還車狀態中卻顯示「代駕開始」。 4. 不知道怎麼回到控制台。 5. 無法從控制台直接對今日訂單做派車，還要再點進訂單管理很不直覺。 6. 批次上架後數字不會立即改變，無法確認是否上架成功。 7. 若是同樣的車型，無法從上架數量中得知上架的是哪一輛。 8. 編輯上架車輛數視窗中，確認按鈕的文字敘述為「處理」，有點奇怪。 9. 要編輯上架車輛數時，不知道可以點選「車型」種類去做編輯。 （使用 Web）
消費者 6	1. 控制台只能看庫存不足的商品，無法連結到補庫存的頁面很不直覺。 2. 顯示數量的藍底白色數字會被誤以為是可點選的按鈕。 3. 不清楚右上方的數字是單頁資料筆數。 4. 用單一車商帳號登入，上架管理的車商選單中卻有其他車商。 5. 訂單管理中的訂單顯示「已還車」，卻還可以派車。 6. 無法從控制台直接對今日訂單做派車，多了一步點進訂單管理的程序。 7. 不清楚怎樣才算上架成功。 （使用 Web）
車商 1	1. 建議訂單中的消費者資訊要加上身分證字號，以利車商辨認身分。 2. 消費者留電話後，平台有無傳送驗證訊息功能？

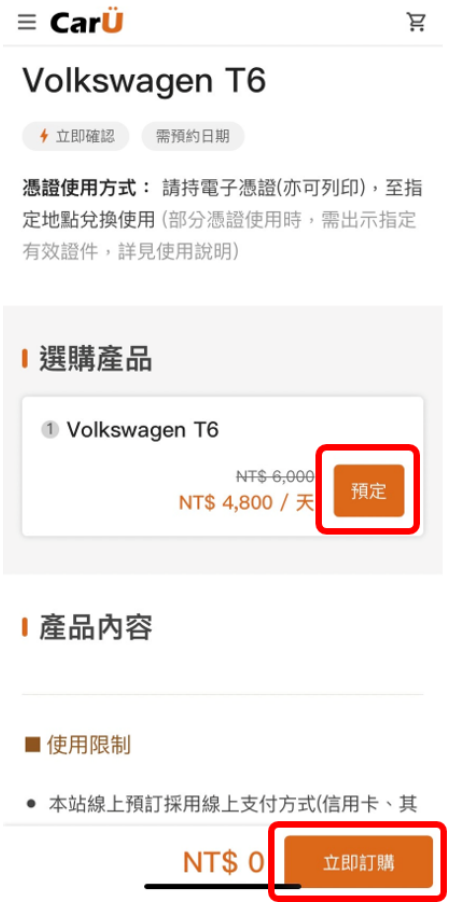
受測者	反饋項目
	3. 控制台除了當日應取/還車，應增加本週/月應取/還車，知悉要來一週/月的狀態，如此才能得知是否有分店重複派車的狀況。 4. 隔日應取/還車是否有提醒機制？因平時不一定會主動看電腦。 5. 要續時要從平台重新預定嗎？還是直接跟司機說或請車商處理？ 6. 消費者的罰單會在還車後才寄到，若車輛要被吊扣，是平台處理還是車商處理？ （使用 Web）
車商 2	1. 上架管理的 ID 排序意義不明。 2. 是按鈕的不像按鈕，不是按鈕的卻長得像按鈕，讓人很困惑。 3. 標籤和按鈕混在一起，主選單的按鈕顏色對比不明顯，不知道它是按鈕。 4. 編輯批次上架後數量沒有變多，不知道要怎麼確認上架狀態。 5. 若消費者續租，平台端會在哪裡有紀錄？平台需要說明超過時間的收費原則。 6. 續租的費用是否需要經過平台再付給車商？若要經過平台刷卡，多次續租將會是一個重複且麻煩的手續。 （使用 Web）
車商 3	1. 已輸入之車輛及站點資訊都無法顯示於手機版頁面。 2. 輸入新增的車輛資訊後，有「儲存」、「儲存&關閉」、「儲存&新增」三個按鈕，不知道要按哪一個。 （使用機型為 Samsung note 10 plus）

(4) 實際測試相關功能畫面截圖：

針對上述受測者之測試回饋，此小節提供部分對應畫面之截圖與描述。

圖 3.2.97 註冊-無先行提示密碼設定限制；手機格式錯誤仍可註冊成功

圖 3.2.98 搜尋商品-進階搜尋中已勾選的項目未顯示在搜尋畫面中



使用者常按了立即訂購才發現要再按一次預訂，此流程不符合邏輯 **(test on 12/5)**

圖 3.2.99 訂購商品-按「立即訂購」的邏輯是直接進行付款，不需再按「預定」

圖 3.2.100 填寫取還車日期-不知道要選擇下方日曆的日期因而重複點選日期欄位

圖 3.2.101 勾選加購服務-取消勾選框內仍有打勾殘影

圖 3.2.102 取還車照片紀錄-上傳速度過慢且無上傳中之提示

圖 3.2.103 我的訂單-我的訂單通常會在主選單內，而非藏於第二層選單中

圖 3.2.104 我的訂單-訂單無 QRcode 之查找提示

圖 3.2.105 行動人員核銷-核銷後左下方的按鈕顯示「掃得很重」

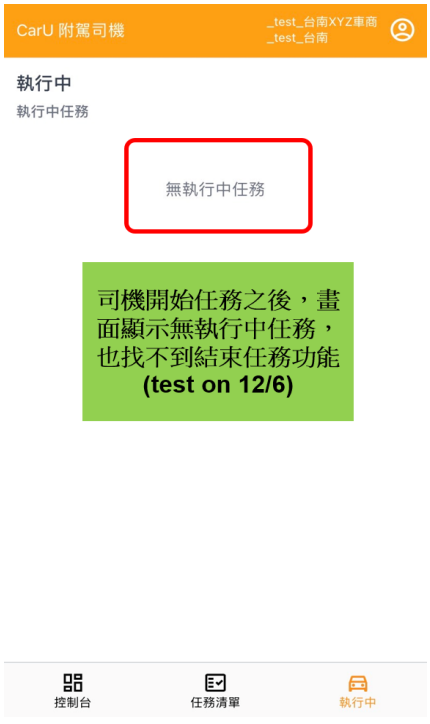


圖 3.2.106 附駕司機核銷-開始任務後無執行中任務，且找不到結束任務功能

圖 3.2.107 後台訂單管理-訂單狀態與付款狀態資訊不一致

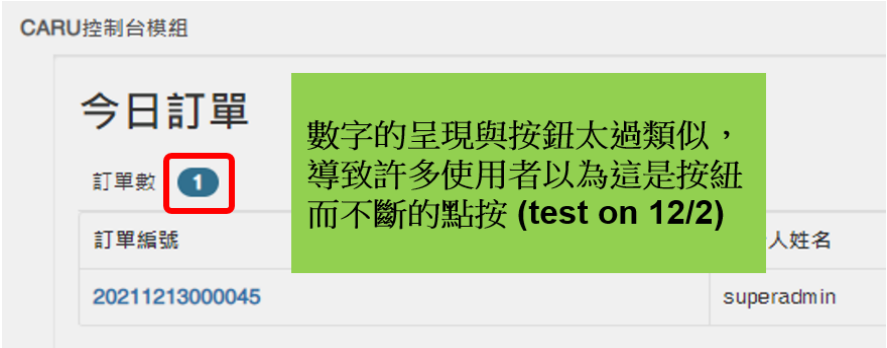


圖 3.2.108 控制台-數字的呈現方式應與通用性之按鈕設計有所區別

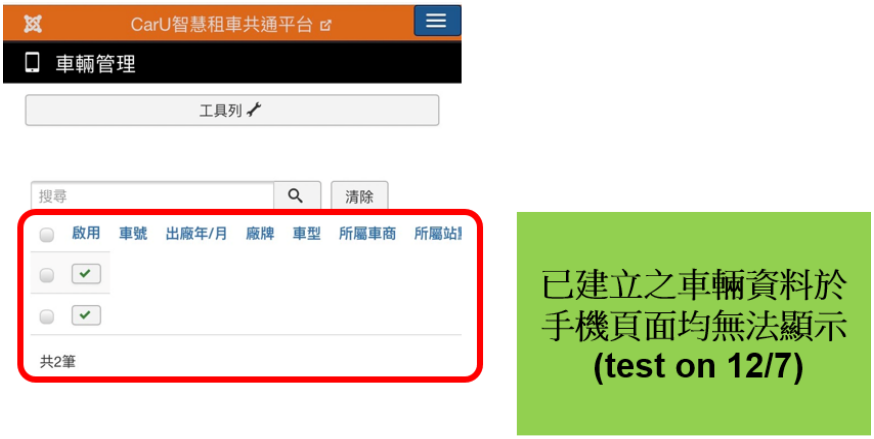


圖 3.2.109 車輛管理-手機版頁面無法顯示已建立之內容

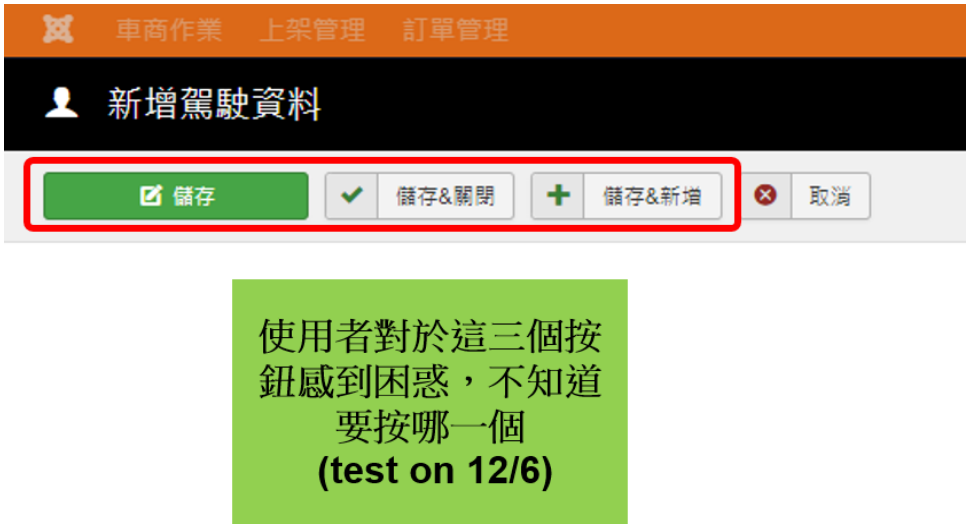


圖 3.2.110 新增駕駛資料-不同的儲存按鈕令使用者感到困惑

圖 3.2.111 上架管理-使用者不清楚上架流程，車輛總數小於上架及庫存數

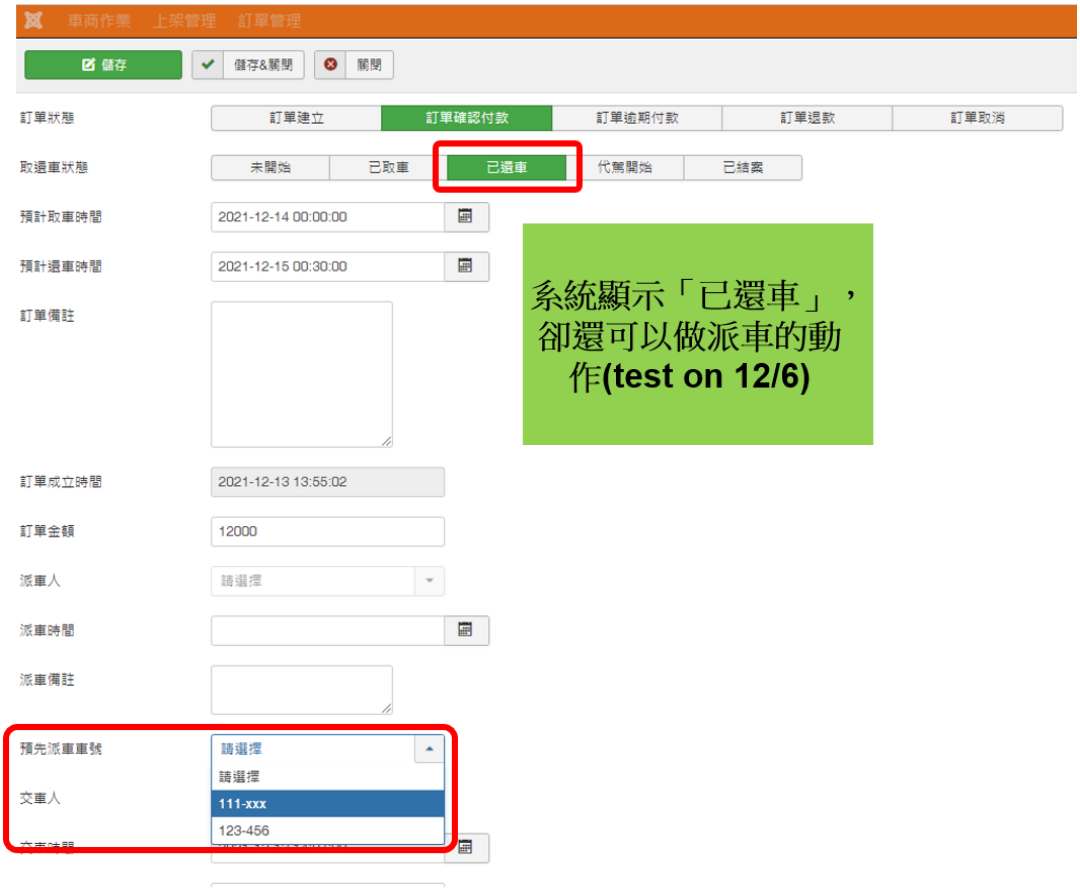


圖 3.2.112 訂單管理-系統顯示「已還車」卻仍可進行派車

圖 3.2.113 訂單管理-空租訂單卻顯示「代駕開始」

圖 3.2.114 訂單管理-過濾時間之功能不明顯

本次易用性測試結果，依照「使用性問題嚴重程度分級表」及「SUS 易用性量表」可得以下結論：

(1) 使用性問題嚴重程度分級表

經由分級表可知，前台的部分最令受測者感到困惑的步驟是「查找 QRcode」，多半是因找不到其位置，或是沒有立即於訂單中取得 QRcode 造成。其次，填寫日期及時間的流程因不符合操作邏輯，導致受測者需額外花費較多的時間來完成。另外，受測者也經常未注意到應先行註冊再做搜尋商品及下單的動作，總是在下單後才跳出註冊及登入的頁面。然而於註冊後，剛才所填入的選項內容卻全部清除，需再填寫一次，令受測者感到繁瑣及麻煩。新智慧租車平台的操作流程則是以上架車輛有較多異常之部分。其中附駕司機 app 中的「結束任務」功能，因在測試期間尚未完成，故分級表上均評為 3 級。除此之外，平台也有些許重複性卻意義不明的操作流程，建議參照受測者反饋表，優先修正評分以 2、3 為多的項目。

(2) SUS 易用性量表

SUS 評量表以 68 分為及格界線。本次測試中綜合得分為 43.3，判定為 E 級 (不及格)。

(3) 改善建議

- 有些流程在無指示狀態下，使用者難以自行完成，或是得費時完成。對於初使用的使用者而言，**建議可加入簡易操作指示或步驟指南**，讓操作

流程更無痛順暢。(CarU 前台)

- 重複性高的動作建議省略，例如：重複填寫時間、重複勾選附駕駛、重複填寫 email 等，**否則可能導致使用者忽略該步驟或感到繁複而放棄使用**。(CarU 前台)
- 部分用詞與實際**操作邏輯不符情形**，例如：點選「立即訂購」並非直接跳付款頁面，建議再重新定義修正。(CarU 前台)
- 按鈕的功能**應避免重複及複雜化**，例如：多種儲存按鈕，常令使用者感到困惑。(新智慧租車平台)
- **同樣顏色的文字**，有些是可點選的功能，有些不是，建議應有所區分，否則使用者會因忽略其功能而無法完成任務。(新智慧租車平台)

更詳盡之內容請詳如附件五。

3.3 監督審驗

3.3.1 品質監督審驗工作與流程

德國萊因公司於本計畫中負責監督、提醒、審核及追蹤建置計畫之各階段品質要求，並管控相關問題與議題，依據德國萊因公司之品質管理要求，除了控管建置商提送之文件(如契約相關文件或系統設計規格書、系統整合測試計畫書、期中與期末報告書、內部整合測試報告、壓力測試報告、標準 API 技術文件、後臺管理操作手冊、系統維運操作手冊、使用手冊等各式系統品質文件)，也同時確認建置商文件的品質，表 3.3-1 為該公司初步規劃將於每份文件均檢查的項目，確保建置商的文件品質一致性。

表 3.3-1 因應品質管理要求的文件審查項目

項次	說明	檢查依據
1	識別	檢查文件編碼、版次、日期等是否正確
2	狀態	確認核准狀態
3	修改紀錄	是否有標註各版次修改歷程記錄
4	作者	是否有提及該負責文件的內容之擔當
5	一般結構	文件格式是否依照核定或合意之文件管理計畫
6	範圍、對象	是否說明文件範圍、適用對象
7	正確性	文件內容與契約規範是否符合

德國萊因公司對專案品質監督審驗的主要目標，是充分滿足客戶現階段與未來可能的需求，並盡可能超出顧客的期望; 以下為德國萊因公司針對本計畫以概略說明 IV&V (Independent Verification and Validation，獨立驗證與確認) 所採用的方法與目的。

如何協助本計畫達到驗證要求並完成認證，總地來說，認證係以法規、法令、標準、契約、品質文件以及檢查結果等正式文件為依據，執行 IV&V，而本計畫認證方式採符合性認證機制，以下逐一說明認證之依據、監督審驗機制以及符合性認證之方法。

1. 認證依據

認證主要依據法規/法令、標準、契約/品質文件、檢查結果和其他專案經驗等，如下逐項說明。

(1) 法規/法令

法規/法令具有強制效力，無論於專案中各階段執行各項作業皆需符合國內相關法規之要求。

(2) 標準

以測試、資訊安全分析等工作為例，認證時主要關注是否依循工作說明書、技術規範書等文件要求，並確認是否遵循上述文件內所要求採用的國內標準、手冊、作業規範等。

(3) 契約/品質文件

本計畫所依循之招標契約、建置商內部品質文件等，德國萊因於收到文件時，將確認來源資料的可信度、正確性、一致性及完整性，並考量其適用性，以作為認證的證據之一。

(4) 檢查結果

針對關鍵零組件或關鍵系統架構所進行的現地驗證紀錄，或檢核計畫相關單位提出之檢查報告也是認證的重要依據，過程中特別注意建置商使用之硬體規格是否合乎規範、軟體工具是否合法使用、系統架構是否符合契約要求等，同時應詳實記錄並保全查核過程產生之佐證。

(5) 其他專案經驗

整合性測試或資訊安全檢查若遇及尚無標準可供遵循，此時須仰賴驗證單位過往之經驗，因應專案特性綜合考量實用性、效率、成本效益及系統價值需求等來建議可行方案。

2. 監督審驗

(1) 德國萊因公司各階段品質監督審驗工作

各階段工作檢核項目除將依照計畫需求與應遵循之標準進行相關查核作業，德國萊因公司亦將使用檢核表單逐一檢查關鍵文件的內容是否完整、是否符合標準要求，此外，現地驗證與定期提交的進度報告也是檢核評估的佐證資料之一，德國萊因公司依過去執行 IV&V 之經驗，說明針對不同項目的檢核評估依據。

執行 IV&V 符合性認證之驗證方法包括以下三大主軸，分別為 1.確認系統品質管理方式、2.確認系統設計文件、系統保證文件、系統測試文件及系統資訊安全文件等功能文件、3.現地見證/稽核，其方法及目的如以下概略說明及參照：

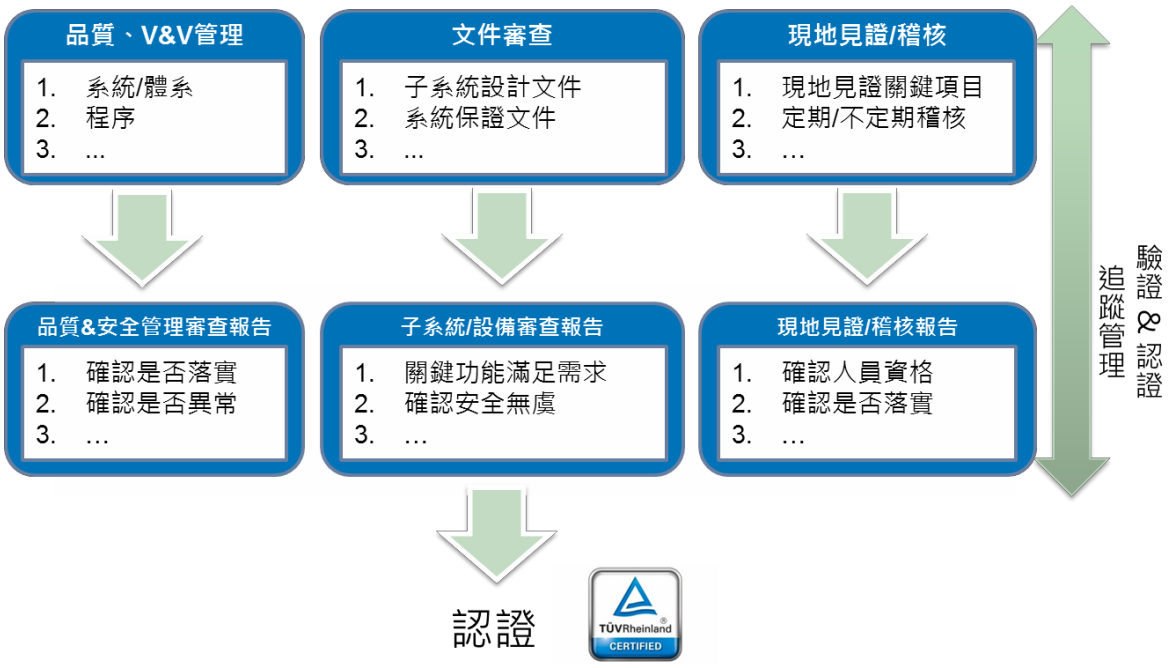


圖 3.3.1 IV&V 評估方法與目的

(2) 確認系統品質管理方式

A. V&V 計畫/資訊安全計畫

(a) 是否有適當的 V&V 計畫；

(b) V&V 組織中成員的職責是否清楚定義；

(c) 計畫是否說明清楚且易於瞭解；

(d) 是否已清楚定義各項應提交文件之需求；

(e) 是否已設計適當的控制手段驗證計畫需求，例如變更控制與型態管理。

B. V&V 文件/資訊安全文件

(a) 是否已界定出計畫所需之相關文件；

(b) 這些文件是否已被產出；

(c) 關於 V&V 與資訊安全文件的計畫是否恰當；

(d) 是否已界定應產出各 V&V 與資訊安全文件的權責單位；

(e) 相關文件是否由應負責的人員產出；

(f) 文件是否有適當、一致標準。

C. 分包商管理

(a) 是否有評估分包商能力的方法；

(b) 此方法是否落實於審核所有分包商；

(c) 每個分包商是否都被給予資訊安全目標或需求；

(d) 是否每個分包商都提出了 V&V 計畫及資訊安全計畫；

(e) 是否依據整體計畫的 V&V 計畫與資訊安全計畫內容來審閱並核准各分包商的 V&V 計畫與資訊安全計畫；

(f) 是否有任何分包商未遵照相關規定的證據。

(3) 系統文件審查

A. 建置管理相關文件

(a) 系統功能

i. 系統規格書是否依照招標契約進行規劃並符合其需求；

ii. 系統測試計畫是否完善確認並依循系統規格書之項目制定；

iii. 系統測試之過程是否妥善保存並具再現性；

iv. 系統是否保留擴增彈性以因應未來趨勢變化；

v. 系統安全是否列入規格中，並具備足夠的資訊安全維護機制；

vi. 系統是否有需符合法規/法令之要求項目。

(b) 建置及維修

i. 系統資訊安全資料及程序，主要評估正常及緊急操作下，相關建置、維修人員所使用之保護裝置及緊急設備相關作業程序等是否適當；

ii. 評估各類設施維修作業(包括預防性與矯正性)之執行步驟、程序、參考資料，以及人力需求、技術層次、工時、所需工具及各設備設施之系統架構圖、功能簡圖或方塊圖、訊號及控制之流程圖等是否詳實；

iii. 備品安全存量之計算依據，例如用途、使用年限、數量、參考價格及待料時間等；

iv. 系統復原手段，包括處理原則、採行方案、決定依據等；

v. 維修所需之人力需求，包括組織、編制人數與人員資格；

vi. 應載明資訊是否完備，例如設備商之緊急連絡方式等。

(c) 人力資源計畫

i. 各類專業人力資源的評估方式，如何確保設計、建置、維修以及管理之各類專業人員所須具備的專長；

ii. 建置、維修、管理、支援人員的訓練，例如先期訓練計畫的建置、設施與系統之操作維護訓練及緊急事故處理；

iii. 評估提出之訓練所需組織及訓練課程、設備等；

iv. 評估訓練合格標準、通過訓練之能力測驗與評定。

B. 測試階段評估項目

(a) V&V 計畫與資訊安全計畫中所要求的測試是否被執行；

(b) 測試所發現的危害是否被記錄，是否研擬出對應的預防與減輕措施；

(c) 測試程序是否能適當展現系統的完整性與資訊安全性。

C. 其他展現（Demonstration）階段評估項目

(a) 執行展現之組織與權責是否恰當；

(b) 資料記錄與修正辦法是否正確；

(c) 評估假設之合理性，例如選擇展現維修度之任務類型；

(d) 確認各項展現作業是否依已核定之計畫書執行；

(e) 執行過程中之各項缺失是否加以登錄並追蹤管制；

(f) 執行之結果是否滿足預期之目標；

(g) 失效分析與後續之改進行動。

(4) 現地見證/稽核目的與流程

稽核之目的在於確保廠商人員資質、獨立性，並抽樣檢查各項程序機制的落實程度；現地驗證則主要於製造、安裝、測試及試運轉階段執行，目的包含：

A. 確認招商文件中對於資訊安全性、功能性及網要性要求已被達成。

B. 確認所有系統功能以及資訊安全驗證的結果，皆可滿足計畫所規劃的目標值。

C. 要求廠商展示所有原始高風險的危害項目及剩餘高風險危害項目，並確認已納入驗證程序中，以確保所對應的危害減輕措施，在具佐證資料下展現其已滿足要求。

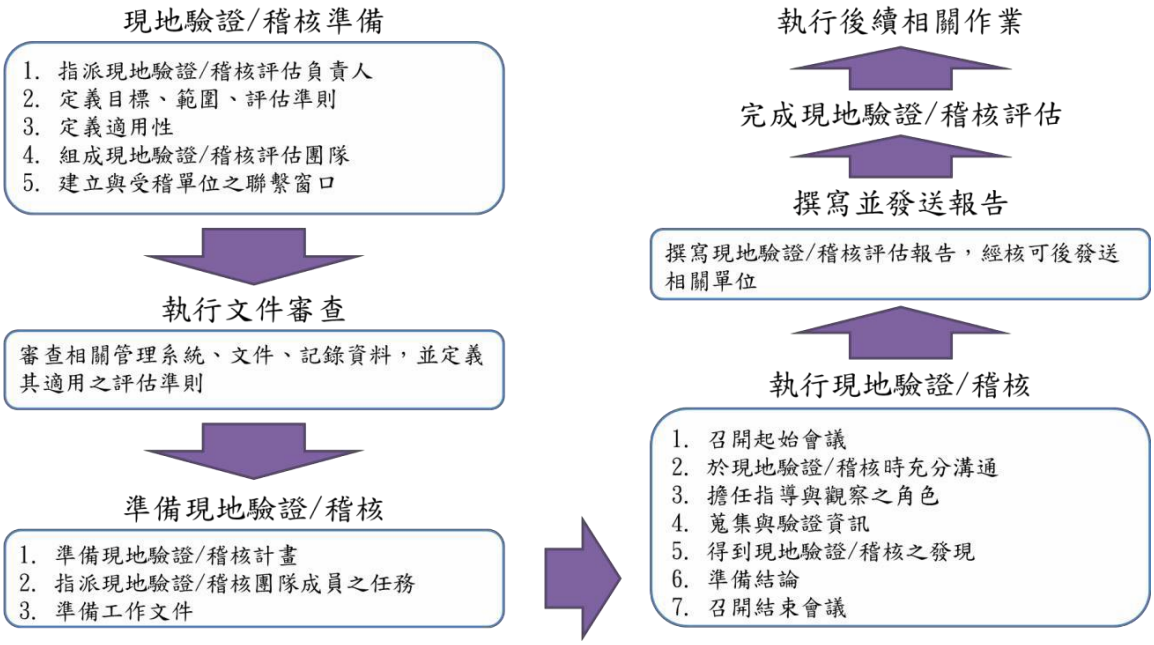


圖 3.3.2 現地見證/稽核流程

A. 現地見證/稽核準備

現地見證/稽核開始前約兩周，建置廠商應提送最新版本之文件、內部稽核報告或認證驗證報告予 V&V 單位，V&V 將根據品質標準審查這些文件資料並準備現地見證/稽核工作。

B. 執行文件審查

在正式準備現地驗證/稽核工作前，IV&V 將審查前述由建置商提供之文件，瞭解這些文件與系統及評估準則的匹配性，這些文件可能包括相關的管理系統文件與紀錄、之前的稽核報告等，審查的時程依系統複雜性、規模而有所差異，有些時候審查作業會一直持續到開始現地驗證/稽核才結束，有些時候在這個階段也會執行初步的現地觀察以便獲得更充分的資訊。

當審查結果發現文件資訊不適當、不夠充分時，現地驗證/稽核團隊負責人將通知受稽核單位作必要的補充或提供充分之資訊，必要時得暫停原訂工作時程，直到關注的問題被解決。

C. 準備現地驗證/稽核

在現地驗證/稽核前，將準備現地驗證/稽核計畫書，並指派任務予參與現地驗證/稽核人員，提供相關之工作文件以利執行現地驗證/稽核工作。

D. 執行現地驗證/稽核

現地驗證/稽核過程中針對觀察項目關注的重點包括：

(a) 執行進度是否與計畫書匹配；

(b) 設計、功能規格是否滿足合約/標準的需求；

(c) 設計、功能規格是否適用於該系統；

(d) 廠商內部品質管理、V&V 管理的執行狀況；

(e) 資訊安全管理是否被落實；

(f) 各式表單充分性與合理性；

(g) 分包商管理、溝通情形。

E. 撰寫並發送報告 由稽核予評估人員撰寫報告，經計畫經理或負責人審核同意後，由計畫管控人員發送報告予相關單位，報告內容包括：

(a) 概述；

(b) 現地驗證/稽核目標；

(c) 受稽單位主要人員；

(d) V&V 單位主要人員；

(e) 地點、時間；

(f) 發現經過；

(g) 結論。

F. 完成現地驗證/稽核評估

當完成所有計畫中應執行現地驗證/稽核項目，並提送報告後即算完成現地驗證/稽核，過程中相關的文件應依照相關單位的協議、合約要求予以保存或銷毀，除非有法律上的需要，原則上不透露相關文件之內容予不相干之單位，當有必要揭露資訊時也應第一時間告知受稽單位與委託單位。

G. 執行後續相關作業

現地驗證/稽核成果可能包含缺失項目並指出須改進處，這些應改進項目通常會被要求在一定期限內執行，並於後續稽核時檢查。

H. 軟體發展確認

德國萊因公司將於系統發展各階段密切關注廠商是否落實軟體發展程序，並特別注意因應後續擴充之軟體設計，其軟體生命週期如圖 3.3.3 所示：

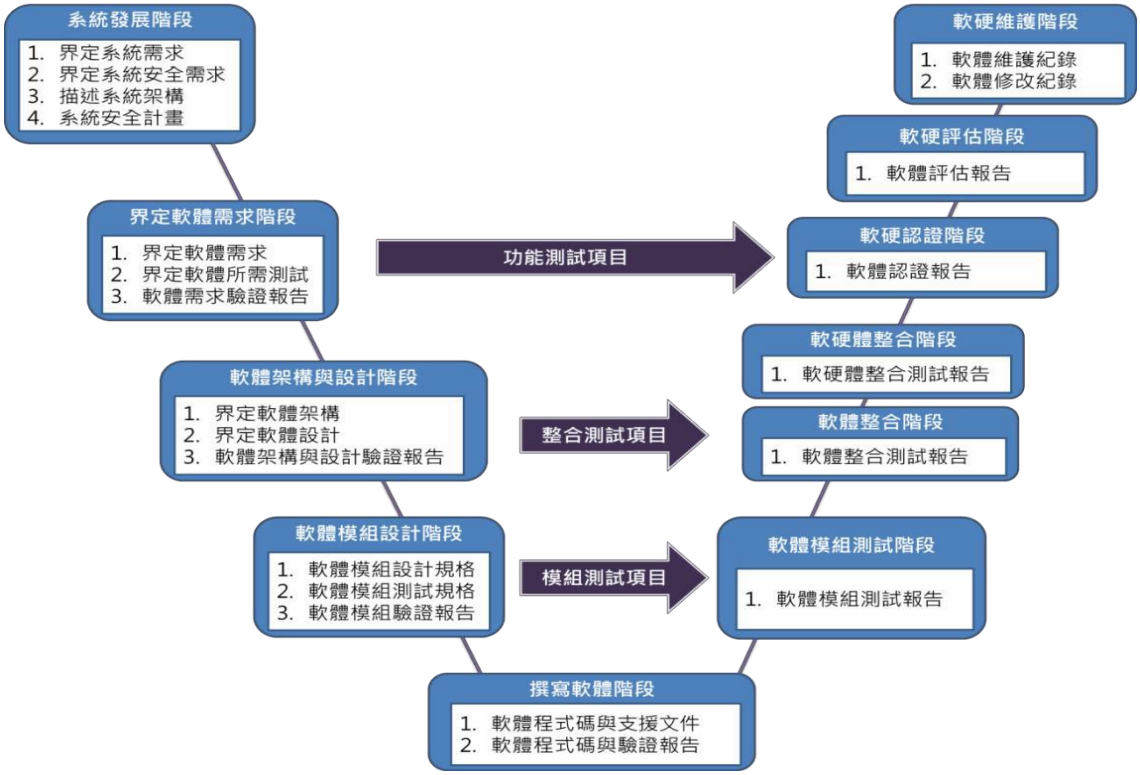


圖 3.3.3 軟體生命週期、相關產出報告與因應之測試

V&V 關注項目如：

(1) 廠商內部軟體團隊的驗證認證採用的過程、方法/技術；

(2) 軟體資訊安全功能分析的完整性；

(3) 容錯設計可否有效降低軟體出錯的機率；

(4) 偵錯功能的完備性；

(5) 測試項目的完整性，即是否透過龐大/多樣的操作情境、資訊安全功能的測試，間接檢查軟體是否有異常情況。

3. 符合性認證方法

針對本計畫中各階段要求的符合性評估報告，德國萊因公司將審查設計文件、相關 IV&V 文件及其可追溯證明、系統保證文件等，確認相關廠商提出之成果滿足各項計畫需求及招標契約之要求。德國萊因公司採用所述之流程執行符合性認證的審查，則說明審查時針對各個評估項目可能產生的結果，只有當審查結果沒

有 A、B、Q 項目後，方授與符合性認證。

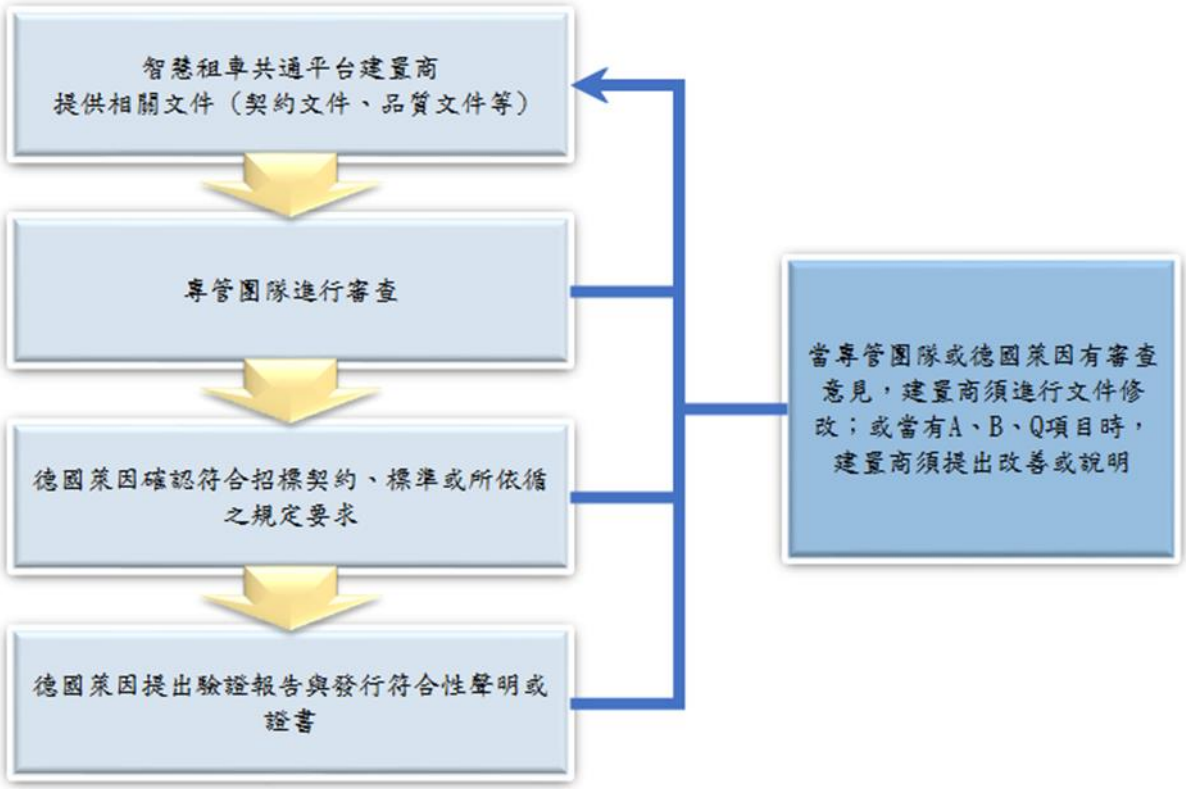


圖 3.3.4 符合性認證流程圖

表 3.3-2 評估等級表

評估等級	敘述	說明
A	嚴重不符	驗證結果與標準/規範需求有差異或有安全疑慮時，且此結果導致設計或程序需重新審視或進行變更，在此項目未解決前，認定此系統並不符合建置需求，此項目應即刻進行改善。
B	部分不符	驗證結果與標準/規範需求有差異或有安全疑慮時，但此結果並不會導致設計或程序需重新審視或進行變更，在此項目未解決前，認定此系統並不符合建置需求，此項目應即刻進行改善。
C	注意事項	驗證結果與標準/規範需求一致，但考量系統之功能性、正確性及安全性應可再進一步精進之項目，並不會導致設計或程序需重新審視或進行變更，此項目可不用立即改善，但可針對此項目擬定精進計畫。

評估等級	敘述	說明
+	已符合	此驗證/認證項目已被正確執行，可接受。
Q	問題	針對關注的問題需要進一步的釐清，在此項目未解決前，認定此系統暫時尚不符合建置需求，此項目應即刻進行改善。
F	格式	格式、錯字問題，不會導致設計、文件、程序的變動，且不一定要再進版更正。
N/A	不適用	此驗證/認證項目在本專案中不適用。

註: 當有 A、B、Q 項目尚未關閉時，將影響發證

4. 認證作業

各項認證工作將依據各系統、各作業提供之文件，對照計畫需求與應遵循之標準來進行檢核，德國萊因公司也會憑藉多年來執行 IV&V 專案經驗，使用檢核表單逐一檢查關鍵文件的內容是否完整及符合計畫需求，依此流程，可分為五個階段進行查核驗證作業，如圖 3.3.5 所示。

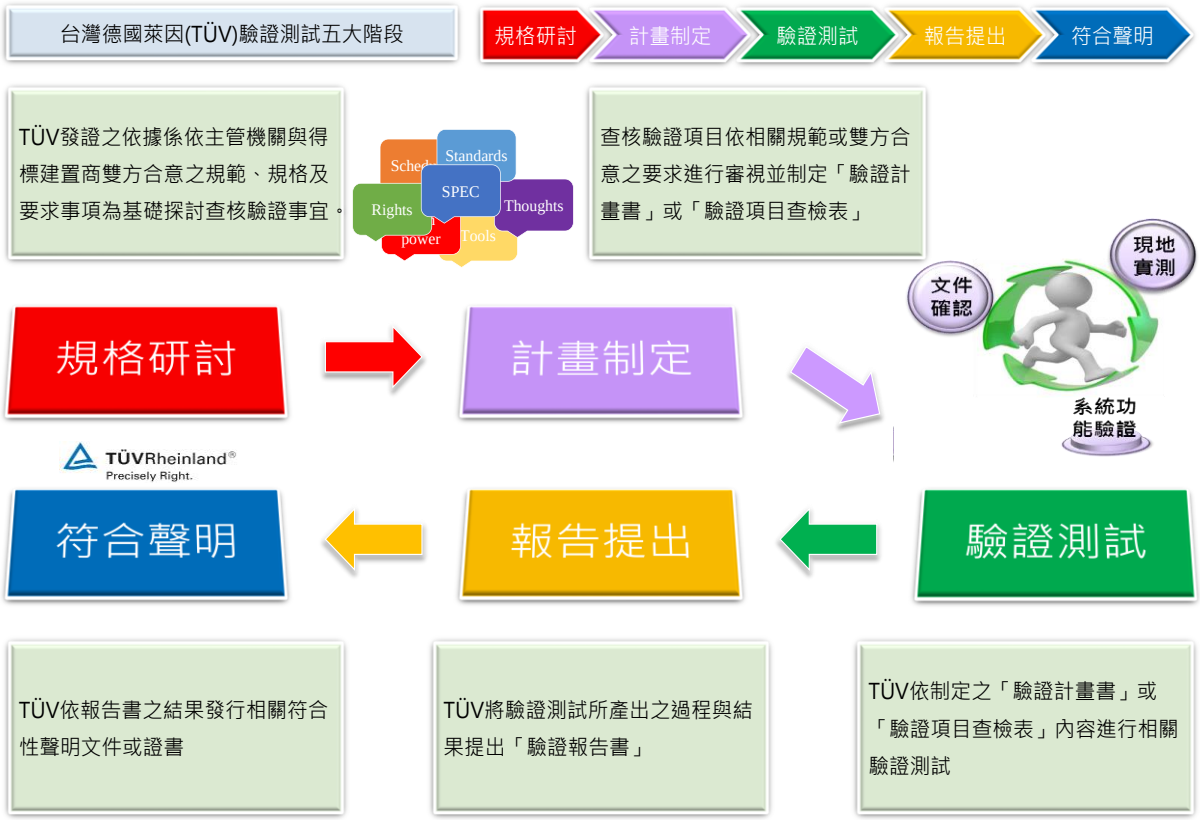


圖 3.3.5 認證作業流程

IV&V 的首要目的乃確保最終興建完成之系統符合功能、品質、安全需求，為了達成此目的，必須於生命週期各階段透過系統性的 IV&V 作業持續追蹤管理各項需求的落實狀況，並驗證、認證相關需求已被滿足。

目前已針對營運廠商依其服務建議書所提出之項目進行監督審驗作業，相關紀錄如下表所列：

表 3.3-3 第三方監督審驗問題表

確認文件	問題描述	漢名科技對應說明	評估等級
招募計畫書與相關調查表	問券的對象似乎與服務建議書中的表 4.4.1 的公會組織似有不同？	已調整	+
招募座談會簡報	1. 簡報"計畫及平台功能介紹"中第六頁痛點說明，有列出痛點介紹，可以建議增加這個平台解決了那些痛點 2. 依據服務建議書章節 4.4.3.項下二、(一)說明，"對租賃車業者最實質之誘因獎項則是由主管機關頒發之獎項及平台回饋之獎勵金，而平台之獎勵金卻是在合作社營運模式中，向各租賃車業者收取之佣金"，這個獎勵金指的是簡報"業者招募說明"中、Page 5、交易服務費的車商獎勵 5%嗎？ 3. 依據服務建議書章節 4.4.3.項下二、(二)說明，"規劃與既有點數平台合作，以平台服務費抽佣之收入向相關業者購置	1. 將於【計畫推動－數位轉型三階段】一併說明。 2. 是的。相關回饋於業者獲消費者之費用皆從所收取之交易服務費來做支應。 3. 將針對紅利點數機制與功能進行開發。	+

確認文件	問題描述	漢名科技對應說明	評估等級
	點數，並以點數作為獎勵忠誠 B2C 消費者之機制"，於簡報中好像沒有看到。 4. 簡報"業者招募說明"中 Page 4 為空白頁面。	4. 已刪除。	
90 天交付系統相關文件	1. 因資策會的平台技轉後的實際應用規劃跟目標不明確，希望漢名可以資策會平台導入後，期望讓使用者作什麼操作應用跟預期的成果，提供文件說明，以便專管團隊根據目標去檢視看還有缺少什麼。 2. 建議提供平台預計以何種形式進行「推動數位轉型」作業的說明，例如上線的網站、使用的 APP 以及相關的版次資訊等。	遵照辦理。已納入「以智慧租車共通平台推動小客車租賃業數位轉型說明書」中。	+
90 天交付系統相關文件-系統彙整報告	相關因應專案狀況進行調整之功能，應與監審測試團隊進行時程確認，以利計畫順遂進行。	待與營運廠商進行確認	?

3.3.2 第三方獨立驗證與認證

除前述有關專案管理及監督審驗工作外，亦進行第三方獨立驗證及確認工作，透過國際性專業第三方獨立單位-臺灣德國萊因技術監護顧問股份有限公司監督本案相關工作之推展進程及相關品質要求，主要目標為充分滿足本案現階段與未來可能的需求，並盡可能超出整體計畫之期望；本案分別於第一年期為智慧租車共通平台(以下簡稱「系統平台」)以及第二年期為「小客車租賃服務整合旅遊生態系平台」於系統上線營運前之驗證測試作業，並依獨立驗證與認證作業之五大

步驟分別逐步進行確認，各階段進度於後續逐一說明。

1. 第一年期-營運廠商建置之智慧租車共通平台

(1) 第一步驟-規格研討

本階段之系統平台係以資訊工業策進會於 109 年 12 月 16 日授權予運輸研究所之系統為基礎，由營運廠商配合營運之行銷需求推動平台精進或功能增訂作業，TÜV 將以營運廠商提供之相關文件如系統規格書、系統測試計畫書等為基礎進行驗證計畫書或驗證項目之研擬撰寫，預計執行時程由運研所與營運廠商之簽約日(即 110 年 5 月 6 日)開始推進，惟配合建置系統調整作業進行時程更動並重新擬定驗證時程如下表 3.3-8、圖 3.3.12 之說明。

(2) 第二步驟-計畫制定

TÜV 依營運廠商所提出之書或營運手冊等資料進行系統平台驗證計畫書或驗證項目撰寫作業，完成驗證項目如下表 3.3-8。

(3) 第三階段-驗證測試

依 TÜV 撰寫之系統平台驗證計畫書或驗證項目之內容進行驗證測試作業，其中 TÜV 將記錄驗證測試之相關設置、驗證地點、驗證時間、參與人員、過程討論及驗證結果等資訊列為驗證測試之佐證資料，本次智慧租車共通平台驗證測試相關資訊如下：

i. 測試時間：110年12月1日-110年12月20日
ii. 測試地點：TÜV臺中分公司、臺中小客車租賃車商
iii. 測試設置：
(a) 本次驗證測試所使用之電腦、行動裝置及對應使用之軟體版本設置下表3.3-4及圖3.3-6~3.3-8所示，相關瀏覽器使用皆以無痕模式進行測試。

表 3.3-4 測試設置說明表

項次	設備	型號	作業系統	使用軟體
1	筆記型電腦	B9400CE	Windows 10專業版 版本：21H1 OS組建： 19043.1348	Google Chrome 版本：96.0.4664.45 (64 位元)
2	行動裝置	iPhone 12 Pro Max	iOS 15.1.1	Safari 15
3	行動裝置	Asus ZenFone 8	Android 11	Chrome

圖 3.3.6 Google Chrome 瀏覽器版本確認圖

(b) 本次驗證測試物件如下表3.3-5及圖3.3-7~圖3.3-11呈現，共計6個物件。

表 3.3-5 測試物件說明表

項次	項目	網址資訊
1	新智慧租車共通平台	https://dealer2.caru.com.tw/administrator/
2	附駕司機PWA	https://driver.caru.com.tw/login
3	行動門市PWA	https://hantek-store.netlify.app/login
4	Taiwan CarU電商平台	https://test-caru.welcometw.com/admin
5	消費者WebSite	https://test-caru.welcometw.com
6	消費者App	未提供

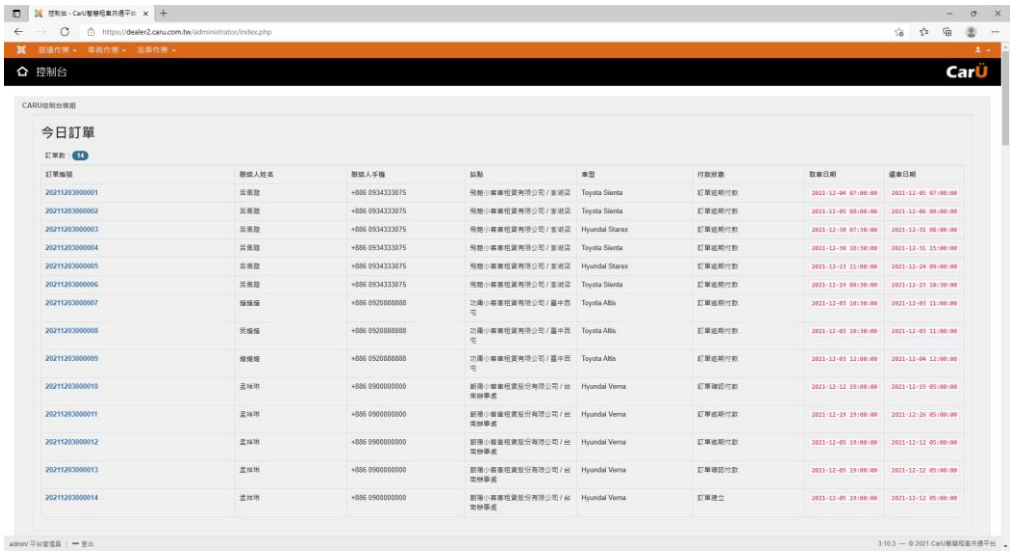


圖 3.3.7 新智慧租車共通平台登入畫面

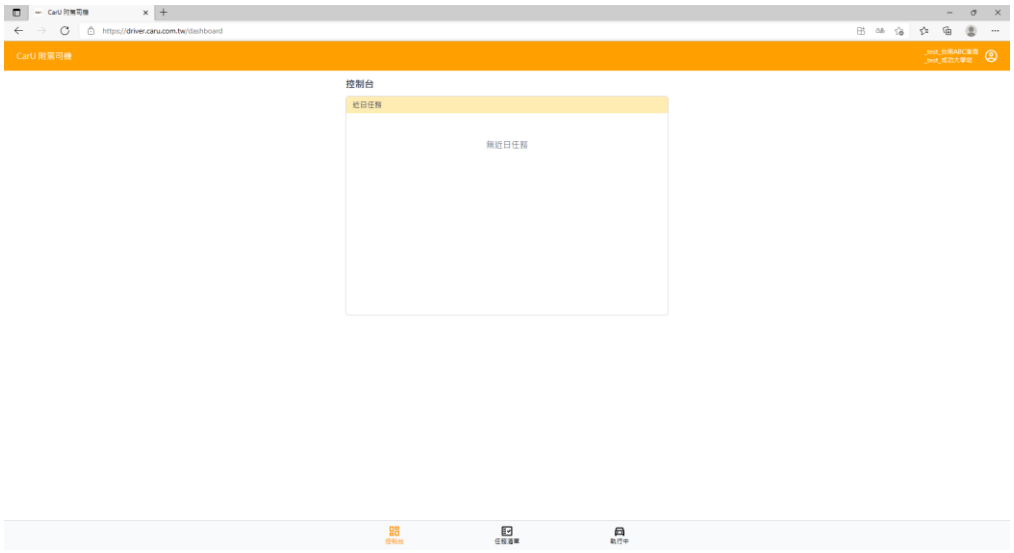


圖 3.3.8 附駕司機 PWA 登入畫面

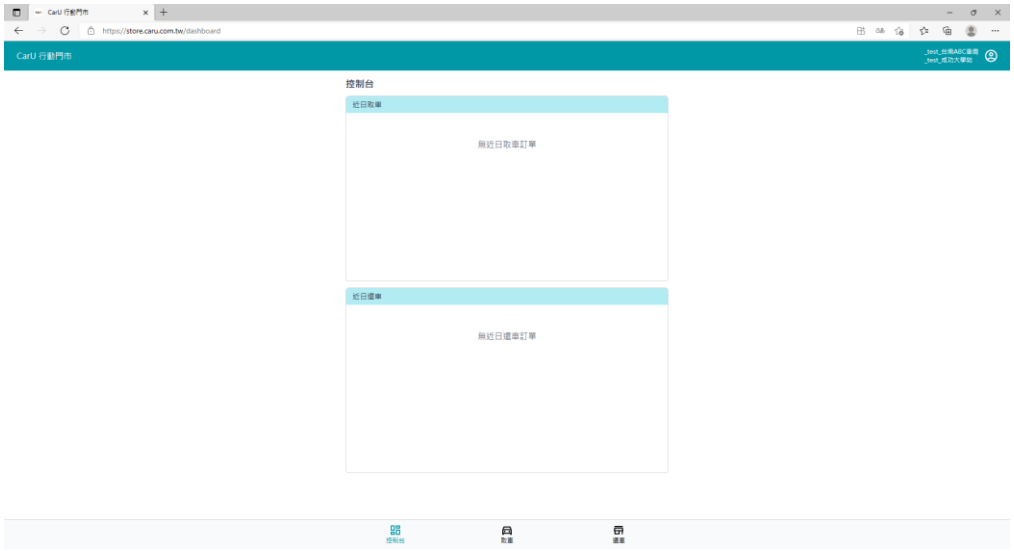


圖 3.3.9 行動門市 PWA 登入畫面

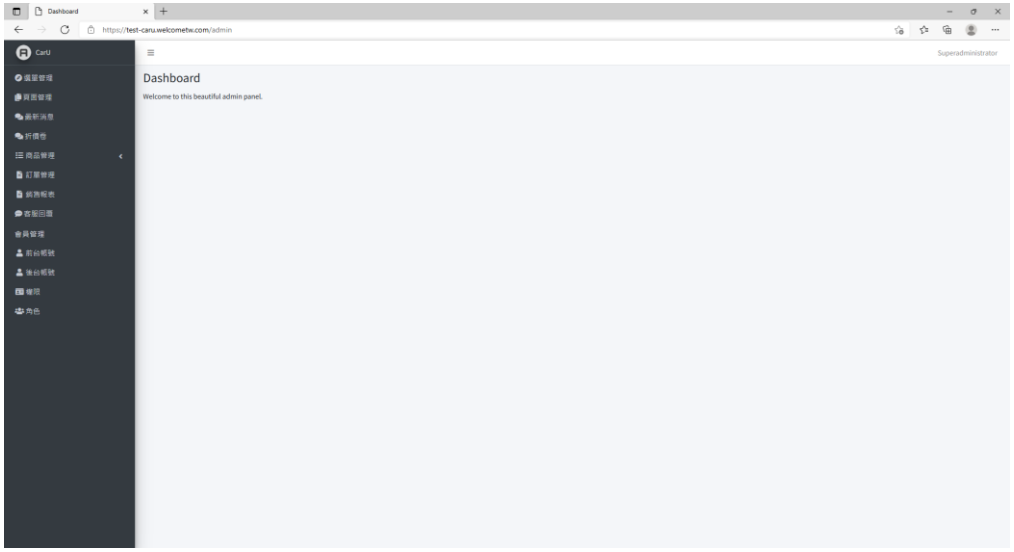


圖 3.3.10 Taiwan CarU 電商平台登入畫面

圖 3.3.11 消費者 WebSite 登入畫面

iv. 測試人員：本次驗證計畫共計一名人員參與，如下表3.3-6所示。

表 3.3-6 驗證測試執行人員表

公司	項目	職稱	人員
TÜV	智慧租車共通平台系統驗證查檢表	資深專案經理	陳郁名

v. 測試方法：

依表 3.3-7 驗證查檢表逐項進行確認，將結果紀錄於發現事項說明中，並依發現結果對照相關文件進行判定。

(4) 第四階段-報告提出

TÜV 依驗證測試之過程與結果撰寫系統平台驗證報告書，本次驗證結果共計 16 項符合，2 項嚴重不符，70 項問題及 2 項不適用，其發現經過說明如表 3.3-7(相關截圖資料請詳附件六 A-01-01~A-61-01)。

(5) 第五階段-符合聲明

TÜV 將依照系統驗證報告書之內容提送申請符合聲明申請(如符合性聲明、符合性證書等)，若其內容符合驗證預期之結果，則發放相關符合文件；因本次驗證系統並未達到符合聲明之要求(判定仍殘留 A 及 Q 之結果)，故無發放相關符合性聲明。

表 3.3-7 新智慧租車平台系統驗證查檢表

項次	驗證項目	完成測試條件	發現事項說明	判定結果
1	確認消費者 Website 具帳號註冊功能。	確認消費者 Website 具備註冊頁面。	以 Google Chrome 瀏覽器進行測試，點選右上角「登入/註冊」字體可進入登入/註冊頁面，該頁面顯示資訊可使用 Facebook、Line 以及 Google 帳號或以 CarU 帳號進行登入；若為新用戶則可點選畫面下方「註冊」字體進入註冊頁面，功能符合驗證項目，詳如附件六 A-01-01。	+
2	以 Google 帳號進行註冊。	確認註冊完成並且平台正確記錄相關資訊。	以 Google Chrome 瀏覽器進行測試，於註冊頁面點選 Google 圖示，登入 Google 帳號確認會員資訊後登出，重新使用 google 帳號登入確認，確認結果可正確登入。 另於 CarU 後台確認帳號資訊亦已加入前台帳號清單中，確認註冊作業完成，功能符合驗證項目，詳如附件六 A-02-01。	+
3	**以 Line 帳號進行註冊。**	**確認註冊完成並且平台正確記錄相關資訊。**	**以 Google Chrome 瀏覽器進行測試，於註冊頁面上方點選 Line 圖示，出現錯誤資訊，無法進行帳號註冊，功能不符合驗證項目，詳如附件六 A-03-01~A-03-04。**	**A**
4	以 Facebook 帳號進行註冊。	確認註冊完成並且平台正確記錄相關資訊。	以 Google Chrome 瀏覽器進行測試，於註冊頁面上方點選 Facebook 圖示，確認會員資訊後登出，重新於登入頁面點選 Facebook 圖示進行登入，確認可正常登入，因此平台係以 mail 帳號建立使用者資訊，此 mail 已使用 google 帳號進行註冊作業，故於後台中並無新增同樣 mail 之帳號，功能符合驗證項目，詳如附件六 A-04-01~A-04-02。	+
5	以 CarU 平台進行註冊	確認註冊完成並且平台正確記錄相關資訊。	以 Google Chrome 瀏覽器進行測試，於註冊頁面填入 CarU 帳號申請資訊，完成帳號申請後確認會員資訊後登出，重新使用 CarU 帳號登入確認，確認結果可正確登入。 另於 CarU 後台確認帳號資訊亦已加入前台帳號清單中，確認註冊作業完成，功能符合驗證項目，詳如附件六 A-05-01。	+

項次	驗證項目	完成測試條件	發現事項說明	判定結果
6	以消費者 Website 進行忘記密碼作業。	重新取得密碼。 確認平台正確記錄相關資訊。	以 Google Chrome 瀏覽器進行測試，於消費者 Website 首頁右上方點選「登入/註冊」後進入註冊頁面，於該頁面下方點選「忘記密碼」進行重新取得密碼或修正密碼之作業，填入註冊的 email 資訊後於信箱可以重設密碼，功能符合驗證項目，詳如附件六 A-06-01~A-06-03。	+
7	以消費者 Website 進行會員資訊維護作業。	確認會員資訊可進行修改作業。 確認平台正確記錄相關資訊。	以 Google Chrome 瀏覽器進行測試，於登入狀態下點選消費者 Website 首頁右上方點選「會員中心」並更新相關個人資訊如生日、性別及地址，完成後點選畫面下方「修改」功能鍵後顯示”帳號更新成功”資訊；於 CarU 後台確認方才修改之帳號亦同步更新相關資訊，功能符合驗證項目，詳如附件六 A-07-01~A-07-04。	+
8	以消費者 Website 進行會員密碼維護作業。	確認會員密碼可進行修改作業。 確認平台正確記錄相關資訊。	以 Google Chrome 瀏覽器進行測試，於登入狀態下點選消費者 Website 首頁右上方點選「會員中心」並點選「變更密碼」進行作業，功能符合驗證項目，詳如附件六 A-08-01~A-08-02。	+
9	**以消費者 Website 進行消費者證件照維護作業。**	**確認證件照可進行上傳作業。 確認平台正確記錄相關資訊。**	**以 Google Chrome 瀏覽器進行測試，目前並無會員維護證件照相關功能，且亦無會員法定年齡限制，即使未滿 18 歲亦可進行車輛租借作業，目前係以產品內容中使用限制中說明如：「承租人（預約人即承租人）於取車時須攜帶本人身份證/護照正本、有效駕照正本並出示當次交易訂單上之電子憑證（QR-Code），（若店家有要求其他文件，則依該店家規定提供），若承租人與當次交易訂單之電子憑證之當事人不同時，當事人需攜帶當次交易訂單之電子憑證（QR-Code）及身份証/護照正本，陪同承租人取車，且在合約上列為共同承租人。）進行規範，現階段無法確認功能符合驗證項目。**	**Q**

項次	驗證項目	完成測試條件	發現事項說明	判定結果
10	以消費者 Website 進行會員登出作業。	確認可正常登出。 確認平台正確記錄相關資訊。	以 Google Chrome 瀏覽器進行測試，於登入狀態下點選消費者 Website 首頁右上方的會員名稱→登出，可正常登出，功能符合驗證項目，詳如附件六 A-10-01。	+
11	**以消費者 Website 進行租車搜尋作業。**	**確認搜尋功能可正確搜尋指定地點之租車公司。**	**以 Google Chrome 瀏覽器進行測試，搜尋功能可正常使用，唯目前操作手冊中顯示資訊與目前線上消費者 Website 不同(如線上消費者 Website 為進階搜尋，操作手冊為進階篩選、線上消費者 Website 有排序，操作手冊並無顯示等)；另仍有多個縣市並無車輛可租借，現階段無法確認功能符合驗證項目，詳如附件六 A11-01-01~A-11-23。**	**Q**
12	以消費者 Website 瀏覽租車定型化契約作業。	確認可瀏覽租車定型化契約。	以 Google Chrome 瀏覽器進行測試，定型化契約於結帳頁面時顯示，功能符合驗證項目，詳如附件 A-12-01。	+
13	**以消費者 Website 瀏覽平台保險契約作業。**	**確認可瀏覽保險契約。**	**以 Google Chrome 瀏覽器進行測試，若車商無設定則無法顯示相關保險資訊，另亦無法透過此需求搜尋符合條件之車商，必須要線下再與車商進行確認，現階段無法確認功能符合驗證項目。**	**Q**
14	以消費者 Website 瀏覽會員條款作業。	確認可瀏覽會員條款。	以 Google Chrome 瀏覽器進行測試，可從消費者 Website 最下方「服務條款」中進行確認，功能符合驗證項目，詳如附件 A-14-01。	+
15	以消費者 Website 進行消費者預約租車作業。	進行指定日期的預約租車作業並完成租車流程。 確認平台正確記錄相關資訊。	以 Google Chrome 瀏覽器進行測試，可完成指定車輛於指定日期的預約租車作業，並於平台中顯示訂單資訊，功能符合驗證項目，詳如附件六 A-15-01~A-15-12。	+
16	**以消費者 Website 進行消費者預約**	**進行指定日期的預約租車作業，並**	**以 Google Chrome 瀏覽器進行測試，於首頁上方雖顯示有甲租乙還之車輛，並可於租車流程中點選此功能，但於現階段**	**Q**

項次	驗證項目	完成測試條件	發現事項說明	判定結果
	租車作業(甲租乙還)。	**使用甲租乙還之條件完成租車流程。 確認平台正確記錄相關資訊。**	**僅以資訊顯示方式進行，並僅以同一車商方可進行此作業，實際甲租乙還之方式仍須與車商直接聯繫確認費用及方法，無法透過平台直接進行,現階段無法確認功能符合驗證項目，詳如附件六 A-16-01。**	
17	**以消費者 Website 進行消費者預約租車(附駕包車)作業。**	**進行指定日期的預約租車作業，並使用附駕包車之條件完成租車流程。 確認平台正確記錄相關資訊。**	**以 Google Chrome 瀏覽器進行測試，於首頁上方雖顯示有附駕包車之車輛，並可於租車流程中點選此功能，附駕包車於付費過程中無法得知司機相關資訊或連繫方式，實際附駕包車之方式仍須與車商直接聯繫確認，現階段無法確認功能符合驗證項目，詳如附件六 A-17-01~A-17-02。**	**Q**
18	**以消費者 Website 進行訂單確認作業。**	**確認訂單資訊正確顯示。 確認平台正確記錄相關資訊。**	**以 Google Chrome 瀏覽器進行測試，於登入狀態下點選右上方點選「我的訂單」可顯示目前訂單，但於消費者 WebSite 顯示之訂單號碼無法與租車共通平台資訊一致,例如 Website 顯示訂單編號為 4327，平台顯示為 20211220001963，兩者無法連結；另完成付款但尚未取車之車輛於狀態中仍顯示已完成會容易造成混淆，建議應有狀態差異，現階段無法確認功能符合驗證項目，詳如附件六 A-18-01~A-18-02。**	**Q**
19	以消費者 Website 進行消費者取消訂單作業。	於派車前完成取消訂單作業。 確認平台正確記錄相關資訊。	以 Google Chrome 瀏覽器進行測試，因目前金流系統仍處於測試階段未完整導入，故此功能無法確認是否可確實進行退款等相關作業，無法進行判定。	N/A
20	以消費者 Website 進行延長訂單作業。	於車輛租用過程中進行延長作業。	現階段系統無法進行相關作業，需直接聯繫車商進行，無法進行判定。	N/A

項次	驗證項目	完成測試條件	發現事項說明	判定結果
		確認平台正確記錄相關資訊。		
21	以消費者 Website 進行查詢交易紀錄作業。	確認可針對過往交易進行查詢作業並與平台相符。	以 Google Chrome 瀏覽器進行測試，於登入狀態下點選右上方點選「我的訂單」可顯示目前訂單，僅有逐項紀錄顯示，並無相關統計資訊，現階段無法確認功能符合驗證項目。	Q
22	確認消費者 App 具帳號註冊功能。	確認消費者 APP 具備註冊頁面。	APP 尚未完成開發，故相關測試無法進行，現階段無法確認功能符合驗證項目。	Q
23	以 Google 帳號進行註冊	確認註冊完成並且平台正確記錄相關資訊。	APP 尚未完成開發，故相關測試無法進行，現階段無法確認功能符合驗證項目。	Q
24	以 Line 帳號進行註冊	確認註冊完成並且平台正確記錄相關資訊。	APP 尚未完成開發，故相關測試無法進行，現階段無法確認功能符合驗證項目。	Q
25	以 Facebook 帳號進行註冊	確認註冊完成並且平台正確記錄相關資訊。	APP 尚未完成開發，故相關測試無法進行，現階段無法確認功能符合驗證項目。	Q
26	以 CarU 平台進行註冊	確認註冊完成並且平台正確記錄相關資訊。	APP 尚未完成開發，故相關測試無法進行，現階段無法確認功能符合驗證項目。	Q
27	以消費者 App 進行忘記密碼作業。	重新取得密碼。 確認平台正確記錄相關資訊。	APP 尚未完成開發，故相關測試無法進行，現階段無法確認功能符合驗證項目。	Q
28	以消費者 App 進行會員資訊維護作業。	確認會員資訊可進行修改作業。 確認平台正確記錄相關資訊。	APP 尚未完成開發，故相關測試無法進行，現階段無法確認功能符合驗證項目。	Q

項次	驗證項目	完成測試條件	發現事項說明	判定結果
29	以消費者 App 進行會員密碼維護作業。	確認會員密碼可進行修改作業。 確認平台正確記錄相關資訊。	APP 尚未完成開發，故相關測試無法進行，現階段無法確認功能符合驗證項目。	Q
30	以消費者 App 進行消費者證件照維護作業。	確認證件照可進行上傳作業。 確認平台正確記錄相關資訊。	APP 尚未完成開發，故相關測試無法進行，現階段無法確認功能符合驗證項目。	Q
31	以消費者 App 進行會員登出作業。	確認可正常登出。 確認平台正確記錄相關資訊。	APP 尚未完成開發，故相關測試無法進行，現階段無法確認功能符合驗證項目。	Q
32	以消費者 App 進行租車搜尋作業。	確認搜尋功能可正確搜尋指定地點之租車公司。	APP 尚未完成開發，故相關測試無法進行，現階段無法確認功能符合驗證項目。	Q
33	以消費者 App 瀏覽租車定型化契約作業。	確認可瀏覽租車定型化契約。	APP 尚未完成開發，故相關測試無法進行，現階段無法確認功能符合驗證項目。	Q
34	以消費者 App 瀏覽平台保險契約作業。	確認可瀏覽保險契約。	APP 尚未完成開發，故相關測試無法進行，現階段無法確認功能符合驗證項目。	Q
35	以消費者 App 瀏覽會員條款作業。	確認可瀏覽會員條款。	APP 尚未完成開發，故相關測試無法進行，現階段無法確認功能符合驗證項目。	Q
36	以消費者 App 進行消費者預約租車作業。	進行指定日期的預約租車作業並完成租車流程。	APP 尚未完成開發，故相關測試無法進行，現階段無法確認功能符合驗證項目。	Q

項次	驗證項目	完成測試條件	發現事項說明	判定結果
		確認平台正確記錄相關資訊。		
37	以消費者 App 進行消費者預約租車作業(甲租乙還)。	進行指定日期的預約租車作業，並使用甲租乙還之條件完成租車流程。 確認平台正確記錄相關資訊。	APP 尚未完成開發，故相關測試無法進行，現階段無法確認功能符合驗證項目。	Q
38	以消費者 App 進行消費者預約租車(附駕包車)作業。	進行指定日期的預約租車作業，並使用附駕包車之條件完成租車流程。 確認平台正確記錄相關資訊。	APP 尚未完成開發，故相關測試無法進行，現階段無法確認功能符合驗證項目。	Q
39	以消費者 App 進行訂單確認作業。	確認訂單資訊正確顯示。 確認平台正確記錄相關資訊。	APP 尚未完成開發，故相關測試無法進行，現階段無法確認功能符合驗證項目。	Q
40	以消費者 App 進行消費者取消訂單作業。	於派車前完成取消訂單作業。 確認平台正確記錄相關資訊。	APP 尚未完成開發，故相關測試無法進行，現階段無法確認功能符合驗證項目。	Q
41	以消費者 App 進行延長訂單作業。	於車輛租用過程中進行延長作業。	APP 尚未完成開發，故相關測試無法進行，現階段無法確認功能符合驗證項目。	Q

項次	驗證項目	完成測試條件	發現事項說明	判定結果
		確認平台正確記錄相關資訊。		
42	**以消費者 App 進行查詢交易紀錄作業。**	**確認可針對過往交易進行查詢作業並與平台相符。**	**APP 尚未完成開發，故相關測試無法進行，現階段無法確認功能符合驗證項目。**	**Q**
43	**確認租車作業金流作業正常**	**確認金流正確透過信用卡扣款。 確認平台正確記錄相關資訊。**	**以 Google Chrome 瀏覽器進行測試，因目前金流仍屬測試階段，故先以測試卡號(卡號 4000-2211-1111-1111，有效月年及背面末三碼皆為任意輸入)進行流程測試，並無實際金流拆分、計算等實際營運作業確認，現階段無法確認功能符合驗證項目。**	**Q**
44	**確認租用車輛合法性符合。**	**確認系統可透過 M3 連線確認車輛合法性。 確認平台正確記錄相關資訊。**	**目前派車作業並無實際 M3 連線檢核機制，無法確認相關租賃車輛是否屬於合法車輛，任意輸入車號(如 1234)皆可進行派車作業，現階段無法確認功能符合驗證項目，詳如附件六 A-44-01。**	**Q**
45	以行動門市 PWA 進行密碼維護作業。	確認密碼可進行修改作業。 確認平台正確記錄相關資訊。	以 ios 系統及 Android 系統安裝行動門市 PWA 並進行密碼修改作業，確定可完成密碼修改並成功登入，功能符合驗證項目，詳如附件六 A-45-01~A-45-02。	+
46	**以行動門市 PWA 掃描 QR Code 功能。**	**確認掃描 QR Code 可正確作業。 確認平台正確記錄相關資訊。**	**以 ios 系統及 Android 系統安裝行動門市 PWA 並進行 QR Code 核銷作業，確定可完成核銷作業，惟若此 QR Code 透過駕駛 PWA 進行掃描亦會核銷，無相關防呆機制，現階段無法確認功能符合驗證項目，詳如附件六 A-46-01~A-46-02。**	**Q**
47	以行動門市 PWA 進行人工核銷作業。	確認掃描人工核銷作業可正確作業。	以 ios 系統及 Android 系統安裝行動門市 PWA 並進行人工核銷作業，確定可完成核銷作業，功能符合驗證項目，詳如附件六 A-47-01。	+

項次	驗證項目	完成測試條件	發現事項說明	判定結果
		確認平台正確記錄相關資訊。		
48	以行動門市 PWA 進行交車作業。	使用行動門市 PWA 進行交車作業。 確認平台正確記錄相關資訊。	以 ios 系統及 Android 系統安裝行動門市 PWA 並進行交車作業，確定可完成契約上傳功能及交車作業，功能符合驗證項目，詳如附件六 A-48-01。	+
49	**以行動門市 PWA 進行結案作業。**	**使用行動門市 PWA 進行結案作業。 確認平台正確記錄相關資訊。**	**以 ios 系統及 Android 系統安裝行動門市 PWA 進行結案完成作業，但於平台僅顯示已還車，未達到結案的狀態，相關使用手冊亦無說明是否需由平台進行人工結案或其他作業，現階段無法確認功能符合驗證項目，詳如附件六 A-49-01。**	**Q**
50	**以行動門市 PWA 進行銷單作業。**	**確認銷單作業可正常進行。 確認平台正確紀錄相關資訊。**	**同測試項目 46 及 47 兩種方法進行銷單作業之結果。**	**Q**
51	以行動門市 PWA 進行未派車車輛確認作業。	確認可由行動門市 PWA 確認未派車車輛。 確認未派車車輛與平台相符。	以 ios 系統及 Android 系統安裝行動門市 PWA 進行確認，可由控制台確認相關未核銷車輛與未取車車輛資訊，與平台相符，功能符合驗證項目，詳如附件六 A-51-01。	+
52	**以行動門市 PWA 確認已完成項目。**	**確認完成銷單之車輛正確顯示於已完成項目中並與平台相符。**	**以 ios 系統及 Android 系統安裝行動門市 PWA 進行確認，無特別分類已完成的車輛，僅能由狀態確認是否已還車，另亦無訂單編號可與後台比對確認，造成比對不易，現階段無法確認功能符合驗證項目。**	**Q**

項次	驗證項目	完成測試條件	發現事項說明	判定結果
53	**確認行動門市 PWA 可使用之功能符合設計規範。**	**確認行動門市 PWA 所有可使用之功能正常並符合設計規範。**	**以 ios 系統及 Android 系統安裝行動門市 PWA 進行確認，除部分功能仍未完善外，相關使用手冊說明過於簡潔，應針對各功能進行逐項說明，以利完整理解該 PWA 所有功能及含意，現階段無法確認功能符合驗證項目。**	**Q**
54	以附駕司機 PWA 進行密碼維護作業。	確認密碼可進行修改作業。 確認平台正確記錄相關資訊。	以 ios 系統及 Android 系統安裝附駕司機 PWA 並進行密碼修改作業，確定可完成密碼修改並成功登入，功能符合驗證項目，詳如附件六 A-54-01。	+
55	**以附駕司機 PWA 進行派車資訊確認作業。**	**確認可由附駕司機 PWA 確認派車資訊。 確認派車資訊與平台相符。**	**以 ios 系統及 Android 系統安裝附駕司機 PWA，無法由控制台確認今日是否有相關任務，另完成任務之車輛亦無法透過此 PWA 進行確認，現階段無法確認功能符合驗證項目，詳如附件六 A-55-01。**	**Q**
56	**以附駕司機 PWA 掃描 QR Code 功能。**	**確認掃描 QR Code 可正確作業。 確認平台正確記錄相關資訊。**	**以 ios 系統及 Android 系統安裝附駕司機 PWA 並進行 QR code 掃描作業，完成掃描後出現「…重新導向至執行中清單」等訊息後即無相關資訊，無法進行結案作業，另亦無法從 app 中輸入相關司機資訊；QR code 點選重新掃描後，未完成核銷的 QR code 即使尚未開始任務一樣會失效而無法使用，現階段無法確認功能符合驗證項目，詳如附件六 A-56-01。**	**Q**
57	**以附駕司機 PWA 進行人工核銷作業。**	**確認掃描人工核銷作業可正確作業。 確認平台正確記錄相關資訊。**	**以 ios 系統及 Android 系統安裝附駕司機 PWA 並進行人工核銷作業，惟此作業需預先於平台的訂單管理中找到此訂單編號，點選派車相關資訊才能進行人工核銷作業，此順序建議應再使用手冊-附駕司機章節中說明，避免作業錯誤，現階段無法確認功能符合驗證項目，詳如附件六 A-57-01。**	**Q**

項次	驗證項目	完成測試條件	發現事項說明	判定結果
58	以附駕司機 PWA 進行結案作業。	使用附駕司機 PWA 進行結案作業。 確認平台正確記錄相關資訊。	以 QR Code 進行任務清單核銷後，沒有轉入執行中頁面，造成此案無法透過司機 PWA 結案，僅能透過平台強制進行結案作業； 以人工核銷進行任務的行程可順利結案，但過程中並無上傳合約等資訊，相關順序應寫於操作手冊中以便車商理解各時間點應進行何種操作，因使用 QR code 出現無法於 PWA 進行結案之情境，功能不符合驗證項目。	A
59	確認附駕司機 PWA 可使用之功能符合設計規範。	確認附駕司機 PWA 所有可使用之功能正常並符合設計規範。	以 ios 系統及 Android 系統安裝附駕司機 PWA 進行確認，除部分功能仍未完善外，相關使用手冊說明過於簡潔，應針對各功能進行逐項說明，以利完整理解該 PWA 所有功能及含意，現階段無法確認功能符合驗證項目。	Q
60	確認智慧租車共通平台帳號管理功能。	確認智慧租車共通平台帳號管理頁面，並進行相關功能確認。 確認平台正確記錄相關資訊。	以 Google Chrome 瀏覽器進行測試，可進行帳號新增及刪除作業，但權限設定僅有 2 種，與設計規格書說明的 5 種並不相符；另操作手冊之說明過於簡潔，應針對各功能進行逐項說明，現階段無法確認功能符合驗證項目。	Q
61	確認智慧租車共通平台車型管理功能。	確認智慧租車共通平台車型管理頁面，並進行相關功能確認。 確認平台正確記錄相關資訊。	以 Google Chrome 瀏覽器進行測試，搜尋功能僅能針對車型名稱進行搜尋，但點選搜尋出現的輔助說明顯示”用廣告看板名稱及別名搜尋”，與本頁面功能似無關係；另操作手冊之說明過於簡潔，應針對各功能進行逐項說明，現階段無法確認功能符合驗證項目，詳如附件六 A-61-01。	Q
62	確認智慧租車共通平台車商管理功能。	確認智慧租車共通平台車商管理	以 Google Chrome 瀏覽器進行測試，相關功能可進操作，惟因操作手冊之說明過於簡潔無法進行確認作業，應針對各功能進行逐項說明，現階段無法確認功能符合驗證項目。	Q

項次	驗證項目	完成測試條件	發現事項說明	判定結果
		頁面，並進行相關功能確認。 確認平台正確記錄相關資訊。		
63	確認智慧租車共通平台參數管理功能。	確認智慧租車共通平台參數管理頁面，並進行相關功能確認。 確認平台正確記錄相關資訊。	以 Google Chrome 瀏覽器進行測試，相關功能可進操作，惟因操作手冊之說明過於簡潔無法進行確認作業，應針對各功能進行逐項說明，現階段無法確認功能符合驗證項目。	Q
64	確認智慧租車共通平台行事曆管理功能。	確認智慧租車共通平台行事曆管理頁面，並進行相關功能確認。 確認平台正確記錄相關資訊。	以 Google Chrome 瀏覽器進行測試，相關功能可進操作，惟因操作手冊之說明過於簡潔無法進行確認作業，應針對各功能進行逐項說明，現階段無法確認功能符合驗證項目。	Q
65	確認智慧租車共通平台價格管理功能。	確認智慧租車共通平台價格管理頁面，並進行相關功能確認。 確認平台正確記錄相關資訊。	以 Google Chrome 瀏覽器進行測試，相關功能可進操作，惟因操作手冊之說明過於簡潔無法進行確認作業，應針對各功能進行逐項說明，另此項目無法於透過此頁面功能新增車輛進行價格管理，建議應一併於操作手冊中說明，現階段無法確認功能符合驗證項目。	Q
66	確認智慧租車共通平台內附項目管理功能。	確認智慧租車共通內附項目管理註冊頁面，並進行相關功能確認。	以 Google Chrome 瀏覽器進行測試，相關功能可進操作，惟因操作手冊之說明過於簡潔無法進行確認作業，應針對各功能進行逐項說明，另此功能相關變動不會立即於消費者側更	Q

項次	驗證項目	完成測試條件	發現事項說明	判定結果
		確認平台正確記錄相關資訊。	新，應於操作手冊中進行說明，現階段無法確認功能符合驗證項目。	
67	確認智慧租車共通平台加購項目管理功能。	確認智慧租車共通平台平台加購項目管理頁面，並進行相關功能確認。 確認平台正確記錄相關資訊。	以 Google Chrome 瀏覽器進行測試，相關功能可進操作，惟因操作手冊之說明過於簡潔無法進行確認作業，應針對各功能進行逐項說明，另此功能相關變動不會立即於消費者側更新，應於操作手冊中進行說明，現階段無法確認功能符合驗證項目。	Q
68	確認智慧租車共通平台站點管理功能。	確認智慧租車共通平台站點管理頁面，並進行相關功能確認。 確認平台正確記錄相關資訊。	以 Google Chrome 瀏覽器進行測試，相關功能可進操作，惟因操作手冊之說明過於簡潔無法進行確認作業，應針對各功能進行逐項說明，現階段無法確認功能符合驗證項目。	Q
69	確認智慧租車共通平台車輛管理功能。	確認智慧租車共通平台車輛管理頁面，並進行相關功能確認。 確認平台正確記錄相關資訊。	以 Google Chrome 瀏覽器進行測試，相關功能可進操作，惟因操作手冊之說明過於簡潔無法進行確認作業，應針對各功能進行逐項說明，現階段無法確認功能符合驗證項目。	Q
70	確認智慧租車共通平台駕駛管理功能。	確認智慧租車共通平台駕駛管理頁面，並進行相關功能確認。	以 Google Chrome 瀏覽器進行測試，相關功能可進操作，惟因操作手冊之說明過於簡潔無法進行確認作業，應針對各功能進行逐項說明，現階段無法確認功能符合驗證項目。	Q

項次	驗證項目	完成測試條件	發現事項說明	判定結果
		確認平台正確記錄相關資訊。		
71	確認智慧租車共通平台員工管理功能。	確認智慧租車共通平台員工管理頁面，並進行相關功能確認。 確認平台正確記錄相關資訊。	以 Google Chrome 瀏覽器進行測試，相關功能可進操作，惟因操作手冊之說明過於簡潔無法進行確認作業，應針對各功能進行逐項說明，現階段無法確認功能符合驗證項目。	Q
72	確認智慧租車共通平台車商價格管理功能。	確認智慧租車共通平台車商價格管理頁面，並進行相關功能確認。 確認平台正確記錄相關資訊。	以 Google Chrome 瀏覽器進行測試，相關功能可進操作，惟因操作手冊之說明過於簡潔無法進行確認作業，應針對各功能進行逐項說明，現階段無法確認功能符合驗證項目。	Q
73	確認智慧租車共通平台站點價格管理功能。	確認智慧租車共通平台站點價格管理頁面，並進行相關功能確認。 確認平台正確記錄相關資訊。	以 Google Chrome 瀏覽器進行測試，相關功能可進操作，惟因操作手冊之說明過於簡潔無法進行確認作業，應針對各功能進行逐項說明，現階段無法確認功能符合驗證項目。	Q
74	確認智慧租車共通平台加購項目價格管理功能。	確認智慧租車共通平台加購項目價格管理頁面，並進行相關功能確認。	以 Google Chrome 瀏覽器進行測試，相關功能可進操作，惟因操作手冊之說明過於簡潔無法進行確認作業，應針對各功能進行逐項說明，另此功能相關變動不會立即於消費者側更新，應於操作手冊中進行說明，現階段無法確認功能符合驗證項目。	Q

項次	驗證項目	完成測試條件	發現事項說明	判定結果
		確認平台正確記錄相關資訊。		
75	確認智慧租車共通平台上架管理功能。	確認智慧租車共通平台上架管理頁面，並進行相關功能確認。 確認平台正確記錄相關資訊。	以 Google Chrome 瀏覽器進行測試，相關功能可進操作，惟因操作手冊之說明過於簡潔無法進行確認作業，應針對各功能進行逐項說明，另此功能相關變動不會立即於消費者側更新，應於操作手冊中進行說明，現階段無法確認功能符合驗證項目。	Q
76	確認智慧租車共通平台訂單管理功能。	確認智慧租車共通平台訂單管理頁面，並進行相關功能確認。 確認平台正確記錄相關資訊。	以 Google Chrome 瀏覽器進行測試，相關功能可進操作，惟因操作手冊之說明過於簡潔無法進行確認作業，應針對各功能進行逐項說明，另此功能相關變動不會立即於消費者側更新，同時消費者所上傳之照片亦無顯示於此，現階段無法確認功能符合驗證項目。	Q
77	確認智慧租車共通平台權限設定功能。	確認平台權限可依實際經營情境進行設定作業。	以 Google Chrome 瀏覽器進行測試，無法透過平台進行相關權限設定，現階段無法確認功能符合驗證項目。	Q
78	確認智慧租車共通平台相關營運報表功能。	確認平台可確認相關營運狀況並產出報表。	以 Google Chrome 瀏覽器進行測試，現況營運報表無法以日報或月報方式呈現，於實際營運使用不易，現階段無法確認功能符合驗證項目。	Q
79	確認智慧租車共通平台可使用之功能符合設計規範。	確認智慧租車共通平台所有可使用之功能正常並符合設計規範。	以 Google Chrome 瀏覽器進行測試，除部分功能仍未完善外，相關使用手冊說明過於簡潔，應針對各功能進行逐項說明，以利完整理解平台所有功能及含意，現階段無法確認功能符合驗證項目。	Q
80	確認成立客服中心。	確認已成立客服中心。	已有相關客服機制如電話、線上小幫手等，惟因目前未正式上線，故相關客服於現階段無法確認功能符合驗證項目。	Q

項次	驗證項目	完成測試條件	發現事項說明	判定結果
81	客服中心-使用者資訊。	確認客服中心可回應各使用者(車商、附駕司機及使用者)所用平台相關資訊	已有相關客服機制如電話、線上小幫手等，惟因目前未正式上線，故相關客服於現階段無法確認功能符合驗證項目。	Q
82	確認客服中心管理機制。	確認客服中心完成相關機制之制定。	雖有部分說明但分散於各階段報告書中，建議應因確認招標計畫需求及營運需求訂定相關文件，現階段無法確認功能符合驗證項目。	Q
83	確認壓力與負載測試。	確認壓力與負載測試完成並符合規範需求。	雖有部分說明但分散於各階段報告書中，建議應因確認招標計畫需求及營運需求訂定相關文件，現階段無法確認功能符合驗證項目。	Q
84	確認完成資安維護計畫。	確認資安維護計畫或相等文件符合規範需求。	雖有部分說明但分散於各階段報告書中，建議應因確認招標計畫需求及營運需求訂定相關文件，現階段無法確認功能符合驗證項目。	Q
85	確認完成營運規章。	確認營運規章或相等文件符合規範需求。	雖有部分說明但分散於各階段報告書中，建議應因確認招標計畫需求及營運需求訂定相關文件，現階段無法確認功能符合驗證項目。	Q
86	確認完成收費機制。	確認收費機制或相等文件符合規範需求。	雖有部分說明但分散於各階段報告書中，建議應因確認招標計畫需求及營運需求訂定相關文件，現階段無法確認功能符合驗證項目。	Q
87	確認完成車輛整備與安全管理。	確認車輛整備與安全管理或相等文件符合規範需求。	雖有部分說明但分散於各階段報告書中，建議應因確認招標計畫需求及營運需求訂定相關文件，現階段無法確認功能符合驗證項目。	Q

項次	驗證項目	完成測試條件	發現事項說明	判定結果
88	**確認完成維運標準。**	**確認維運標準或相等文件符合規範需求。**	**雖有部分說明但分散於各階段報告書中，建議應因確認招標計畫需求及營運需求訂定相關文件，現階段無法確認功能符合驗證項目。**	**Q**
89	**確認完成平台操作手冊與教育訓練。**	**確認平台操作手冊與教育訓練或相等文件符合規範需求。**	**雖有部分說明但分散於各階段報告書中，建議應因確認招標計畫需求及營運需求訂定相關文件，另操作手冊雖已有提供但內容過於簡潔，無法進行確認作業，應針對各功能進行逐項說明，現階段無法確認功能符合驗證項目。**	**Q**
90	**確認相關資安檢測結果。**	**確認相關資安檢測報告完成並依相關建議改善**	**雖有部分說明但分散於各階段報告書中，另現階段使用之六個測試物件都應提供相關資安檢測報告，現階段無法確認功能符合驗證項目。**	**Q**

表 3.3-8 第一年期-新智慧租車平台認證期程表

任務名稱	開始時間	完成時間	任務時間（日曆天）	文件	說明	擔當
規格研討	7/17/2021	9/30/2021	75	系統規格書*	包含APP、網站與後台相關之細部規格說明	營運廠商
				系統測試報告*	包含APP、網站與後台依規格進行測試驗證，測試項目包含功能驗證、安全性驗證、正確性驗證以及壓力驗證等項目。	
				系統維運與資安維護手冊*	包含APP、網站與後台如何持續營運並確保資安維護之說明。	
				* 或等同上述資訊之文件		
				規格確認	依上述營運廠商所提系統認證相關文件進行多方溝通討論，並確立其最終規格與其系統關鍵指標。	德國萊因 & 營運廠商
計畫制定	10/1/2021	10/13/2021	12	德國萊因- 系統平台驗證計畫書 / 驗證項目	完成由三方(即運研所、營運廠商及德國萊因)合意之「系統平台驗證計畫書」之撰寫。	德國萊因 & 營運廠商 & 運研所
驗證測試	12/1/2021	12/10/2021	9	德國萊因- 系統平台驗證計畫書 / 驗證項目	依三方合意之「系統平台驗證計畫書」之內容據以執行系統驗證作業。	德國萊因 & 營運廠商
技術討論	10/1/2021	12/10/2021	70	德國萊因-系統平台驗證記錄	詳實紀錄執行系統平台驗證測試作業時各項工作時之情形及發現，若有待釐清之事項或相關技術問題則需進行三方技術會議，確認相關驗證結果落實規範。	德國萊因 & 營運廠商 & 運研所
報告提出	12/10/2021	12/15/2021	5	德國萊因- 系統平台驗證報告書	依系統平台驗證作業之過程與結果製作報告書。	德國萊因
符合聲明	12/16/2021	12/24/2021	8	德國萊因- 系統平台符合聲明文件	若其系統平台驗證之關鍵指標可全數符合系統平台驗證計畫書之規範，則發放相關符合聲明(如符合性證書、符合性聲明等)。	德國萊因

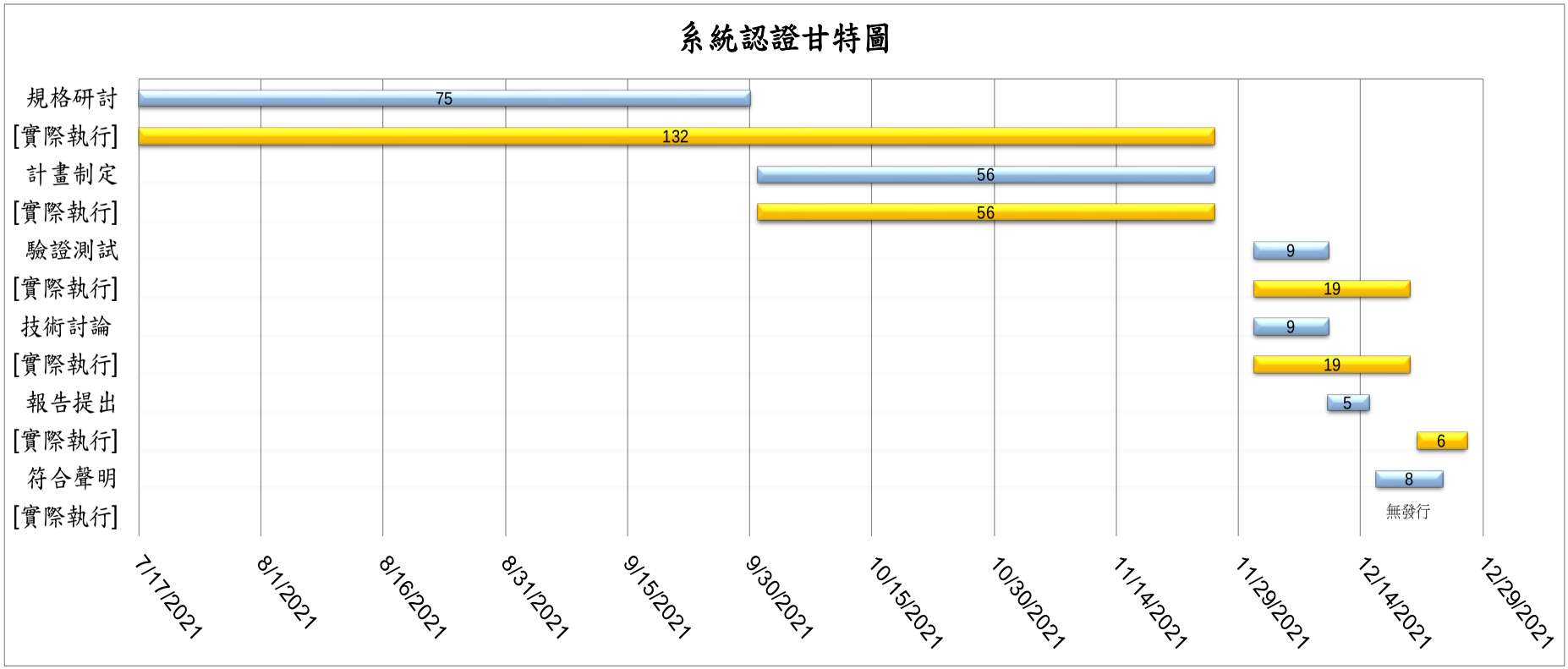


圖 3.3.12 第一年期-新智慧租車平台認證甘特圖

2. 第二年期-小客車租賃服務整合旅遊生態系平台

(1) 第一步驟-規格研討

本階段之平台係以前述第一年期所完成之系統平台為基礎，由營運廠商藉由數位旅遊行動服務整合，以餐飲、飯店旅館、觀光景點、特色商品面向，整合「行」的一站式旅運服務，完成此一小客車租賃服務整合旅遊生態系平台，TÜV 將以營運廠商提供之相關文件如系統規格書、系統測試計畫書等為基礎進行驗證計畫書或驗證項目之研擬撰寫，預計執行時程由第二年期啟動日(以下簡稱 D-Day)開始推進，擬定驗證時程如下表 3.3-9、圖 3.3.13 之說明，實際執行視營運廠商規劃與契約時程進行動態調整作業，因平台精進及功能與 KPI 高度相關，最終上線之平台仍需研議各驗證項目以符合營運需求。

(2) 第二步驟-計畫制定

TÜV 依營運廠商所提出之小客車租賃服務整合旅遊生態系平台相關規格書或營運手冊等資料進行系統平台驗證計畫書或驗證項目撰寫作業，並完成經由三方(即運研所、營運廠商及 TÜV)合意認可之驗證計畫書或驗證項目。

(3) 第三階段-驗證測試

依 TÜV 撰寫之系統平台驗證計畫書或驗證項目之內容進行驗證測試作業，其中 TÜV 將記錄驗證測試之相關設置、驗證地點、驗證時間、參與人員、過程討論及驗證結果等資訊列為驗證測試之佐證資料。

(4) 第四階段-報告提出

TÜV 依驗證測試之過程與結果撰寫系統平台驗證報告書。

(5) 第五階段-符合聲明

TÜV 將依照系統驗證報告書之內容提送申請符合聲明申請(如符合性聲明、符合性證書等)，若其內容符合驗證預期之結果，則發放相關符合文件。

表 3.3-9 第二年期-小客車租賃服務整合旅遊生態系平台認證期程表

任務名稱	開始時間	完成時間	任務時間（日曆天）	文件	說明	擔當
規格研討	D-Day	D + 75	75	系統規格書*	包含APP、網站與後台相關之細部規格說明	營運廠商
				系統測試報告*	包含APP、網站與後台依規格進行測試驗證，測試項目包含功能驗證、安全性驗證、正確性驗證以及壓力驗證等項目。	
				系統維運與資安維護手冊*	包含APP、網站與後台如何持續營運並確保資安維護之說明。	
				* 或等同上述資訊之文件		
				規格確認	依上述營運廠商所提系統認證相關文件進行多方溝通討論，並確立其最終規格與其系統關鍵指標。	德國萊因 & 營運廠商
計畫制定	D + 75	D + 90	15	德國萊因- 系統平台驗證計畫書 / 驗證項目	完成由三方(即運研所、營運廠商及德國萊因)合意之「系統平台驗證計畫書」之撰寫。	德國萊因 & 營運廠商 & 運研所
驗證測試	D + 90	D + 120	30	德國萊因- 系統平台驗證計畫書 / 驗證項目	依三方合意之「系統平台驗證計畫書」之內容據以執行系統驗證作業。	德國萊因 & 營運廠商
技術討論	D + 90	D + 120	30	德國萊因-系統平台驗證記錄	詳實紀錄執行系統平台驗證測試作業時各項工作時之情形及發現，若有待釐清之事項或相關技術問題則需進行三方技術會議，確認相關驗證結果落實規範。	德國萊因 & 營運廠商 & 運研所
報告提出	D + 120	D + 135	15	德國萊因- 系統平台驗證報告書	依系統平台驗證作業之過程與結果製作報告書。	德國萊因
符合聲明	D + 135	D + 150	15	德國萊因- 系統平台符合聲明文件	若其系統平台驗證之關鍵指標可全數符合系統平台驗證計畫書之規範，則發放相關符合聲明(如符合性證書、符合性聲明等)。	德國萊因

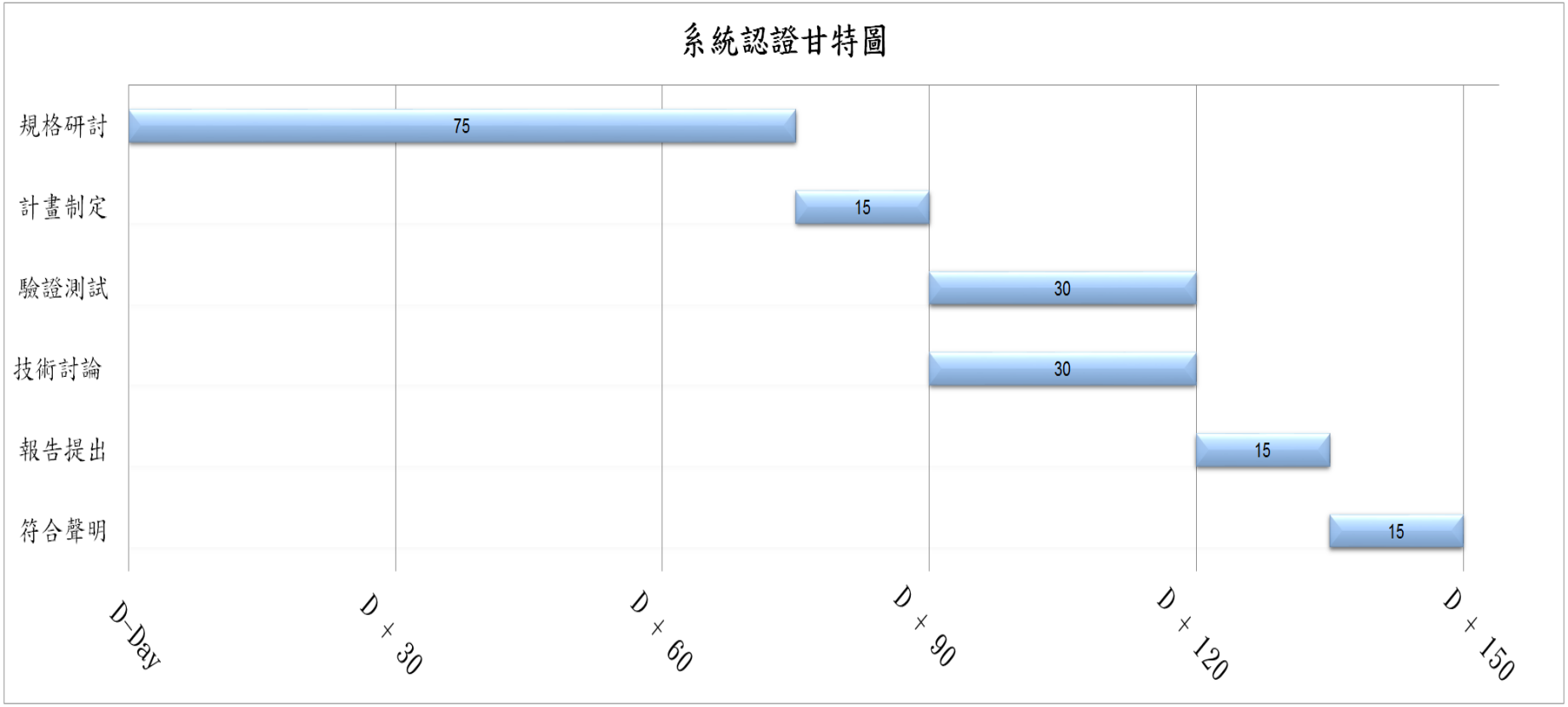


圖 3.3.13 第二年期-小客車租賃服務整合旅遊生態系平台認證甘特圖

第四章 結論與建議

本計畫執行目的是針對小客車租賃業數位轉型計畫之建置廠商-漢名科技進行專案管理與監督審驗，依照專案預計時程規劃執行，並提供特殊專業技能諮詢(交通、專案管理)，及導入第三方獨立監督審驗機制，透過完善測試規劃與驗測等，確保平台符合建置團隊、小客車租賃業者等各方之需求，亦能提升民眾使用便利性，創造多贏局面。

4.1 結論

以下針對本計畫主要三大工作項目，包含專案管理服務、專業知識諮詢與獨立監督審驗，所執行之成果進行綜整說明如下：

(一) 專案管理服務

1. 自 110 年 5 月 11 日起，截至 12 月 27 日止，已辦理 13 場次聯合工作會議，邀集主管機關、漢名科技、小客車租賃公會與業者代表等，共同參與會議，瞭解主計畫建置與推廣狀況，並釐清相關疑慮等。
2. 協助辦理分項二「智慧租車服務營運規劃與推動實務」子項一「商業模式設計與數位轉型推動實務」之採購、期初報告審查、期中報告審查、期末報告審查、經費支用查核(依科技部補助專題研究計畫經費處理原則)等行政作業。
3. 逐月管控主計畫之風險與相關疑慮。在公會對於主計畫可能產生疑慮之風險下，研提相對應之措施，如請漢名團隊與全聯會商談達成共識，於漢名團隊多次拜訪全聯會後，化解此疑慮。最終達成由全聯會輔導業者籌組營運團隊，並協助完成相關工作項目。
4. 針對漢名科技所提出之服務方案、研究方法、期初發表會簡報與企劃、招募計畫、深度計畫、系統技術文件等相關議題，研提意見與建議。

(二)專業知識諮詢

1. 多次與漢名科技討論第三方審驗認證期程與流程規劃，並要求相關技術文件之提供，以確保後續之第三方獨立監督審驗可順利進行。
2. 針對漢名科技之文件與企劃內容，提供交通與其他相關專業知識諮詢，以確保主計畫系統建置與推廣成果，能符合本計畫所需，並能增加可用性。

(三)獨立監督審驗

針對漢名科技於計畫期初之「智慧租車共通平台」，及功能優化建置之「新智

慧租車平台搭配旅遊生態系平台」，進行相關技術文件(如設計規格書、使用手冊、測試計畫書等)檢視，並研提相關建議與意見，及確認資安驗測與功能驗測之結果，於 110 年 12 月 1 日陸續取得漢名科技提供之「新智慧租車平台搭配旅遊生態系平台」完整系統開發、文件撰寫等內容後，完整檢視其相關資訊，並進行實際之整體功能驗測作業、資安驗測結果確認後，研提相關建議與意見，確保相關開發成果符合計畫目標。

由上述所執行之相關工作項目，及檢視漢名科技辦理成果與進度後，已初步完成系統開發，惟截至 110 年 12 月 27 日之整體實際功能驗測與測試後，仍有部分功能不符合計畫要求，已請漢名科技儘速完成相關功能修正。

4.2 建議

綜整本年度執行專案管理與監督審驗之經驗，研提建議俾供後續於辦理相關建置系統平台與推廣作業時，可做為借鏡參考。

1. 主計畫因涉及產業面實際運作，於召開相關工作會議、座談會或是說明會，建議均應邀請相關公協會單位與業者代表一同參與，更可瞭解產業面的想法與實際之做法。
2. 主計畫於建置平台時，因受功能優化與精進之影響，由原資策會平台轉為自行建置相關平台，在系統開發上耗費許多人力與經費，建議應於系統開發初期，完成需求規格書，並先行提供相關設計圖與流程示意圖，以此與產官學各界確認相關功能開發是否符合期待，將可減少系統開發時程。
3. 因平台智慧財產權歸屬本所，未來可能開放授權使用，建置團隊於系統建置階段，應確實完成相關技術文件，確保未來接手平台之人員，可依照技術文件內容，自行組建平台，並應提供系統維運手冊，俾利後續系統維運與優化。

參考文獻

1. 交通部統計處，106 年小客貨車租賃業營運狀況調查，民國 107 年 11 月。
2. Dabnery, B. J. and Barber, G. 2003. Direct ROI of software IV&V methodology and initial case studies. Assurance Technology Symposium, 5th June.
3. Charles, P. and Turner, P. Capabilities base acquisition: From theory to reality. Chips, Vol. 22, No. 3, pp. 38-49.
4. Rahman, R. A., Fhang, M. C. S., and Tong, W. W. 2018. IV&V experience framework: An experience paper on IV&V implementation in government project. 7th International Conference on Software and Computer Application, Kuantan Malaysia, Feb. 8-10, pp. 290-296.
5. Akella, P. S. and Rao, K. N. 2011. Effective independent quality assessment using IV&V, International Journal of Computer Science & Information Technology, Vol. 3, No. 3. pp. 188-198.
6. Easterbrook, S. 1996. The role of independent V&V in upstream software development process. 2nd World Conference on Integrated Design and Process Technology, Austin Texas, December 1-4.
7. Arthur, J. D., Groner, M. K. Hayhurst, J. K., and Holloway, C. M. 1999. Evaluating the effectiveness of independent verification and validation. IEEE, Vol. 32, Issue: 10.
8. Nielsen, J. and Landauer, T. K. 1993. “A mathematical model of the finding of usability problems,” Proceedings of ACM INTERCHI'93 Conference (Amsterdam, The Netherlands, 24-29 April 1993), pp. 206-213.

附件一 期中審查意見回覆表

交通部運輸研究所合作研究計畫

期中報告審查意見處理情形表

一、編號：MOTC-IOT-110-MEB005

二、計畫名稱：小客車租賃業數位轉型發展計畫-商業模式設計與數位轉型推動實務之專案管理及監督審驗

三、執行單位：逢甲大學

審查委員	審查意見	合作研究單位 處理情形	本所計畫 承辦單位 審查意見
交通部觀光局趙志民副主任	建議補充說明國內外小客車租賃業經營模式等相關文獻內容，並可參考運研所運輸資訊組「Taiwan Pass 數位旅遊服務整合平台規劃案」所分析之相關經營模式，作為後續主計畫「智慧租車共通平台」營運之參考依據。	感謝委員建議，後續將整理相關文獻補充於期末報告 2.1 節中。	同意研究單位處理意見。
	建議補充說明目前交通部與經濟部等部會所推行之相似案例(如：觀光圈、好玩卡等)，並檢視主計畫「旅遊生態系平台」與上開計畫整合之可行性。	遵照辦理，相關內容補充於期末報告 2.1 節中說明。	同意研究單位處理意見。
	主計畫招募業者期間，建議本計畫可協助訂定上下架機制、評鑑機制等，確保營運規範之建立。	遵照辦理，研究團隊已於相關會議中，協助主計畫訂定相關營運規範。	同意研究單位處理意見。
	除附件一滲透測試外，建議補充說明主計畫建置「智慧	遵照辦理，研究團隊將針對主計畫進行之資安測試結果進行	同意研究單位處理

審查委員	審查意見	合作研究單位 處理情形	本所計畫 承辦單位 審查意見
	租車共通平台」之原碼檢測、弱點掃描等資安測試結果，或是針對主計畫自主資安測試，進行結果檢視。	檢視，並補充於期末報告 3.2.2 節中。	意見。
國立陽明交通大學邱裕鈞教授	建議補充說明國內外小客車租賃業經營模式、獨立驗證與認證 (Independent Verification and Validation, IV&V)用於平台開發之相關文獻內容。	感謝委員建議，因小客車租賃系統平台之 IV&V 並無發現相關文獻。因系統平台開發包含軟體開發環節，故於期末報告 2.2 節中增加軟體開發的 IV&V 說明。	同意研究單位處理意見。
	目前已針對主計畫提出之企劃書或相關文件研提意見，建議後續可採用意見追蹤管考表的方式，追蹤主計畫辦理狀況，並可針對主計畫文件更新與整理狀況進行說明。	遵照辦理，意見追蹤管考表將補充於期末報告 3.1.3 節中。	同意研究單位處理意見。
	除將小客車租賃業者招募家數，列入風險控管外，建議也可將 10,000 筆人車路數據資料、出租率提升 3%等工作項目，納入風險控管中，定期檢視達成狀況，避免風險產生。	遵照辦理，相關風險將納入期末報告 3.1.6 節中。	同意研究單位處理意見。
看見臺灣基金會脫宗華顧問	建議補充說明國外對於獨立驗證與認證 (Independent Verification and Validation, IV&V)用於小客車租賃業平台之相關文獻。	感謝委員建議，因小客車租賃系統平台之 IV&V 並無發現相關文獻。因系統平台開發包含軟體開發環節，故於期末報告 2.2 節中增加軟體開發的 IV&V	同意研究單位處理意見。

審查委員	審查意見	合作研究單位 處理情形	本所計畫 承辦單位 審查意見
		說明。	
	建議補充說明小客車租賃商業同業公會與業者對於主計畫執行中可能產生之風險，並說明對應之處理措施與解決方案，以期降低風險發生機率。	遵照辦理，相關風險將納入期末報告 3.1.6 節中。	同意研究單位處理意見。
	建議補充說明本計畫對於主計畫進行監督與審驗之執行細節，及最終審查結果。	遵照辦理，針對主計畫相關審查結果將納入期末報告第四章說明。	同意研究單位處理意見。
淡江大學羅孝賢副教授	建議補充說明本計畫之定位與角色。	感謝委員建議，研究團隊將補充計畫之定位與角色，並納入期末報告中 1.3 節中。	同意研究單位處理意見。
	建議確認主計畫目前應屬於概念驗證(Proof of Concept, POC)、服務驗證(Proof of Service, POS)或是商業驗證(Proof of Business, POB)之執行階段，並監督主計畫執行狀況，確保商業模式、服務流程、營運主體得以永續營運。	遵照辦理，將納入期末報告第四章說明。	同意研究單位處理意見。
	建議補充說明小客車租賃商業同業公會、主管機關對於主計畫之態度，所可能產生之風險，及後續對應之處理措施。	遵照辦理，相關風險將納入期末報告 3.1.6 節中說明。	同意研究單位處理意見。
	因應目前資安檢測相關規定較為嚴苛，建議補充說明主	遵照辦理，研究團隊將檢視主計畫資安測試結果，並補充於	同意研究單位處理

審查委員	審查意見	合作研究單位 處理情形	本所計畫 承辦單位 審查意見
	計畫建置之平台，能否於計畫結束前，完成相關資安認證與檢測，確保後續平台能順利上線營運。	期末報告 3.2.2 節中。	意見。

附件二 期末審查意見回覆表

交通部運輸研究所合作研究計畫

期末報告審查意見處理情形表

一、編號：MOTC-IOT-110-MEB005

二、計畫名稱：小客車租賃業數位轉型發展計畫-商業模式設計與數位轉型推動實務之專案管理及監督審驗

三、執行單位：逢甲大學

審查委員	審查意見	合作研究單位 處理情形	本所計畫 承辦單位 審查意見
淡江大學羅孝賢副教授	請補充說明本計畫專案管理風險控管之成果。因建置商尚未完成系統建置與開發、數據匯入等工作項目，且僅完成 POC，未完成 POS 與 POB 階段，似有進度落後情形，請補充說明相對應之風險管控對策與處理情形。	本案建置商於 12 月 1 日完成系統初步開發並提供本所進行測試，針對系統功能、資料內容、使用流程、易用性等項目進行測試，並提供相關意見供建置商進行後續修正。本計畫透過即時溝通，並請建置商即時修正，以此爭取時間來控制風險。	同意研究單位處理意見。
	請補充說明調查小客車租賃業者與消費者之接受度，係屬建置商之工作，或由本計畫執行？其相關結果為何？建請補充說明。	感謝委員建議，關於小客車租賃業者與消費者之接受度調查，係由建置商來執行，並由本所提供相關意見。	同意研究單位處理意見。
	請補充說明本計畫在資安查核驗測部分的角色，係由建置商或是本計畫執行？系統平台正式上線前，應完成行動應用 APP 基本資安檢測基準 V3.1。	資安查核應由建置商自行提出，確保相關功能建置商均已自行初測後，再由本所協助檢視，相關驗測成果之正確性。今年度建置商以開發 PWA 為主，後續如有完成開發 APP，會再協助確認是否已完成行動應用	同意研究單位處理意見。

審查委員	審查意見	合作研究單位 處理情形	本所計畫 承辦單位 審查意見
		APP 基本資安檢測。	
	小客車租賃業者對於「智慧租車平台搭配旅遊生態系平台」之接受程度與態度如何？未來平台營運商為何？建請補充說明。	建置商已完成辦理兩場次系統功能展示說明暨意見交流座談會議，公會與小客車租賃業者認同該平台。計畫期間漢名科技為平台營運商，後續俟完成技術授權後，將另尋確平台營運商，目前全聯會表達將承接該平台營運意願。	同意研究單位處理意見。
國立陽明交通大學邱裕鈞教授	KPI 數據(如提升出租率 3%、10000 筆人車路交易資料)建議研究團隊提供主計畫相關計算方法之建議。	遵照辦理，已於 11 月 12 日工作會議中提出相關建議：(1)可先針對加入區域聯盟之小客車租賃業者，進行輔導推動前、後之出租率狀況比較，並完整說明下年期執行提升出租率之具體作法；(2)關於 10000 筆人車路交易資料，建置商已規劃相關試營運計畫，亦預計於 12 月底前完成該項 KPI。	同意研究單位處理意見。
	建議研究團隊針對監督審驗過程中所發現之問題，應歸類於哪個等級，及建置商是否於限期中完成或是延遲至何時才完成，建議持續進行列管，並建立追蹤列管表，納入期末報告中呈現。	遵照辦理，已綜整並新增追蹤列管表，詳如 3.1.2 節所示。	同意研究單位處理意見。
	小客車租賃業者大者恆大、單一廠商獨立市場之論述，似不宜作為本平台推動之主	感謝委員建議，已修正 2.3 節相關內容，以更貼近市場現況。	同意研究單位處理

審查委員	審查意見	合作研究單位 處理情形	本所計畫 承辦單位 審查意見
	因。		意見。
	建議測試結果與報告修訂內容應相對應，並修飾相關用字遣詞。	遵照辦理，已修訂 3.2 節用字遣詞。	同意研究單位處理意見。
國立成功大學陳勁甫特聘教授	建議研究團隊確認主計畫進行系統優化功能之完成度，及是否達成專案預期目標、預期功能？建議補充說明。	本案建置商於 12 月 1 日完成系統初步開發並提供本所進行測試，本所已於 12 月 22 日提供相關意見供建置商進行後續修正，並經溝通討論後，確保建置商確實完成修正，以達成專案目標。	同意研究單位處理意見。
	報告書中關於全國聯合會對於旅遊生態系功能優化有所疑慮，是否已確實解決？應明確說明，並列為下年度風險控管項目。	遵照辦理，已補充相關風險控制措施及說明於 3.1.5 節。	同意研究單位處理意見。
	請補充說明如何產出相關驗測題目？及相關測試項目之測試次數等內容，並請確認建置商是否依此測試結果進行系統修正與優化。	遵照辦理，產出驗測題目、測試次數等均已補充說明於 3.2.2.2 節中。	同意研究單位處理意見。
	請補充說明易用性測試之情境如何設計？科技接受有用性及接受度為數位轉型成功關鍵，請多加著墨說明。	遵照辦理，已補充說明於 3.2.2.2 節中。	同意研究單位處理意見。
	監督審驗所提出之測試物件之問題，是否已確實改善？後續應如何追蹤？並確認是	因建置商仍持續進行系統改善作業，後續可由報告書中相關測試結果如表 3.3-7 中之說明進	同意研究單位處理意見。

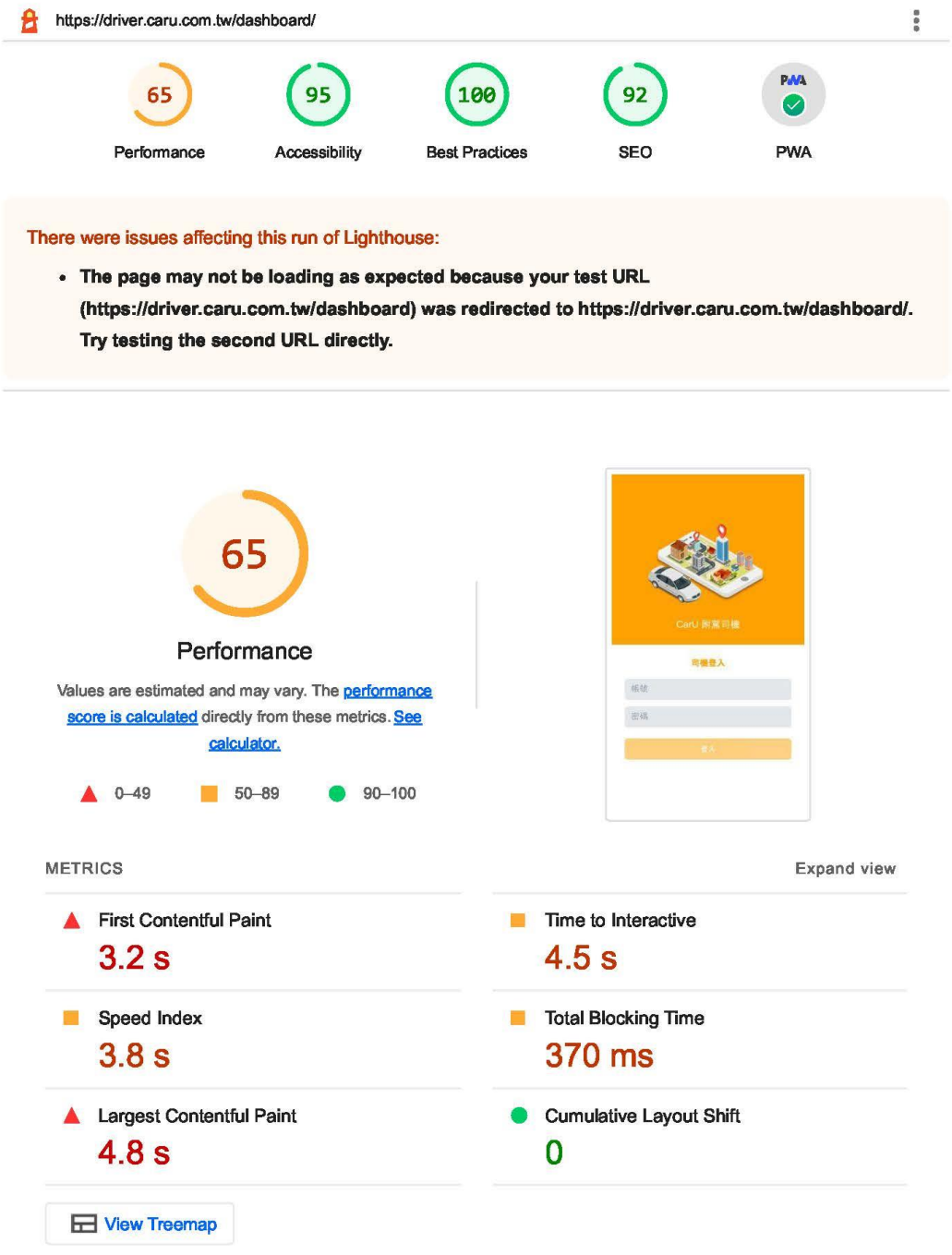
審查委員	審查意見	合作研究單位 處理情形	本所計畫 承辦單位 審查意見
	否已完成驗證(Verification)與認證(Validation)。	行追蹤作業，本次報告因系統仍持續進行改善，故僅以驗證(Verification)進行驗證作業，Validation 仍無法完整進行。	
逢甲大學李克聰退休教授	建議報告內容仍須依照研究主題與重點中之工作項目逐項撰寫，並補充說明本計畫實際發生之風險及控管情形，例如逐月滾動風險控管過程及實際內容與成效。	遵照辦理，已綜整並新增追蹤列管表，詳如 3.1.2 節所示。並補充相關風險控制措施及說明於 3.1.5 節。	同意研究單位處理意見。
	目前僅處於 POC 階段，後續 POS 與 POB 階段，建議須釐清結果。針對建置商所提出之使用者與小客車租賃業者接受度，協助研提相關意見。	遵照辦理，將納入期末報告第四章說明。關於小客車租賃業者與消費者之接受度調查，將由建置商來執行，惟建置商尚未完成相關調查，故尚無法協助提供相關意見。	同意研究單位處理意見。
	期末報告中，表 3.3-4 之發現事項說明與判定結果均為空白，建請依照實際驗測結果補充說明。	遵照辦理，已將實際測試結果說明補充於表 3.3-7。	同意研究單位處理意見。
	建置商之 KPI 是否均有達成？如未達成而造成減價驗收，研究團隊是否須擔負相關責任？建請補充說明。	每週定期追蹤建置商辦理狀況，於工作會議上，針對逾期未辦事項進行提醒，並協助瞭解其困難之處，若建置商於契約執行期間仍未完成相關工作，依契約規範，將採取減價驗收。	同意研究單位處理意見。
交通部路政司張舜	主計畫專案進度延後，建置商、研究團隊之責任為何？	每週定期追蹤建置商辦理狀況，於工作會議上，針對逾期未	同意研究單位處理

審查委員	審查意見	合作研究單位 處理情形	本所計畫 承辦單位 審查意見
清副司長	建請補充說明。	辦事項進行提醒，並協助瞭解其困難之處，若建置商於契約執行期間仍未完成相關工作，依契約規範，將採取減價驗收。	意見。
	期末報告審查簡報中 p.45-52 之易用性情境，是否符合主計畫所需或是 600 多家小客車租賃業者之需求？4 家小客車租賃車商進行測試之代表性是否足夠？建議補充說明。	遵照辦理，已補充說明於 3.2.2.2 節中。	同意研究單位處理意見。
	關於第二年計畫之旅遊生態系內容，請考量其後續對策與提出配套方案，並納入下年度風險控管內容。	感謝委員建議，鑒於建置商執行狀況，已綜整各類別工作項目辦理情形，討論契約規範內容後，納入明年度招標文件中。	同意研究單位處理意見。
本所運輸經營管理組陳組長其華	因應主計畫之建置與開發成果延宕，影響本計畫 12 月 1 日提送之期末報告書之完整性，後續建請研究團隊進行補充說明。	遵照辦理，已補充說明測試成果與相關內容。	同意研究單位處理意見。
	針對研究團隊今日所提出相關意見，建請建置商完成相關內容修訂。	敬悉。	同意研究單位處理意見。
本所運輸經營管理組(書面)	本案契約規定提送期末報告時間為 12 月 1 日，當時主計畫尚未完全提供研發成果，致使部分測試項目在提送期末報告後才能進行，相關測	遵照辦理，已將實際測試結果說明補充於表 3.3-7。	同意研究單位處理意見。

審查委員	審查意見	合作研究單位 處理情形	本所計畫 承辦單位 審查意見
	試結果已於今日簡報說明，請將測試結果納入期末修訂報告。		
交通部公路總局	針對期末報告審查簡報P.45，選定之4位小客車租賃業者是否具代表性？建請補充說明。	遵照辦理，已補充說明於3.2.2.2節中。	同意研究單位處理意見。

附件三 PWA 頁面驗證(PWA Scan report by Lighthouse)

driver.caru.com.tw



Show audits relevant to: All FCP TBT LCP CLS

OPPORTUNITIES

Opportunity	Estimated Savings
Serve images in next-gen formats	0.9 s
Properly size images	0.6 s
Reduce unused JavaScript	0.3 s
Avoid serving legacy JavaScript to modern browsers	0.3 s

These suggestions can help your page load faster. They don't directly affect the Performance score.

DIAGNOSTICS

- Largest Contentful Paint image was lazily loaded
- Image elements do not have explicit `width` and `height`
- Serve static assets with an efficient cache policy — 8 resources found
- First Contentful Paint (3G) — 5883 ms
- Avoid chaining critical requests — 1 chain found
- Keep request counts low and transfer sizes small — 10 requests • 429 KiB
- Largest Contentful Paint element — 1 element found
- Avoid long main-thread tasks — 6 long tasks found
- Avoid non-composited animations — 1 animated element found

More information about the performance of your application. These numbers don't directly affect the Performance score.

PASSED AUDITS (26)

Show

Accessibility

These checks highlight opportunities to improve the accessibility of your web app. Only a subset of accessibility issues can be automatically detected so manual testing is also encouraged.

CONTRAST

▲ Background and foreground colors do not have a sufficient contrast ratio.

These are opportunities to improve the legibility of your content.

ADDITIONAL ITEMS TO MANUALLY CHECK (10)

Show

These items address areas which an automated testing tool cannot cover. Learn more in our guide on conducting an accessibility review.

PASSED AUDITS (9)

Show

NOT APPLICABLE (34)

Show

Best Practices

TRUST AND SAFETY

Ensure CSP is effective against XSS attacks

GENERAL

Detected JavaScript libraries

PASSED AUDITS (14) Show

NOT APPLICABLE (1) Show

SEO

These checks ensure that your page is following basic search engine optimization advice. There are many additional factors Lighthouse does not score here that may affect your search ranking, including performance on Core Web Vitals. Learn more.

CONTENT BEST PRACTICES

Document does not have a meta description Description text is empty.

Format your HTML in a way that enables crawlers to better understand your app's content.

ADDITIONAL ITEMS TO MANUALLY CHECK (1) Show

Run these additional validators on your site to check additional SEO best practices.

PASSED AUDITS (11) Show

NOT APPLICABLE (2) Show

PWA

These checks validate the aspects of a Progressive Web App. Learn more.

INSTALLABLE

- Web app manifest and service worker meet the installability requirements

PWA OPTIMIZED

- Registers a service worker that controls page and `start_url`
- Configured for a custom splash screen
- Sets a theme color for the address bar.
- Content is sized correctly for the viewport
- Has a `<meta name="viewport">` tag with `width` or `initial-scale`
- Provides a valid `apple-touch-icon`
- Manifest has a maskable icon

ADDITIONAL ITEMS TO MANUALLY CHECK (3) Show

store.caru.com.tw

https://store.caru.com.tw/dashboard/

Performance	Accessibility	Best Practices	SEO	PWA
68	95	100	92	

There were issues affecting this run of Lighthouse:

- **The page may not be loading as expected because your test URL (https://store.caru.com.tw/dashboard) was redirected to https://store.caru.com.tw/dashboard/. Try testing the second URL directly.**

68

Performance

Values are estimated and may vary. The performance score is calculated directly from these metrics. See calculator.

▲ 0–49 ■ 50–89 ● 90–100

METRICS Expand view

▲ First Contentful Paint 3.2 s	■ Time to Interactive 4.5 s
■ Speed Index 3.8 s	■ Total Blocking Time 340 ms
▲ Largest Contentful Paint 4.5 s	● Cumulative Layout Shift 0

View Treemap

Show audits relevant to: All FCP TBT LCP CLS

OPPORTUNITIES

Opportunity	Estimated Savings
Properly size images	0.62 s
Serve images in next-gen formats	0.62 s
Reduce unused JavaScript	0.3 s
Avoid serving legacy JavaScript to modern browsers	0.3 s

These suggestions can help your page load faster. They don't directly affect the Performance score.

DIAGNOSTICS

- Largest Contentful Paint image was lazily loaded
- Image elements do not have explicit `width` and `height`
- Serve static assets with an efficient cache policy — 9 resources found
- First Contentful Paint (3G) — 5889 ms
- Avoid chaining critical requests — 1 chain found
- Keep request counts low and transfer sizes small — 11 requests • 368 KiB
- Largest Contentful Paint element — 1 element found
- Avoid long main-thread tasks — 5 long tasks found
- Avoid non-composited animations — 1 animated element found

More information about the performance of your application. These numbers don't directly affect the Performance score.

PASSED AUDITS (26)

Show

Accessibility

These checks highlight opportunities to improve the accessibility of your web app. Only a subset of accessibility issues can be automatically detected so manual testing is also encouraged.

CONTRAST

▲ **Background and foreground colors do not have a sufficient contrast ratio.**

These are opportunities to improve the legibility of your content.

ADDITIONAL ITEMS TO MANUALLY CHECK (10) Show

These items address areas which an automated testing tool cannot cover. Learn more in our guide on conducting an accessibility review.

PASSED AUDITS (9) Show

NOT APPLICABLE (34) Show

Best Practices

TRUST AND SAFETY

Ensure CSP is effective against XSS attacks

GENERAL

Detected JavaScript libraries

PASSED AUDITS (14) Show

NOT APPLICABLE (1) Show

SEO

These checks ensure that your page is following basic search engine optimization advice. There are many additional factors Lighthouse does not score here that may affect your search ranking, including performance on Core Web Vitals. Learn more.

CONTENT BEST PRACTICES

Document does not have a meta description Description text is empty.

Format your HTML in a way that enables crawlers to better understand your app's content.

ADDITIONAL ITEMS TO MANUALLY CHECK (1) Show

Run these additional validators on your site to check additional SEO best practices.

PASSED AUDITS (11) Show

NOT APPLICABLE (2) Show

PWA

These checks validate the aspects of a Progressive Web App. Learn more.

INSTALLABLE

- Web app manifest and service worker meet the installability requirements

PWA OPTIMIZED

- Registers a service worker that controls page and `start_url`
- Configured for a custom splash screen
- Sets a theme color for the address bar.
- Content is sized correctly for the viewport
- Has a `<meta name="viewport">` tag with `width` or `initial-scale`
- Provides a valid `apple-touch-icon`
- Manifest has a maskable icon

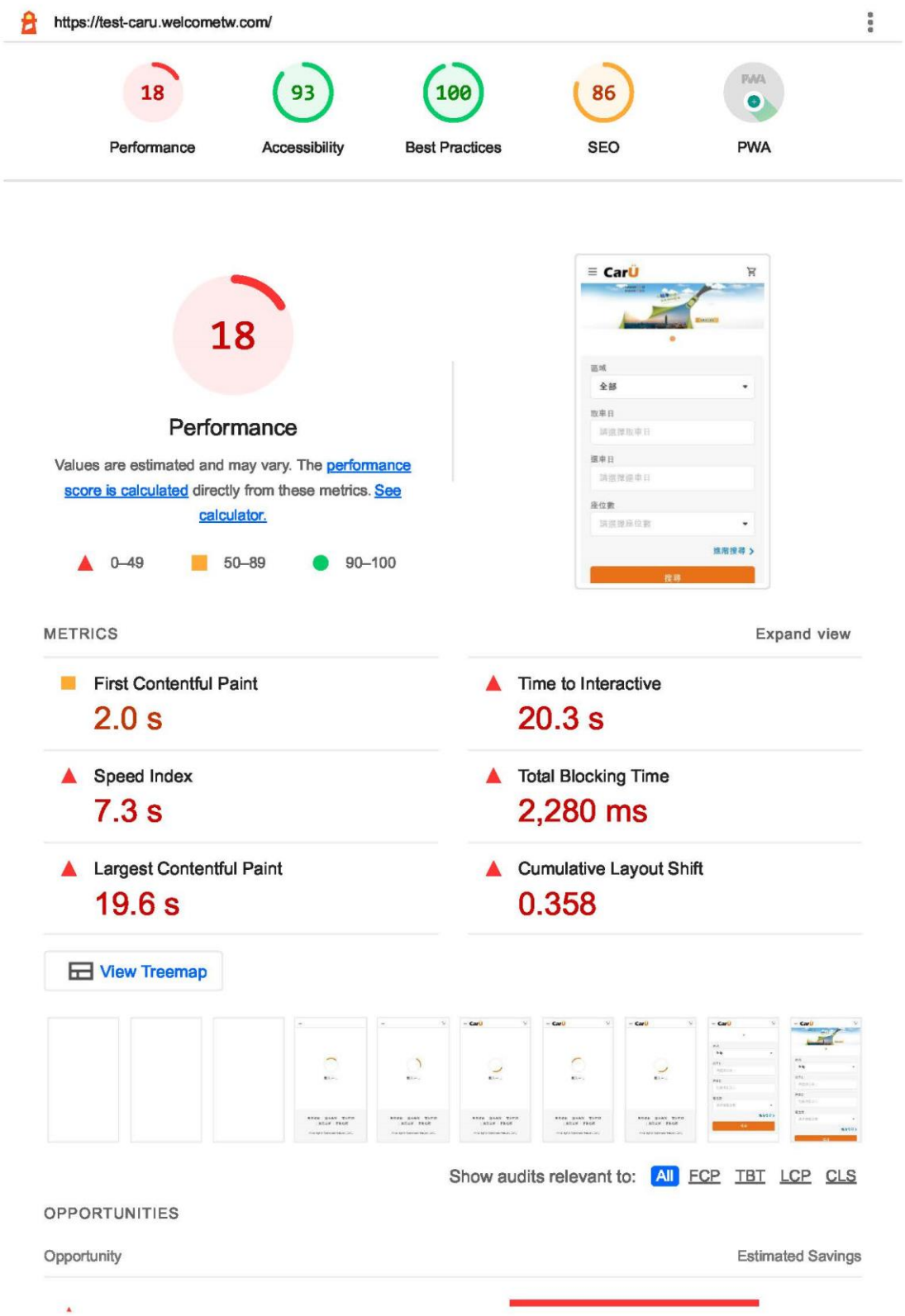
ADDITIONAL ITEMS TO MANUALLY CHECK (3) Show

These checks are required by the baseline PWA Checklist but are not automatically checked by Lighthouse. They do not affect your score but it's important that you verify them manually.

Captured at Dec 3, 2021, 1:15 PM GMT+8	Emulated Moto G4 with Lighthouse 9.0.0	Single page load
Initial page load	Unknown	Using HeadlessChromium 95.0.4638.69 with lr

Generated by **Lighthouse** 9.0.0 | File an issue

test-caru.welcometw.com



▲	Serve images in next-gen formats	44.1 s
▲	Properly size images	18.15 s
▲	Enable text compression	12.3 s
▲	Reduce unused JavaScript	7.35 s
▲	Minify JavaScript	7.2 s
▲	Efficiently encode images	2.55 s
▲	Eliminate render-blocking resources	0.92 s
■	Reduce unused CSS	0.3 s
■	Minify CSS	0.15 s

These suggestions can help your page load faster. They don't directly affect the Performance score.

DIAGNOSTICS

▲	Avoid enormous network payloads — Total size was 16,528 KiB
▲	Serve static assets with an efficient cache policy — 78 resources found
▲	Does not use passive listeners to improve scrolling performance
▲	Image elements do not have explicit `width` and `height`
▲	Minimize main-thread work — 7.5 s
▲	Avoid an excessive DOM size — 1,751 elements
■	First Contentful Paint (3G) — 3990 ms
■	Reduce JavaScript execution time — 2.6 s
○	Avoid chaining critical requests — 1 chain found
○	Keep request counts low and transfer sizes small — 85 requests • 16,528 KiB
○	Largest Contentful Paint element — 1 element found
○	Avoid large layout shifts — 3 elements found
○	Avoid long main-thread tasks — 11 long tasks found

Avoid non-composited animations — 81 animated elements found

More information about the performance of your application. These numbers don't directly affect the Performance score.

PASSED AUDITS (16) Show

Accessibility

These checks highlight opportunities to improve the accessibility of your web app. Only a subset of accessibility issues can be automatically detected so manual testing is also encouraged.

ARIA

[aria-hidden="true"] elements contain focusable descendents

These are opportunities to improve the usage of ARIA in your application which may enhance the experience for users of assistive technology, like a screen reader.

CONTRAST

Background and foreground colors do not have a sufficient contrast ratio.

These are opportunities to improve the legibility of your content.

NAMES AND LABELS

Links do not have a discernible name

These are opportunities to improve the semantics of the controls in your application. This may enhance the experience for users of assistive technology, like a screen reader.

ADDITIONAL ITEMS TO MANUALLY CHECK (10) Show

These items address areas which an automated testing tool cannot cover. Learn more in our guide on conducting an accessibility review.

PASSED AUDITS (17) Show

NOT APPLICABLE (24) Show

Best Practices

TRUST AND SAFETY

- Ensure CSP is effective against XSS attacks

GENERAL

- Detected JavaScript libraries
- Missing source maps for large first-party JavaScript

PASSED AUDITS (13) Show

NOT APPLICABLE (1) Show

SEO

These checks ensure that your page is following basic search engine optimization advice. There are many additional factors Lighthouse does not score here that may affect your search ranking, including performance on Core Web Vitals. Learn more.

CONTENT BEST PRACTICES

▲ Document does not have a meta description

Format your HTML in a way that enables crawlers to better understand your app's content.

MOBILE FRIENDLY

▲ Tap targets are not sized appropriately — 18% appropriately sized tap targets

Make sure your pages are mobile friendly so users don't have to pinch or zoom in order to read the content pages. Learn more.

ADDITIONAL ITEMS TO MANUALLY CHECK (1)

Show

Run these additional validators on your site to check additional SEO best practices.

PASSED AUDITS (11)

Show

NOT APPLICABLE (1)

Show

PWA

These checks validate the aspects of a Progressive Web App. Learn more.

INSTALLABLE

- Web app manifest and service worker meet the installability requirements

PWA OPTIMIZED

- Registers a service worker that controls page and `start_url`
- Configured for a custom splash screen
- Does not set a theme color for the address bar.
  Failures: No `<meta name="theme-color">` tag found.
- Content is sized correctly for the viewport
- Has a `<meta name="viewport">` tag with `width` or `initial-scale`
- Does not provide a valid `apple-touch-icon`
- Manifest doesn't have a maskable icon

ADDITIONAL ITEMS TO MANUALLY CHECK (3)

Show

These checks are required by the baseline PWA Checklist but are not automatically checked by Lighthouse. They do not affect your score but it's important that you verify them manually.

Captured at Dec 3, 2021, 1:11 PM GMT+8
Initial page load
Emulated Moto G4 with Lighthouse 9.0.0
Unknown
Single page load
Using HeadlessChromium 95.0.4638.69 with lr

附件四 弱點掃描

b2b-api.caru.com.tw

Burp Scanner Report

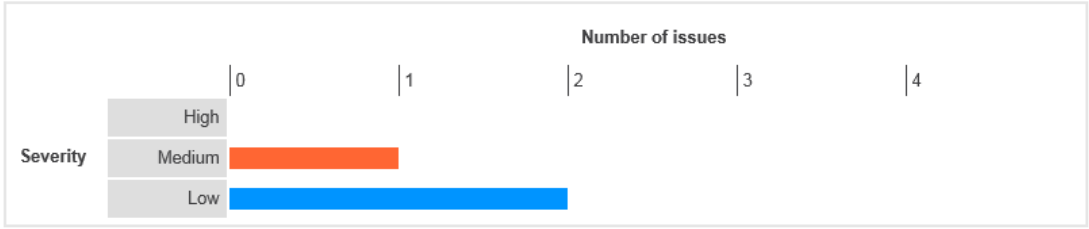
Burp Suite Professional

Summary

The table below shows the numbers of issues identified in different categories. Issues are classified according to severity as High, Medium, Low or Information. This reflects the likely impact of each issue for a typical organization. Issues are also classified according to confidence as Certain, Firm or Tentative. This reflects the inherent reliability of the technique that was used to identify the issue.

Severity	Confidence			
	Certain	Firm	Tentative	Total
High	0	0	0	0
Medium	1	0	0	1
Low	2	0	0	2
Information	1	1	0	2

The chart below shows the aggregated numbers of issues identified in each category. Solid colored bars represent issues with a confidence level of Certain, and the bars fade as the confidence level falls.



Contents

1. TLS certificate
2. Password field with autocomplete enabled
3. Strict transport security not enforced
4. Frameable response (potential Clickjacking)
5. Robots.txt file

1. TLS certificate

Next

Summary

Severity:	**Medium**
Confidence:	**Certain**
Host:	**https://b2b-api.caru.com.tw**
Path:	**/**

Issue detail

The following problem was identified with the server's TLS certificate:

- The server's certificate is not trusted.

Note: Burp relies on the Java trust store to determine whether certificates are trusted. The Java trust store does not include every root CA certificate that is included within browser trust stores. Burp might incorrectly report that a certificate is not trusted, if a valid root CA certificate is being used that is not included in the Java trust store.

The server presented the following certificates:

Server certificate

Issued to: dealer2.caru.com.tw, b2b-api.caru.com.tw, test-dev.caru.com.tw
Issued by: R3
Valid from: Tue Nov 02 22:28:26 GMT+08:00 2021
Valid to: Mon Jan 31 22:28:25 GMT+08:00 2022

Certificate chain #1

Issued to: R3
Issued by: ISRG Root X1
Valid from: Fri Sep 04 08:00:00 GMT+08:00 2020
Valid to: Tue Sep 16 00:00:00 GMT+08:00 2025

Certificate chain #2

Issued to: ISRG Root X1
Issued by: DST Root CA X3
Valid from: Thu Jan 21 03:14:03 GMT+08:00 2021
Valid to: Tue Oct 01 02:14:03 GMT+08:00 2024

Issue background

TLS (or SSL) helps to protect the confidentiality and integrity of information in transit between the browser and server, and to provide authentication of the server's identity. To serve this purpose, the server must present an TLS certificate that is valid for the server's hostname, is issued by a trusted authority and is valid for the current date. If any one of these requirements is not met, TLS connections to the server will not provide the full protection for which TLS is designed.

It should be noted that various attacks exist against TLS in general, and in the context of HTTPS web connections in particular. It may be possible for a determined and suitably-positioned attacker to compromise TLS connections without user detection even when a valid TLS certificate is used.

References

- SSL/TLS Configuration Guide

Vulnerability classifications

- CWE-295: Improper Certificate Validation
- CWE-326: Inadequate Encryption Strength
- CWE-327: Use of a Broken or Risky Cryptographic Algorithm

2. Password field with autocomplete enabled

Previous Next

Summary

Severity:	Low
Confidence:	Certain
Host:	https://b2b-api.caru.com.tw
Path:	/

Issue detail

The page contains a form with the following action URL:

- https://b2b-api.caru.com.tw/index.php

The form contains the following password field with autocomplete enabled:

- password

Issue background

Most browsers have a facility to remember user credentials that are entered into HTML forms. This function can be configured by the user and also by applications that employ user credentials. If the function is enabled, then credentials entered by the user are stored on their local computer and retrieved by the browser on future visits to the same application.

The stored credentials can be captured by an attacker who gains control over the user's computer. Further, an attacker who finds a separate application vulnerability such as cross-site scripting may be able to exploit this to retrieve a user's browser-stored credentials.

Issue remediation

To prevent browsers from storing credentials entered into HTML forms, include the attribute **autocomplete="off"** within the FORM tag (to protect all form fields) or within the relevant INPUT tags (to protect specific individual fields).

Please note that modern web browsers may ignore this directive. In spite of this there is a chance that not disabling autocomplete may cause problems obtaining PCI compliance.

Vulnerability classifications

- CWE-200: Information Exposure

Request

```
GET / HTTP/1.1
Host: b2b-api.caru.com.tw
Cookie: 85f1e6839dee694ea47b2e9ffe89d244=atcbq73vmi03lhlciat7kshani
Cache-Control: max-age=0
Sec-Ch-Ua: " Not A;Brand";v="99", "Chromium";v="96", "Google Chrome";v="96"
```

```
Sec-Ch-Ua: " Not A;Brand";v="99", "Chromium";v="96", "Google Chrome";v="96"
Sec-Ch-Ua-Mobile: ?0
Sec-Ch-Ua-Platform: "Windows"
Dnt: 1
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/96.0.4664.45 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
Sec-Fetch-Site: none
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Sec-Fetch-Dest: document
Accept-Encoding: gzip, deflate
Accept-Language: zh-TW,zh;q=0.9,ja-JP;q=0.8,ja;q=0.7,en-US;q=0.6,en;q=0.5
Connection: close
```

Response

```
HTTP/1.1 503 Service Unavailable
Date: Thu, 02 Dec 2021 05:34:59 GMT
Server: Apache/2.4.41 (Ubuntu)
X-Content-Type-Options: nosniff
Expires: Wed, 17 Aug 2005 00:00:00 GMT
Last-Modified: Thu, 02 Dec 2021 05:34:59 GMT
Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0
Pragma: no-cache
Content-Length: 3153
Connection: close
Content-Type: text/html; charset=utf-8

<!DOCTYPE html>
<html lang="en-gb" dir="ltr">
<head>
  <meta name="viewport" content="width=device-width, initial-scale=1.0" />
  <meta charset="utf-8" />
  <meta name="robots" content="noindex, nofollow
...[SNIP]...
</div>
```

3. Strict transport security not enforced

Previous Next

Summary

Severity:	**Low**
Confidence:	**Certain**
Host:	**https://b2b-api.caru.com.tw**
Path:	**/**

Issue description

The application fails to prevent users from connecting to it over unencrypted connections. An attacker able to modify a legitimate user's network traffic could bypass the application's use of SSL/TLS encryption, and use the application as a platform for attacks against its users. This attack is performed by rewriting HTTPS links as HTTP, so that if a targeted user follows a link to the site from an HTTP page, their browser never attempts to use an encrypted connection. The sslstrip tool

automates this process.

To exploit this vulnerability, an attacker must be suitably positioned to intercept and modify the victim's network traffic.This scenario typically occurs when a client communicates with the server over an insecure connection such as public Wi-Fi, or a corporate or home network that is shared with a compromised computer. Common defenses such as switched networks are not sufficient to prevent this. An attacker situated in the user's ISP or the application's hosting infrastructure could also perform this attack. Note that an advanced adversary could potentially target any connection made over the Internet's core infrastructure.

Issue remediation

The application should instruct web browsers to only access the application using HTTPS. To do this, enable HTTP Strict Transport Security (HSTS) by adding a response header with the name 'Strict-Transport-Security' and the value 'max-age=expireTime', where expireTime is the time in seconds that browsers should remember that the site should only be accessed using HTTPS. Consider adding the 'includeSubDomains' flag if appropriate.

Note that because HSTS is a "trust on first use" (TOFU) protocol, a user who has never accessed the application will never have seen the HSTS header, and will therefore still be vulnerable to SSL stripping attacks. To mitigate this risk, you can optionally add the 'preload' flag to the HSTS header, and submit the domain for review by browser vendors.

References

- HTTP Strict Transport Security
- sslstrip
- HSTS Preload Form

Vulnerability classifications

- CWE-523: Unprotected Transport of Credentials
- CAPEC-94: Man in the Middle Attack
- CAPEC-157: Sniffing Attacks

Request

```
GET / HTTP/1.1
Host: b2b-api.caru.com.tw
Cookie: 85f1e6839dee694ea47b2e9ffe89d244=atcbq73vmi03lhlciat7kshani
Cache-Control: max-age=0
Sec-Ch-Ua: " Not A;Brand";v="99", "Chromium";v="96", "Google Chrome";v="96"
Sec-Ch-Ua-Mobile: ?0
Sec-Ch-Ua-Platform: "Windows"
Dnt: 1
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/96.0.4664.45 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
Sec-Fetch-Site: none
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Sec-Fetch-Dest: document
Accept-Encoding: gzip, deflate
Accept-Language: zh-TW,zh;q=0.9,ja-JP;q=0.8,ja;q=0.7,en-US;q=0.6,en;q=0.5
Connection: close
```

Response

```
HTTP/1.1 503 Service Unavailable
Date: Thu, 02 Dec 2021 05:34:59 GMT
Server: Apache/2.4.41 (Ubuntu)
X-Content-Type-Options: nosniff
Expires: Wed, 17 Aug 2005 00:00:00 GMT
Last-Modified: Thu, 02 Dec 2021 05:34:59 GMT
Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0
Pragma: no-cache
```

```
Content-Length: 3153
Connection: close
Content-Type: text/html; charset=utf-8

<!DOCTYPE html>
<html lang="en-gb" dir="ltr">
<head>
  <meta name="viewport" content="width=device-width, initial-scale=1.0" />
  <meta charset="utf-8" />
  <meta name="robots" content="noindex, nofollow
...[SNIP]...
```

4. Frameable response (potential Clickjacking)

Previous Next

Summary

Severity:	**Information**
Confidence:	**Firm**
Host:	**https://b2b-api.caru.com.tw**
Path:	**/**

Issue description

If a page fails to set an appropriate X-Frame-Options or Content-Security-Policy HTTP header, it might be possible for a page controlled by an attacker to load it within an iframe. This may enable a clickjacking attack, in which the attacker's page overlays the target application's interface with a different interface provided by the attacker. By inducing victim users to perform actions such as mouse clicks and keystrokes, the attacker can cause them to unwittingly carry out actions within the application that is being targeted. This technique allows the attacker to circumvent defenses against cross-site request forgery, and may result in unauthorized actions.

Note that some applications attempt to prevent these attacks from within the HTML page itself, using "framebusting" code. However, this type of defense is normally ineffective and can usually be circumvented by a skilled attacker.

You should determine whether any functions accessible within frameable pages can be used by application users to perform any sensitive actions within the application.

Issue remediation

To effectively prevent framing attacks, the application should return a response header with the name **X-Frame-Options** and the value **DENY** to prevent framing altogether, or the value **SAMEORIGIN** to allow framing only by pages on the same origin as the response itself. Note that the SAMEORIGIN header can be partially bypassed if the application itself can be made to frame untrusted websites.

References

- Web Security Academy: Clickjacking
- X-Frame-Options

Vulnerability classifications

- CWE-693: Protection Mechanism Failure
- CAPEC-103: Clickjacking

Request

```
GET / HTTP/1.1
Host: b2b-api.caru.com.tw
Cookie: 85f1e6839dee694ea47b2e9ffe89d244=atcbq73vmi03lhlciat7kshani
Cache-Control: max-age=0
Sec-Ch-Ua: " Not A;Brand";v="99", "Chromium";v="96", "Google Chrome";v="96"
Sec-Ch-Ua-Mobile: ?0
Sec-Ch-Ua-Platform: "Windows"
Dnt: 1
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/96.0.4664.45 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
Sec-Fetch-Site: none
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Sec-Fetch-Dest: document
Accept-Encoding: gzip, deflate
Accept-Language: zh-TW,zh;q=0.9,ja-JP;q=0.8,ja;q=0.7,en-US;q=0.6,en;q=0.5
Connection: close
```

Response

```
HTTP/1.1 503 Service Unavailable
Date: Thu, 02 Dec 2021 05:34:59 GMT
Server: Apache/2.4.41 (Ubuntu)
X-Content-Type-Options: nosniff
Expires: Wed, 17 Aug 2005 00:00:00 GMT
Last-Modified: Thu, 02 Dec 2021 05:34:59 GMT
Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0
Pragma: no-cache
Content-Length: 3153
Connection: close
Content-Type: text/html; charset=utf-8

<!DOCTYPE html>
<html lang="en-gb" dir="ltr">
<head>
  <meta name="viewport" content="width=device-width, initial-scale=1.0" />
  <meta charset="utf-8" />
  <meta name="robots" content="noindex, nofollow
...[SNIP]...
```

5. Robots.txt file

Previous

Summary

Severity:	**Information**
Confidence:	**Certain**
Host:	**https://b2b-api.caru.com.tw**
Path:	**/robots.txt**

Issue detail

The web server contains a robots.txt file.

The web server contains a robots.txt file.

Issue background

The file robots.txt is used to give instructions to web robots, such as search engine crawlers, about locations within the web site that robots are allowed, or not allowed, to crawl and index.

The presence of the robots.txt does not in itself present any kind of security vulnerability. However, it is often used to identify restricted or private areas of a site's contents. The information in the file may therefore help an attacker to map out the site's contents, especially if some of the locations identified are not linked from elsewhere in the site. If the application relies on robots.txt to protect access to these areas, and does not enforce proper access control over them, then this presents a serious vulnerability.

Issue remediation

The robots.txt file is not itself a security threat, and its correct use can represent good practice for non-security reasons. You should not assume that all web robots will honor the file's instructions. Rather, assume that attackers will pay close attention to any locations identified in the file. Do not rely on robots.txt to provide any kind of protection over unauthorized access.

Vulnerability classifications

- CWE-200: Information Exposure

Request

```
GET /robots.txt HTTP/1.1
Host: b2b-api.caru.com.tw
Accept-Encoding: gzip, deflate
Accept: */*
Accept-Language: en
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/95.0.4638.54 Safari/537.36
Connection: close
Cookie: ce7aa5e6e16df284e15c74ec72b2acb1=t6u32k5bt9c4a7b678kvicsdqv
```

Response

```
HTTP/1.1 200 OK
Date: Thu, 02 Dec 2021 05:35:01 GMT
Server: Apache/2.4.41 (Ubuntu)
X-Content-Type-Options: nosniff
Last-Modified: Sun, 11 Apr 2021 22:53:30 GMT
ETag: "2ec-5bfba440bce80-gzip"
Accept-Ranges: bytes
Vary: Accept-Encoding
Content-Length: 748
Connection: close
Content-Type: text/plain

# If the Joomla site is installed within a folder
# eg www.example.com/joomla/ then the robots.txt file
# MUST be moved to the site root
# eg www.example.com/robots.txt
# AND the joomla folder name MU
...[SNIP]...
```

Report generated by Burp Suite web vulnerability scanner v2021.9.1, at Thu Dec 02 13:46:35 GMT+08:00 2021.

dealer2.caru.com.tw

Burp Scanner Report

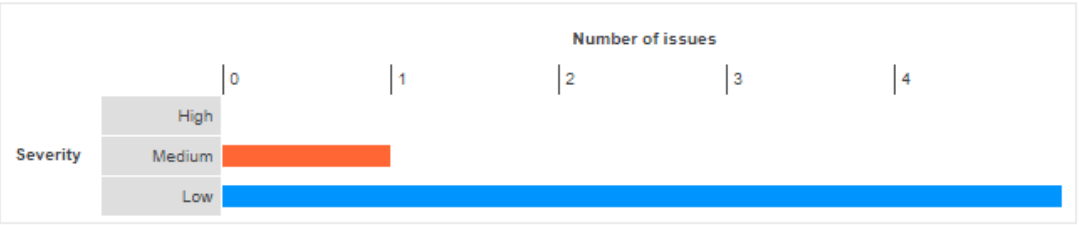
Burp Suite Professional

Summary

The table below shows the numbers of issues identified in different categories. Issues are classified according to severity as High, Medium, Low or Information. This reflects the likely impact of each issue for a typical organization. Issues are also classified according to confidence as Certain, Firm or Tentative. This reflects the inherent reliability of the technique that was used to identify the issue.

Severity	Confidence			
	Certain	Firm	Tentative	Total
High	0	0	0	0
Medium	1	0	0	1
Low	5	0	0	5
Information	1	0	1	2

The chart below shows the aggregated numbers of issues identified in each category. Solid colored bars represent issues with a confidence level of Certain, and the bars fade as the confidence level falls.



Contents

1. TLS certificate

2. Password field with autocomplete enabled

3. Strict transport security not enforced

3.1. https://dealer2.caru.com.tw/administrator
3.2. https://dealer2.caru.com.tw/administrator/index.php
3.3. https://dealer2.caru.com.tw/administrator/templates/isis/css/custom.css
3.4. https://dealer2.caru.com.tw/administrator/templates/isis/css/template.css

4. Cross-site request forgery

5. Robots.txt file

1. TLS certificate

Next

Summary

Severity:	**Medium**
Confidence:	**Certain**
Host:	**https://dealer2.caru.com.tw**
Path:	**/**

Issue detail

The following problem was identified with the server's TLS certificate:

- The server's certificate is not trusted.

Note: Burp relies on the Java trust store to determine whether certificates are trusted. The Java trust store does not include every root CA certificate that is included within browser trust stores. Burp might incorrectly report that a certificate is not trusted, if a valid root CA certificate is being used that is not included in the Java trust store.

The server presented the following certificates:

Server certificate

Issued to: dealer2.caru.com.tw, b2b-api.caru.com.tw, test-dev.caru.com.tw
Issued by: R3
Valid from: Tue Nov 02 22:28:26 GMT+08:00 2021
Valid to: Mon Jan 31 22:28:25 GMT+08:00 2022

Certificate chain #1

Issued to: R3
Issued by: ISRG Root X1
Valid from: Fri Sep 04 08:00:00 GMT+08:00 2020
Valid to: Tue Sep 16 00:00:00 GMT+08:00 2025

Certificate chain #2

Issued to: ISRG Root X1
Issued by: DST Root CA X3
Valid from: Thu Jan 21 03:14:03 GMT+08:00 2021
Valid to: Tue Oct 01 02:14:03 GMT+08:00 2024

Issue background

TLS (or SSL) helps to protect the confidentiality and integrity of information in transit between the browser and server, and to provide authentication of the server's identity. To serve this purpose, the server must present an TLS certificate that is valid for the server's hostname, is issued by a trusted authority and is valid for the current date. If any one of these requirements is not met, TLS connections to the server will not provide the full protection for which TLS is designed.

It should be noted that various attacks exist against TLS in general, and in the context of HTTPS web connections in particular. It may be possible for a determined and suitably-positioned attacker to compromise TLS connections without user detection even when a valid TLS certificate is used.

References

- SSL/TLS Configuration Guide

Vulnerability classifications

- CWE-295: Improper Certificate Validation
- CWE-326: Inadequate Encryption Strength
- CWE-327: Use of a Broken or Risky Cryptographic Algorithm

2. Password field with autocomplete enabled

Previous Next

Summary

Severity:	**Low**
Confidence:	**Certain**
Host:	**https://dealer2.caru.com.tw**
Path:	**/administrator/index.php**

Issue detail

The page contains a form with the following action URL:

- https://dealer2.caru.com.tw/administrator/index.php

The form contains the following password field with autocomplete enabled:

- passwd

This issue was found in multiple locations under the reported path.

Issue background

Most browsers have a facility to remember user credentials that are entered into HTML forms. This function can be configured by the user and also by applications that employ user credentials. If the function is enabled, then credentials entered by the user are stored on their local computer and retrieved by the browser on future visits to the same application.

The stored credentials can be captured by an attacker who gains control over the user's computer. Further, an attacker who finds a separate application vulnerability such as cross-site scripting may be able to exploit this to retrieve a user's browser-stored credentials.

Issue remediation

To prevent browsers from storing credentials entered into HTML forms, include the attribute **autocomplete="off"** within the FORM tag (to protect all form fields) or within the relevant INPUT tags (to protect specific individual fields).

Please note that modern web browsers may ignore this directive. In spite of this there is a chance that not disabling autocomplete may cause problems obtaining PCI compliance.

Vulnerability classifications

- CWE-200: Information Exposure

Request 1

```
POST /administrator/index.php HTTP/1.1
Host: dealer2.caru.com.tw
Origin: https://dealer2.caru.com.tw
Cookie: ce7aa5e6e16df284e15c74ec72b2acb1=9sp5jnujv4oj6eiebj3gi3t2d6
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
Upgrade-Insecure-Requests: 1
Referer: https://dealer2.caru.com.tw/administrator/index.php
Content-Type: application/x-www-form-urlencoded
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en-GB;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/95.0.4638.54 Safari/537.36
Connection: close
Cache-Control: max-age=0
Content-Length: 133

username=lVlyFGfv&passwd=n4N%21l3s%21M5&lang=en-
GB&option=com_login&task=login&return=aW5kZXgucGhw&655914e8aa6b7b947274933c0abf126f=1
```

Response 1

```
HTTP/1.1 200 OK
Date: Thu, 02 Dec 2021 06:24:08 GMT
Server: Apache/2.4.41 (Ubuntu)
X-Content-Type-Options: nosniff
X-Frame-Options: SAMEORIGIN
Expires: Wed, 17 Aug 2005 00:00:00 GMT
Last-Modified: Thu, 02 Dec 2021 06:24:08 GMT
Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0
Pragma: no-cache
Vary: Accept-Encoding
Content-Length: 6803
Connection: close
Content-Type: text/html; charset=utf-8

<!DOCTYPE html>
<html lang="en-gb" dir="ltr">
<head>
  <meta name="viewport" content="width=device-width, initial-scale=1.0">
  <meta http-equiv="X-UA-Compatible" content="IE=edge" />
  <meta charset="ut
...[SNIP]...
</div>
```

Request 2

```
POST /administrator/index.php HTTP/1.1
Host: dealer2.caru.com.tw
Origin: https://dealer2.caru.com.tw
Cookie: ce7aa5e6e16df284e15c74ec72b2acb1=phntjcb32nbe41hp6hpq3opdc2
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
Upgrade-Insecure-Requests: 1
Referer: https://dealer2.caru.com.tw/administrator/
Content-Type: application/x-www-form-urlencoded
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en-GB;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/95.0.4638.54 Safari/537.36
Connection: close
Cache-Control: max-age=0
Content-Length: 133

username=RdKFGWFn&passwd=p3A%21a9s%21E9&lang=zh-
TW&option=com_login&task=login&return=aW5kZXgucGhw&667098aa30968e1b75b5bc0322cd5195=1
```

Response 2

```
HTTP/1.1 200 OK
Date: Thu, 02 Dec 2021 06:23:49 GMT
Server: Apache/2.4.41 (Ubuntu)
X-Content-Type-Options: nosniff
X-Frame-Options: SAMEORIGIN
Expires: Wed, 17 Aug 2005 00:00:00 GMT
Last-Modified: Thu, 02 Dec 2021 06:23:49 GMT
Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0
Pragma: no-cache
Vary: Accept-Encoding
Content-Length: 6791
Connection: close
Content-Type: text/html; charset=utf-8

<!DOCTYPE html>
<html lang="zh-tw" dir="ltr">
<head>
  <meta name="viewport" content="width=device-width, initial-scale=1.0">
  <meta http-equiv="X-UA-Compatible" content="IE=edge" />
  <meta charset="ut
...[SNIP]...
</div>
```

Request 3

```
POST /administrator/index.php HTTP/1.1
Host: dealer2.caru.com.tw
Origin: https://dealer2.caru.com.tw
Cookie: ce7aa5e6e16df284e15c74ec72b2acb1=uohdhjof263uouqu5hdvrr1aeq
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
Upgrade-Insecure-Requests: 1
Referer: https://dealer2.caru.com.tw/administrator/
Content-Type: application/x-www-form-urlencoded
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en-GB;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/95.0.4638.54 Safari/537.36
Connection: close
Cache-Control: max-age=0
Content-Length: 133

username=iCCKZqgS&passwd=a4T%21o1j%21W7&lang=en-
GB&option=com_login&task=login&return=aW5kZXgucGhw&b987d69164d9ce0e06bdd82c3b9ce9b1=1
```

Response 3

```
HTTP/1.1 200 OK
Date: Thu, 02 Dec 2021 06:24:11 GMT
Server: Apache/2.4.41 (Ubuntu)
X-Content-Type-Options: nosniff
X-Frame-Options: SAMEORIGIN
Expires: Wed, 17 Aug 2005 00:00:00 GMT
Last-Modified: Thu, 02 Dec 2021 06:24:11 GMT
Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0
Pragma: no-cache
Vary: Accept-Encoding
```

```
Vary: Accept-Encoding
Content-Length: 6803
Connection: close
Content-Type: text/html; charset=utf-8

<!DOCTYPE html>
<html lang="en-gb" dir="ltr">
<head>
  <meta name="viewport" content="width=device-width, initial-scale=1.0">
  <meta http-equiv="X-UA-Compatible" content="IE=edge" />
  <meta charset="ut
...[SNIP]...
</div>
```

3. Strict transport security not enforced

Previous Next

There are 4 instances of this issue:

- /administrator
- /administrator/index.php
- /administrator/templates/isis/css/custom.css
- /administrator/templates/isis/css/template.css

Issue background

The application fails to prevent users from connecting to it over unencrypted connections. An attacker able to modify a legitimate user's network traffic could bypass the application's use of SSL/TLS encryption, and use the application as a platform for attacks against its users. This attack is performed by rewriting HTTPS links as HTTP, so that if a targeted user follows a link to the site from an HTTP page, their browser never attempts to use an encrypted connection. The sslstrip tool automates this process.

To exploit this vulnerability, an attacker must be suitably positioned to intercept and modify the victim's network traffic.This scenario typically occurs when a client communicates with the server over an insecure connection such as public Wi-Fi, or a corporate or home network that is shared with a compromised computer. Common defenses such as switched networks are not sufficient to prevent this. An attacker situated in the user's ISP or the application's hosting infrastructure could also perform this attack. Note that an advanced adversary could potentially target any connection made over the Internet's core infrastructure.

Issue remediation

The application should instruct web browsers to only access the application using HTTPS. To do this, enable HTTP Strict Transport Security (HSTS) by adding a response header with the name 'Strict-Transport-Security' and the value 'max-age=expireTime', where expireTime is the time in seconds that browsers should remember that the site should only be accessed using HTTPS. Consider adding the 'includeSubDomains' flag if appropriate.

Note that because HSTS is a "trust on first use" (TOFU) protocol, a user who has never accessed the application will never have seen the HSTS header, and will therefore still be vulnerable to SSL stripping attacks. To mitigate this risk, you can optionally add the 'preload' flag to the HSTS header, and submit the domain for review by browser vendors.

References

- HTTP Strict Transport Security
- sslstrip
- HSTS Preload Form

Vulnerability classifications

- CWE-523: Unprotected Transport of Credentials
- CAPEC-94: Man in the Middle Attack
- CAPEC-157: Sniffing Attacks

3.1. https://dealer2.caru.com.tw/administrator

Next

Summary

Severity:	Low
Confidence:	Certain
Host:	https://dealer2.caru.com.tw

Issue detail

This issue was found in multiple locations under the reported path.

Request 1

```
GET /administrator/templates/isis/css/custom.css?1bfe8dd9b0bcbb019c6d3cf4048801fd HTTP/1.1
Host: dealer2.caru.com.tw
Cookie: ce7aa5e6e16df284e15c74ec72b2acb1=60s0e3h4qm8sci5eddm29cgqmk
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
Upgrade-Insecure-Requests: 1
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en-GB;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/95.0.4638.54 Safari/537.36
Connection: close
Cache-Control: max-age=0
```

Response 1

```
HTTP/1.1 200 OK
Date: Thu, 02 Dec 2021 06:24:26 GMT
Server: Apache/2.4.41 (Ubuntu)
X-Content-Type-Options: nosniff
Last-Modified: Fri, 12 Nov 2021 07:46:40 GMT
ETag: "1a5-5d092a8d6b800-gzip"
Accept-Ranges: bytes
Vary: Accept-Encoding
Content-Length: 421
Connection: close
Content-Type: text/css

textarea {
width: unset;
}

body.site.com_login.view-login .icon-joomla {
display: none;
}


.brand.visible-desktop.visible-tablet {
```

3.2. https://dealer2.caru.com.tw/administrator/index.php

Previous Next

Summary

Severity:	**Low**
Confidence:	**Certain**
Host:	**https://dealer2.caru.com.tw**
Path:	**/administrator/index.php**

Request 1

```
POST /administrator/index.php HTTP/1.1
Host: dealer2.caru.com.tw
Cookie: ce7aa5e6e16df284e15c74ec72b2acb1=hbq6iuhhe8i508oa15p71pn26n
Content-Length: 129
Cache-Control: max-age=0
Sec-Ch-Ua: " Not A;Brand";v="99", "Chromium";v="96", "Google Chrome";v="96"
Sec-Ch-Ua-Mobile: ?0
Sec-Ch-Ua-Platform: "Windows"
Dnt: 1
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/96.0.4664.45 Safari/537.36
Origin: https://dealer2.caru.com.tw
Content-Type: application/x-www-form-urlencoded
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
```

```
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Sec-Fetch-Dest: document
Referer: https://dealer2.caru.com.tw/administrator/
Accept-Encoding: gzip, deflate
Accept-Language: zh-TW,zh;q=0.9,ja-JP;q=0.8,ja;q=0.7,en-US;q=0.6,en;q=0.5
Connection: close
```

Response 1

```
HTTP/1.1 303 See other
Date: Thu, 02 Dec 2021 06:26:04 GMT
Server: Apache/2.4.41 (Ubuntu)
X-Content-Type-Options: nosniff
Location: https://dealer2.caru.com.tw/administrator/
Expires: Wed, 17 Aug 2005 00:00:00 GMT
Last-Modified: Thu, 02 Dec 2021 06:26:04 GMT
Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0
Pragma: no-cache
Content-Length: 0
Connection: close
Content-Type: text/html; charset=utf-8
```

3.3. https://dealer2.caru.com.tw/administrator/templates/isis/css/custom.css

Previous Next

Summary

Severity:	**Low**
Confidence:	**Certain**
Host:	**https://dealer2.caru.com.tw**
Path:	**/administrator/templates/isis/css/custom.css**

Request 1

```
GET /administrator/templates/isis/css/custom.css?1bfe8dd9b0bcbb019c6d3cf4048801fd HTTP/1.1
Host: dealer2.caru.com.tw
Cookie: ce7aa5e6e16df284e15c74ec72b2acb1=q0ce13v0a3hcithku8fihec39c
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
Upgrade-Insecure-Requests: 1
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en-GB;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/95.0.4638.54 Safari/537.36
Connection: close
Cache-Control: max-age=0
```

Response 1

```
HTTP/1.1 200 OK
Date: Thu, 02 Dec 2021 06:55:37 GMT
Server: Apache/2.4.41 (Ubuntu)
X-Content-Type-Options: nosniff
Last-Modified: Fri, 12 Nov 2021 07:46:40 GMT
ETag: "1a5-5d092a8d6b800-gzip"
Accept-Ranges: bytes
Vary: Accept-Encoding
Content-Length: 421
Connection: close
Content-Type: text/css

textarea {
width: unset;
}

body.site.com_login.view-login .icon-joomla {
display: none;
}
```

.brand.visible-desktop.visible-tablet {

3.4. https://dealer2.caru.com.tw/administrator/templates/isis/css/template.css

Previous

Summary

Severity:	Low
Confidence:	Certain
Host:	https://dealer2.caru.com.tw
Path:	/administrator/templates/isis/css/template.css

Request 1

```
GET /administrator/templates/isis/css/template.css?1bfe8dd9b0bcbb019c6d3cf4048801fd HTTP/1.1
Host: dealer2.caru.com.tw
Cookie: ce7aa5e8e16df284e15c74ec72b2acb1=929eihpjk59jr2hl3gjnou6o3v
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
Upgrade-Insecure-Requests: 1
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en-GB;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/95.0.4638.54 Safari/537.36
Connection: close
Cache-Control: max-age=0
```

Response 1

```
HTTP/1.1 200 OK
Date: Thu, 02 Dec 2021 06:55:30 GMT
Server: Apache/2.4.41 (Ubuntu)
X-Content-Type-Options: nosniff
Last-Modified: Thu, 21 Oct 2021 07:46:50 GMT
ETag: "2df20-5ced818ed0e80-gzip"
Accept-Ranges: bytes
Vary: Accept-Encoding
Content-Length: 188192
Connection: close
Content-Type: text/css

article,
aside,
details,
figcaption,
figure,
footer,
header,
hgroup,
nav,
section {
```

4. Cross-site request forgery

Previous Next

Summary

Severity:	Information
Confidence:	Tentative
Host:	https://dealer2.caru.com.tw
Path:	/administrator/index.php

Issue detail

The request appears to be vulnerable to cross-site request forgery (CSRF) attacks against unauthenticated functionality. This is unlikely to constitute a security

vulnerability in its own right, however it may facilitate exploitation of other vulnerabilities affecting application users.

The original request contains parameters that look like they may be anti-CSRF tokens. However the request is successful if these parameters are removed.

The original request contains parameters that look like they may be anti-CSRF tokens. However, the values of these parameters do not change if the submitting form is reloaded without supplying any cookies. Hence, the parameters are probably not being used as anti-CSRF tokens.

Issue background

Cross-site request forgery (CSRF) vulnerabilities may arise when applications rely solely on HTTP cookies to identify the user that has issued a particular request. Because browsers automatically add cookies to requests regardless of their origin, it may be possible for an attacker to create a malicious web site that forges a cross-domain request to the vulnerable application. For a request to be vulnerable to CSRF, the following conditions must hold:

- The request can be issued cross-domain, for example using an HTML form. If the request contains non-standard headers or body content, then it may only be issuable from a page that originated on the same domain.
- The application relies solely on HTTP cookies or Basic Authentication to identify the user that issued the request. If the application places session-related tokens elsewhere within the request, then it may not be vulnerable.
- The request performs some privileged action within the application, which modifies the application's state based on the identity of the issuing user.
- The attacker can determine all the parameters required to construct a request that performs the action. If the request contains any values that the attacker cannot determine or predict, then it is not vulnerable.

Issue remediation

The most effective way to protect against CSRF vulnerabilities is to include within relevant requests an additional token that is not transmitted in a cookie: for example, a parameter in a hidden form field. This additional token should contain sufficient entropy, and be generated using a cryptographic random number generator, such that it is not feasible for an attacker to determine or predict the value of any token that was issued to another user. The token should be associated with the user's session, and the application should validate that the correct token is received before performing any action resulting from the request.

An alternative approach, which may be easier to implement, is to validate that Host and Referer headers in relevant requests are both present and contain the same domain name. However, this approach is somewhat less robust: historically, quirks in browsers and plugins have often enabled attackers to forge cross-domain requests that manipulate these headers to bypass such defenses.

References

- Web Security Academy: Cross-site request forgery
- Using Burp to Test for Cross-Site Request Forgery
- The Deputies Are Still Confused

Vulnerability classifications

- CWE-352: Cross-Site Request Forgery (CSRF)
- CAPEC-62: Cross Site Request Forgery

Request 1

```
POST /administrator/index.php HTTP/1.1
Host: dealer2.caru.com.tw
Origin: https://dealer2.caru.com.tw
Cookie: ce7aa5e6e16df284e15c74ec72b2acb1=9sp5jnujv4oj6eiebj3gi3t2d6
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
Upgrade-Insecure-Requests: 1
Referer: https://dealer2.caru.com.tw/administrator/index.php
Content-Type: application/x-www-form-urlencoded
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en-GB;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/95.0.4638.54 Safari/537.36
Connection: close
Cache-Control: max-age=0
Content-Length: 133

username=lVlyFGfv&passwd=n4N%21l3s%21M5&lang=en-
GB&option=com_login&task=login&return=aW5kZXgucGhw&655914e8aa6b7b947274933c0abf126f=1
```

Response 1

```
HTTP/1.1 200 OK
Date: Thu, 02 Dec 2021 06:24:08 GMT
Server: Apache/2.4.41 (Ubuntu)
X-Content-Type-Options: nosniff
X-Frame-Options: SAMEORIGIN
Expires: Wed, 17 Aug 2005 00:00:00 GMT
Last-Modified: Thu, 02 Dec 2021 06:24:08 GMT
Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0
Pragma: no-cache
Vary: Accept-Encoding
Content-Length: 6803
Connection: close
```

```
Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0
Pragma: no-cache
Vary: Accept-Encoding
Content-Length: 6803
Connection: close
Content-Type: text/html; charset=utf-8

<!DOCTYPE html>
<html lang="en-gb" dir="ltr">
<head>
  <meta name="viewport" content="width=device-width, initial-scale=1.0">
  <meta http-equiv="X-UA-Compatible" content="IE=edge" />
  <meta charset="ut
...[SNIP]...
```

Request 2

```
POST /administrator/index.php HTTP/1.1
Host: dealer2.caru.com.tw
Origin: https://dealer2.caru.com.tw
Cookie: ce7aa5e6e16df284e15c74ec72b2acb1=c67lk2qbmi7ho04rgjq5msca3f
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
Upgrade-Insecure-Requests: 1
Referer: https://raWjfKuJuedrRoS.com/administrator/index.php
Content-Type: application/x-www-form-urlencoded
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en-GB;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/95.0.4638.54 Safari/537.36
Connection: close
Cache-Control: max-age=0
Content-Length: 133

username=ZlVVzfHi&passwd=l7N%21q2j%21R9&lang=en-
GB&option=com_login&task=login&return=aW5kZXgucGhw&cb7e8381eaf588d98b25764398c1109a=1
```

Response 2

```
HTTP/1.1 200 OK
Date: Thu, 02 Dec 2021 06:55:09 GMT
Server: Apache/2.4.41 (Ubuntu)
X-Content-Type-Options: nosniff
X-Frame-Options: SAMEORIGIN
Expires: Wed, 17 Aug 2005 00:00:00 GMT
Last-Modified: Thu, 02 Dec 2021 06:55:09 GMT
Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0
Pragma: no-cache
Vary: Accept-Encoding
Content-Length: 6803
Connection: close
Content-Type: text/html; charset=utf-8

<!DOCTYPE html>
<html lang="en-gb" dir="ltr">
<head>
  <meta name="viewport" content="width=device-width, initial-scale=1.0">
  <meta http-equiv="X-UA-Compatible" content="IE=edge" />
  <meta charset="ut
...[SNIP]...
```

5. Robots.txt file

Previous

Summary

Severity:	**Information**
Confidence:	**Certain**
Host:	**https://dealer2.caru.com.tw**
Path:	**/robots.txt**

Issue detail

The web server contains a robots.txt file.

Previous

Summary

Severity:	**Information**
Confidence:	**Certain**
Host:	**https://dealer2.caru.com.tw**
Path:	**/robots.txt**

Issue detail

The web server contains a robots.txt file.

Issue background

The file robots.txt is used to give instructions to web robots, such as search engine crawlers, about locations within the web site that robots are allowed, or not allowed, to crawl and index.

The presence of the robots.txt does not in itself present any kind of security vulnerability. However, it is often used to identify restricted or private areas of a site's contents. The information in the file may therefore help an attacker to map out the site's contents, especially if some of the locations identified are not linked from elsewhere in the site. If the application relies on robots.txt to protect access to these areas, and does not enforce proper access control over them, then this presents a serious vulnerability.

Issue remediation

The robots.txt file is not itself a security threat, and its correct use can represent good practice for non-security reasons. You should not assume that all web robots will honor the file's instructions. Rather, assume that attackers will pay close attention to any locations identified in the file. Do not rely on robots.txt to provide any kind of protection over unauthorized access.

Vulnerability classifications

- CWE-200: Information Exposure

Request 1

```
GET /robots.txt HTTP/1.1
Host: dealer2.caru.com.tw
Accept-Encoding: gzip, deflate
Accept: */*
Accept-Language: en
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/95.0.4638.54 Safari/537.36
Connection: close
Cookie: ce7aa5e6e16df284e15c74ec72b2acb1=t6u32k5bt9c4a7b678kvicsdqv
```

Response 1

```
HTTP/1.1 200 OK
Date: Thu, 02 Dec 2021 06:24:27 GMT
Server: Apache/2.4.41 (Ubuntu)
X-Content-Type-Options: nosniff
Last-Modified: Sun, 11 Apr 2021 22:53:30 GMT
ETag: "2ec-5bfba440bce80-gzip"
Accept-Ranges: bytes
Vary: Accept-Encoding
Content-Length: 748
Connection: close
Content-Type: text/plain

# If the Joomla site is installed within a folder
# eg www.example.com/joomla/ then the robots.txt file
# MUST be moved to the site root
# eg www.example.com/robots.txt
# AND the joomla folder name MU
...[SNIP]...
```

driver.caru.com.tw

Burp Scanner Report

Burp Suite Professional

Summary

The table below shows the numbers of issues identified in different categories. Issues are classified according to severity as High, Medium, Low or Information. This reflects the likely impact of each issue for a typical organization. Issues are also classified according to confidence as Certain, Firm or Tentative. This reflects the inherent reliability of the technique that was used to identify the issue.

Severity	Confidence			
	Certain	Firm	Tentative	Total
High	0	0	0	0
Medium	1	0	0	1
Low	1	0	0	1
Information	3	10	0	13

The chart below shows the aggregated numbers of issues identified in each category. Solid colored bars represent issues with a confidence level of Certain, and the bars fade as the confidence level falls.

Contents

1. TLS certificate
2. Strict transport security not enforced
3. Frameable response (potential Clickjacking)
   - 3.1. https://driver.caru.com.tw/
   - 3.2. https://driver.caru.com.tw/login/
4. DOM data manipulation (DOM-based)
   - 4.1. https://driver.caru.com.tw/
   - 4.2. https://driver.caru.com.tw/
   - 4.3. https://driver.caru.com.tw/
   - 4.4. https://driver.caru.com.tw/
   - 4.5. https://driver.caru.com.tw/login/
   - 4.6. https://driver.caru.com.tw/login/
   - 4.7. https://driver.caru.com.tw/login/
   - 4.8. https://driver.caru.com.tw/login/
5. Cacheable HTTPS response
   - 5.1. https://driver.caru.com.tw/
   - 5.2. https://driver.caru.com.tw/_nuxt/manifest.d0e9c203.json
   - 5.3. https://driver.caru.com.tw/login/

1. TLS certificate

Next

Summary

Severity:	**Medium**
Confidence:	**Certain**
Host:	**https://driver.caru.com.tw**
Path:	/

Issue detail

The following problem was identified with the server's TLS certificate:

- The server's certificate is not trusted.

Note: Burp relies on the Java trust store to determine whether certificates are trusted. The Java trust store does not include every root CA certificate that is included within browser trust stores. Burp might incorrectly report that a certificate is not trusted, if a valid root CA certificate is being used that is not included in the Java trust store.

The server presented the following certificates:

Server certificate

Issued to: driver.caru.com.tw
Issued by: R3
Valid from: Sun Nov 07 21:08:19 GMT+08:00 2021
Valid to: Sat Feb 05 21:08:18 GMT+08:00 2022

Certificate chain #1

Issued to: R3
Issued by: ISRG Root X1
Valid from: Fri Sep 04 08:00:00 GMT+08:00 2020
Valid to: Tue Sep 16 00:00:00 GMT+08:00 2025

Certificate chain #2

Issued to: ISRG Root X1
Issued by: DST Root CA X3
Valid from: Thu Jan 21 03:14:03 GMT+08:00 2021
Valid to: Tue Oct 01 02:14:03 GMT+08:00 2024

Issue background

TLS (or SSL) helps to protect the confidentiality and integrity of information in transit between the browser and server, and to provide authentication of the server's identity. To serve this purpose, the server must present an TLS certificate that is valid for the server's hostname, is issued by a trusted authority and is valid for the current date. If any one of these requirements is not met, TLS connections to the server will not provide the full protection for which TLS is designed.

It should be noted that various attacks exist against TLS in general, and in the context of HTTPS web connections in particular. It may be possible for a determined and suitably-positioned attacker to compromise TLS connections without user detection even when a valid TLS certificate is used.

References

- SSL/TLS Configuration Guide

Vulnerability classifications

- CWE-295: Improper Certificate Validation
- CWE-326: Inadequate Encryption Strength
- CWE-327: Use of a Broken or Risky Cryptographic Algorithm

2. Strict transport security not enforced

Previous Next

Summary

Severity:	**Low**
Confidence:	**Certain**

Host:	https://driver.caru.com.tw
Path:	/

Issue detail

This issue was found in multiple locations under the reported path.

Issue background

The application fails to prevent users from connecting to it over unencrypted connections. An attacker able to modify a legitimate user's network traffic could bypass the application's use of SSL/TLS encryption, and use the application as a platform for attacks against its users. This attack is performed by rewriting HTTPS links as HTTP, so that if a targeted user follows a link to the site from an HTTP page, their browser never attempts to use an encrypted connection. The sslstrip tool automates this process.

To exploit this vulnerability, an attacker must be suitably positioned to intercept and modify the victim's network traffic.This scenario typically occurs when a client communicates with the server over an insecure connection such as public Wi-Fi, or a corporate or home network that is shared with a compromised computer. Common defenses such as switched networks are not sufficient to prevent this. An attacker situated in the user's ISP or the application's hosting infrastructure could also perform this attack. Note that an advanced adversary could potentially target any connection made over the Internet's core infrastructure.

Issue remediation

The application should instruct web browsers to only access the application using HTTPS. To do this, enable HTTP Strict Transport Security (HSTS) by adding a response header with the name 'Strict-Transport-Security' and the value 'max-age=expireTime', where expireTime is the time in seconds that browsers should remember that the site should only be accessed using HTTPS. Consider adding the 'includeSubDomains' flag if appropriate.

Note that because HSTS is a "trust on first use" (TOFU) protocol, a user who has never accessed the application will never have seen the HSTS header, and will therefore still be vulnerable to SSL stripping attacks. To mitigate this risk, you can optionally add the 'preload' flag to the HSTS header, and submit the domain for review by browser vendors.

References

- HTTP Strict Transport Security
- sslstrip
- HSTS Preload Form

Vulnerability classifications

- CWE-523: Unprotected Transport of Credentials
- CAPEC-94: Man in the Middle Attack
- CAPEC-157: Sniffing Attacks

Request

```
GET /_nuxt/eb0ca7a.js HTTP/1.1
Host: driver.caru.com.tw
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
Upgrade-Insecure-Requests: 1
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en-GB;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/95.0.4638.54 Safari/537.36
Connection: close
Cache-Control: max-age=0
```

Response

```
HTTP/1.1 200 OK
Date: Thu, 02 Dec 2021 06:43:33 GMT
Server: Apache/2.4.41 (Ubuntu)
Last-Modified: Fri, 26 Nov 2021 09:56:39 GMT
ETag: "37174-5d1ae1b846768-gzip"
Accept-Ranges: bytes
Vary: Accept-Encoding
Connection: close
Content-Type: application/javascript
Content-Length: 225652

/*! For license information please see LICENSES */
(window.webpackJsonp=window.webpackJsonp||[]).push([[1],[,function(t,e,n){(function(e){var n=function(t){return t&&t.Math==Math&&t};t.exports=n("obje
...[SNIP]...
```

3. Frameable response (potential Clickjacking)

Previous Next

There are 2 instances of this issue:

- /
- /login/

Issue description

If a page fails to set an appropriate X-Frame-Options or Content-Security-Policy HTTP header, it might be possible for a page controlled by an attacker to load it within an iframe. This may enable a clickjacking attack, in which the attacker's page overlays the target application's interface with a different interface provided by the attacker. By inducing victim users to perform actions such as mouse clicks and keystrokes, the attacker can cause them to unwittingly carry out actions within the application that is being targeted. This technique allows the attacker to circumvent defenses against cross-site request forgery, and may result in unauthorized actions.

Note that some applications attempt to prevent these attacks from within the HTML page itself, using "framebusting" code. However, this type of defense is normally ineffective and can usually be circumvented by a skilled attacker.

You should determine whether any functions accessible within frameable pages can be used by application users to perform any sensitive actions within the application.

Issue remediation

To effectively prevent framing attacks, the application should return a response header with the name **X-Frame-Options** and the value **DENY** to prevent framing altogether, or the value **SAMEORIGIN** to allow framing only by pages on the same origin as the response itself. Note that the SAMEORIGIN header can be partially bypassed if the application itself can be made to frame untrusted websites.

References

- Web Security Academy: Clickjacking
- X-Frame-Options

Vulnerability classifications

- CWE-693: Protection Mechanism Failure
- CAPEC-103: Clickjacking

3.1. https://driver.caru.com.tw/

Next

Summary

Severity:	**Information**
Confidence:	**Firm**
Host:	**https://driver.caru.com.tw**
Path:	/

Request

```
GET / HTTP/1.1
Host: driver.caru.com.tw
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
Upgrade-Insecure-Requests: 1
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en-GB;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/95.0.4638.54 Safari/537.36
Connection: close
Cache-Control: max-age=0
```

Response

```
HTTP/1.1 200 OK
Date: Thu, 02 Dec 2021 06:42:24 GMT
Server: Apache/2.4.41 (Ubuntu)
Last-Modified: Fri, 26 Nov 2021 09:56:37 GMT
ETag: "e9f-5d1ae1b62d5ae-gzip"
```

```
ETag: "e9f-5d1ae1b4d6951-gzip"
Accept-Ranges: bytes
Vary: Accept-Encoding
Content-Length: 3743
Connection: close
Content-Type: text/html

<!doctype html>
<html lang="en" data-n-head="%7B%22lang%22:%7B%221%22:%22en%22%7D%7D">
<head>
<title>CarU .....</title><meta data-n-head="1" charset="utf-8"><meta data-n-head="1" name="vi
...[SNIP]...
```

3.2. https://driver.caru.com.tw/login/

Previous Next

Summary

Severity:	**Information**
Confidence:	**Firm**
Host:	**https://driver.caru.com.tw**
Path:	**/login/**

Request

```
GET /login/? HTTP/1.1
Host: driver.caru.com.tw
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
Upgrade-Insecure-Requests: 1
Referer: https://driver.caru.com.tw/login/
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en-GB;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/95.0.4638.54 Safari/537.36
Connection: close
Cache-Control: max-age=0
```

Response

```
HTTP/1.1 200 OK
Date: Thu, 02 Dec 2021 06:42:37 GMT
Server: Apache/2.4.41 (Ubuntu)
Last-Modified: Fri, 26 Nov 2021 09:56:36 GMT
ETag: "e9f-5d1ae1b4d6951-gzip"
Accept-Ranges: bytes
Vary: Accept-Encoding
Content-Length: 3743
Connection: close
Content-Type: text/html

<!doctype html>
<html lang="en" data-n-head="%7B%22lang%22:%7B%221%22:%22en%22%7D%7D">
<head>
<title>CarU .....</title><meta data-n-head="1" charset="utf-8"><meta data-n-head="1" name="vi
...[SNIP]...
```

4. DOM data manipulation (DOM-based)

Previous Next

There are 8 instances of this issue:

- /
- /
- /
- /
- /login/
- /login/

- /login/
- /login/

Issue background

DOM-based vulnerabilities arise when a client-side script reads data from a controllable part of the DOM (for example, the URL) and processes this data in an unsafe way.

DOM data manipulation arises when a script writes controllable data to a field within the DOM that is used within the visible UI or client-side application logic. An attacker may be able to use the vulnerability to construct a URL that, if visited by another application user, will modify the appearance or behavior of the client-side UI. An attacker may be able to leverage this to perform virtual defacement of the application, or possibly to induce the user to perform unintended actions.

Burp Suite automatically identifies this issue using static code analysis, which may lead to false positives that are not actually exploitable. The relevant code and execution paths should be reviewed to determine whether this vulnerability is indeed present, or whether mitigations are in place that would prevent exploitation.

Issue remediation

The most effective way to avoid DOM-based DOM data manipulation vulnerabilities is not to dynamically write to DOM data fields any data that originated from any untrusted source. If the desired functionality of the application means that this behavior is unavoidable, then defenses must be implemented within the client-side code to prevent malicious data from being stored. In general, this is best achieved by using a whitelist of permitted values.

References

- Web Security Academy: DOM data manipulation

Vulnerability classifications

- CWE-20: Improper Input Validation
- CAPEC-153: Input Data Manipulation

4.1. https://driver.caru.com.tw/

Previous Next

Summary

Severity:	**Information**
Confidence:	**Firm**
Host:	**https://driver.caru.com.tw**
Path:	/

Issue detail

The application may be vulnerable to DOM-based DOM data manipulation. Data is read from **location.href** and passed to **history.replaceState**.

Request

```
GET / HTTP/1.1
Host: driver.caru.com.tw
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
Upgrade-Insecure-Requests: 1
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en-GB;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/95.0.4638.54 Safari/537.36
Connection: close
Cache-Control: max-age=0
```

Response

```
HTTP/1.1 200 OK
Date: Thu, 02 Dec 2021 06:42:24 GMT
Server: Apache/2.4.41 (Ubuntu)
Last-Modified: Fri, 26 Nov 2021 09:56:37 GMT
ETag: "e9f-5d1ae1b62d5ae-gzip"
Accept-Ranges: bytes
Vary: Accept-Encoding
```

```
Content-Length: 3743
Connection: close
Content-Type: text/html

<!doctype html>
<html lang="en" data-n-head="%7B%22lang%22:%7B%221%22:%22en%22%7D%7D">
<head>
<title>CarU .....</title><meta data-n-head="1" charset="utf-8"><meta data-n-head="1" name="vi
...[SNIP]...
```

Dynamic analysis

Data is read from **location.href** and passed to **history.replaceState**.

The following value was injected into the source and reached the sink without any modification:

```
?p6elyyv1o1=p6elyyv1o1%27%22`'"/p6elyyv1o1/><p6elyyv1o1/\>hof907jqg4&
```

The stack trace at the source was:

```
at Object._0x16d0e7 [as proxiedGetterCallback] (<anonymous>:1:591983)
at Object.get href [as href] (<anonymous>:1:299867)
at mt (https://driver.caru.com.tw/_nuxt/eb0ca7a.js:2:146810)
at e.setupListeners (https://driver.caru.com.tw/_nuxt/eb0ca7a.js:2:154306)
at r (https://driver.caru.com.tw/_nuxt/eb0ca7a.js:2:158850)
at https://driver.caru.com.tw/_nuxt/eb0ca7a.js:2:151664
at https://driver.caru.com.tw/_nuxt/eb0ca7a.js:2:153653
at r (https://driver.caru.com.tw/_nuxt/eb0ca7a.js:2:148741)
at Tt (https://driver.caru.com.tw/_nuxt/eb0ca7a.js:2:148787)
at https://driver.caru.com.tw/_nuxt/eb0ca7a.js:2:153554
at r (https://driver.caru.com.tw/_nuxt/eb0ca7a.js:2:148741)
at https://driver.caru.com.tw/_nuxt/eb0ca7a.js:2:148769
at https://driver.caru.com.tw/_nuxt/eb0ca7a.js:2:153261
at https://driver.caru.com.tw/_nuxt/eb0ca7a.js:2:150100
at x (https://driver.caru.com.tw/_nuxt/eb0ca7a.js:2:152895)
at r (https://driver.caru.com.tw/_nuxt/eb0ca7a.js:2:148750)
at Tt (https://driver.caru.com.tw/_nuxt/eb0ca7a.js:2:148787)
at e.Vt.confirmTransition (https://driver.caru.com.tw/_nuxt/eb0ca7a.js:2:153285)
at e.Vt.transitionTo (https://driver.caru.com.tw/_nuxt/eb0ca7a.js:2:151612)
at ee.init (https://driver.caru.com.tw/_nuxt/eb0ca7a.js:2:158965)
at Dn.beforeCreate (https://driver.caru.com.tw/_nuxt/eb0ca7a.js:2:161173)
at ee (https://driver.caru.com.tw/_nuxt/eb0ca7a.js:2:11828)
at vn (https://driver.caru.com.tw/_nuxt/eb0ca7a.js:2:26234)
at Dn.t._init (https://driver.caru.com.tw/_nuxt/eb0ca7a.js:2:33662)
at new Dn (https://driver.caru.com.tw/_nuxt/eb0ca7a.js:2:31251)
at https://driver.caru.com.tw/_nuxt/4f5d376.js:2:290474
at h (https://driver.caru.com.tw/_nuxt/4f5d376.js:2:101657)
at Generator._invoke (https://driver.caru.com.tw/_nuxt/4f5d376.js:2:101445)
at Generator.E.forEach.e.<computed> [as next] (https://driver.caru.com.tw/_nuxt/4f5d376.js:2:102080)
at r (https://driver.caru.com.tw/_nuxt/eb0ca7a.js:2:66614)
```

The stack trace at the sink was:

```
at History.replaceState (<anonymous>:1:582436)
at mt (https://driver.caru.com.tw/_nuxt/eb0ca7a.js:2:146891)
at e.setupListeners (https://driver.caru.com.tw/_nuxt/eb0ca7a.js:2:154306)
at r (https://driver.caru.com.tw/_nuxt/eb0ca7a.js:2:158850)
at https://driver.caru.com.tw/_nuxt/eb0ca7a.js:2:151664
at https://driver.caru.com.tw/_nuxt/eb0ca7a.js:2:153653
at r (https://driver.caru.com.tw/_nuxt/eb0ca7a.js:2:148741)
at Tt (https://driver.caru.com.tw/_nuxt/eb0ca7a.js:2:148787)
at https://driver.caru.com.tw/_nuxt/eb0ca7a.js:2:153554
at r (https://driver.caru.com.tw/_nuxt/eb0ca7a.js:2:148741)
at https://driver.caru.com.tw/_nuxt/eb0ca7a.js:2:148769
at https://driver.caru.com.tw/_nuxt/eb0ca7a.js:2:153261
at https://driver.caru.com.tw/_nuxt/eb0ca7a.js:2:150100
at x (https://driver.caru.com.tw/_nuxt/eb0ca7a.js:2:152895)
at r (https://driver.caru.com.tw/_nuxt/eb0ca7a.js:2:148750)
at Tt (https://driver.caru.com.tw/_nuxt/eb0ca7a.js:2:148787)
at e.Vt.confirmTransition (https://driver.caru.com.tw/_nuxt/eb0ca7a.js:2:153285)
at e.Vt.transitionTo (https://driver.caru.com.tw/_nuxt/eb0ca7a.js:2:151612)
at ee.init (https://driver.caru.com.tw/_nuxt/eb0ca7a.js:2:158965)
at Dn.beforeCreate (https://driver.caru.com.tw/_nuxt/eb0ca7a.js:2:161173)
at ee (https://driver.caru.com.tw/_nuxt/eb0ca7a.js:2:11828)
at vn (https://driver.caru.com.tw/_nuxt/eb0ca7a.js:2:26234)
at Dn.t._init (https://driver.caru.com.tw/_nuxt/eb0ca7a.js:2:33662)
at new Dn (https://driver.caru.com.tw/_nuxt/eb0ca7a.js:2:31251)
at https://driver.caru.com.tw/_nuxt/4f5d376.js:2:290474
```

```
at https://driver.caru.com.tw/_nuxt/eb0ca7a.js:2:148769
at https://driver.caru.com.tw/_nuxt/eb0ca7a.js:2:153261
at https://driver.caru.com.tw/_nuxt/eb0ca7a.js:2:150100
at x (https://driver.caru.com.tw/_nuxt/eb0ca7a.js:2:152895)
at r (https://driver.caru.com.tw/_nuxt/eb0ca7a.js:2:148750)
at Tt (https://driver.caru.com.tw/_nuxt/eb0ca7a.js:2:148787)
at e.Vt.confirmTransition (https://driver.caru.com.tw/_nuxt/eb0ca7a.js:2:153285)
at e.Vt.transitionTo (https://driver.caru.com.tw/_nuxt/eb0ca7a.js:2:151612)
at ee.init (https://driver.caru.com.tw/_nuxt/eb0ca7a.js:2:158965)
at Dn.beforeCreate (https://driver.caru.com.tw/_nuxt/eb0ca7a.js:2:161173)
at ee (https://driver.caru.com.tw/_nuxt/eb0ca7a.js:2:11828)
at vn (https://driver.caru.com.tw/_nuxt/eb0ca7a.js:2:26234)
at Dn.t._init (https://driver.caru.com.tw/_nuxt/eb0ca7a.js:2:33662)
at new Dn (https://driver.caru.com.tw/_nuxt/eb0ca7a.js:2:31251)
at https://driver.caru.com.tw/_nuxt/4f5d376.js:2:290474
at h (https://driver.caru.com.tw/_nuxt/4f5d376.js:2:101657)
at Generator._invoke (https://driver.caru.com.tw/_nuxt/4f5d376.js:2:101445)
at Generator.E.forEach.e.<computed> [as next] (https://driver.caru.com.tw/_nuxt/4f5d376.js:2:102080)
at r (https://driver.caru.com.tw/_nuxt/eb0ca7a.js:2:66614)
at l (https://driver.caru.com.tw/_nuxt/eb0ca7a.js:2:66817)
```

4.2. https://driver.caru.com.tw/

Previous Next

Summary

Severity:	**Information**
Confidence:	**Firm**
Host:	**https://driver.caru.com.tw**
Path:	/

Issue detail

The application may be vulnerable to DOM-based DOM data manipulation. Data is read from **location.pathname** and passed to **history.replaceState**.

Request

```
GET / HTTP/1.1
Host: driver.caru.com.tw
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
Upgrade-Insecure-Requests: 1
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en-GB;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/95.0.4638.54 Safari/537.36
Connection: close
Cache-Control: max-age=0
```

Response

```
HTTP/1.1 200 OK
Date: Thu, 02 Dec 2021 06:42:24 GMT
Server: Apache/2.4.41 (Ubuntu)
Last-Modified: Fri, 26 Nov 2021 09:56:37 GMT
ETag: "e9f-5d1ae1b62d5ae-gzip"
Accept-Ranges: bytes
Vary: Accept-Encoding
Content-Length: 3743
Connection: close
Content-Type: text/html

<!doctype html>
<html lang="en" data-n-head="%7B%22lang%22:%7B%221%22:%22en%22%7D%7D">
<head>
<title>CarU .....</title><meta data-n-head="1" charset="utf-8"><meta data-n-head="1" name="vi
...[SNIP]...
```

Dynamic analysis

Data is read from **location.pathname** and passed to **history.replaceState**.

The following value was injected into the source:

```
/////ywwmf3a7nn%27%22%60'%22/ywwmf3a7nn/%3E%3Cywwmf3a7nn//%3Egv8de8uz27&
```

The previous value reached the sink as:

```
/ywwmf3a7nn%27%22%60'%22/ywwmf3a7nn/%3E%3Cywwmf3a7nn/%3Egv8de8uz27&?dkvkumps8c=dkvkumps8c%27%22%60%27%22%2Fdkvkumps8c%2F%3E%3Cdkvkur
```

The stack trace at the source was:

```
at Object._0x16d0e7 [as proxiedGetterCallback] (<anonymous>:1:591983)
at Object.get pathname [as pathname] (<anonymous>:1:299963)
at Wt (https://driver.caru.com.tw/_nuxt/eb0ca7a.js:2:155162)
at e.getCurrentLocation (https://driver.caru.com.tw/_nuxt/eb0ca7a.js:2:155097)
at ee.init (https://driver.caru.com.tw/_nuxt/eb0ca7a.js:2:158980)
at Dn.beforeCreate (https://driver.caru.com.tw/_nuxt/eb0ca7a.js:2:161173)
at ee (https://driver.caru.com.tw/_nuxt/eb0ca7a.js:2:11828)
at vn (https://driver.caru.com.tw/_nuxt/eb0ca7a.js:2:26234)
at Dn.t._init (https://driver.caru.com.tw/_nuxt/eb0ca7a.js:2:33662)
at new Dn (https://driver.caru.com.tw/_nuxt/eb0ca7a.js:2:31251)
at https://driver.caru.com.tw/_nuxt/4f5d376.js:2:290474
at h (https://driver.caru.com.tw/_nuxt/4f5d376.js:2:101657)
at Generator._invoke (https://driver.caru.com.tw/_nuxt/4f5d376.js:2:101445)
at Generator.E.forEach.e.<computed> [as next] (https://driver.caru.com.tw/_nuxt/4f5d376.js:2:102080)
at r (https://driver.caru.com.tw/_nuxt/eb0ca7a.js:2:66614)
at l (https://driver.caru.com.tw/_nuxt/eb0ca7a.js:2:66817)
at https://driver.caru.com.tw/_nuxt/eb0ca7a.js:2:66876
at new Promise (<anonymous>)
at https://driver.caru.com.tw/_nuxt/eb0ca7a.js:2:66757
at U (https://driver.caru.com.tw/_nuxt/4f5d376.js:2:291448)
at https://driver.caru.com.tw/_nuxt/4f5d376.js:2:291524
```

The stack trace at the sink was:

```
at History.replaceState (<anonymous>:1:582436)
at jt (https://driver.caru.com.tw/_nuxt/eb0ca7a.js:2:148558)
at Ct (https://driver.caru.com.tw/_nuxt/eb0ca7a.js:2:148683)
at e.ensureURL (https://driver.caru.com.tw/_nuxt/eb0ca7a.js:2:155040)
at https://driver.caru.com.tw/_nuxt/eb0ca7a.js:2:151671
at https://driver.caru.com.tw/_nuxt/eb0ca7a.js:2:153653
at r (https://driver.caru.com.tw/_nuxt/eb0ca7a.js:2:148741)
at Tt (https://driver.caru.com.tw/_nuxt/eb0ca7a.js:2:148787)
at https://driver.caru.com.tw/_nuxt/eb0ca7a.js:2:153554
at r (https://driver.caru.com.tw/_nuxt/eb0ca7a.js:2:148741)
at https://driver.caru.com.tw/_nuxt/eb0ca7a.js:2:148769
at https://driver.caru.com.tw/_nuxt/eb0ca7a.js:2:153261
at https://driver.caru.com.tw/_nuxt/eb0ca7a.js:2:150100
at x (https://driver.caru.com.tw/_nuxt/eb0ca7a.js:2:152895)
at r (https://driver.caru.com.tw/_nuxt/eb0ca7a.js:2:148750)
at Tt (https://driver.caru.com.tw/_nuxt/eb0ca7a.js:2:148787)
at e.Vt.confirmTransition (https://driver.caru.com.tw/_nuxt/eb0ca7a.js:2:153285)
at e.Vt.transitionTo (https://driver.caru.com.tw/_nuxt/eb0ca7a.js:2:151612)
at ee.init (https://driver.caru.com.tw/_nuxt/eb0ca7a.js:2:158965)
at Dn.beforeCreate (https://driver.caru.com.tw/_nuxt/eb0ca7a.js:2:161173)
at ee (https://driver.caru.com.tw/_nuxt/eb0ca7a.js:2:11828)
at vn (https://driver.caru.com.tw/_nuxt/eb0ca7a.js:2:26234)
at Dn.t._init (https://driver.caru.com.tw/_nuxt/eb0ca7a.js:2:33662)
at new Dn (https://driver.caru.com.tw/_nuxt/eb0ca7a.js:2:31251)
at https://driver.caru.com.tw/_nuxt/4f5d376.js:2:290474
at h (https://driver.caru.com.tw/_nuxt/4f5d376.js:2:101657)
at Generator._invoke (https://driver.caru.com.tw/_nuxt/4f5d376.js:2:101445)
at Generator.E.forEach.e.<computed> [as next] (https://driver.caru.com.tw/_nuxt/4f5d376.js:2:102080)
at r (https://driver.caru.com.tw/_nuxt/eb0ca7a.js:2:66614)
at l (https://driver.caru.com.tw/_nuxt/eb0ca7a.js:2:66817)
```

4.3. https://driver.caru.com.tw/

Previous Next

Summary

Severity:	Information
Confidence:	Firm
Host:	https://driver.caru.com.tw
Path:	/

Issue detail

The application may be vulnerable to DOM-based DOM data manipulation. Data is read from **location.search** and passed to **history.replaceState**.

Request

```
GET / HTTP/1.1
Host: driver.caru.com.tw
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
Upgrade-Insecure-Requests: 1
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en-GB;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/95.0.4638.54 Safari/537.36
Connection: close
Cache-Control: max-age=0
```

Response

```
HTTP/1.1 200 OK
Date: Thu, 02 Dec 2021 06:42:24 GMT
Server: Apache/2.4.41 (Ubuntu)
Last-Modified: Fri, 26 Nov 2021 09:56:37 GMT
ETag: "e9f-5d1ae1b62d5ae-gzip"
Accept-Ranges: bytes
Vary: Accept-Encoding
Content-Length: 3743
Connection: close
Content-Type: text/html

<!doctype html>
<html lang="en" data-n-head="%7B%22lang%22:%7B%221%22:%22en%22%7D%7D">
<head>
<title>CarU .....</title><meta data-n-head="1" charset="utf-8"><meta data-n-head="1" name="vi
...[SNIP]...
```

Dynamic analysis

Data is read from **location.search** and passed to **history.replaceState**.

The following value was injected into the source:

```
?dkvkumps8c=dkvkumps8c%27%22`'"/dkvkumps8c/><dkvkumps8c/\>c3f0am3ffz&
```

The previous value reached the sink as:

```
/ywwmf3a7nn%27%22%60'%22/ywwmf3a7nn/%3E%3Cywwmf3a7nn/%3Egv8de8uz27&?dkvkumps8c=dkvkumps8c%27%22%60%27%22%2Fdkvkumps8c%2F%3E%3Cdkvkump
```

The stack trace at the source was:

```
at Object._0x16d0e7 [as proxiedGetterCallback] (<anonymous>:1:591983)
at Object.get search [as search] (<anonymous>:1:299118)
at Wt (https://driver.caru.com.tw/_nuxt/eb0ca7a.js:2:155317)
at e.getCurrentLocation (https://driver.caru.com.tw/_nuxt/eb0ca7a.js:2:155097)
at ee.init (https://driver.caru.com.tw/_nuxt/eb0ca7a.js:2:158980)
at Dn.beforeCreate (https://driver.caru.com.tw/_nuxt/eb0ca7a.js:2:161173)
at ee (https://driver.caru.com.tw/_nuxt/eb0ca7a.js:2:11828)
at vn (https://driver.caru.com.tw/_nuxt/eb0ca7a.js:2:26234)
at Dn.t._init (https://driver.caru.com.tw/_nuxt/eb0ca7a.js:2:33662)
at new Dn (https://driver.caru.com.tw/_nuxt/eb0ca7a.js:2:31251)
at https://driver.caru.com.tw/_nuxt/4f5d376.js:2:290474
at h (https://driver.caru.com.tw/_nuxt/4f5d376.js:2:101657)
at Generator._invoke (https://driver.caru.com.tw/_nuxt/4f5d376.js:2:101445)
at Generator.E.forEach.e.<computed> [as next] (https://driver.caru.com.tw/_nuxt/4f5d376.js:2:102080)
at r (https://driver.caru.com.tw/_nuxt/eb0ca7a.js:2:66614)
at l (https://driver.caru.com.tw/_nuxt/eb0ca7a.js:2:66817)
at https://driver.caru.com.tw/_nuxt/eb0ca7a.js:2:66876
at new Promise (<anonymous>)
at https://driver.caru.com.tw/_nuxt/eb0ca7a.js:2:66757
at U (https://driver.caru.com.tw/_nuxt/4f5d376.js:2:291448)
at https://driver.caru.com.tw/_nuxt/4f5d376.js:2:291524
```

The stack trace at the sink was:

```
at History.replaceState (<anonymous>:1:582436)
```

```
at History.replaceState (<anonymous>:1:582436)
at jt (https://driver.caru.com.tw/_nuxt/eb0ca7a.js:2:148558)
at Ct (https://driver.caru.com.tw/_nuxt/eb0ca7a.js:2:148683)
at e.ensureURL (https://driver.caru.com.tw/_nuxt/eb0ca7a.js:2:155040)
at https://driver.caru.com.tw/_nuxt/eb0ca7a.js:2:151671
at https://driver.caru.com.tw/_nuxt/eb0ca7a.js:2:153653
at r (https://driver.caru.com.tw/_nuxt/eb0ca7a.js:2:148741)
at Tt (https://driver.caru.com.tw/_nuxt/eb0ca7a.js:2:148787)
at https://driver.caru.com.tw/_nuxt/eb0ca7a.js:2:153554
at r (https://driver.caru.com.tw/_nuxt/eb0ca7a.js:2:148741)
at https://driver.caru.com.tw/_nuxt/eb0ca7a.js:2:148769
at https://driver.caru.com.tw/_nuxt/eb0ca7a.js:2:153261
at https://driver.caru.com.tw/_nuxt/eb0ca7a.js:2:150100
at x (https://driver.caru.com.tw/_nuxt/eb0ca7a.js:2:152895)
at r (https://driver.caru.com.tw/_nuxt/eb0ca7a.js:2:148750)
at Tt (https://driver.caru.com.tw/_nuxt/eb0ca7a.js:2:148787)
at e.Vt.confirmTransition (https://driver.caru.com.tw/_nuxt/eb0ca7a.js:2:153285)
at e.Vt.transitionTo (https://driver.caru.com.tw/_nuxt/eb0ca7a.js:2:151612)
at ee.init (https://driver.caru.com.tw/_nuxt/eb0ca7a.js:2:158965)
at Dn.beforeCreate (https://driver.caru.com.tw/_nuxt/eb0ca7a.js:2:161173)
at ee (https://driver.caru.com.tw/_nuxt/eb0ca7a.js:2:11828)
at vn (https://driver.caru.com.tw/_nuxt/eb0ca7a.js:2:26234)
at Dn.t._init (https://driver.caru.com.tw/_nuxt/eb0ca7a.js:2:33662)
at new Dn (https://driver.caru.com.tw/_nuxt/eb0ca7a.js:2:31251)
at https://driver.caru.com.tw/_nuxt/4f5d376.js:2:290474
at h (https://driver.caru.com.tw/_nuxt/4f5d376.js:2:101657)
at Generator._invoke (https://driver.caru.com.tw/_nuxt/4f5d376.js:2:101445)
at Generator.E.forEach.e.<computed> [as next] (https://driver.caru.com.tw/_nuxt/4f5d376.js:2:102080)
at r (https://driver.caru.com.tw/_nuxt/eb0ca7a.js:2:66614)
at l (https://driver.caru.com.tw/_nuxt/eb0ca7a.js:2:66817)
```

4.4. https://driver.caru.com.tw/

Previous Next

Summary

Severity:	**Information**
Confidence:	**Firm**
Host:	**https://driver.caru.com.tw**
Path:	/

Issue detail

The application may be vulnerable to DOM-based DOM data manipulation. Data is read from **location.hash** and passed to **history.replaceState**.

Request

```
GET / HTTP/1.1
Host: driver.caru.com.tw
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
Upgrade-Insecure-Requests: 1
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en-GB;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/95.0.4638.54 Safari/537.36
Connection: close
Cache-Control: max-age=0
```

Response

```
HTTP/1.1 200 OK
Date: Thu, 02 Dec 2021 06:42:24 GMT
Server: Apache/2.4.41 (Ubuntu)
Last-Modified: Fri, 26 Nov 2021 09:56:37 GMT
ETag: "e9f-5d1ae1b62d5ae-gzip"
Accept-Ranges: bytes
Vary: Accept-Encoding
Content-Length: 3743
Connection: close
Content-Type: text/html

<!doctype html>
<html lang="en" data-n-head="%7B%22lang%22:%7B%221%22:%22en%22%7D%7D">
```

```
<head>
<title>CarU .....</title><meta data-n-head="1" charset="utf-8"><meta data-n-head="1" name="vi
...[SNIP]...
```

Dynamic analysis

Data is read from **location.hash** and passed to **history.replaceState**.

The following value was injected into the source:

```
#kuimwaeetw=kuimwaeetw%27%22`'"/kuimwaeetw/><kuimwaeetw/\>ity59hjaoh&
```

The previous value reached the sink as:

```
/ywwmf3a7nn%27%22%60'%22/ywwmf3a7nn/%3E%3Cywwmf3a7nn/%3Egv8de8uz27&?dkvkumps8c=dkvkumps8c%27%22%60%27%22%2Fdkvkumps8c%2F%3E%3Cdkvku
```

The stack trace at the source was:

```
at Object._0x16d0e7 [as proxiedGetterCallback] (<anonymous>:1:591983)
at Object.get hash [as hash] (<anonymous>:1:299763)
at Wt (https://driver.caru.com.tw/_nuxt/eb0ca7a.js:2:155340)
at e.getCurrentLocation (https://driver.caru.com.tw/_nuxt/eb0ca7a.js:2:155097)
at ee.init (https://driver.caru.com.tw/_nuxt/eb0ca7a.js:2:158980)
at Dn.beforeCreate (https://driver.caru.com.tw/_nuxt/eb0ca7a.js:2:161173)
at ee (https://driver.caru.com.tw/_nuxt/eb0ca7a.js:2:11828)
at vn (https://driver.caru.com.tw/_nuxt/eb0ca7a.js:2:26234)
at Dn.t._init (https://driver.caru.com.tw/_nuxt/eb0ca7a.js:2:33662)
at new Dn (https://driver.caru.com.tw/_nuxt/eb0ca7a.js:2:31251)
at https://driver.caru.com.tw/_nuxt/4f5d376.js:2:290474
at h (https://driver.caru.com.tw/_nuxt/4f5d376.js:2:101657)
at Generator._invoke (https://driver.caru.com.tw/_nuxt/4f5d376.js:2:101445)
at Generator.E.forEach.e.<computed> [as next] (https://driver.caru.com.tw/_nuxt/4f5d376.js:2:102080)
at r (https://driver.caru.com.tw/_nuxt/eb0ca7a.js:2:66614)
at l (https://driver.caru.com.tw/_nuxt/eb0ca7a.js:2:66817)
at https://driver.caru.com.tw/_nuxt/eb0ca7a.js:2:66876
at new Promise (<anonymous>)
at https://driver.caru.com.tw/_nuxt/eb0ca7a.js:2:66757
at U (https://driver.caru.com.tw/_nuxt/4f5d376.js:2:291448)
at https://driver.caru.com.tw/_nuxt/4f5d376.js:2:291524
```

The stack trace at the sink was:

```
at History.replaceState (<anonymous>:1:582436)
at jt (https://driver.caru.com.tw/_nuxt/eb0ca7a.js:2:148558)
at Ct (https://driver.caru.com.tw/_nuxt/eb0ca7a.js:2:148683)
at e.ensureURL (https://driver.caru.com.tw/_nuxt/eb0ca7a.js:2:155040)
at https://driver.caru.com.tw/_nuxt/eb0ca7a.js:2:151671
at https://driver.caru.com.tw/_nuxt/eb0ca7a.js:2:153653
at r (https://driver.caru.com.tw/_nuxt/eb0ca7a.js:2:148741)
at Tt (https://driver.caru.com.tw/_nuxt/eb0ca7a.js:2:148787)
at https://driver.caru.com.tw/_nuxt/eb0ca7a.js:2:153554
at r (https://driver.caru.com.tw/_nuxt/eb0ca7a.js:2:148741)
at https://driver.caru.com.tw/_nuxt/eb0ca7a.js:2:148769
at https://driver.caru.com.tw/_nuxt/eb0ca7a.js:2:153261
at https://driver.caru.com.tw/_nuxt/eb0ca7a.js:2:150100
at x (https://driver.caru.com.tw/_nuxt/eb0ca7a.js:2:152895)
at r (https://driver.caru.com.tw/_nuxt/eb0ca7a.js:2:148750)
at Tt (https://driver.caru.com.tw/_nuxt/eb0ca7a.js:2:148787)
at e.Vt.confirmTransition (https://driver.caru.com.tw/_nuxt/eb0ca7a.js:2:153285)
at e.Vt.transitionTo (https://driver.caru.com.tw/_nuxt/eb0ca7a.js:2:151612)
at ee.init (https://driver.caru.com.tw/_nuxt/eb0ca7a.js:2:158965)
at Dn.beforeCreate (https://driver.caru.com.tw/_nuxt/eb0ca7a.js:2:161173)
at ee (https://driver.caru.com.tw/_nuxt/eb0ca7a.js:2:11828)
at vn (https://driver.caru.com.tw/_nuxt/eb0ca7a.js:2:26234)
at Dn.t._init (https://driver.caru.com.tw/_nuxt/eb0ca7a.js:2:33662)
at new Dn (https://driver.caru.com.tw/_nuxt/eb0ca7a.js:2:31251)
at https://driver.caru.com.tw/_nuxt/4f5d376.js:2:290474
at h (https://driver.caru.com.tw/_nuxt/4f5d376.js:2:101657)
at Generator._invoke (https://driver.caru.com.tw/_nuxt/4f5d376.js:2:101445)
at Generator.E.forEach.e.<computed> [as next] (https://driver.caru.com.tw/_nuxt/4f5d376.js:2:102080)
at r (https://driver.caru.com.tw/_nuxt/eb0ca7a.js:2:66614)
at l (https://driver.caru.com.tw/_nuxt/eb0ca7a.js:2:66817)
```

4.5. https://driver.caru.com.tw/login/

Previous Next

Summary

Severity:	**Information**
Confidence:	**Firm**
Host:	**https://driver.caru.com.tw**
Path:	**/login/**

Issue detail

The application may be vulnerable to DOM-based DOM data manipulation. Data is read from **location.href** and passed to **history.replaceState**.

Request

```
GET /login/? HTTP/1.1
Host: driver.caru.com.tw
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
Upgrade-Insecure-Requests: 1
Referer: https://driver.caru.com.tw/login/
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en-GB;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/95.0.4638.54 Safari/537.36
Connection: close
Cache-Control: max-age=0
```

Response

```
HTTP/1.1 200 OK
Date: Thu, 02 Dec 2021 06:42:37 GMT
Server: Apache/2.4.41 (Ubuntu)
Last-Modified: Fri, 26 Nov 2021 09:56:36 GMT
ETag: "e9f-5d1ae1b4d8951-gzip"
Accept-Ranges: bytes
Vary: Accept-Encoding
Content-Length: 3743
Connection: close
Content-Type: text/html

<!doctype html>
<html lang="en" data-n-head="%7B%22lang%22:%7B%221%22:%22en%22%7D%7D">
<head>
<title>CarU .....</title><meta data-n-head="1" charset="utf-8"><meta data-n-head="1" name="vi
...[SNIP]...
```

Dynamic analysis

Data is read from **location.href** and passed to **history.replaceState**.

The following value was injected into the source and reached the sink without any modification:

```
?uo1ppk7b9e=uo1ppk7b9e%27%22`'"/uo1ppk7b9e/><uo1ppk7b9e/\>w6ieqfyb8b&
```

The stack trace at the source was:

```
at Object._0x16d0e7 [as proxiedGetterCallback] (<anonymous>:1:591983)
at Object.get href [as href] (<anonymous>:1:299867)
at mt (https://driver.caru.com.tw/_nuxt/eb0ca7a.js:2:146810)
at e.setupListeners (https://driver.caru.com.tw/_nuxt/eb0ca7a.js:2:154306)
at r (https://driver.caru.com.tw/_nuxt/eb0ca7a.js:2:158850)
at https://driver.caru.com.tw/_nuxt/eb0ca7a.js:2:151664
at https://driver.caru.com.tw/_nuxt/eb0ca7a.js:2:153653
at r (https://driver.caru.com.tw/_nuxt/eb0ca7a.js:2:148741)
at Tt (https://driver.caru.com.tw/_nuxt/eb0ca7a.js:2:148787)
at https://driver.caru.com.tw/_nuxt/eb0ca7a.js:2:153554
at r (https://driver.caru.com.tw/_nuxt/eb0ca7a.js:2:148741)
at https://driver.caru.com.tw/_nuxt/eb0ca7a.js:2:148769
at https://driver.caru.com.tw/_nuxt/eb0ca7a.js:2:153261
at https://driver.caru.com.tw/_nuxt/eb0ca7a.js:2:150100
at x (https://driver.caru.com.tw/_nuxt/eb0ca7a.js:2:152895)
at r (https://driver.caru.com.tw/_nuxt/eb0ca7a.js:2:148750)
at Tt (https://driver.caru.com.tw/_nuxt/eb0ca7a.js:2:148787)
at e.Vt.confirmTransition (https://driver.caru.com.tw/_nuxt/eb0ca7a.js:2:153285)
```

```
at e.Vt.transitionTo (https://driver.caru.com.tw/_nuxt/eb0ca7a.js:2:151612)
at ee.init (https://driver.caru.com.tw/_nuxt/eb0ca7a.js:2:158965)
at Dn.beforeCreate (https://driver.caru.com.tw/_nuxt/eb0ca7a.js:2:161173)
at ee (https://driver.caru.com.tw/_nuxt/eb0ca7a.js:2:11828)
at vn (https://driver.caru.com.tw/_nuxt/eb0ca7a.js:2:26234)
at Dn.t._init (https://driver.caru.com.tw/_nuxt/eb0ca7a.js:2:33662)
at new Dn (https://driver.caru.com.tw/_nuxt/eb0ca7a.js:2:31251)
at https://driver.caru.com.tw/_nuxt/4f5d376.js:2:290474
at h (https://driver.caru.com.tw/_nuxt/4f5d376.js:2:101657)
at Generator._invoke (https://driver.caru.com.tw/_nuxt/4f5d376.js:2:101445)
at Generator.E.forEach.e.<computed> [as next] (https://driver.caru.com.tw/_nuxt/4f5d376.js:2:102080)
at r (https://driver.caru.com.tw/_nuxt/eb0ca7a.js:2:66614)
```

The stack trace at the sink was:

```
at History.replaceState (<anonymous>:1:582436)
at mt (https://driver.caru.com.tw/_nuxt/eb0ca7a.js:2:146891)
at e.setupListeners (https://driver.caru.com.tw/_nuxt/eb0ca7a.js:2:154306)
at r (https://driver.caru.com.tw/_nuxt/eb0ca7a.js:2:158850)
at https://driver.caru.com.tw/_nuxt/eb0ca7a.js:2:151664
at https://driver.caru.com.tw/_nuxt/eb0ca7a.js:2:153653
at r (https://driver.caru.com.tw/_nuxt/eb0ca7a.js:2:148741)
at Tt (https://driver.caru.com.tw/_nuxt/eb0ca7a.js:2:148787)
at https://driver.caru.com.tw/_nuxt/eb0ca7a.js:2:153554
at r (https://driver.caru.com.tw/_nuxt/eb0ca7a.js:2:148741)
at https://driver.caru.com.tw/_nuxt/eb0ca7a.js:2:148769
at https://driver.caru.com.tw/_nuxt/eb0ca7a.js:2:153261
at https://driver.caru.com.tw/_nuxt/eb0ca7a.js:2:150100
at x (https://driver.caru.com.tw/_nuxt/eb0ca7a.js:2:152895)
at r (https://driver.caru.com.tw/_nuxt/eb0ca7a.js:2:148750)
at Tt (https://driver.caru.com.tw/_nuxt/eb0ca7a.js:2:148787)
at e.Vt.confirmTransition (https://driver.caru.com.tw/_nuxt/eb0ca7a.js:2:153285)
at e.Vt.transitionTo (https://driver.caru.com.tw/_nuxt/eb0ca7a.js:2:151612)
at ee.init (https://driver.caru.com.tw/_nuxt/eb0ca7a.js:2:158965)
at Dn.beforeCreate (https://driver.caru.com.tw/_nuxt/eb0ca7a.js:2:161173)
at ee (https://driver.caru.com.tw/_nuxt/eb0ca7a.js:2:11828)
at vn (https://driver.caru.com.tw/_nuxt/eb0ca7a.js:2:26234)
at Dn.t._init (https://driver.caru.com.tw/_nuxt/eb0ca7a.js:2:33662)
at new Dn (https://driver.caru.com.tw/_nuxt/eb0ca7a.js:2:31251)
at https://driver.caru.com.tw/_nuxt/4f5d376.js:2:290474
at h (https://driver.caru.com.tw/_nuxt/4f5d376.js:2:101657)
at Generator._invoke (https://driver.caru.com.tw/_nuxt/4f5d376.js:2:101445)
at Generator.E.forEach.e.<computed> [as next] (https://driver.caru.com.tw/_nuxt/4f5d376.js:2:102080)
at r (https://driver.caru.com.tw/_nuxt/eb0ca7a.js:2:66614)
at l (https://driver.caru.com.tw/_nuxt/eb0ca7a.js:2:66817)
```

4.6. https://driver.caru.com.tw/login/

Previous Next

Summary

Severity:	**Information**
Confidence:	**Firm**
Host:	**https://driver.caru.com.tw**
Path:	**/login/**

Issue detail

The application may be vulnerable to DOM-based DOM data manipulation. Data is read from **location.pathname** and passed to **history.replaceState**.

Request

```
GET /login/? HTTP/1.1
Host: driver.caru.com.tw
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
Upgrade-Insecure-Requests: 1
Referer: https://driver.caru.com.tw/login/
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en-GB;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/95.0.4638.54 Safari/537.36
Connection: close
Cache-Control: max-age=0
```

Response

```
HTTP/1.1 200 OK
Date: Thu, 02 Dec 2021 06:42:37 GMT
Server: Apache/2.4.41 (Ubuntu)
Last-Modified: Fri, 26 Nov 2021 09:56:36 GMT
ETag: "e9f-5d1ae1b4d6951-gzip"
Accept-Ranges: bytes
Vary: Accept-Encoding
Content-Length: 3743
Connection: close
Content-Type: text/html

<!doctype html>
<html lang="en" data-n-head="%7B%22lang%22:%7B%221%22:%22en%22%7D%7D">
<head>
<title>CarU .....</title><meta data-n-head="1" charset="utf-8"><meta data-n-head="1" name="vi
...[SNIP]...
```

Dynamic analysis

Data is read from **location.pathname** and passed to **history.replaceState**.

The following value was injected into the source:

```
///login///wtrsg84nzb%27%22%60'%22/wtrsg84nzb/%3E%3Cwtrsg84nzb//%3Ezox1z8c890&
```

The previous value reached the sink as:

```
/login/wtrsg84nzb%27%22%60'%22/wtrsg84nzb/%3E%3Cwtrsg84nzb/%3Ezox1z8c890&?ehjtnuuqgp=ehjtnuuqgp%27%22%60%27%22%2Fehjtnuuqgp%2F%3E%3
```

The stack trace at the source was:

```
at Object._0x16d0e7 [as proxiedGetterCallback] (<anonymous>:1:591983)
at Object.get pathname [as pathname] (<anonymous>:1:299963)
at Wt (https://driver.caru.com.tw/_nuxt/eb0ca7a.js:2:155162)
at e.getCurrentLocation (https://driver.caru.com.tw/_nuxt/eb0ca7a.js:2:155097)
at ee.init (https://driver.caru.com.tw/_nuxt/eb0ca7a.js:2:158980)
at Dn.beforeCreate (https://driver.caru.com.tw/_nuxt/eb0ca7a.js:2:161173)
at ee (https://driver.caru.com.tw/_nuxt/eb0ca7a.js:2:11828)
at vn (https://driver.caru.com.tw/_nuxt/eb0ca7a.js:2:26234)
at Dn.t._init (https://driver.caru.com.tw/_nuxt/eb0ca7a.js:2:33662)
at new Dn (https://driver.caru.com.tw/_nuxt/eb0ca7a.js:2:31251)
at https://driver.caru.com.tw/_nuxt/4f5d376.js:2:290474
at h (https://driver.caru.com.tw/_nuxt/4f5d376.js:2:101657)
at Generator._invoke (https://driver.caru.com.tw/_nuxt/4f5d376.js:2:101445)
at Generator.E.forEach.e.<computed> [as next] (https://driver.caru.com.tw/_nuxt/4f5d376.js:2:102080)
at r (https://driver.caru.com.tw/_nuxt/eb0ca7a.js:2:66614)
at l (https://driver.caru.com.tw/_nuxt/eb0ca7a.js:2:66817)
at https://driver.caru.com.tw/_nuxt/eb0ca7a.js:2:66876
at new Promise (<anonymous>)
at https://driver.caru.com.tw/_nuxt/eb0ca7a.js:2:66757
at U (https://driver.caru.com.tw/_nuxt/4f5d376.js:2:291448)
at https://driver.caru.com.tw/_nuxt/4f5d376.js:2:291524
```

The stack trace at the sink was:

```
at History.replaceState (<anonymous>:1:582436)
at jt (https://driver.caru.com.tw/_nuxt/eb0ca7a.js:2:148558)
at Ct (https://driver.caru.com.tw/_nuxt/eb0ca7a.js:2:148683)
at e.ensureURL (https://driver.caru.com.tw/_nuxt/eb0ca7a.js:2:155040)
at https://driver.caru.com.tw/_nuxt/eb0ca7a.js:2:151671
at https://driver.caru.com.tw/_nuxt/eb0ca7a.js:2:153653
at r (https://driver.caru.com.tw/_nuxt/eb0ca7a.js:2:148741)
at Tt (https://driver.caru.com.tw/_nuxt/eb0ca7a.js:2:148787)
at https://driver.caru.com.tw/_nuxt/eb0ca7a.js:2:153554
at r (https://driver.caru.com.tw/_nuxt/eb0ca7a.js:2:148741)
at https://driver.caru.com.tw/_nuxt/eb0ca7a.js:2:148769
at https://driver.caru.com.tw/_nuxt/eb0ca7a.js:2:153261
at https://driver.caru.com.tw/_nuxt/eb0ca7a.js:2:150100
at x (https://driver.caru.com.tw/_nuxt/eb0ca7a.js:2:152895)
at r (https://driver.caru.com.tw/_nuxt/eb0ca7a.js:2:148750)
at Tt (https://driver.caru.com.tw/_nuxt/eb0ca7a.js:2:148787)
at e.Vt.confirmTransition (https://driver.caru.com.tw/_nuxt/eb0ca7a.js:2:153285)
at e.Vt.transitionTo (https://driver.caru.com.tw/_nuxt/eb0ca7a.js:2:151612)
at ee.init (https://driver.caru.com.tw/_nuxt/eb0ca7a.js:2:158965)
at Dn.beforeCreate (https://driver.caru.com.tw/_nuxt/eb0ca7a.js:2:161173)
at ee (https://driver.caru.com.tw/_nuxt/eb0ca7a.js:2:11828)
```

```
at Dn.beforeCreate (https://driver.caru.com.tw/_nuxt/eb0ca7a.js:2:161173)
at ee (https://driver.caru.com.tw/_nuxt/eb0ca7a.js:2:11828)
at vn (https://driver.caru.com.tw/_nuxt/eb0ca7a.js:2:26234)
at Dn.t._init (https://driver.caru.com.tw/_nuxt/eb0ca7a.js:2:33662)
at new Dn (https://driver.caru.com.tw/_nuxt/eb0ca7a.js:2:31251)
at https://driver.caru.com.tw/_nuxt/4f5d376.js:2:290474
at h (https://driver.caru.com.tw/_nuxt/4f5d376.js:2:101657)
at Generator._invoke (https://driver.caru.com.tw/_nuxt/4f5d376.js:2:101445)
at Generator.E.forEach.e.<computed> [as next] (https://driver.caru.com.tw/_nuxt/4f5d376.js:2:102080)
at r (https://driver.caru.com.tw/_nuxt/eb0ca7a.js:2:66614)
at l (https://driver.caru.com.tw/_nuxt/eb0ca7a.js:2:66817)
```

4.7. https://driver.caru.com.tw/login/

Previous Next

Summary

Severity:	**Information**
Confidence:	**Firm**
Host:	**https://driver.caru.com.tw**
Path:	**/login/**

Issue detail

The application may be vulnerable to DOM-based DOM data manipulation. Data is read from **location.search** and passed to **history.replaceState**.

Request

```
GET /login/? HTTP/1.1
Host: driver.caru.com.tw
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
Upgrade-Insecure-Requests: 1
Referer: https://driver.caru.com.tw/login/
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en-GB;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/95.0.4638.54 Safari/537.36
Connection: close
Cache-Control: max-age=0
```

Response

```
HTTP/1.1 200 OK
Date: Thu, 02 Dec 2021 06:42:37 GMT
Server: Apache/2.4.41 (Ubuntu)
Last-Modified: Fri, 26 Nov 2021 09:56:36 GMT
ETag: "e9f-5d1ae1b4d6951-gzip"
Accept-Ranges: bytes
Vary: Accept-Encoding
Content-Length: 3743
Connection: close
Content-Type: text/html

<!doctype html>
<html lang="en" data-n-head="%7B%22lang%22:%7B%221%22:%22en%22%7D%7D">
<head>
<title>CarU .....</title><meta data-n-head="1" charset="utf-8"><meta data-n-head="1" name="vi
...[SNIP]...
```

Dynamic analysis

Data is read from **location.search** and passed to **history.replaceState**.

The following value was injected into the source:

```
?ehjtnuuqgp=ehjtnuuqgp%27%22`'"/ehjtnuuqgp/><ehjtnuuqgp/\>x3chmzps6b&
```

The previous value reached the sink as:

/login/wtrsg84nzb%27%22%60'%22/wtrsg84nzb/%3E%3Cwtrsg84nzb/%3Ezox1z8c890&?ehjtnuuqgp=ehjtnuuqgp%27%22%60%27%22%2Fehjtnuuqgp%2F%3E%3Ce

The stack trace at the source was:

```
at Object._0x16d0e7 [as proxiedGetterCallback] (<anonymous>:1:591983)
at Object.get search [as search] (<anonymous>:1:299118)
at Wt (https://driver.caru.com.tw/_nuxt/eb0ca7a.js:2:155317)
at e.getCurrentLocation (https://driver.caru.com.tw/_nuxt/eb0ca7a.js:2:155097)
at ee.init (https://driver.caru.com.tw/_nuxt/eb0ca7a.js:2:158980)
at Dn.beforeCreate (https://driver.caru.com.tw/_nuxt/eb0ca7a.js:2:161173)
at ee (https://driver.caru.com.tw/_nuxt/eb0ca7a.js:2:11828)
at vn (https://driver.caru.com.tw/_nuxt/eb0ca7a.js:2:26234)
at Dn.t._init (https://driver.caru.com.tw/_nuxt/eb0ca7a.js:2:33662)
at new Dn (https://driver.caru.com.tw/_nuxt/eb0ca7a.js:2:31251)
at https://driver.caru.com.tw/_nuxt/4f5d376.js:2:290474
at h (https://driver.caru.com.tw/_nuxt/4f5d376.js:2:101657)
at Generator._invoke (https://driver.caru.com.tw/_nuxt/4f5d376.js:2:101445)
at Generator.E.forEach.e.<computed> [as next] (https://driver.caru.com.tw/_nuxt/4f5d376.js:2:102080)
at r (https://driver.caru.com.tw/_nuxt/eb0ca7a.js:2:66614)
at l (https://driver.caru.com.tw/_nuxt/eb0ca7a.js:2:66817)
at https://driver.caru.com.tw/_nuxt/eb0ca7a.js:2:66876
at new Promise (<anonymous>)
at https://driver.caru.com.tw/_nuxt/eb0ca7a.js:2:66757
at U (https://driver.caru.com.tw/_nuxt/4f5d376.js:2:291448)
at https://driver.caru.com.tw/_nuxt/4f5d376.js:2:291524
```

The stack trace at the sink was:

```
at History.replaceState (<anonymous>:1:582436)
at jt (https://driver.caru.com.tw/_nuxt/eb0ca7a.js:2:148558)
at Ct (https://driver.caru.com.tw/_nuxt/eb0ca7a.js:2:148683)
at e.ensureURL (https://driver.caru.com.tw/_nuxt/eb0ca7a.js:2:155040)
at https://driver.caru.com.tw/_nuxt/eb0ca7a.js:2:151671
at https://driver.caru.com.tw/_nuxt/eb0ca7a.js:2:153653
at r (https://driver.caru.com.tw/_nuxt/eb0ca7a.js:2:148741)
at Tt (https://driver.caru.com.tw/_nuxt/eb0ca7a.js:2:148787)
at https://driver.caru.com.tw/_nuxt/eb0ca7a.js:2:153554
at r (https://driver.caru.com.tw/_nuxt/eb0ca7a.js:2:148741)
at https://driver.caru.com.tw/_nuxt/eb0ca7a.js:2:148769
at https://driver.caru.com.tw/_nuxt/eb0ca7a.js:2:153261
at https://driver.caru.com.tw/_nuxt/eb0ca7a.js:2:150100
at x (https://driver.caru.com.tw/_nuxt/eb0ca7a.js:2:152895)
at r (https://driver.caru.com.tw/_nuxt/eb0ca7a.js:2:148750)
at Tt (https://driver.caru.com.tw/_nuxt/eb0ca7a.js:2:148787)
at e.Vt.confirmTransition (https://driver.caru.com.tw/_nuxt/eb0ca7a.js:2:153285)
at e.Vt.transitionTo (https://driver.caru.com.tw/_nuxt/eb0ca7a.js:2:151612)
at ee.init (https://driver.caru.com.tw/_nuxt/eb0ca7a.js:2:158965)
at Dn.beforeCreate (https://driver.caru.com.tw/_nuxt/eb0ca7a.js:2:161173)
at ee (https://driver.caru.com.tw/_nuxt/eb0ca7a.js:2:11828)
at vn (https://driver.caru.com.tw/_nuxt/eb0ca7a.js:2:26234)
at Dn.t._init (https://driver.caru.com.tw/_nuxt/eb0ca7a.js:2:33662)
at new Dn (https://driver.caru.com.tw/_nuxt/eb0ca7a.js:2:31251)
at https://driver.caru.com.tw/_nuxt/4f5d376.js:2:290474
at h (https://driver.caru.com.tw/_nuxt/4f5d376.js:2:101657)
at Generator._invoke (https://driver.caru.com.tw/_nuxt/4f5d376.js:2:101445)
at Generator.E.forEach.e.<computed> [as next] (https://driver.caru.com.tw/_nuxt/4f5d376.js:2:102080)
at r (https://driver.caru.com.tw/_nuxt/eb0ca7a.js:2:66614)
at l (https://driver.caru.com.tw/_nuxt/eb0ca7a.js:2:66817)
```

4.8. https://driver.caru.com.tw/login/

Previous Next

Summary

Severity:	**Information**
Confidence:	**Firm**
Host:	**https://driver.caru.com.tw**
Path:	**/login/**

Issue detail

The application may be vulnerable to DOM-based DOM data manipulation. Data is read from **location.hash** and passed to **history.replaceState**.

Request

```
GET /login/? HTTP/1.1
Host: driver.caru.com.tw
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
Upgrade-Insecure-Requests: 1
Referer: https://driver.caru.com.tw/login/
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en-GB;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/95.0.4638.54 Safari/537.36
Connection: close
Cache-Control: max-age=0
```

Response

```
HTTP/1.1 200 OK
Date: Thu, 02 Dec 2021 06:42:37 GMT
Server: Apache/2.4.41 (Ubuntu)
Last-Modified: Fri, 26 Nov 2021 09:56:36 GMT
ETag: "e9f-5d1ae1b4d6951-gzip"
Accept-Ranges: bytes
Vary: Accept-Encoding
Content-Length: 3743
Connection: close
Content-Type: text/html

<!doctype html>
<html lang="en" data-n-head="%7B%22lang%22:%7B%221%22:%22en%22%7D%7D">
<head>
<title>CarU .....</title><meta data-n-head="1" charset="utf-8"><meta data-n-head="1" name="vi
...[SNIP]...
```

Dynamic analysis

Data is read from **location.hash** and passed to **history.replaceState**.

The following value was injected into the source:

```
#y84yag7jc3=y84yag7jc3%27%22`'"/y84yag7jc3/><y84yag7jc3/\>i57uqeaukh&
```

The previous value reached the sink as:

```
/login/wtrsg84nzb%27%22%60'%22/wtrsg84nzb/%3E%3Cwtrsg84nzb/%3Ezox1z8c890&?ehjtnuuqgp=ehjtnuuqgp%27%22%60%27%22%2Fehjtnuuqgp%2F%3E%3
```

The stack trace at the source was:

```
at Object._0x16d0e7 [as proxiedGetterCallback] (<anonymous>:1:591983)
at Object.get hash [as hash] (<anonymous>:1:299763)
at Wt (https://driver.caru.com.tw/_nuxt/eb0ca7a.js:2:155340)
at e.getCurrentLocation (https://driver.caru.com.tw/_nuxt/eb0ca7a.js:2:155097)
at ee.init (https://driver.caru.com.tw/_nuxt/eb0ca7a.js:2:158980)
at Dn.beforeCreate (https://driver.caru.com.tw/_nuxt/eb0ca7a.js:2:161173)
at ee (https://driver.caru.com.tw/_nuxt/eb0ca7a.js:2:11828)
at vn (https://driver.caru.com.tw/_nuxt/eb0ca7a.js:2:26234)
at Dn.t._init (https://driver.caru.com.tw/_nuxt/eb0ca7a.js:2:33662)
at new Dn (https://driver.caru.com.tw/_nuxt/eb0ca7a.js:2:31251)
at https://driver.caru.com.tw/_nuxt/4f5d376.js:2:290474
at h (https://driver.caru.com.tw/_nuxt/4f5d376.js:2:101657)
at Generator._invoke (https://driver.caru.com.tw/_nuxt/4f5d376.js:2:101445)
at Generator.E.forEach.e.<computed> [as next] (https://driver.caru.com.tw/_nuxt/4f5d376.js:2:102080)
at r (https://driver.caru.com.tw/_nuxt/eb0ca7a.js:2:66614)
at l (https://driver.caru.com.tw/_nuxt/eb0ca7a.js:2:66817)
at https://driver.caru.com.tw/_nuxt/eb0ca7a.js:2:66876
at new Promise (<anonymous>)
at https://driver.caru.com.tw/_nuxt/eb0ca7a.js:2:66757
at U (https://driver.caru.com.tw/_nuxt/4f5d376.js:2:291448)
at https://driver.caru.com.tw/_nuxt/4f5d376.js:2:291524
```

The stack trace at the sink was:

```
at History.replaceState (<anonymous>:1:582436)
at jt (https://driver.caru.com.tw/_nuxt/eb0ca7a.js:2:148558)
at Ct (https://driver.caru.com.tw/_nuxt/eb0ca7a.js:2:148683)
at e.ensureURL (https://driver.caru.com.tw/_nuxt/eb0ca7a.js:2:155040)
at https://driver.caru.com.tw/_nuxt/eb0ca7a.js:2:151671
at https://driver.caru.com.tw/_nuxt/eb0ca7a.js:2:153653
at r (https://driver.caru.com.tw/_nuxt/eb0ca7a.js:2:148741)
```

```
at l (https://driver.caru.com.tw/_nuxt/eb0ca7a.js:2:66817)
at https://driver.caru.com.tw/_nuxt/eb0ca7a.js:2:66876
at new Promise (<anonymous>)
at https://driver.caru.com.tw/_nuxt/eb0ca7a.js:2:66757
at U (https://driver.caru.com.tw/_nuxt/4f5d376.js:2:291448)
at https://driver.caru.com.tw/_nuxt/4f5d376.js:2:291524
```

The stack trace at the sink was:

```
at History.replaceState (<anonymous>:1:582436)
at jt (https://driver.caru.com.tw/_nuxt/eb0ca7a.js:2:148558)
at Ct (https://driver.caru.com.tw/_nuxt/eb0ca7a.js:2:148683)
at e.ensureURL (https://driver.caru.com.tw/_nuxt/eb0ca7a.js:2:155040)
at https://driver.caru.com.tw/_nuxt/eb0ca7a.js:2:151671
at https://driver.caru.com.tw/_nuxt/eb0ca7a.js:2:153653
at r (https://driver.caru.com.tw/_nuxt/eb0ca7a.js:2:148741)
at Tt (https://driver.caru.com.tw/_nuxt/eb0ca7a.js:2:148787)
at https://driver.caru.com.tw/_nuxt/eb0ca7a.js:2:153554
at r (https://driver.caru.com.tw/_nuxt/eb0ca7a.js:2:148741)
at https://driver.caru.com.tw/_nuxt/eb0ca7a.js:2:148769
at https://driver.caru.com.tw/_nuxt/eb0ca7a.js:2:153261
at https://driver.caru.com.tw/_nuxt/eb0ca7a.js:2:150100
at x (https://driver.caru.com.tw/_nuxt/eb0ca7a.js:2:152895)
at r (https://driver.caru.com.tw/_nuxt/eb0ca7a.js:2:148750)
at Tt (https://driver.caru.com.tw/_nuxt/eb0ca7a.js:2:148787)
at e.Vt.confirmTransition (https://driver.caru.com.tw/_nuxt/eb0ca7a.js:2:153285)
at e.Vt.transitionTo (https://driver.caru.com.tw/_nuxt/eb0ca7a.js:2:151612)
at ee.init (https://driver.caru.com.tw/_nuxt/eb0ca7a.js:2:158965)
at Dn.beforeCreate (https://driver.caru.com.tw/_nuxt/eb0ca7a.js:2:161173)
at ee (https://driver.caru.com.tw/_nuxt/eb0ca7a.js:2:11828)
at vn (https://driver.caru.com.tw/_nuxt/eb0ca7a.js:2:26234)
at Dn.t._init (https://driver.caru.com.tw/_nuxt/eb0ca7a.js:2:33662)
at new Dn (https://driver.caru.com.tw/_nuxt/eb0ca7a.js:2:31251)
at https://driver.caru.com.tw/_nuxt/4f5d376.js:2:290474
at h (https://driver.caru.com.tw/_nuxt/4f5d376.js:2:101657)
at Generator._invoke (https://driver.caru.com.tw/_nuxt/4f5d376.js:2:101445)
at Generator.E.forEach.e.<computed> [as next] (https://driver.caru.com.tw/_nuxt/4f5d376.js:2:102080)
at r (https://driver.caru.com.tw/_nuxt/eb0ca7a.js:2:66614)
at l (https://driver.caru.com.tw/_nuxt/eb0ca7a.js:2:66817)
```

5. Cacheable HTTPS response

Previous

There are 3 instances of this issue:

- /
- /_nuxt/manifest.d0e9c203.json
- /login/

Issue description

Unless directed otherwise, browsers may store a local cached copy of content received from web servers. Some browsers, including Internet Explorer, cache content accessed via HTTPS. If sensitive information in application responses is stored in the local cache, then this may be retrieved by other users who have access to the same computer at a future time.

Issue remediation

Applications should return caching directives instructing browsers not to store local copies of any sensitive data. Often, this can be achieved by configuring the web server to prevent caching for relevant paths within the web root. Alternatively, most web development platforms allow you to control the server's caching directives from within individual scripts. Ideally, the web server should return the following HTTP headers in all responses containing sensitive content:

- Cache-control: no-store
- Pragma: no-cache

References

- Web Security Academy: Information disclosure

Vulnerability classifications

- CWE-524: Information Exposure Through Caching
- CWE-525: Information Exposure Through Browser Caching
- CAPEC-37: Retrieve Embedded Sensitive Data

5.1. https://driver.caru.com.tw/

Previous Next

Summary

Severity:	**Information**
Confidence:	**Certain**
Host:	**https://driver.caru.com.tw**
Path:	**/**

Request

```
GET / HTTP/1.1
Host: driver.caru.com.tw
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
Upgrade-Insecure-Requests: 1
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en-GB;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/95.0.4638.54 Safari/537.36
Connection: close
Cache-Control: max-age=0
```

Response

```
HTTP/1.1 200 OK
Date: Thu, 02 Dec 2021 06:42:24 GMT
Server: Apache/2.4.41 (Ubuntu)
Last-Modified: Fri, 26 Nov 2021 09:56:37 GMT
ETag: "e9f-5d1ae1b62d5ae-gzip"
Accept-Ranges: bytes
Vary: Accept-Encoding
Content-Length: 3743
Connection: close
Content-Type: text/html

<!doctype html>
<html lang="en" data-n-head="%7B%22lang%22:%7B%221%22:%22en%22%7D%7D">
<head>
<title>CarU .....</title><meta data-n-head="1" charset="utf-8"><meta data-n-head="1" name="vi
...[SNIP]...
```

5.2. https://driver.caru.com.tw/_nuxt/manifest.d0e9c203.json

Previous Next

Summary

Severity:	**Information**
Confidence:	**Certain**
Host:	**https://driver.caru.com.tw**
Path:	**/_nuxt/manifest.d0e9c203.json**

Request

```
GET /_nuxt/manifest.d0e9c203.json HTTP/1.1
Host: driver.caru.com.tw
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
Upgrade-Insecure-Requests: 1
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en-GB;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/95.0.4638.54 Safari/537.36
Connection: close
Cache-Control: max-age=0
```

Response

```
HTTP/1.1 200 OK
Date: Thu, 02 Dec 2021 06:43:19 GMT
Server: Apache/2.4.41 (Ubuntu)
Last-Modified: Fri, 26 Nov 2021 09:56:40 GMT
ETag: "51d-5d1ae1b955f25"
Accept-Ranges: bytes
Content-Length: 1309
Connection: close
Content-Type: application/json

{
"name": "CarU .....",
"short_name": "CarU .....",
"description": "## Build Setup",
"icons": [
{
"src": "/_nuxt/icons/icon_64x64.2924ce.png",
"sizes": "64x64",
"
...[SNIP]...
```

5.3. https://driver.caru.com.tw/login/

Previous

Summary

Severity:	**Information**
Confidence:	**Certain**
Host:	**https://driver.caru.com.tw**
Path:	**/login/**

Request

```
GET /login/? HTTP/1.1
Host: driver.caru.com.tw
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
Upgrade-Insecure-Requests: 1
Referer: https://driver.caru.com.tw/login/
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en-GB;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/95.0.4638.54 Safari/537.36
Connection: close
Cache-Control: max-age=0
```

Response

```
HTTP/1.1 200 OK
Date: Thu, 02 Dec 2021 06:42:37 GMT
Server: Apache/2.4.41 (Ubuntu)
Last-Modified: Fri, 26 Nov 2021 09:56:36 GMT
ETag: "e9f-5d1ae1b4d6951-gzip"
Accept-Ranges: bytes
Vary: Accept-Encoding
Content-Length: 3743
Connection: close
Content-Type: text/html

<!doctype html>
<html lang="en" data-n-head="%7B%22lang%22:%7B%221%22:%22en%22%7D%7D">
<head>
<title>CarU .....</title><meta data-n-head="1" charset="utf-8"><meta data-n-head="1" name="vi
...[SNIP]...
```

---

store.caru.com.tw

Burp Scanner Report

Burp Suite Professional

Summary

The table below shows the numbers of issues identified in different categories. Issues are classified according to severity as High, Medium, Low or Information. This reflects the likely impact of each issue for a typical organization. Issues are also classified according to confidence as Certain, Firm or Tentative. This reflects the inherent reliability of the technique that was used to identify the issue.

Severity	Confidence			
	Certain	Firm	Tentative	Total
High	0	0	0	0
Medium	1	0	0	1
Low	1	0	0	1
Information	3	10	0	13

The chart below shows the aggregated numbers of issues identified in each category. Solid colored bars represent issues with a confidence level of Certain, and the bars fade as the confidence level falls.

Contents

1. TLS certificate
2. Strict transport security not enforced
3. Frameable response (potential Clickjacking)
   - 3.1. https://store.caru.com.tw/
   - 3.2. https://store.caru.com.tw/login/
4. DOM data manipulation (DOM-based)
   - 4.1. https://store.caru.com.tw/
   - 4.2. https://store.caru.com.tw/
   - 4.3. https://store.caru.com.tw/
   - 4.4. https://store.caru.com.tw/
   - 4.5. https://store.caru.com.tw/login/
   - 4.6. https://store.caru.com.tw/login/
   - 4.7. https://store.caru.com.tw/login/
   - 4.8. https://store.caru.com.tw/login/
5. Cacheable HTTPS response
   - 5.1. https://store.caru.com.tw/
   - 5.2. https://store.caru.com.tw/_nuxt/manifest.f2313aaf.json
   - 5.3. https://store.caru.com.tw/login/

1. TLS certificate

Next

Summary

Severity:	**Medium**
Confidence:	**Certain**
Host:	**https://store.caru.com.tw**
Path:	/

Issue detail

The following problem was identified with the server's TLS certificate:

- The server's certificate is not trusted.

Note: Burp relies on the Java trust store to determine whether certificates are trusted. The Java trust store does not include every root CA certificate that is included within browser trust stores. Burp might incorrectly report that a certificate is not trusted, if a valid root CA certificate is being used that is not included in the Java trust store.

The server presented the following certificates:

Server certificate

Issued to: store.caru.com.tw
Issued by: R3
Valid from: Sun Nov 07 21:10:42 GMT+08:00 2021
Valid to: Sat Feb 05 21:10:41 GMT+08:00 2022

Certificate chain #1

Issued to: R3
Issued by: ISRG Root X1
Valid from: Fri Sep 04 08:00:00 GMT+08:00 2020
Valid to: Tue Sep 16 00:00:00 GMT+08:00 2025

Certificate chain #2

Issued to: ISRG Root X1
Issued by: DST Root CA X3
Valid from: Thu Jan 21 03:14:03 GMT+08:00 2021
Valid to: Tue Oct 01 02:14:03 GMT+08:00 2024

Issue background

TLS (or SSL) helps to protect the confidentiality and integrity of information in transit between the browser and server, and to provide authentication of the server's identity. To serve this purpose, the server must present an TLS certificate that is valid for the server's hostname, is issued by a trusted authority and is valid for the current date. If any one of these requirements is not met, TLS connections to the server will not provide the full protection for which TLS is designed.

It should be noted that various attacks exist against TLS in general, and in the context of HTTPS web connections in particular. It may be possible for a determined and suitably-positioned attacker to compromise TLS connections without user detection even when a valid TLS certificate is used.

References

- SSL/TLS Configuration Guide

Vulnerability classifications

- CWE-295: Improper Certificate Validation
- CWE-326: Inadequate Encryption Strength
- CWE-327: Use of a Broken or Risky Cryptographic Algorithm

2. Strict transport security not enforced

Previous Next

Summary

Severity:	Low
Confidence:	Certain
Host:	https://store.caru.com.tw
Path:	/

Issue detail

This issue was found in multiple locations under the reported path.

Issue background

The application fails to prevent users from connecting to it over unencrypted connections. An attacker able to modify a legitimate user's network traffic could bypass the application's use of SSL/TLS encryption, and use the application as a platform for attacks against its users. This attack is performed by rewriting HTTPS links as HTTP, so that if a targeted user follows a link to the site from an HTTP page, their browser never attempts to use an encrypted connection. The sslstrip tool automates this process.

To exploit this vulnerability, an attacker must be suitably positioned to intercept and modify the victim's network traffic.This scenario typically occurs when a client communicates with the server over an insecure connection such as public Wi-Fi, or a corporate or home network that is shared with a compromised computer. Common defenses such as switched networks are not sufficient to prevent this. An attacker situated in the user's ISP or the application's hosting infrastructure could also perform this attack. Note that an advanced adversary could potentially target any connection made over the Internet's core infrastructure.

Issue remediation

The application should instruct web browsers to only access the application using HTTPS. To do this, enable HTTP Strict Transport Security (HSTS) by adding a response header with the name 'Strict-Transport-Security' and the value 'max-age=expireTime', where expireTime is the time in seconds that browsers should remember that the site should only be accessed using HTTPS. Consider adding the 'includeSubDomains' flag if appropriate.

Note that because HSTS is a "trust on first use" (TOFU) protocol, a user who has never accessed the application will never have seen the HSTS header, and will therefore still be vulnerable to SSL stripping attacks. To mitigate this risk, you can optionally add the 'preload' flag to the HSTS header, and submit the domain for review by browser vendors.

References

- HTTP Strict Transport Security
- sslstrip
- HSTS Preload Form

Vulnerability classifications

- CWE-523: Unprotected Transport of Credentials
- CAPEC-94: Man in the Middle Attack
- CAPEC-157: Sniffing Attacks

Request

```
GET /login/? HTTP/1.1
Host: store.caru.com.tw
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
Upgrade-Insecure-Requests: 1
Referer: https://store.caru.com.tw/login
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en-GB;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/95.0.4638.54 Safari/537.36
Connection: close
Cache-Control: max-age=0
```

Response

```
HTTP/1.1 200 OK
Date: Thu, 02 Dec 2021 04:13:17 GMT
Server: Apache/2.4.41 (Ubuntu)
Last-Modified: Tue, 30 Nov 2021 09:01:12 GMT
ETag: "e9e-5d1fdcc8d52f5-gzip"
Accept-Ranges: bytes
Vary: Accept-Encoding
Content-Length: 3742
Connection: close
Content-Type: text/html

<!doctype html>
<html lang="en" data-n-head="%7B%22lang%22:%7B%221%22:%22en%22%7D%7D">
```

```
<title>CarU .....</title><meta data-n-head="1" charset="utf-8"><meta data-n-head="1" name="vi
...[SNIP]...
```

3. Frameable response (potential Clickjacking)

Previous Next

There are 2 instances of this issue:

- /
- /login/

Issue description

If a page fails to set an appropriate X-Frame-Options or Content-Security-Policy HTTP header, it might be possible for a page controlled by an attacker to load it within an iframe. This may enable a clickjacking attack, in which the attacker's page overlays the target application's interface with a different interface provided by the attacker. By inducing victim users to perform actions such as mouse clicks and keystrokes, the attacker can cause them to unwittingly carry out actions within the application that is being targeted. This technique allows the attacker to circumvent defenses against cross-site request forgery, and may result in unauthorized actions.

Note that some applications attempt to prevent these attacks from within the HTML page itself, using "framebusting" code. However, this type of defense is normally ineffective and can usually be circumvented by a skilled attacker.

You should determine whether any functions accessible within frameable pages can be used by application users to perform any sensitive actions within the application.

Issue remediation

To effectively prevent framing attacks, the application should return a response header with the name **X-Frame-Options** and the value **DENY** to prevent framing altogether, or the value **SAMEORIGIN** to allow framing only by pages on the same origin as the response itself. Note that the SAMEORIGIN header can be partially bypassed if the application itself can be made to frame untrusted websites.

References

- Web Security Academy: Clickjacking
- X-Frame-Options

Vulnerability classifications

- CWE-693: Protection Mechanism Failure
- CAPEC-103: Clickjacking

3.1. https://store.caru.com.tw/

Next

Summary

Severity:	**Information**
Confidence:	**Firm**
Host:	**https://store.caru.com.tw**
Path:	**/**

Request

```
GET / HTTP/1.1
Host: store.caru.com.tw
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
Upgrade-Insecure-Requests: 1
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en-GB;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/95.0.4638.54 Safari/537.36
Connection: close
```

```
Cache-Control: max-age=0
```

Response

```
HTTP/1.1 200 OK
Date: Thu, 02 Dec 2021 04:03:41 GMT
Server: Apache/2.4.41 (Ubuntu)
Last-Modified: Tue, 30 Nov 2021 09:01:13 GMT
ETag: "e9e-5d1fdcc9decf2-gzip"
Accept-Ranges: bytes
Vary: Accept-Encoding
Content-Length: 3742
Connection: close
Content-Type: text/html

<!doctype html>
<html lang="en" data-n-head="%7B%22lang%22:%7B%221%22:%22en%22%7D%7D">
<head>
<title>CarU .....</title><meta data-n-head="1" charset="utf-8"><meta data-n-head="1" name="vi
...[SNIP]...
```

3.2. https://store.caru.com.tw/login/

Previous Next

Summary

Severity:	**Information**
Confidence:	**Firm**
Host:	**https://store.caru.com.tw**
Path:	**/login/**

Request

```
GET /login/? HTTP/1.1
Host: store.caru.com.tw
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
Upgrade-Insecure-Requests: 1
Referer: https://store.caru.com.tw/login
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en-GB;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/95.0.4638.54 Safari/537.36
Connection: close
Cache-Control: max-age=0
```

Response

```
HTTP/1.1 200 OK
Date: Thu, 02 Dec 2021 04:13:17 GMT
Server: Apache/2.4.41 (Ubuntu)
Last-Modified: Tue, 30 Nov 2021 09:01:12 GMT
ETag: "e9e-5d1fdcc8d52f5-gzip"
Accept-Ranges: bytes
Vary: Accept-Encoding
Content-Length: 3742
Connection: close
Content-Type: text/html

<!doctype html>
<html lang="en" data-n-head="%7B%22lang%22:%7B%221%22:%22en%22%7D%7D">
<head>
<title>CarU .....</title><meta data-n-head="1" charset="utf-8"><meta data-n-head="1" name="vi
...[SNIP]...
```

4. DOM data manipulation (DOM-based)

Previous Next

There are 8 instances of this issue:

- /
- /
- /
- /
- /login/
- /login/
- /login/
- /login/

Issue background

DOM-based vulnerabilities arise when a client-side script reads data from a controllable part of the DOM (for example, the URL) and processes this data in an unsafe way.

DOM data manipulation arises when a script writes controllable data to a field within the DOM that is used within the visible UI or client-side application logic. An attacker may be able to use the vulnerability to construct a URL that, if visited by another application user, will modify the appearance or behavior of the client-side UI. An attacker may be able to leverage this to perform virtual defacement of the application, or possibly to induce the user to perform unintended actions.

Burp Suite automatically identifies this issue using static code analysis, which may lead to false positives that are not actually exploitable. The relevant code and execution paths should be reviewed to determine whether this vulnerability is indeed present, or whether mitigations are in place that would prevent exploitation.

Issue remediation

The most effective way to avoid DOM-based DOM data manipulation vulnerabilities is not to dynamically write to DOM data fields any data that originated from any untrusted source. If the desired functionality of the application means that this behavior is unavoidable, then defenses must be implemented within the client-side code to prevent malicious data from being stored. In general, this is best achieved by using a whitelist of permitted values.

References

- Web Security Academy: DOM data manipulation

Vulnerability classifications

- CWE-20: Improper Input Validation
- CAPEC-153: Input Data Manipulation

4.1. https://store.caru.com.tw/

Previous Next

Summary

Severity:	**Information**
Confidence:	**Firm**
Host:	**https://store.caru.com.tw**
Path:	/

Issue detail

The application may be vulnerable to DOM-based DOM data manipulation. Data is read from **location.href** and passed to **history.replaceState**.

Request

```
GET / HTTP/1.1
Host: store.caru.com.tw
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
Upgrade-Insecure-Requests: 1
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en-GB;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/95.0.4638.54 Safari/537.36
Connection: close
Cache-Control: max-age=0
```

Response

```
HTTP/1.1 200 OK
Date: Thu, 02 Dec 2021 04:03:41 GMT
Server: Apache/2.4.41 (Ubuntu)
Last-Modified: Tue, 30 Nov 2021 09:01:13 GMT
ETag: "e9e-5d1fdcc9decf2-gzip"
Accept-Ranges: bytes
Vary: Accept-Encoding
Content-Length: 3742
Connection: close
Content-Type: text/html

<!doctype html>
<html lang="en" data-n-head="%7B%22lang%22:%7B%221%22:%22en%22%7D%7D">
<head>
<title>CarU .....</title><meta data-n-head="1" charset="utf-8"><meta data-n-head="1" name="vi
...[SNIP]...
```

Dynamic analysis

Data is read from **location.href** and passed to **history.replaceState**.

The following value was injected into the source and reached the sink without any modification:

```
?sakmg7ljlk=sakmg7ljlk%27%22`'"/sakmg7ljlk/><sakmg7ljlk/\>e1r2o265we&
```

The stack trace at the source was:

```
at Object._0x16d0e7 [as proxiedGetterCallback] (<anonymous>:1:591983)
at Object.get href [as href] (<anonymous>:1:299867)
at mt (https://store.caru.com.tw/_nuxt/4ff1ebf.js:2:146806)
at e.setupListeners (https://store.caru.com.tw/_nuxt/4ff1ebf.js:2:154302)
at r (https://store.caru.com.tw/_nuxt/4ff1ebf.js:2:158846)
at https://store.caru.com.tw/_nuxt/4ff1ebf.js:2:151660
at https://store.caru.com.tw/_nuxt/4ff1ebf.js:2:153649
at r (https://store.caru.com.tw/_nuxt/4ff1ebf.js:2:148737)
at Tt (https://store.caru.com.tw/_nuxt/4ff1ebf.js:2:148783)
at https://store.caru.com.tw/_nuxt/4ff1ebf.js:2:153550
at r (https://store.caru.com.tw/_nuxt/4ff1ebf.js:2:148737)
at https://store.caru.com.tw/_nuxt/4ff1ebf.js:2:148765
at https://store.caru.com.tw/_nuxt/4ff1ebf.js:2:153257
at https://store.caru.com.tw/_nuxt/4ff1ebf.js:2:150096
at x (https://store.caru.com.tw/_nuxt/4ff1ebf.js:2:152891)
at r (https://store.caru.com.tw/_nuxt/4ff1ebf.js:2:148746)
at Tt (https://store.caru.com.tw/_nuxt/4ff1ebf.js:2:148783)
at e.Vt.confirmTransition (https://store.caru.com.tw/_nuxt/4ff1ebf.js:2:153281)
at e.Vt.transitionTo (https://store.caru.com.tw/_nuxt/4ff1ebf.js:2:151608)
at ee.init (https://store.caru.com.tw/_nuxt/4ff1ebf.js:2:158961)
at Dn.beforeCreate (https://store.caru.com.tw/_nuxt/4ff1ebf.js:2:161169)
at ee (https://store.caru.com.tw/_nuxt/4ff1ebf.js:2:11828)
at vn (https://store.caru.com.tw/_nuxt/4ff1ebf.js:2:26234)
at Dn.t._init (https://store.caru.com.tw/_nuxt/4ff1ebf.js:2:33662)
at new Dn (https://store.caru.com.tw/_nuxt/4ff1ebf.js:2:31251)
at https://store.caru.com.tw/_nuxt/36ec727.js:2:290475
at h (https://store.caru.com.tw/_nuxt/36ec727.js:2:101656)
at Generator._invoke (https://store.caru.com.tw/_nuxt/36ec727.js:2:101444)
at Generator.E.forEach.e.<computed> [as next] (https://store.caru.com.tw/_nuxt/36ec727.js:2:102079)
at r (https://store.caru.com.tw/_nuxt/4ff1ebf.js:2:66614)
```

The stack trace at the sink was:

```
at History.replaceState (<anonymous>:1:582436)
at mt (https://store.caru.com.tw/_nuxt/4ff1ebf.js:2:146887)
at e.setupListeners (https://store.caru.com.tw/_nuxt/4ff1ebf.js:2:154302)
at r (https://store.caru.com.tw/_nuxt/4ff1ebf.js:2:158846)
at https://store.caru.com.tw/_nuxt/4ff1ebf.js:2:151660
at https://store.caru.com.tw/_nuxt/4ff1ebf.js:2:153649
at r (https://store.caru.com.tw/_nuxt/4ff1ebf.js:2:148737)
at Tt (https://store.caru.com.tw/_nuxt/4ff1ebf.js:2:148783)
```

```
at https://store.caru.com.tw/_nuxt/4ff1ebf.js:2:153550
at r (https://store.caru.com.tw/_nuxt/4ff1ebf.js:2:148737)
at https://store.caru.com.tw/_nuxt/4ff1ebf.js:2:148765
at https://store.caru.com.tw/_nuxt/4ff1ebf.js:2:153257
at https://store.caru.com.tw/_nuxt/4ff1ebf.js:2:150096
at x (https://store.caru.com.tw/_nuxt/4ff1ebf.js:2:152891)
at r (https://store.caru.com.tw/_nuxt/4ff1ebf.js:2:148746)
at Tt (https://store.caru.com.tw/_nuxt/4ff1ebf.js:2:148783)
at e.Vt.confirmTransition (https://store.caru.com.tw/_nuxt/4ff1ebf.js:2:153281)
at e.Vt.transitionTo (https://store.caru.com.tw/_nuxt/4ff1ebf.js:2:151608)
at ee.init (https://store.caru.com.tw/_nuxt/4ff1ebf.js:2:158961)
at Dn.beforeCreate (https://store.caru.com.tw/_nuxt/4ff1ebf.js:2:161169)
at ee (https://store.caru.com.tw/_nuxt/4ff1ebf.js:2:11828)
at vn (https://store.caru.com.tw/_nuxt/4ff1ebf.js:2:26234)
at Dn.t._init (https://store.caru.com.tw/_nuxt/4ff1ebf.js:2:33662)
at new Dn (https://store.caru.com.tw/_nuxt/4ff1ebf.js:2:31251)
at https://store.caru.com.tw/_nuxt/36ec727.js:2:290475
at h (https://store.caru.com.tw/_nuxt/36ec727.js:2:101656)
at Generator._invoke (https://store.caru.com.tw/_nuxt/36ec727.js:2:101444)
at Generator.E.forEach.e.<computed> [as next] (https://store.caru.com.tw/_nuxt/36ec727.js:2:102079)
at r (https://store.caru.com.tw/_nuxt/4ff1ebf.js:2:66614)
at l (https://store.caru.com.tw/_nuxt/4ff1ebf.js:2:66817)
```

4.2. https://store.caru.com.tw/

Previous Next

Summary

Severity:	**Information**
Confidence:	**Firm**
Host:	**https://store.caru.com.tw**
Path:	/

Issue detail

The application may be vulnerable to DOM-based DOM data manipulation. Data is read from **location.pathname** and passed to **history.replaceState**.

Request

```
GET / HTTP/1.1
Host: store.caru.com.tw
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
Upgrade-Insecure-Requests: 1
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en-GB;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/95.0.4638.54 Safari/537.36
Connection: close
Cache-Control: max-age=0
```

Response

```
HTTP/1.1 200 OK
Date: Thu, 02 Dec 2021 04:03:41 GMT
Server: Apache/2.4.41 (Ubuntu)
Last-Modified: Tue, 30 Nov 2021 09:01:13 GMT
ETag: "e9e-5d1fdcc9decf2-gzip"
Accept-Ranges: bytes
Vary: Accept-Encoding
Content-Length: 3742
Connection: close
Content-Type: text/html

<!doctype html>
<html lang="en" data-n-head="%7B%22lang%22:%7B%221%22:%22en%22%7D%7D">
<head>
```

```
<title>CarU .....</title><meta data-n-head="1" charset="utf-8"><meta data-n-head="1" name="vi
...[SNIP]...
```

Dynamic analysis

Data is read from **location.pathname** and passed to **history.replaceState**.

The following value was injected into the source:

```
/////o3q9f6jiu1%27%22%60'%22/o3q9f6jiu1/%3E%3Co3q9f6jiu1//%3Egucjn3ff37&
```

The previous value reached the sink as:

```
/o3q9f6jiu1%27%22%60'%22/o3q9f6jiu1/%3E%3Co3q9f6jiu1/%3Egucjn3ff37&?si166mmyuj=si166mmyuj%27%22%60%27%22%2Fsi166mmyuj%2F%3E%3Csi1
```

The stack trace at the source was:

```
at Object._0x16d0e7 [as proxiedGetterCallback] (<anonymous>:1:591983)
at Object.get pathname [as pathname] (<anonymous>:1:299963)
at Wt (https://store.caru.com.tw/_nuxt/4ff1ebf.js:2:155158)
at e.getCurrentLocation (https://store.caru.com.tw/_nuxt/4ff1ebf.js:2:155093)
at ee.init (https://store.caru.com.tw/_nuxt/4ff1ebf.js:2:158976)
at Dn.beforeCreate (https://store.caru.com.tw/_nuxt/4ff1ebf.js:2:161169)
at ee (https://store.caru.com.tw/_nuxt/4ff1ebf.js:2:11828)
at vn (https://store.caru.com.tw/_nuxt/4ff1ebf.js:2:26234)
at Dn.t._init (https://store.caru.com.tw/_nuxt/4ff1ebf.js:2:33662)
at new Dn (https://store.caru.com.tw/_nuxt/4ff1ebf.js:2:31251)
at https://store.caru.com.tw/_nuxt/36ec727.js:2:290475
at h (https://store.caru.com.tw/_nuxt/36ec727.js:2:101656)
at Generator._invoke (https://store.caru.com.tw/_nuxt/36ec727.js:2:101444)
at Generator.E.forEach.e.<computed> [as next] (https://store.caru.com.tw/_nuxt/36ec727.js:2:102079)
at r (https://store.caru.com.tw/_nuxt/4ff1ebf.js:2:66614)
at l (https://store.caru.com.tw/_nuxt/4ff1ebf.js:2:66817)
at https://store.caru.com.tw/_nuxt/4ff1ebf.js:2:66876
at new Promise (<anonymous>)
at https://store.caru.com.tw/_nuxt/4ff1ebf.js:2:66757
at U (https://store.caru.com.tw/_nuxt/36ec727.js:2:291449)
at https://store.caru.com.tw/_nuxt/36ec727.js:2:291525
```

The stack trace at the sink was:

```
at History.replaceState (<anonymous>:1:582436)
at jt (https://store.caru.com.tw/_nuxt/4ff1ebf.js:2:148554)
at Ct (https://store.caru.com.tw/_nuxt/4ff1ebf.js:2:148679)
at e.ensureURL (https://store.caru.com.tw/_nuxt/4ff1ebf.js:2:155036)
at https://store.caru.com.tw/_nuxt/4ff1ebf.js:2:151667
at https://store.caru.com.tw/_nuxt/4ff1ebf.js:2:153649
at r (https://store.caru.com.tw/_nuxt/4ff1ebf.js:2:148737)
at Tt (https://store.caru.com.tw/_nuxt/4ff1ebf.js:2:148783)
at https://store.caru.com.tw/_nuxt/4ff1ebf.js:2:153550
at r (https://store.caru.com.tw/_nuxt/4ff1ebf.js:2:148737)
at https://store.caru.com.tw/_nuxt/4ff1ebf.js:2:148765
at https://store.caru.com.tw/_nuxt/4ff1ebf.js:2:153257
at https://store.caru.com.tw/_nuxt/4ff1ebf.js:2:150096
at x (https://store.caru.com.tw/_nuxt/4ff1ebf.js:2:152891)
at r (https://store.caru.com.tw/_nuxt/4ff1ebf.js:2:148746)
at Tt (https://store.caru.com.tw/_nuxt/4ff1ebf.js:2:148783)
at e.Vt.confirmTransition (https://store.caru.com.tw/_nuxt/4ff1ebf.js:2:153281)
at e.Vt.transitionTo (https://store.caru.com.tw/_nuxt/4ff1ebf.js:2:151608)
at ee.init (https://store.caru.com.tw/_nuxt/4ff1ebf.js:2:158961)
at Dn.beforeCreate (https://store.caru.com.tw/_nuxt/4ff1ebf.js:2:161169)
at ee (https://store.caru.com.tw/_nuxt/4ff1ebf.js:2:11828)
at vn (https://store.caru.com.tw/_nuxt/4ff1ebf.js:2:26234)
at Dn.t._init (https://store.caru.com.tw/_nuxt/4ff1ebf.js:2:33662)
at new Dn (https://store.caru.com.tw/_nuxt/4ff1ebf.js:2:31251)
at https://store.caru.com.tw/_nuxt/36ec727.js:2:290475
at h (https://store.caru.com.tw/_nuxt/36ec727.js:2:101656)
```

```
at Generator._invoke (https://store.caru.com.tw/_nuxt/36ec727.js:2:101444)
at Generator.E.forEach.e.<computed> [as next] (https://store.caru.com.tw/_nuxt/36ec727.js:2:102079)
at r (https://store.caru.com.tw/_nuxt/4ff1ebf.js:2:66614)
at l (https://store.caru.com.tw/_nuxt/4ff1ebf.js:2:66817)
```

4.3. https://store.caru.com.tw/

Previous Next

Summary

Severity:	**Information**
Confidence:	**Firm**
Host:	**https://store.caru.com.tw**
Path:	/

Issue detail

The application may be vulnerable to DOM-based DOM data manipulation. Data is read from **location.search** and passed to **history.replaceState**.

Request

```
GET / HTTP/1.1
Host: store.caru.com.tw
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
Upgrade-Insecure-Requests: 1
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en-GB;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/95.0.4638.54 Safari/537.36
Connection: close
Cache-Control: max-age=0
```

Response

```
HTTP/1.1 200 OK
Date: Thu, 02 Dec 2021 04:03:41 GMT
Server: Apache/2.4.41 (Ubuntu)
Last-Modified: Tue, 30 Nov 2021 09:01:13 GMT
ETag: "e9e-5d1fdcc9decf2-gzip"
Accept-Ranges: bytes
Vary: Accept-Encoding
Content-Length: 3742
Connection: close
Content-Type: text/html

<!doctype html>
<html lang="en" data-n-head="%7B%22lang%22:%7B%221%22:%22en%22%7D%7D">
<head>
<title>CarU .....</title><meta data-n-head="1" charset="utf-8"><meta data-n-head="1" name="vi
...[SNIP]...
```

Dynamic analysis

Data is read from **location.search** and passed to **history.replaceState**.

The following value was injected into the source:

```
?si166mmyuj=si166mmyuj%27%22`'"/si166mmyuj/><si166mmyuj/\>gkt6ov8wa4&
```

The previous value reached the sink as:

```
/o3q9f6jiu1%27%22%60'%22/o3q9f6jiu1/%3E%3Co3q9f6jiu1/%3Egucjn3ff37&?si166mmyuj=si166mmyuj%27%22%60%27%22%2Fsi166mmyuj%2F%3E%3Csi166mm
```

The stack trace at the source was:

```
at Object._0x16d0e7 [as proxiedGetterCallback] (<anonymous>:1:591983)
at Object.get search [as search] (<anonymous>:1:299118)
at Wt (https://store.caru.com.tw/_nuxt/4ff1ebf.js:2:155313)
at e.getCurrentLocation (https://store.caru.com.tw/_nuxt/4ff1ebf.js:2:155093)
at ee.init (https://store.caru.com.tw/_nuxt/4ff1ebf.js:2:158976)
at Dn.beforeCreate (https://store.caru.com.tw/_nuxt/4ff1ebf.js:2:161169)
at ee (https://store.caru.com.tw/_nuxt/4ff1ebf.js:2:11828)
at vn (https://store.caru.com.tw/_nuxt/4ff1ebf.js:2:26234)
at Dn.t._init (https://store.caru.com.tw/_nuxt/4ff1ebf.js:2:33662)
at new Dn (https://store.caru.com.tw/_nuxt/4ff1ebf.js:2:31251)
at https://store.caru.com.tw/_nuxt/36ec727.js:2:290475
at h (https://store.caru.com.tw/_nuxt/36ec727.js:2:101656)
at Generator._invoke (https://store.caru.com.tw/_nuxt/36ec727.js:2:101444)
at Generator.E.forEach.e.<computed> [as next] (https://store.caru.com.tw/_nuxt/36ec727.js:2:102079)
at r (https://store.caru.com.tw/_nuxt/4ff1ebf.js:2:66614)
at l (https://store.caru.com.tw/_nuxt/4ff1ebf.js:2:66817)
at https://store.caru.com.tw/_nuxt/4ff1ebf.js:2:66876
at new Promise (<anonymous>)
at https://store.caru.com.tw/_nuxt/4ff1ebf.js:2:66757
at U (https://store.caru.com.tw/_nuxt/36ec727.js:2:291449)
at https://store.caru.com.tw/_nuxt/36ec727.js:2:291525
```

The stack trace at the sink was:

```
at History.replaceState (<anonymous>:1:582436)
at jt (https://store.caru.com.tw/_nuxt/4ff1ebf.js:2:148554)
at Ct (https://store.caru.com.tw/_nuxt/4ff1ebf.js:2:148679)
at e.ensureURL (https://store.caru.com.tw/_nuxt/4ff1ebf.js:2:155036)
at https://store.caru.com.tw/_nuxt/4ff1ebf.js:2:151667
at https://store.caru.com.tw/_nuxt/4ff1ebf.js:2:153649
at r (https://store.caru.com.tw/_nuxt/4ff1ebf.js:2:148737)
at Tt (https://store.caru.com.tw/_nuxt/4ff1ebf.js:2:148783)
at https://store.caru.com.tw/_nuxt/4ff1ebf.js:2:153550
at r (https://store.caru.com.tw/_nuxt/4ff1ebf.js:2:148737)
at https://store.caru.com.tw/_nuxt/4ff1ebf.js:2:148765
at https://store.caru.com.tw/_nuxt/4ff1ebf.js:2:153257
at https://store.caru.com.tw/_nuxt/4ff1ebf.js:2:150096
at x (https://store.caru.com.tw/_nuxt/4ff1ebf.js:2:152891)
at r (https://store.caru.com.tw/_nuxt/4ff1ebf.js:2:148746)
at Tt (https://store.caru.com.tw/_nuxt/4ff1ebf.js:2:148783)
at e.Vt.confirmTransition (https://store.caru.com.tw/_nuxt/4ff1ebf.js:2:153281)
at e.Vt.transitionTo (https://store.caru.com.tw/_nuxt/4ff1ebf.js:2:151608)
at ee.init (https://store.caru.com.tw/_nuxt/4ff1ebf.js:2:158961)
at Dn.beforeCreate (https://store.caru.com.tw/_nuxt/4ff1ebf.js:2:161169)
at ee (https://store.caru.com.tw/_nuxt/4ff1ebf.js:2:11828)
at vn (https://store.caru.com.tw/_nuxt/4ff1ebf.js:2:26234)
at Dn.t._init (https://store.caru.com.tw/_nuxt/4ff1ebf.js:2:33662)
at new Dn (https://store.caru.com.tw/_nuxt/4ff1ebf.js:2:31251)
at https://store.caru.com.tw/_nuxt/36ec727.js:2:290475
at h (https://store.caru.com.tw/_nuxt/36ec727.js:2:101656)
at Generator._invoke (https://store.caru.com.tw/_nuxt/36ec727.js:2:101444)
at Generator.E.forEach.e.<computed> [as next] (https://store.caru.com.tw/_nuxt/36ec727.js:2:102079)
at r (https://store.caru.com.tw/_nuxt/4ff1ebf.js:2:66614)
at l (https://store.caru.com.tw/_nuxt/4ff1ebf.js:2:66817)
```

4.4. https://store.caru.com.tw/

Previous Next

Summary

Severity:	Information
Confidence:	Firm
Host:	https://store.caru.com.tw
Path:	/

Issue detail

The application may be vulnerable to DOM-based DOM data manipulation. Data is read from **location.hash** and passed to **history.replaceState**.

Request

```
GET / HTTP/1.1
Host: store.caru.com.tw
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
Upgrade-Insecure-Requests: 1
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en-GB;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/95.0.4638.54 Safari/537.36
Connection: close
Cache-Control: max-age=0
```

Response

```
HTTP/1.1 200 OK
Date: Thu, 02 Dec 2021 04:03:41 GMT
Server: Apache/2.4.41 (Ubuntu)
Last-Modified: Tue, 30 Nov 2021 09:01:13 GMT
ETag: "e9e-5d1fdcc9decf2-gzip"
Accept-Ranges: bytes
Vary: Accept-Encoding
Content-Length: 3742
Connection: close
Content-Type: text/html

<!doctype html>
<html lang="en" data-n-head="%7B%22lang%22:%7B%221%22:%22en%22%7D%7D">
<head>
<title>CarU .....</title><meta data-n-head="1" charset="utf-8"><meta data-n-head="1" name="vi
...[SNIP]...
```

Dynamic analysis

Data is read from **location.hash** and passed to **history.replaceState**.

The following value was injected into the source:

```
#dkaz5xoe6p=dkaz5xoe6p%27%22`'"/dkaz5xoe6p/><dkaz5xoe6p/\>y4ms0wv6dx&
```

The previous value reached the sink as:

```
/o3q9f6jiu1%27%22%60'%22/o3q9f6jiu1/%3E%3Co3q9f6jiu1/%3Egucjn3ff37&?si166mmyuj=si166mmyuj%27%22%60%27%22%2Fsi166mmyuj%2F%3E%3Csi166mm
```

The stack trace at the source was:

```
at Object._0x16d0e7 [as proxiedGetterCallback] (<anonymous>:1:591983)
at Object.get hash [as hash] (<anonymous>:1:299763)
at Wt (https://store.caru.com.tw/_nuxt/4ff1ebf.js:2:155336)
at e.getCurrentLocation (https://store.caru.com.tw/_nuxt/4ff1ebf.js:2:155093)
at ee.init (https://store.caru.com.tw/_nuxt/4ff1ebf.js:2:158976)
at Dn.beforeCreate (https://store.caru.com.tw/_nuxt/4ff1ebf.js:2:161169)
at ee (https://store.caru.com.tw/_nuxt/4ff1ebf.js:2:11828)
at vn (https://store.caru.com.tw/_nuxt/4ff1ebf.js:2:26234)
at Dn.t._init (https://store.caru.com.tw/_nuxt/4ff1ebf.js:2:33662)
at new Dn (https://store.caru.com.tw/_nuxt/4ff1ebf.js:2:31251)
at https://store.caru.com.tw/_nuxt/36ec727.js:2:290475
at h (https://store.caru.com.tw/_nuxt/36ec727.js:2:101656)
at Generator._invoke (https://store.caru.com.tw/_nuxt/36ec727.js:2:101444)
at Generator.E.forEach.e.<computed> [as next] (https://store.caru.com.tw/_nuxt/36ec727.js:2:102079)
at r (https://store.caru.com.tw/_nuxt/4ff1ebf.js:2:66614)
at l (https://store.caru.com.tw/_nuxt/4ff1ebf.js:2:66817)
at https://store.caru.com.tw/_nuxt/4ff1ebf.js:2:66876
at new Promise (<anonymous>)
at https://store.caru.com.tw/_nuxt/4ff1ebf.js:2:66757
at U (https://store.caru.com.tw/_nuxt/36ec727.js:2:291449)
```

```
at https://store.caru.com.tw/_nuxt/36ec727.js:2:291525
```

The stack trace at the sink was:

```
at History.replaceState (<anonymous>:1:582436)
at jt (https://store.caru.com.tw/_nuxt/4ff1ebf.js:2:148554)
at Ct (https://store.caru.com.tw/_nuxt/4ff1ebf.js:2:148679)
at e.ensureURL (https://store.caru.com.tw/_nuxt/4ff1ebf.js:2:155036)
at https://store.caru.com.tw/_nuxt/4ff1ebf.js:2:151667
at https://store.caru.com.tw/_nuxt/4ff1ebf.js:2:153649
at r (https://store.caru.com.tw/_nuxt/4ff1ebf.js:2:148737)
at Tt (https://store.caru.com.tw/_nuxt/4ff1ebf.js:2:148783)
at https://store.caru.com.tw/_nuxt/4ff1ebf.js:2:153550
at r (https://store.caru.com.tw/_nuxt/4ff1ebf.js:2:148737)
at https://store.caru.com.tw/_nuxt/4ff1ebf.js:2:148765
at https://store.caru.com.tw/_nuxt/4ff1ebf.js:2:153257
at https://store.caru.com.tw/_nuxt/4ff1ebf.js:2:150096
at x (https://store.caru.com.tw/_nuxt/4ff1ebf.js:2:152891)
at r (https://store.caru.com.tw/_nuxt/4ff1ebf.js:2:148746)
at Tt (https://store.caru.com.tw/_nuxt/4ff1ebf.js:2:148783)
at e.Vt.confirmTransition (https://store.caru.com.tw/_nuxt/4ff1ebf.js:2:153281)
at e.Vt.transitionTo (https://store.caru.com.tw/_nuxt/4ff1ebf.js:2:151608)
at ee.init (https://store.caru.com.tw/_nuxt/4ff1ebf.js:2:158961)
at Dn.beforeCreate (https://store.caru.com.tw/_nuxt/4ff1ebf.js:2:161169)
at ee (https://store.caru.com.tw/_nuxt/4ff1ebf.js:2:11828)
at vn (https://store.caru.com.tw/_nuxt/4ff1ebf.js:2:26234)
at Dn.t._init (https://store.caru.com.tw/_nuxt/4ff1ebf.js:2:33662)
at new Dn (https://store.caru.com.tw/_nuxt/4ff1ebf.js:2:31251)
at https://store.caru.com.tw/_nuxt/36ec727.js:2:290475
at h (https://store.caru.com.tw/_nuxt/36ec727.js:2:101656)
at Generator._invoke (https://store.caru.com.tw/_nuxt/36ec727.js:2:101444)
at Generator.E.forEach.e.<computed> [as next] (https://store.caru.com.tw/_nuxt/36ec727.js:2:102079)
at r (https://store.caru.com.tw/_nuxt/4ff1ebf.js:2:66614)
at l (https://store.caru.com.tw/_nuxt/4ff1ebf.js:2:66817)
```

4.5. https://store.caru.com.tw/login/

Previous Next

Summary

Severity:	**Information**
Confidence:	**Firm**
Host:	**https://store.caru.com.tw**
Path:	**/login/**

Issue detail

The application may be vulnerable to DOM-based DOM data manipulation. Data is read from **location.href** and passed to **history.replaceState**.

Request

```
GET /login/? HTTP/1.1
Host: store.caru.com.tw
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
Upgrade-Insecure-Requests: 1
Referer: https://store.caru.com.tw/login/
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en-GB;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/95.0.4638.54 Safari/537.36
Connection: close
Cache-Control: max-age=0
```

Response

```
HTTP/1.1 200 OK
Date: Thu, 02 Dec 2021 04:13:23 GMT
Server: Apache/2.4.41 (Ubuntu)
Last-Modified: Tue, 30 Nov 2021 09:01:12 GMT
ETag: "e9e-5d1fdcc8d52f5-gzip"
Accept-Ranges: bytes
Vary: Accept-Encoding
Content-Length: 3742
Connection: close
Content-Type: text/html

<!doctype html>
<html lang="en" data-n-head="%7B%22lang%22:%7B%221%22:%22en%22%7D%7D">
<head>
<title>CarU .....</title><meta data-n-head="1" charset="utf-8"><meta data-n-head="1" name="vi
...[SNIP]...
```

Dynamic analysis

Data is read from **location.href** and passed to **history.replaceState**.

The following value was injected into the source and reached the sink without any modification:

```
?qly6qnqeah=qly6qnqeah%27%22`'"/qly6qnqeah/><qly6qnqeah/\>epdpbqr5lq&
```

The stack trace at the source was:

```
at Object._0x16d0e7 [as proxiedGetterCallback] (<anonymous>:1:591983)
at Object.get href [as href] (<anonymous>:1:299867)
at mt (https://store.caru.com.tw/_nuxt/4ff1ebf.js:2:146806)
at e.setupListeners (https://store.caru.com.tw/_nuxt/4ff1ebf.js:2:154302)
at r (https://store.caru.com.tw/_nuxt/4ff1ebf.js:2:158846)
at https://store.caru.com.tw/_nuxt/4ff1ebf.js:2:151660
at https://store.caru.com.tw/_nuxt/4ff1ebf.js:2:153649
at r (https://store.caru.com.tw/_nuxt/4ff1ebf.js:2:148737)
at Tt (https://store.caru.com.tw/_nuxt/4ff1ebf.js:2:148783)
at https://store.caru.com.tw/_nuxt/4ff1ebf.js:2:153550
at r (https://store.caru.com.tw/_nuxt/4ff1ebf.js:2:148737)
at https://store.caru.com.tw/_nuxt/4ff1ebf.js:2:148765
at https://store.caru.com.tw/_nuxt/4ff1ebf.js:2:153257
at https://store.caru.com.tw/_nuxt/4ff1ebf.js:2:150096
at x (https://store.caru.com.tw/_nuxt/4ff1ebf.js:2:152891)
at r (https://store.caru.com.tw/_nuxt/4ff1ebf.js:2:148746)
at Tt (https://store.caru.com.tw/_nuxt/4ff1ebf.js:2:148783)
at e.Vt.confirmTransition (https://store.caru.com.tw/_nuxt/4ff1ebf.js:2:153281)
at e.Vt.transitionTo (https://store.caru.com.tw/_nuxt/4ff1ebf.js:2:151608)
at ee.init (https://store.caru.com.tw/_nuxt/4ff1ebf.js:2:158961)
at Dn.beforeCreate (https://store.caru.com.tw/_nuxt/4ff1ebf.js:2:161169)
at ee (https://store.caru.com.tw/_nuxt/4ff1ebf.js:2:11828)
at vn (https://store.caru.com.tw/_nuxt/4ff1ebf.js:2:26234)
at Dn.t._init (https://store.caru.com.tw/_nuxt/4ff1ebf.js:2:33662)
at new Dn (https://store.caru.com.tw/_nuxt/4ff1ebf.js:2:31251)
at https://store.caru.com.tw/_nuxt/36ec727.js:2:290475
at h (https://store.caru.com.tw/_nuxt/36ec727.js:2:101656)
at Generator._invoke (https://store.caru.com.tw/_nuxt/36ec727.js:2:101444)
at Generator.E.forEach.e.<computed> [as next] (https://store.caru.com.tw/_nuxt/36ec727.js:2:102079)
at r (https://store.caru.com.tw/_nuxt/4ff1ebf.js:2:66614)
```

The stack trace at the sink was:

```
at History.replaceState (<anonymous>:1:582436)
at mt (https://store.caru.com.tw/_nuxt/4ff1ebf.js:2:146887)
at e.setupListeners (https://store.caru.com.tw/_nuxt/4ff1ebf.js:2:154302)
at r (https://store.caru.com.tw/_nuxt/4ff1ebf.js:2:158846)
at https://store.caru.com.tw/_nuxt/4ff1ebf.js:2:151660
at https://store.caru.com.tw/_nuxt/4ff1ebf.js:2:153649
at r (https://store.caru.com.tw/_nuxt/4ff1ebf.js:2:148737)
at Tt (https://store.caru.com.tw/_nuxt/4ff1ebf.js:2:148783)
at https://store.caru.com.tw/_nuxt/4ff1ebf.js:2:153550
at r (https://store.caru.com.tw/_nuxt/4ff1ebf.js:2:148737)
```

```
at https://store.caru.com.tw/_nuxt/4ff1ebf.js:2:153257
at https://store.caru.com.tw/_nuxt/4ff1ebf.js:2:150096
at x (https://store.caru.com.tw/_nuxt/4ff1ebf.js:2:152891)
at r (https://store.caru.com.tw/_nuxt/4ff1ebf.js:2:148746)
at Tt (https://store.caru.com.tw/_nuxt/4ff1ebf.js:2:148783)
at e.Vt.confirmTransition (https://store.caru.com.tw/_nuxt/4ff1ebf.js:2:153281)
at e.Vt.transitionTo (https://store.caru.com.tw/_nuxt/4ff1ebf.js:2:151608)
at ee.init (https://store.caru.com.tw/_nuxt/4ff1ebf.js:2:158961)
at Dn.beforeCreate (https://store.caru.com.tw/_nuxt/4ff1ebf.js:2:161169)
at ee (https://store.caru.com.tw/_nuxt/4ff1ebf.js:2:11828)
at vn (https://store.caru.com.tw/_nuxt/4ff1ebf.js:2:26234)
at Dn.t._init (https://store.caru.com.tw/_nuxt/4ff1ebf.js:2:33662)
at new Dn (https://store.caru.com.tw/_nuxt/4ff1ebf.js:2:31251)
at https://store.caru.com.tw/_nuxt/36ec727.js:2:290475
at h (https://store.caru.com.tw/_nuxt/36ec727.js:2:101656)
at Generator._invoke (https://store.caru.com.tw/_nuxt/36ec727.js:2:101444)
at Generator.E.forEach.e.<computed> [as next] (https://store.caru.com.tw/_nuxt/36ec727.js:2:102079)
at r (https://store.caru.com.tw/_nuxt/4ff1ebf.js:2:66614)
at l (https://store.caru.com.tw/_nuxt/4ff1ebf.js:2:66817)
```

4.6. https://store.caru.com.tw/login/

Previous Next

Summary

Severity:	**Information**
Confidence:	**Firm**
Host:	**https://store.caru.com.tw**
Path:	**/login/**

Issue detail

The application may be vulnerable to DOM-based DOM data manipulation. Data is read from **location.pathname** and passed to **history.replaceState**.

Request

```
GET /login/? HTTP/1.1
Host: store.caru.com.tw
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
Upgrade-Insecure-Requests: 1
Referer: https://store.caru.com.tw/login/
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en-GB;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/95.0.4638.54 Safari/537.36
Connection: close
Cache-Control: max-age=0
```

Response

```
HTTP/1.1 200 OK
Date: Thu, 02 Dec 2021 04:13:23 GMT
Server: Apache/2.4.41 (Ubuntu)
Last-Modified: Tue, 30 Nov 2021 09:01:12 GMT
ETag: "e9e-5d1fdcc8d52f5-gzip"
Accept-Ranges: bytes
Vary: Accept-Encoding
Content-Length: 3742
Connection: close
Content-Type: text/html

<!doctype html>
<html lang="en" data-n-head="%7B%22lang%22:%7B%221%22:%22en%22%7D%7D">
<head>
<title>CarU .....</title><meta data-n-head="1" charset="utf-8"><meta data-n-head="1" name="vi
...[SNIP]...
```

Dynamic analysis

Data is read from **location.pathname** and passed to **history.replaceState**.

The following value was injected into the source:

```
///login///xs7b0ayt0g%27%22%60'%22/xs7b0ayt0g/%3E%3Cxs7b0ayt0g//%3Ecrxztrbm5t&
```

The previous value reached the sink as:

```
/login/xs7b0ayt0g%27%22%60'%22/xs7b0ayt0g/%3E%3Cxs7b0ayt0g/%3Ecrxztrbm5t&?u86nyz2htg=u86nyz2htg%27%22%60%27%22%2Fu86nyz2htg%2F%3E%3C
```

The stack trace at the source was:

```
at Object._0x16d0e7 [as proxiedGetterCallback] (<anonymous>:1:591983)
at Object.get pathname [as pathname] (<anonymous>:1:299963)
at Wt (https://store.caru.com.tw/_nuxt/4ff1ebf.js:2:155158)
at e.getCurrentLocation (https://store.caru.com.tw/_nuxt/4ff1ebf.js:2:155093)
at ee.init (https://store.caru.com.tw/_nuxt/4ff1ebf.js:2:158976)
at Dn.beforeCreate (https://store.caru.com.tw/_nuxt/4ff1ebf.js:2:161169)
at ee (https://store.caru.com.tw/_nuxt/4ff1ebf.js:2:11828)
at vn (https://store.caru.com.tw/_nuxt/4ff1ebf.js:2:26234)
at Dn.t._init (https://store.caru.com.tw/_nuxt/4ff1ebf.js:2:33662)
at new Dn (https://store.caru.com.tw/_nuxt/4ff1ebf.js:2:31251)
at https://store.caru.com.tw/_nuxt/36ec727.js:2:290475
at h (https://store.caru.com.tw/_nuxt/36ec727.js:2:101656)
at Generator._invoke (https://store.caru.com.tw/_nuxt/36ec727.js:2:101444)
at Generator.E.forEach.e.<computed> [as next] (https://store.caru.com.tw/_nuxt/36ec727.js:2:102079)
at r (https://store.caru.com.tw/_nuxt/4ff1ebf.js:2:66614)
at l (https://store.caru.com.tw/_nuxt/4ff1ebf.js:2:66817)
at https://store.caru.com.tw/_nuxt/4ff1ebf.js:2:66876
at new Promise (<anonymous>)
at https://store.caru.com.tw/_nuxt/4ff1ebf.js:2:66757
at U (https://store.caru.com.tw/_nuxt/36ec727.js:2:291449)
at https://store.caru.com.tw/_nuxt/36ec727.js:2:291525
```

The stack trace at the sink was:

```
at History.replaceState (<anonymous>:1:582436)
at jt (https://store.caru.com.tw/_nuxt/4ff1ebf.js:2:148554)
at Ct (https://store.caru.com.tw/_nuxt/4ff1ebf.js:2:148679)
at e.ensureURL (https://store.caru.com.tw/_nuxt/4ff1ebf.js:2:155036)
at https://store.caru.com.tw/_nuxt/4ff1ebf.js:2:151667
at https://store.caru.com.tw/_nuxt/4ff1ebf.js:2:153649
at r (https://store.caru.com.tw/_nuxt/4ff1ebf.js:2:148737)
at Tt (https://store.caru.com.tw/_nuxt/4ff1ebf.js:2:148783)
at https://store.caru.com.tw/_nuxt/4ff1ebf.js:2:153550
at r (https://store.caru.com.tw/_nuxt/4ff1ebf.js:2:148737)
at https://store.caru.com.tw/_nuxt/4ff1ebf.js:2:148765
at https://store.caru.com.tw/_nuxt/4ff1ebf.js:2:153257
at https://store.caru.com.tw/_nuxt/4ff1ebf.js:2:150096
at x (https://store.caru.com.tw/_nuxt/4ff1ebf.js:2:152891)
at r (https://store.caru.com.tw/_nuxt/4ff1ebf.js:2:148746)
at Tt (https://store.caru.com.tw/_nuxt/4ff1ebf.js:2:148783)
at e.Vt.confirmTransition (https://store.caru.com.tw/_nuxt/4ff1ebf.js:2:153281)
at e.Vt.transitionTo (https://store.caru.com.tw/_nuxt/4ff1ebf.js:2:151608)
at ee.init (https://store.caru.com.tw/_nuxt/4ff1ebf.js:2:158961)
at Dn.beforeCreate (https://store.caru.com.tw/_nuxt/4ff1ebf.js:2:161169)
at ee (https://store.caru.com.tw/_nuxt/4ff1ebf.js:2:11828)
at vn (https://store.caru.com.tw/_nuxt/4ff1ebf.js:2:26234)
at Dn.t._init (https://store.caru.com.tw/_nuxt/4ff1ebf.js:2:33662)
at new Dn (https://store.caru.com.tw/_nuxt/4ff1ebf.js:2:31251)
at https://store.caru.com.tw/_nuxt/36ec727.js:2:290475
at h (https://store.caru.com.tw/_nuxt/36ec727.js:2:101656)
at Generator._invoke (https://store.caru.com.tw/_nuxt/36ec727.js:2:101444)
at Generator.E.forEach.e.<computed> [as next] (https://store.caru.com.tw/_nuxt/36ec727.js:2:102079)
at r (https://store.caru.com.tw/_nuxt/4ff1ebf.js:2:66614)
```

```
at e.Vt.confirmTransition (https://store.caru.com.tw/_nuxt/4ff1ebf.js:2:153281)
at e.Vt.transitionTo (https://store.caru.com.tw/_nuxt/4ff1ebf.js:2:151608)
at ee.init (https://store.caru.com.tw/_nuxt/4ff1ebf.js:2:158961)
at Dn.beforeCreate (https://store.caru.com.tw/_nuxt/4ff1ebf.js:2:161169)
at ee (https://store.caru.com.tw/_nuxt/4ff1ebf.js:2:11828)
at vn (https://store.caru.com.tw/_nuxt/4ff1ebf.js:2:26234)
at Dn.t._init (https://store.caru.com.tw/_nuxt/4ff1ebf.js:2:33662)
at new Dn (https://store.caru.com.tw/_nuxt/4ff1ebf.js:2:31251)
at https://store.caru.com.tw/_nuxt/36ec727.js:2:290475
at h (https://store.caru.com.tw/_nuxt/36ec727.js:2:101656)
at Generator._invoke (https://store.caru.com.tw/_nuxt/36ec727.js:2:101444)
at Generator.E.forEach.e.<computed> [as next] (https://store.caru.com.tw/_nuxt/36ec727.js:2:102079)
at r (https://store.caru.com.tw/_nuxt/4ff1ebf.js:2:66614)
at l (https://store.caru.com.tw/_nuxt/4ff1ebf.js:2:66817)
```

4.7. https://store.caru.com.tw/login/

Previous Next

Summary

Severity:	**Information**
Confidence:	**Firm**
Host:	**https://store.caru.com.tw**
Path:	**/login/**

Issue detail

The application may be vulnerable to DOM-based DOM data manipulation. Data is read from **location.search** and passed to **history.replaceState**.

Request

```
GET /login/? HTTP/1.1
Host: store.caru.com.tw
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
Upgrade-Insecure-Requests: 1
Referer: https://store.caru.com.tw/login/
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en-GB;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/95.0.4638.54 Safari/537.36
Connection: close
Cache-Control: max-age=0
```

Response

```
HTTP/1.1 200 OK
Date: Thu, 02 Dec 2021 04:13:23 GMT
Server: Apache/2.4.41 (Ubuntu)
Last-Modified: Tue, 30 Nov 2021 09:01:12 GMT
ETag: "e9e-5d1fdcc8d52f5-gzip"
Accept-Ranges: bytes
Vary: Accept-Encoding
Content-Length: 3742
Connection: close
Content-Type: text/html

<!doctype html>
<html lang="en" data-n-head="%7B%22lang%22:%7B%221%22:%22en%22%7D%7D">
<head>
<title>CarU .....</title><meta data-n-head="1" charset="utf-8"><meta data-n-head="1" name="vi
...[SNIP]...
```

Dynamic analysis

Data is read from **location.search** and passed to **history.replaceState**.

The following value was injected into the source:

```
?u86nyz2htg=u86nyz2htg%27%22`'"/u86nyz2htg/><u86nyz2htg/\>hnb0piekwe&
```

The previous value reached the sink as:

```
/login/xs7b0ayt0g%27%22%60'%22/xs7b0ayt0g/%3E%3Cxs7b0ayt0g/%3Ecrxztrbm5t&?u86nyz2htg=u86nyz2htg%27%22%60%27%22%2Fu86nyz2htg%2F%3E
```

The stack trace at the source was:

```
at Object._0x16d0e7 [as proxiedGetterCallback] (<anonymous>:1:591983)
at Object.get search [as search] (<anonymous>:1:299118)
at Wt (https://store.caru.com.tw/_nuxt/4ff1ebf.js:2:155313)
at e.getCurrentLocation (https://store.caru.com.tw/_nuxt/4ff1ebf.js:2:155093)
at ee.init (https://store.caru.com.tw/_nuxt/4ff1ebf.js:2:158976)
at Dn.beforeCreate (https://store.caru.com.tw/_nuxt/4ff1ebf.js:2:161169)
at ee (https://store.caru.com.tw/_nuxt/4ff1ebf.js:2:11828)
at vn (https://store.caru.com.tw/_nuxt/4ff1ebf.js:2:26234)
at Dn.t._init (https://store.caru.com.tw/_nuxt/4ff1ebf.js:2:33662)
at new Dn (https://store.caru.com.tw/_nuxt/4ff1ebf.js:2:31251)
at https://store.caru.com.tw/_nuxt/36ec727.js:2:290475
at h (https://store.caru.com.tw/_nuxt/36ec727.js:2:101656)
at Generator._invoke (https://store.caru.com.tw/_nuxt/36ec727.js:2:101444)
at Generator.E.forEach.e.<computed> [as next] (https://store.caru.com.tw/_nuxt/36ec727.js:2:102079)
at r (https://store.caru.com.tw/_nuxt/4ff1ebf.js:2:66614)
at l (https://store.caru.com.tw/_nuxt/4ff1ebf.js:2:66817)
at https://store.caru.com.tw/_nuxt/4ff1ebf.js:2:66876
at new Promise (<anonymous>)
at https://store.caru.com.tw/_nuxt/4ff1ebf.js:2:66757
at U (https://store.caru.com.tw/_nuxt/36ec727.js:2:291449)
at https://store.caru.com.tw/_nuxt/36ec727.js:2:291525
```

The stack trace at the sink was:

```
at History.replaceState (<anonymous>:1:582436)
at jt (https://store.caru.com.tw/_nuxt/4ff1ebf.js:2:148554)
at Ct (https://store.caru.com.tw/_nuxt/4ff1ebf.js:2:148679)
at e.ensureURL (https://store.caru.com.tw/_nuxt/4ff1ebf.js:2:155036)
at https://store.caru.com.tw/_nuxt/4ff1ebf.js:2:151667
at https://store.caru.com.tw/_nuxt/4ff1ebf.js:2:153649
at r (https://store.caru.com.tw/_nuxt/4ff1ebf.js:2:148737)
at Tt (https://store.caru.com.tw/_nuxt/4ff1ebf.js:2:148783)
at https://store.caru.com.tw/_nuxt/4ff1ebf.js:2:153550
at r (https://store.caru.com.tw/_nuxt/4ff1ebf.js:2:148737)
at https://store.caru.com.tw/_nuxt/4ff1ebf.js:2:148765
at https://store.caru.com.tw/_nuxt/4ff1ebf.js:2:153257
at https://store.caru.com.tw/_nuxt/4ff1ebf.js:2:150096
at x (https://store.caru.com.tw/_nuxt/4ff1ebf.js:2:152891)
at r (https://store.caru.com.tw/_nuxt/4ff1ebf.js:2:148746)
at Tt (https://store.caru.com.tw/_nuxt/4ff1ebf.js:2:148783)
at e.Vt.confirmTransition (https://store.caru.com.tw/_nuxt/4ff1ebf.js:2:153281)
at e.Vt.transitionTo (https://store.caru.com.tw/_nuxt/4ff1ebf.js:2:151608)
at ee.init (https://store.caru.com.tw/_nuxt/4ff1ebf.js:2:158961)
at Dn.beforeCreate (https://store.caru.com.tw/_nuxt/4ff1ebf.js:2:161169)
at ee (https://store.caru.com.tw/_nuxt/4ff1ebf.js:2:11828)
at vn (https://store.caru.com.tw/_nuxt/4ff1ebf.js:2:26234)
at Dn.t._init (https://store.caru.com.tw/_nuxt/4ff1ebf.js:2:33662)
at new Dn (https://store.caru.com.tw/_nuxt/4ff1ebf.js:2:31251)
at https://store.caru.com.tw/_nuxt/36ec727.js:2:290475
at h (https://store.caru.com.tw/_nuxt/36ec727.js:2:101656)
at Generator._invoke (https://store.caru.com.tw/_nuxt/36ec727.js:2:101444)
at Generator.E.forEach.e.<computed> [as next] (https://store.caru.com.tw/_nuxt/36ec727.js:2:102079)
at r (https://store.caru.com.tw/_nuxt/4ff1ebf.js:2:66614)
at l (https://store.caru.com.tw/_nuxt/4ff1ebf.js:2:66817)
```

4.8. https://store.caru.com.tw/login/

Previous Next

Summary

Severity:	**Information**
Confidence:	**Firm**
Host:	**https://store.caru.com.tw**
Path:	**/login/**

Issue detail

The application may be vulnerable to DOM-based DOM data manipulation. Data is read from **location.hash** and passed to **history.replaceState**.

Request

```
GET /login/? HTTP/1.1
Host: store.caru.com.tw
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
Upgrade-Insecure-Requests: 1
Referer: https://store.caru.com.tw/login/
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en-GB;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/95.0.4638.54 Safari/537.36
Connection: close
Cache-Control: max-age=0
```

Response

```
HTTP/1.1 200 OK
Date: Thu, 02 Dec 2021 04:13:23 GMT
Server: Apache/2.4.41 (Ubuntu)
Last-Modified: Tue, 30 Nov 2021 09:01:12 GMT
ETag: "e9e-5d1fdcc8d52f5-gzip"
Accept-Ranges: bytes
Vary: Accept-Encoding
Content-Length: 3742
Connection: close
Content-Type: text/html

<!doctype html>
<html lang="en" data-n-head="%7B%22lang%22:%7B%221%22:%22en%22%7D%7D">
<head>
<title>CarU .....</title><meta data-n-head="1" charset="utf-8"><meta data-n-head="1" name="vi
...[SNIP]...
```

Dynamic analysis

Data is read from **location.hash** and passed to **history.replaceState**.

The following value was injected into the source:

```
#cm1f2jqwqp=cm1f2jqwqp%27%22`'"/cm1f2jqwqp/><cm1f2jqwqp/\>tql13ikjwh&
```

The previous value reached the sink as:

```
/login/xs7b0ayt0g%27%22%60'%22/xs7b0ayt0g/%3E%3Cxs7b0ayt0g/%3Ecrxztrbm5t&?u86nyz2htg=u86nyz2htg%27%22%60%27%22%2Fu86nyz2htg%2F%3E%3C
```

The stack trace at the source was:

```
at Object._0x16d0e7 [as proxiedGetterCallback] (<anonymous>:1:591983)
at Object.get hash [as hash] (<anonymous>:1:299763)
at Wt (https://store.caru.com.tw/_nuxt/4ff1ebf.js:2:155336)
at e.getCurrentLocation (https://store.caru.com.tw/_nuxt/4ff1ebf.js:2:155093)
at ee.init (https://store.caru.com.tw/_nuxt/4ff1ebf.js:2:158976)
at Dn.beforeCreate (https://store.caru.com.tw/_nuxt/4ff1ebf.js:2:161169)
at ee (https://store.caru.com.tw/_nuxt/4ff1ebf.js:2:11828)
at vn (https://store.caru.com.tw/_nuxt/4ff1ebf.js:2:26234)
```

```
at Dn.t._init (https://store.caru.com.tw/_nuxt/4ff1ebf.js:2:33662)
at new Dn (https://store.caru.com.tw/_nuxt/4ff1ebf.js:2:31251)
at https://store.caru.com.tw/_nuxt/36ec727.js:2:290475
at h (https://store.caru.com.tw/_nuxt/36ec727.js:2:101656)
at Generator._invoke (https://store.caru.com.tw/_nuxt/36ec727.js:2:101444)
at Generator.E.forEach.e.<computed> [as next] (https://store.caru.com.tw/_nuxt/36ec727.js:2:102079)
at r (https://store.caru.com.tw/_nuxt/4ff1ebf.js:2:66614)
at l (https://store.caru.com.tw/_nuxt/4ff1ebf.js:2:66817)
at https://store.caru.com.tw/_nuxt/4ff1ebf.js:2:66876
at new Promise (<anonymous>)
at https://store.caru.com.tw/_nuxt/4ff1ebf.js:2:66757
at U (https://store.caru.com.tw/_nuxt/36ec727.js:2:291449)
at https://store.caru.com.tw/_nuxt/36ec727.js:2:291525
```

The stack trace at the sink was:

```
at History.replaceState (<anonymous>:1:582436)
at jt (https://store.caru.com.tw/_nuxt/4ff1ebf.js:2:148554)
at Ct (https://store.caru.com.tw/_nuxt/4ff1ebf.js:2:148679)
at e.ensureURL (https://store.caru.com.tw/_nuxt/4ff1ebf.js:2:155036)
at https://store.caru.com.tw/_nuxt/4ff1ebf.js:2:151667
at https://store.caru.com.tw/_nuxt/4ff1ebf.js:2:153649
at r (https://store.caru.com.tw/_nuxt/4ff1ebf.js:2:148737)
at Tt (https://store.caru.com.tw/_nuxt/4ff1ebf.js:2:148783)
at https://store.caru.com.tw/_nuxt/4ff1ebf.js:2:153550
at r (https://store.caru.com.tw/_nuxt/4ff1ebf.js:2:148737)
at https://store.caru.com.tw/_nuxt/4ff1ebf.js:2:148765
at https://store.caru.com.tw/_nuxt/4ff1ebf.js:2:153257
at https://store.caru.com.tw/_nuxt/4ff1ebf.js:2:150096
at x (https://store.caru.com.tw/_nuxt/4ff1ebf.js:2:152891)
at r (https://store.caru.com.tw/_nuxt/4ff1ebf.js:2:148746)
at Tt (https://store.caru.com.tw/_nuxt/4ff1ebf.js:2:148783)
at e.Vt.confirmTransition (https://store.caru.com.tw/_nuxt/4ff1ebf.js:2:153281)
at e.Vt.transitionTo (https://store.caru.com.tw/_nuxt/4ff1ebf.js:2:151608)
at ee.init (https://store.caru.com.tw/_nuxt/4ff1ebf.js:2:158961)
at Dn.beforeCreate (https://store.caru.com.tw/_nuxt/4ff1ebf.js:2:161169)
at ee (https://store.caru.com.tw/_nuxt/4ff1ebf.js:2:11828)
at vn (https://store.caru.com.tw/_nuxt/4ff1ebf.js:2:26234)
at Dn.t._init (https://store.caru.com.tw/_nuxt/4ff1ebf.js:2:33662)
at new Dn (https://store.caru.com.tw/_nuxt/4ff1ebf.js:2:31251)
at https://store.caru.com.tw/_nuxt/36ec727.js:2:290475
at h (https://store.caru.com.tw/_nuxt/36ec727.js:2:101656)
at Generator._invoke (https://store.caru.com.tw/_nuxt/36ec727.js:2:101444)
at Generator.E.forEach.e.<computed> [as next] (https://store.caru.com.tw/_nuxt/36ec727.js:2:102079)
at r (https://store.caru.com.tw/_nuxt/4ff1ebf.js:2:66614)
at l (https://store.caru.com.tw/_nuxt/4ff1ebf.js:2:66817)
```

5. Cacheable HTTPS response

Previous

There are 3 instances of this issue:

- /
- /_nuxt/manifest.f2313aaf.json
- /login/

Issue description

Unless directed otherwise, browsers may store a local cached copy of content received from web servers. Some browsers, including Internet Explorer, cache content accessed via HTTPS. If sensitive information in application responses is stored in the local cache, then this may be retrieved by other users who have access to the same computer at a future time.

Issue remediation

Applications should return caching directives instructing browsers not to store local copies of any sensitive data. Often, this can be achieved by configuring the web

Applications should return caching directives instructing browsers not to store local copies of any sensitive data. Often, this can be achieved by configuring the web server to prevent caching for relevant paths within the web root. Alternatively, most web development platforms allow you to control the server's caching directives from within individual scripts. Ideally, the web server should return the following HTTP headers in all responses containing sensitive content:

- Cache-control: no-store
- Pragma: no-cache

References

- Web Security Academy: Information disclosure

Vulnerability classifications

- CWE-524: Information Exposure Through Caching
- CWE-525: Information Exposure Through Browser Caching
- CAPEC-37: Retrieve Embedded Sensitive Data

5.1. https://store.caru.com.tw/

Previous Next

Summary

Severity:	**Information**
Confidence:	**Certain**
Host:	**https://store.caru.com.tw**
Path:	**/**

Request

```
GET / HTTP/1.1
Host: store.caru.com.tw
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
Upgrade-Insecure-Requests: 1
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en-GB;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/95.0.4638.54 Safari/537.36
Connection: close
Cache-Control: max-age=0
```

Response

```
HTTP/1.1 200 OK
Date: Thu, 02 Dec 2021 04:03:41 GMT
Server: Apache/2.4.41 (Ubuntu)
Last-Modified: Tue, 30 Nov 2021 09:01:13 GMT
ETag: "e9e-5d1fdcc9decf2-gzip"
Accept-Ranges: bytes
Vary: Accept-Encoding
Content-Length: 3742
Connection: close
Content-Type: text/html

<!doctype html>
<html lang="en" data-n-head="%7B%22lang%22:%7B%221%22:%22en%22%7D%7D">
<head>
<title>CarU .....</title><meta data-n-head="1" charset="utf-8"><meta data-n-head="1" name="vi
...[SNIP]...
```

5.2. https://store.caru.com.tw/_nuxt/manifest.f2313aaf.json

Previous Next

Summary

Severity:	**Information**
Confidence:	**Certain**
Host:	**https://store.caru.com.tw**
Path:	**/_nuxt/manifest.f2313aaf.json**

Request

```
GET /_nuxt/manifest.f2313aaf.json HTTP/1.1
Host: store.caru.com.tw
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
Upgrade-Insecure-Requests: 1
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en-GB;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/95.0.4638.54 Safari/537.36
Connection: close
Cache-Control: max-age=0
```

Response

```
HTTP/1.1 200 OK
Date: Thu, 02 Dec 2021 04:13:46 GMT
Server: Apache/2.4.41 (Ubuntu)
Last-Modified: Tue, 30 Nov 2021 09:01:16 GMT
ETag: "51d-5d1fdccd47da7"
Accept-Ranges: bytes
Content-Length: 1309
Connection: close
Content-Type: application/json

{
"name": "CarU .....",
"short_name": "CarU .....",
"description": "## Build Setup",
"icons": [
{
"src": "/_nuxt/icons/icon_64x64.2924ce.png",
"sizes": "64x64",
"
...[SNIP]...
```

5.3. https://store.caru.com.tw/login/

Previous

Summary

Severity:	**Information**
Confidence:	**Certain**
Host:	**https://store.caru.com.tw**
Path:	**/login/**

Request

```
GET /login/? HTTP/1.1
Host: store.caru.com.tw
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
Upgrade-Insecure-Requests: 1
Referer: https://store.caru.com.tw/login/
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en-GB;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/95.0.4638.54 Safari/537.36
Connection: close
Cache-Control: max-age=0
```

Response

```
HTTP/1.1 200 OK
Date: Thu, 02 Dec 2021 04:13:23 GMT
Server: Apache/2.4.41 (Ubuntu)
Last-Modified: Tue, 30 Nov 2021 09:01:12 GMT
ETag: "e9e-5d1fdcc8d52f5-gzip"
Accept-Ranges: bytes
Vary: Accept-Encoding
Content-Length: 3742
Connection: close
Content-Type: text/html

<!doctype html>
<html lang="en" data-n-head="%7B%22lang%22:%7B%221%22:%22en%22%7D%7D">
<head>
<title>CarU .....</title><meta data-n-head="1" charset="utf-8"><meta data-n-head="1" name="vi
...[SNIP]...
```

test-caru.welcometw.com

Burp Scanner Report

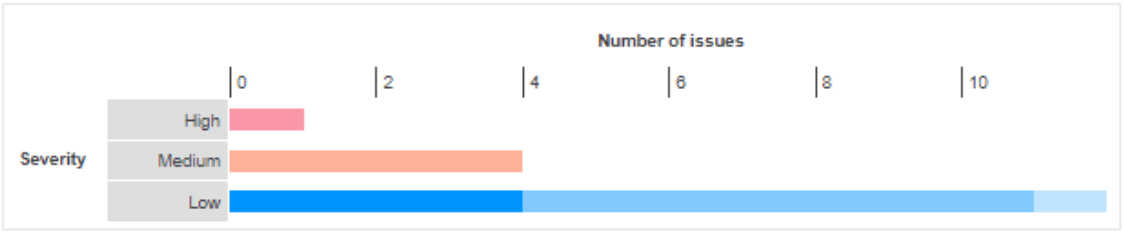
Burp Suite Professional

Summary

The table below shows the numbers of issues identified in different categories. Issues are classified according to severity as High, Medium, Low or Information. This reflects the likely impact of each issue for a typical organization. Issues are also classified according to confidence as Certain, Firm or Tentative. This reflects the inherent reliability of the technique that was used to identify the issue.

Severity	Confidence			
	Certain	Firm	Tentative	Total
High	0	1	0	1
Medium	0	4	0	4
Low	4	7	1	12
Information	12	11	0	23

The chart below shows the aggregated numbers of issues identified in each category. Solid colored bars represent issues with a confidence level of Certain, and the bars fade as the confidence level falls.



Contents

1. SQL injection
2. TLS cookie without secure flag set
   2.1. https://test-caru.welcometw.com/
   2.2. https://test-caru.welcometw.com/
   2.3. https://test-caru.welcometw.com/admin
   2.4. https://test-caru.welcometw.com/login
   2.5. https://test-caru.welcometw.com/login
3. Cookie without HttpOnly flag set
   3.1. https://test-caru.welcometw.com/
   3.2. https://test-caru.welcometw.com/admin
   3.3. https://test-caru.welcometw.com/login
4. Password field with autocomplete enabled
5. Ajax request header manipulation (DOM-based)
6. Link manipulation (reflected DOM-based)
   6.1. https://test-caru.welcometw.com/loginbgoydjwd7u [URL path filename]
   6.2. https://test-caru.welcometw.com/loginn7mn4v6bek [URL path filename]
   6.3. https://test-caru.welcometw.com/loginyztjz2hz7e [URL path filename]
7. Source code disclosure
8. Strict transport security not enforced

8.1. https://test-caru.welcometw.com/
8.2. https://test-caru.welcometw.com/admin
8.3. https://test-caru.welcometw.com/login

9. Input returned in response (reflected)

9.1. https://test-caru.welcometw.com/admin [XSRF-TOKEN cookie]
9.2. https://test-caru.welcometw.com/admin [caru_session cookie]
9.3. https://test-caru.welcometw.com/admin [remember_web_59ba36addc2b2f9401580f014c7f58ea4e30989d cookie]
9.4. https://test-caru.welcometw.com/login [URL path filename]

10. Cross-domain script include

10.1. https://test-caru.welcometw.com/
10.2. https://test-caru.welcometw.com/admin

11. Frameable response (potential Clickjacking)

11.1. https://test-caru.welcometw.com/
11.2. https://test-caru.welcometw.com/admin
11.3. https://test-caru.welcometw.com/login
11.4. https://test-caru.welcometw.com/password/reset

12. Email addresses disclosed

13. Robots.txt file

14. Cacheable HTTPS response

14.1. https://test-caru.welcometw.com/robots.txt
14.2. https://test-caru.welcometw.com/svg/logo.svg

15. Base64-encoded data in parameter

15.1. https://test-caru.welcometw.com/admin
15.2. https://test-caru.welcometw.com/admin
15.3. https://test-caru.welcometw.com/login
15.4. https://test-caru.welcometw.com/login
15.5. https://test-caru.welcometw.com/login
15.6. https://test-caru.welcometw.com/login
15.7. https://test-caru.welcometw.com/robots.txt

16. TLS certificate

1. SQL injection

Next

Summary

Severity:	**High**
Confidence:	**Firm**
Host:	**https://test-caru.welcometw.com**
Path:	**/login**

Issue detail

The URL path filename appears to be vulnerable to SQL injection attacks. The payload ' was submitted in the URL path filename, and a database error message was returned. You should review the contents of the error message, and the application's handling of other input, to confirm whether a vulnerability is present.

The database appears to be Microsoft SQL Server.

Remediation detail

The application should handle errors gracefully and prevent SQL error messages from being returned in responses.

Issue background

SQL injection vulnerabilities arise when user-controllable data is incorporated into database SQL queries in an unsafe manner. An attacker can supply crafted input to break out of the data context in which their input appears and interfere with the structure of the surrounding query.

SQL injection vulnerabilities arise when user-controllable data is incorporated into database SQL queries in an unsafe manner. An attacker can supply crafted input to break out of the data context in which their input appears and interfere with the structure of the surrounding query.

A wide range of damaging attacks can often be delivered via SQL injection, including reading or modifying critical application data, interfering with application logic, escalating privileges within the database and taking control of the database server.

Remediation background

The most effective way to prevent SQL injection attacks is to use parameterized queries (also known as prepared statements) for all database access. This method uses two steps to incorporate potentially tainted data into SQL queries: first, the application specifies the structure of the query, leaving placeholders for each item of user input; second, the application specifies the contents of each placeholder. Because the structure of the query has already been defined in the first step, it is not possible for malformed data in the second step to interfere with the query structure. You should review the documentation for your database and application platform to determine the appropriate APIs which you can use to perform parameterized queries. It is strongly recommended that you parameterize *every* variable data item that is incorporated into database queries, even if it is not obviously tainted, to prevent oversights occurring and avoid vulnerabilities being introduced by changes elsewhere within the code base of the application.

You should be aware that some commonly employed and recommended mitigations for SQL injection vulnerabilities are not always effective:

- One common defense is to double up any single quotation marks appearing within user input before incorporating that input into a SQL query. This defense is designed to prevent malformed data from terminating the string into which it is inserted. However, if the data being incorporated into queries is numeric, then the defense may fail, because numeric data may not be encapsulated within quotes, in which case only a space is required to break out of the data context and interfere with the query. Further, in second-order SQL injection attacks, data that has been safely escaped when initially inserted into the database is subsequently read from the database and then passed back to it again. Quotation marks that have been doubled up initially will return to their original form when the data is reused, allowing the defense to be bypassed.
- Another often cited defense is to use stored procedures for database access. While stored procedures can provide security benefits, they are not guaranteed to prevent SQL injection attacks. The same kinds of vulnerabilities that arise within standard dynamic SQL queries can arise if any SQL is dynamically constructed within stored procedures. Further, even if the procedure is sound, SQL injection can arise if the procedure is invoked in an unsafe manner using user-controllable data.

References

- Web Security Academy: SQL injection
- Using Burp to Test for Injection Flaws
- Web Security Academy: SQL Injection Cheat Sheet

Vulnerability classifications

- CWE-89: Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')
- CWE-94: Improper Control of Generation of Code ('Code Injection')
- CWE-116: Improper Encoding or Escaping of Output
- CAPEC-66: SQL Injection

Request


```
POST /login! HTTP/1.1
Host: test-caru.welcometw.com
Cookie: XSRF-
TOKEN=eyJpdiI6IkY4OUM3M0V6REt4QmZWd3VJRVAwbVE9PSIsInZhbHVlIjoiS3hEa05MUTlYajRSUVhKeHN0cmtCQ2hYb2xqUkdHZ01HVk9UaTUwdU1C
c2dTRFhqM3RlSVkydU50eGpxMnJON2lwdUt3QmpDbkJya3pSK2RKOXVqS2hSWkFvYm80d0FPenFtUFphZWJvOFRtU3YxeG9OTmZ3ZWVDMmZGVm93
NlAiLCJtYWMiOiJlNDc3YTY1YzQwNzBiOTJlOWFjZDI1Nzk1NWE4MjBjMjU4ZWZjYWFlODQzZWFjM2I2M2MzMzVkMGZlYWJhMDdkIn0%3D;
caru_session=eyJpdiI6IkR1RXczazFZdk05S2RlQTVKSGtrNEE9PSIsInZhbHVlIjoiV3crcUp5OE5yNDl4S09Rd2xkUEVGNjV1U1lUR0lTMXRzRENMeVpiS3Fu
MnBBKzMxUCtkYjFvcCtGMWVPcmNMVUZoeDMrMkRjbzhaMS9LZzFrclpLS0pYUDczN1A5M2tLYnp3dFlSRnd1UU9td0EwbWJaZEdDLzduRTYwRmo3YnliL
CJtYWMiOiI0ZTNhNGJjODk0MzFiZjNlOGQ4YmE3OTc3YmFhOTJlNzdlNjgyNWFhMmRkOGExMThlYjc1MWUyZTg2NzA3N2YyIn0%3D
Content-Length: 113
Cache-Control: max-age=0
Sec-Ch-Ua: " Not A;Brand";v="99", "Chromium";v="96", "Google Chrome";v="96"
Sec-Ch-Ua-Mobile: ?0
Sec-Ch-Ua-Platform: "Windows"
Dnt: 1
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/96.0.4664.45 Safari/537.36
Origin: https://test-caru.welcometw.com
Content-Type: application/x-www-form-urlencoded
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
Sec-Fetch-Site: same-origin
```


Response


```
HTTP/1.1 405 Method Not Allowed
Server: nginx/1.21.3
Content-Type: text/html; charset=UTF-8
Connection: close
allow: GET, HEAD
Cache-Control: no-cache, private
date: Thu, 02 Dec 2021 02:45:23 GMT
Content-Length: 572621

<!doctype html>
<html class="theme-light">
<!--
```

Symfony\Component\HttpKernel\Exception\MethodNotAllowedHttpException: The POST method is not supported for this route. Supported methods: GET, HEAD.
in
...[SNIP]...
,"SCROLL","SEARCH","SECOND","SECONDS","SECQTY","SECURITY","SENSITIVE","SEQUENCE","SESSION","SESSION_USER","SIGNAL","SIMILAR","SIMPLE","SMALLINT","SNAN","SOME","SOURCE","SPECIFIC","SPECIFICTYPE","SQL","SQLEXCEPTION","SQLID","SQLSTATE","SQLWARNING","SQRT","STACKED","STANDARD","START","STARTING","STATEMENT","STATIC","STATMENT","STAY","STDDEV_POP","STDDEV_SAMP","STOGROUP","STORES","STYLE","SUBMULTISET","SUBSTRING",
...[SNIP]...

2. TLS cookie without secure flag set

Previous Next

There are 5 instances of this issue:

- /
- /
- /admin
- /login
- /login

Issue background

If the secure flag is set on a cookie, then browsers will not submit the cookie in any requests that use an unencrypted HTTP connection, thereby preventing the cookie from being trivially intercepted by an attacker monitoring network traffic. If the secure flag is not set, then the cookie will be transmitted in clear-text if the user visits any HTTP URLs within the cookie's scope. An attacker may be able to induce this event by feeding a user suitable links, either directly or via another web site. Even if the domain that issued the cookie does not host any content that is accessed over HTTP, an attacker may be able to use links of the form http://example.com:443/ to perform the same attack.

To exploit this vulnerability, an attacker must be suitably positioned to eavesdrop on the victim's network traffic. This scenario typically occurs when a client communicates with the server over an insecure connection such as public Wi-Fi, or a corporate or home network that is shared with a compromised computer. Common defenses such as switched networks are not sufficient to prevent this. An attacker situated in the user's ISP or the application's hosting infrastructure could also perform this attack. Note that an advanced adversary could potentially target any connection made over the Internet's core infrastructure.

Issue remediation

The secure flag should be set on all cookies that are used for transmitting sensitive data when accessing content over HTTPS. If cookies are used to transmit session tokens, then areas of the application that are accessed over HTTPS should employ their own session handling mechanism, and the session tokens used should never be transmitted over unencrypted communications.

Vulnerability classifications

- CWE-614: Sensitive Cookie in HTTPS Session Without 'Secure' Attribute

---

2.1. https://test-caru.welcometw.com/

Next

Summary

Severity:	**Medium**
Confidence:	**Firm**
Host:	**https://test-caru.welcometw.com**
Path:	/

Issue detail

The following cookie was issued by the application and does not have the secure flag set:

- **XSRF-TOKEN**

The cookie appears to contain a session token, which may increase the risk associated with this issue. You should review the contents of the cookie to determine its function.This issue was found in multiple locations under the reported path.

Request 1

GET /facebook/auth HTTP/1.1
Host: test-caru.welcometw.com

```
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/95.0.4638.54 Safari/537.36
Connection: close
```

Response 1

```
HTTP/1.1 302 Found
Server: nginx/1.21.3
Content-Type: text/html; charset=UTF-8
Connection: close
Cache-Control: no-cache, private
Date: Thu, 02 Dec 2021 02:29:12 GMT
Location: https://www.facebook.com/v3.3/dialog/oauth?client_id=143808007828334&redirect_uri=https%3A%2F%2Ftest-caru.welcometw.com%2Ffacebook%2Fauthcallback&scope=email&response_type=code&state=HAQptkGrfQl0lFLtEhOQBVyblB57SbFs0Vb7ZuoV
Set-Cookie: XSRF-TOKEN=eyJpdiI6InNnMDJyRmU3TnlKU0ZYa0FzYVprbWc9PSIsInZhbHVlIjoiOFhwbENmSHo0a29Wc3lSNXRkVmhTRkptQ1FJaDJlVU0vcTlEaVE2RWtseGJDVnFEUHZJUHZ6L1c2cG8vUG5yQUs0Vk9hUDQrZDdjaUUzbHo4eXAzd1FNRHg0eEZXWGhDVlZqcWpjUDY4UlJCdkdCNld1WVNodmtHOThtVERTd20iLCJtYWMiOiJlZDdmMTZkYTA4MzZlM2IwMGY1Nzk1ZTJhZDlmZDcwYzFmOWVkZGViZDIzYjEyOGE3YmNmNzIyMWYwZGU3YTU5In0%3D; expires=Thu, 02-Dec-2021 04:29:12 GMT; Max-Age=7200; path=/; samesite=lax
Set-Cookie: caru_session=eyJpdiI6IkdtTUZvVU1sdVBIcmlSR2VTZmY0SVE9PSIsInZhbHVlIjoidStGR1IndFZnUjVIQ2NjMkMzVlBiYWpnT3A5Z0dCZERwbWlzR0RrSmNiZG56SkZEdmlVak5xejhORE1aQ0VWL1doSjFFQnZzOWovU2tSelM5WXpKSVNaYXZvaEpKSCtKQ1hEVXpjSjlpYnd2VUQ4eFdUN0pNYVo2SkUxOENQZ0ciLCJtYWMiOiJiZTMxNTVkMjc2OTU1YTdlMjlxMmQ5ZjQ2NzY0MmQ4OTkzOGQ2NzcxMGFiNzM5NWZmYzgzYTMxOTJhYzc4ZTI5In0%3D; expires=Thu, 02-Dec-2021 04:29:12 GMT; Max-Age=7200; path=/; httponly; samesite=lax
Content-Length: 1202

<!DOCTYPE html>
```

Request 2

```
POST /login HTTP/1.1
Host: test-caru.welcometw.com
Cookie: XSRF-TOKEN=eyJpdiI6IkZWQ0h5K1JldWFHQ28rY25sSzlrVlE9PSIsInZhbHVlIjoiaWoxT3FIQTE0WUZEazcrRVE4SUhNSDVTZlIrRnJHMVowalRZelVoQ3hibFFTVHp4OUt6Q3k1S2YxVE1FT25uRzJ3aWlkRExsRXdCV0Rib0FKbDhVOTI5NExseXNGTzZSRmMwSHM0L0kyRzVJoC9ZWmNRdkd6WjBnMDgwMVRyUzgiLCJtYWMiOiJhMmU1ZjI0MzUwMTM4MzkwYzE5MDI4NGRhOTEyNGQwMmMwYTdmMTVhMjNjNzliOWMxNTMzM2EwY2Q3NDdjMDdhIn0%3D; caru_session=eyJpdiI6IlJQc2pPNzdYZ0V2L1lURDRIM0VGVGc9PSIsInZhbHVlIjoiZ0dzUkJHS0hueXUwbWQxZ2VPMGpmdWNCdlhaR1RQaHhFSlFXeTlwVzQyS0h2a0lrUWtpYXl0cTQxaFJ6Rzdycng0azA5VWt5TmpWRngyelB2dWZNcEY1c1JOSDdHbSsxV3pramdmNnZ5N2hRejdnNW8yWlNZWHNPWnBMTmhUZXYiLCJtYWMiOiIxYWM0MjFkNTRlYzI5MDA1MWI0ZDg0NjFiZTgxYWNiZjgyY2ExMjVjNTM5ZTc4ZDVhYmM0ODc5OTBkNWIwMzU3In0%3D
Content-Length: 113
Cache-Control: max-age=0
Sec-Ch-Ua: " Not A;Brand";v="99", "Chromium";v="96", "Google Chrome";v="96"
Sec-Ch-Ua-Mobile: ?0
Sec-Ch-Ua-Platform: "Windows"
Origin: https://test-caru.welcometw.com
Upgrade-Insecure-Requests: 1
Dnt: 1
Content-Type: application/x-www-form-urlencoded
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/96.0.4664.45 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
Sec-Fetch-Site: same-origin
```

Response 2

```
HTTP/1.1 302 Found
Server: nginx/1.21.3
Content-Type: text/html; charset=UTF-8
Connection: close
Cache-Control: no-cache, private
Date: Thu, 02 Dec 2021 01:37:48 GMT
Location: https://test-caru.welcometw.com/admin
Set-Cookie: XSRF-TOKEN=eyJpdiI6Ik5sUjJZQWQxeWs1aWpNQkVFbnovRmc9PSIsInZhbHVlIjoiTnVWcFhqSWxRM2VyeDlvVUlWZFk1WlFDTW5PWW8yZ0h4UVFpMU55MWNBN2JXTlJ2OUZKeDR2T0pzSDkwVU5PYUUxcGhPc1FEMlZMOVo5VHNDSFR2VmkxRUF6QnZTZHNGVFRQTVB5blkrRHFyZnJMelNmbU9VRTFTbWg2MnA1UG8iLCJtYWMiOiI0OTdlYjM4YmM3NjQ2YzUxZTVkNzU0NzFlNjM0MDAyNjY2YWFmYTVlYTk4N2I2M2JiOGM5OTEyYzdlMGYxMWIzIn0%3D; expires=Thu, 02-Dec-2021 03:37:48 GMT; Max-Age=7200; path=/; samesite=lax
Set-Cookie: caru_session=eyJpdiI6IklxZ3VSVTZLZEs1QmFkSHRvSERranc9PSIsInZhbHVlIjoiZk9TY3ZRMVg3WHNCV1ZZYkRmYjBLbUkvVFJZOGdpMk1SN1hlNUplY1VzNmFNMDEzQ3F6K1IBZjRlNEsycytLSHlzojUvQTBMaExRZGsxRGMxdEhWejFjTEgwY1IBMUVtYWxVYlA5VzVqRktSUlloN28vSHBCMDZSQXptT0pYZGEiLCJtYWMiOiI3NDJmNThlODZhZjVkNTFhYzJjOWU3ZTQyYWM0ZTI0ZDA4ODM4Yjc4NjYwN2E4ZmM3ZTUyYTQyZmU2ZjRmMzdkln0%3D; expires=Thu, 02-Dec-2021 03:37:48 GMT; Max-Age=7200; path=/; httponly; samesite=lax
Set-Cookie: remember_web_59ba36addc2b2f9401580f014c7f58ea4e30989d=eyJpdiI6Im1jNWltZERONURQYUc5SzI0SXowN2c9PSIsInZhbHVlIjoiUi95RHp6RTh1S0RWd0dCTkRrZWUvd0hPb1lSb0E3a0oybStuR2dVT3dldnpqbjRsUzVMYTdWVUN0U0libjE2OXp4Q2dlUG1ER3JhZjY1WXJTZG9XYldhNG5UU0FFUUZNRDJNVk9rdWhSakgvMEZUWFp4M3BtZGpoRHd1clB0alErNmtXTGFOVnhqbkl5cDh1Y0VoVWlzV3BRdzVnbGRiL09xVk9mWTI0NXRJRExaQVpieHppRlJEVTZwb2h
```

Request 3

```
POST /login HTTP/1.1
```

```
POST /login HTTP/1.1
Host: test-caru.welcometw.com
Cookie: XSRF-
TOKEN=eyJpdiI6IkY4OUM3M0V6REt4QmZWd3VJRVAwbVE9PSIsInZhbHVlIjoiS3hEa05MUTlYajRSUVhKeHN0cmtCQ2hYb2xqUkdHZ01HVk9UaTUwdU1C
c2dTRFhqM3RlSVkydU50eGpxMnJON2lwdUt3QmpDbkJya3pSK2RKOXVqS2hSWkFvYm80d0FPenFtUFphZWJvOFRtU3YxeG9OTmZ3ZWVDMmZGVm93
NlAiLCJtYWMiOiJlNDc3YTY1YzQwNzBiOTJlOWFjZDI1Nzk1NWE4MjBjMjU4ZWZjYWFlODQzZWFjM2I2M2MzMzVkMGZlYWJhMDdkIn0%3D;
caru_session=eyJpdiI6IkR1RXczazFZdk05S2RlQTVKSGtrNEE9PSIsInZhbHVlIjoiV3crcUp5OE5yNDI4S09Rd2xkUEVGNjV1U1lUR0lTMXRzRENMeVpiS3Fu
MnBBKzMxUCtkYjFvcCtGMWVPcmNMVUZoeDMrMkRjbzhaMS9LZzFrclpLS0pYUDczN1A5M2tLYnp3dFlSRnd1UU9td0EwbWJaZEdDLzduRTYwRmo3YnliL
CJtYWMiOiI0ZTNhNGJjODk0MzFiZjNlOGQ4YmE3OTc3YmFhOTJlNzdlNjgyNWFhMmRkOGExMThlYjc1MWUyZTg2NzA3N2YyIn0%3D
Content-Length: 113
Cache-Control: max-age=0
Sec-Ch-Ua: " Not A;Brand";v="99", "Chromium";v="96", "Google Chrome";v="96"
Sec-Ch-Ua-Mobile: ?0
Sec-Ch-Ua-Platform: "Windows"
Dnt: 1
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/96.0.4664.45 Safari/537.36
Origin: https://test-caru.welcometw.com
Content-Type: application/x-www-form-urlencoded
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
Sec-Fetch-Site: same-origin
```

Response 3

```
HTTP/1.1 302 Found
Server: nginx/1.21.3
Content-Type: text/html; charset=UTF-8
Connection: close
Cache-Control: no-cache, private
Date: Thu, 02 Dec 2021 01:32:14 GMT
Location: https://test-caru.welcometw.com/admin
Set-Cookie: XSRF-
TOKEN=eyJpdiI6IkpDcVU2Q2pqOGJlYWRySTFUTGpjWHc9PSIsInZhbHVlIjoiWnBMMkJTY3U0d2F6UEtYUFlGWmthVTRlMU5LNFlhS2s0R2k2dEd6ekJkel
EybVVrUUFXdkVOWFRkNzlCRHRZNkt6a29FMm9MN3J4a0MranpWcjI3MjZaZEx6Q2p3dnJOb1kwQ2I2UjU1R3hLNGpaM2RWYkFhRmc2bXlLbFZOSkYiLC
JtYWMiOiI0ZTE4NGM1MWQzNjljYTFiYTMyNmEyZGI1MzI0MjFlZWQ5ZWNlNjczNDIxNGI2YzFlZjM1NDlhYzU5MzQwYmE1In0%3D; expires=Thu, 02-Dec-
2021 03:32:14 GMT; Max-Age=7200; path=/; samesite=lax
Set-Cookie:
caru_session=eyJpdiI6IlpLbVpVM0s5TlVVQVFyOVBzZ3NSUkE9PSIsInZhbHVlIjoiSFoxVXRJQWlUOVoxWjhjaWNNR1VUMzI0OXg5cHB3MkNPT3puUzhmb
0YwT3QyK2hDa0VMVUtzYXRHQWFLckkzL3VweXh2K20zZ203UVBBcU10L3gyMnFqdDc4akhzbDJKRnkwRlYvWUxveGE5VElzd1dHS0dzMGtETFV0MjNjU
0YiLCJtYWMiOiI1YmQ4OTRkZTBjNjU0N2U0MDUxNTM1NTBlMGEwZTIzZWUxYTNjY2RkYTA0N2M1NDBhNmNmMDI5NjE5ZDA5MTEyIn0%3D;
expires=Thu, 02-Dec-2021 03:32:14 GMT; Max-Age=7200; path=/; httponly; samesite=lax
Content-Length: 394

<!DOCTYPE html>
<html>
```

2.2. https://test-caru.welcometw.com/

Previous Next

Summary

Severity:	**Medium**
Confidence:	**Firm**
Host:	**https://test-caru.welcometw.com**
Path:	**/**

Issue detail

The following cookie was issued by the application and does not have the secure flag set:

- **caru_session**

The cookie appears to contain a session token, which may increase the risk associated with this issue. You should review the contents of the cookie to determine its function.This issue was found in multiple locations under the reported path.

Request 1

```
GET /facebook/auth HTTP/1.1
Host: test-caru.welcometw.com
Accept-Encoding: gzip, deflate
Accept: */*
Accept-Language: en
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/95.0.4638.54 Safari/537.36
Connection: close
```

```
Cache-Control: no-cache, private
Date: Thu, 02 Dec 2021 02:29:12 GMT
Location: https://www.facebook.com/v3.3/dialog/oauth?client_id=143808007828334&redirect_uri=https%3A%2F%2Ftest-
caru.welcometw.com%2Ffacebook%2Fauthcallback&scope=email&response_type=code&state=HAQptkGrfQI0IFLtEhOQBVybIB57SbFs0Vb7ZuoV
Set-Cookie: XSRF-
TOKEN=eyJpdiI6InNnMDJyRmU3TnlKU0ZYa0FzYVprbWc9PSIsInZhbHVlIjoiOFhwbENmSHo0a29Wc3ISNXRkVmhTRkptQ1FJaDJlVU0vcTlEaVE2RWtseGJ
DVnFEUHZJUHZ6L1c2cG8vUG5yQUs0Vk9hUDQrZDdjaUUzbHo4eXAzd1FNRHg0eEZXWGhDVlZqcWpjUDY4UlJCdkdCNld1WVNodmtHOThtVERTd20iLC
JtYWMiOiJlZDdmMTZkYTA4MzZlM2IwMGY1Nzk1ZTJhZDlmZDcwYzFmOWVkZGViZDIzYjEyOGE3YmNmNzIyMWYwZGU3YTU5In0%3D; expires=Thu, 02-
Dec-2021 04:29:12 GMT; Max-Age=7200; path=/; samesite=lax
Set-Cookie:
caru_session=eyJpdiI6IkdtTUZvVU1sdVBlcmlSR2VTZmY0SVE9PSIsInZhbHVlIjoidStGR1lndFZnUjVlQ2NjMkMzVlBiYWpnT3A5Z0dCZERwbWlzR0RrSmNiZ
G56SkZEdmlVak5xejhORE1aQ0VWL1doSjFFQnZzOWovU2tSelM5WXpKSVNaYXZvaEpKSCtKQ1hEVXpjSjlpYnd2VUQ4eFdUN0pNYVo2SkUxOENQZ0ciL
CJtYWMiOiJiZTMxNTVkMjc2OTU1YTdlMjIxMmQ5ZjQ2NzY0MmQ4OTkzOGQ2NzcxMGFiNzM5NWZmYzgzYTMxOTJhYzc4ZTI5In0%3D; expires=Thu, 02-
Dec-2021 04:29:12 GMT; Max-Age=7200; path=/; httponly; samesite=lax
Content-Length: 1202

<!DOCTYPE html>
```

Request 2

```
POST /login HTTP/1.1
Host: test-caru.welcometw.com
Cookie: XSRF-
TOKEN=eyJpdiI6IkZWQ0h5K1JldWFHQ28rY25sSzlrVlE9PSIsInZhbHVlIjoiaWxoT3FIQTE0WUZEazcrRVE4SUhNSDVTZlIrRnJHMVcwalRZelVoQ3hibFFTVH
p4OUt6Q3k1S2YxVE1FT25uRzJ3aWlkRExsRXdCV0Rib0FKbDhVOTI5NExseXNGTzZSRmMwSHM0L0kyRzVJcC9ZWmNRdkd6WjBnMDgwMVRyUzgiLCJt
YWMiOiJhMmU1ZjI0MzUwMTM4MzkwYzE5MDI4NGRhOTEyNGQwMmMwYTdmMTVhMjNjNzliOWMxNTMzM2EwY2Q3NDdjMDdhIn0%3D;
caru_session=eyJpdiI6IlJQc2pPNzdYZ0V2L1lURDRIM0VGVGc9PSIsInZhbHVlIjoiZ0dzUkJHS0hueXUwbWQxZ2VPMGpmdWNCdlhaR1RQaHhFSlFXeTlwV
zQyS0h2a0lrUWtpYXl0cTQxaFJ6Rzdycng0azA5VWt5TmpWRngyelB2dWZNcEY1c1JOSDdHbSsxV3pramdmNnZ5N2hRejdnNW8yWlNZWHNPWnBMTmhU
ZXYiLCJtYWMiOiIxYWM0MjFkNTRlYzI5MDA1MWI0ZDg0NjFiZTgxYWNiZjgyY2ExMjVjNTM5ZTc4ZDVhYmM0ODc5OTBkNWIwMzU3In0%3D
Content-Length: 113
Cache-Control: max-age=0
Sec-Ch-Ua: " Not A;Brand";v="99", "Chromium";v="96", "Google Chrome";v="96"
Sec-Ch-Ua-Mobile: ?0
Sec-Ch-Ua-Platform: "Windows"
Origin: https://test-caru.welcometw.com
Upgrade-Insecure-Requests: 1
Dnt: 1
Content-Type: application/x-www-form-urlencoded
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/96.0.4664.45 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
Sec-Fetch-Site: same-origin
```

Response 2

```
HTTP/1.1 302 Found
Server: nginx/1.21.3
Content-Type: text/html; charset=UTF-8
Connection: close
Cache-Control: no-cache, private
Date: Thu, 02 Dec 2021 01:37:48 GMT
Location: https://test-caru.welcometw.com/admin
Set-Cookie: XSRF-
TOKEN=eyJpdiI6Ik5sUjJZQWQxeWs1aWpNQkVFbnovRmc9PSIsInZhbHVlIjoiTnVWcFhqSWkxRM2VyeDlvVUlWZFk1WlFDTW5PWW8yZ0h4UVFpMU55MW
NBN2JXTlJ2OUZKeDR2T0pzSDkwVU5PYUUxcGhPc1FEMlZMOVo5VHNDSFR2VmkxRUF6QnZTZHNGVFRQTVB5blkrRHFyZnJMelNmbU9VRTFTbWg2M
nA1UG8iLCJtYWMiOiI0OTdlYjM4YmM3NjQ2YzUxZTVkNzU0NzFlNjM0MDAyNjY2YWFmYTVlYTk4N2I2M2JiOGM5OTEyYzdlMGYxMWIzIn0%3D;
expires=Thu, 02-Dec-2021 03:37:48 GMT; Max-Age=7200; path=/; samesite=lax
Set-Cookie:
caru_session=eyJpdiI6IklxZ3VSVTZLZEs1QmFkSHRvSERranc9PSIsInZhbHVlIjoiZk9TY3ZRMVg3WHNCV1ZZYkRmYjBLbUkvVFJZOGdpMk1SN1hlNUplY1
VzNmFNMDEzQ3F6K1lBZjRlNEsycytLSHlzcjUvQTBMaExxRZGsxRGMxdEhWejFjTEgwY1lBMUVtYWxVYlA5VzVqRktSUlloN28vSHBCMDZSQXptT0pYZGEi
LCJtYWMiOiI3NDJmNThlODZhZjVkNTFhYzJjOWU3ZTQyYWM0ZTI0ZDA4ODM4Yjc4NjYwN2E4ZmM3ZTUyYTQyZmU2ZjRmMzdkIn0%3D; expires=Thu,
02-Dec-2021 03:37:48 GMT; Max-Age=7200; path=/; httponly; samesite=lax
Set-Cookie:
remember_web_59ba36addc2b2f9401580f014c7f58ea4e30989d=eyJpdiI6Im1jNWltZERONURQYUc5SzI0SXowN2c9PSIsInZhbHVlIjoiUi95RHp6RTh1S0RW
d0dCTkRrZWUvd0hPb1lSb0E3a0oybStuR2dVT3dldnpqbjRsUzVMYTdWVUN0U0libjE2OXp4Q2dlUG1ER3JhZjY1WXJTZG9XYldhNG5UU0FFUUZNRDJNV
k9rdWhSakovMEZUWFo4M3BtZGpoRHd1clB0alErNmtXTGFOVnhqbkl5cDh1Y0VoVWlzV3BRdzVnbGRiL09xVk9mWTI0NXRJREexaQVoieHpoRlJEVTZwb2h
```

Request 3

```
POST /login HTTP/1.1
Host: test-caru.welcometw.com
Cookie: XSRF-
TOKEN=eyJpdiI6IkY4OUM3M0V6REt4QmZWd3VJRVAwbVE9PSIsInZhbHVlIjoiS3hEa05MUTlYajRSUVhKeHN0cmtCQ2hYb2xqUkdHZ01HVk9UaTUwdU1C
c2dTRFhqM3RlSVkydU50eGpxMnJON2lwdUt3QmpDbkJya3pSK2RKOXVqS2hSWkFvYm80d0FPenFtUFphZWJvOFRtU3YxeG9OTmZ3ZWVDMmZGVm93
NlAiLCJtYWMiOiJlNDc3YTY1YzQwNzBiOTJlOWFjZDI1Nzk1NWE4MjBjMjU4ZWZjYWFlODQzZWFjM2I2M2MzMzVkMGZlYWJhMDdkIn0%3D;
caru_session=eyJpdiI6IkR1RXczazFZdk05S2RlQTVKSGtrNEE9PSIsInZhbHVlIjoiV3crcUp5OE5yNDl4S09Rd2xkUEVGNjV1U1lUR0lTMXRzRENMeVpiS3Fu
MnBBKzMxUCtkYjFvcCtGMWVPcmNMVUZoeDMrMkRjbzhaMS9LZzFrclpLS0pYUDczN1A5M2tLYnp3dFlSRnd1UU9td0EwbWJaZEdDLzduRTYwRmo3YnliL
CJtYWMiOiI0ZTNhNGJjODk0MzFiZjNlOGQ4YmE3OTc3YmFhOTJlNzdlNjgyNWFhMmRkOGExMThlYjc1MWUyZTg2NzA3N2YyIn0%3D
Content-Length: 113
Cache-Control: max-age=0
Sec-Ch-Ua: " Not A;Brand";v="99", "Chromium";v="96", "Google Chrome";v="96"
Sec-Ch-Ua-Mobile: ?0
```

```
Set-Cookie: XSRF-
TOKEN=eyJpdiI6IkpDcVU2Q2pqOGJIYWRySTFUTGpjWHc9PSIsInZhbHVlIjoiWnBMMkJTY3U0d2F6UEtYUFlGWmthVTRlMU5LNFlhS2s0R2k2dEd6ekJkel
EybVVrUUFXdkVOWFRkNzlCRHRZNkt6a29FMm9MN3J4a0MranpWcjI3MjZaZEx6Q2p3dnJOb1kwQ2I2UjU1R3hLNGpaM2RWYkFhRmc2bXlLbFZOSkYiLC
JtYWMiOiI0ZTE4NGM1MWQzNjljYTFiYTMyNmEyZGI1MzI0MjFlZWQ5ZWNlNjczNDIxNGI2YzFlZjM1NDlhYzU5MzQwYmE1In0%3D; expires=Thu, 02-Dec-
2021 03:32:14 GMT; Max-Age=7200; path=/; samesite=lax
Set-Cookie:
caru_session=eyJpdiI6IlpLbVpVM0s5TlVVQVFyOVBzZ3NSUkE9PSIsInZhbHVlIjoiSFoxVXRJQWlUOVoxWjhjaWNNR1VUMzI0OXg5cHB3MkNPT3puUzhmb
0YwT3QyK2hDa0VMVUtzYXRHQWFLckkzL3VweXh2K20zZ203UVBBcU10L3gyMnFqdDc4akhzbDJKRnkwRlYvWUxveGE5VElzd1dHS0dzMGtETFV0MjNjU
0YiLCJtYWMiOiI1YmQ4OTRkZTBjNjU0N2U0MDUxNTM1NTBlMGEwZTIzZWUxYTNjY2RkYTA0N2M1NDBhNmNmMDI5NjE5ZDA5MTEyIn0%3D;
expires=Thu, 02-Dec-2021 03:32:14 GMT; Max-Age=7200; path=/; httponly; samesite=lax
Content-Length: 394

<!DOCTYPE html>
<html>
```

2.3. https://test-caru.welcometw.com/admin

Previous Next

Summary

Severity:	**Medium**
Confidence:	**Firm**
Host:	**https://test-caru.welcometw.com**
Path:	**/admin**

Issue detail

The following cookies were issued by the application and do not have the secure flag set:

- **XSRF-TOKEN**
- **caru_session**

The cookies appear to contain session tokens, which may increase the risk associated with this issue. You should review the contents of the cookies to determine their function.

Request 1

```
GET /admin HTTP/1.1
Host: test-caru.welcometw.com
Cookie: XSRF-
TOKEN=eyJpdiI6IkpDcVU2Q2pqOGJIYWRySTFUTGpjWHc9PSIsInZhbHVlIjoiWnBMMkJTY3U0d2F6UEtYUFlGWmthVTRlMU5LNFlhS2s0R2k2dEd6ekJkel
EybVVrUUFXdkVOWFRkNzlCRHRZNkt6a29FMm9MN3J4a0MranpWcjI3MjZaZEx6Q2p3dnJOb1kwQ2I2UjU1R3hLNGpaM2RWYkFhRmc2bXlLbFZOSkYiLC
JtYWMiOiI0ZTE4NGM1MWQzNjljYTFiYTMyNmEyZGI1MzI0MjFlZWQ5ZWNlNjczNDIxNGI2YzFlZjM1NDlhYzU5MzQwYmE1In0%3D;
caru_session=eyJpdiI6IlpLbVpVM0s5TlVVQVFyOVBzZ3NSUkE9PSIsInZhbHVlIjoiSFoxVXRJQWlUOVoxWjhjaWNNR1VUMzI0OXg5cHB3MkNPT3puUzhmb
0YwT3QyK2hDa0VMVUtzYXRHQWFLckkzL3VweXh2K20zZ203UVBBcU10L3gyMnFqdDc4akhzbDJKRnkwRlYvWUxveGE5VElzd1dHS0dzMGtETFV0MjNjU
0YiLCJtYWMiOiI1YmQ4OTRkZTBjNjU0N2U0MDUxNTM1NTBlMGEwZTIzZWUxYTNjY2RkYTA0N2M1NDBhNmNmMDI5NjE5ZDA5MTEyIn0%3D
Cache-Control: max-age=0
Dnt: 1
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/96.0.4664.45 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Sec-Fetch-Dest: document
Sec-Ch-Ua: " Not A;Brand";v="99", "Chromium";v="96", "Google Chrome";v="96"
Sec-Ch-Ua-Mobile: ?0
Sec-Ch-Ua-Platform: "Windows"
```

Response 1

```
HTTP/1.1 302 Found
Server: nginx/1.21.3
Content-Type: text/html; charset=UTF-8
Connection: close
Cache-Control: no-cache, private
Date: Thu, 02 Dec 2021 01:36:35 GMT
Location: https://test-caru.welcometw.com/login
Set-Cookie: XSRF-
TOKEN=eyJpdiI6IklkVVNncnRhQXprbHNtbGhHa3FUblE9PSIsInZhbHVlIjoiTUkyTWdDcUlZWUhKVWJXdk40bHltN29pVlBiajMzVXlyZFBtRVRGWi9zSS9NYV
BNbEVubGhpRUEwV3Nlcitwb1FYaE5KMjZHUExrcGlNR2kxRG9lVVlTUXRkSng4emxuZlZhdndzSitFc0xSUUt4T3RaTlRUZ0VBemJNVHZ1N1YiLCJtYWMiOi
JiMWRhZmNiMWE3NzNiZTkyNDcwNDRmODk5NjRjOGQ0Zjk5ODA3YmRlZWZhZTU3OTMzMzc3MzFmYzlmNWE4MjU1In0%3D; expires=Thu, 02-Dec-
2021 03:36:35 GMT; Max-Age=7200; path=/; samesite=lax
Set-Cookie:
caru_session=eyJpdiI6ImpraVNYZUJTS1lpUXFnWFY3RUt4d0E9PSIsInZhbHVlIjoiMmlpdVBlYjlwTmk5UkVkMWFsQnBZY1dibnBpd0xuUmdiQWFtellkV0NET
```

```
BNbEVubGhpRUEwV3Nlcitwb1FYaE5KMjZHUExrcGlNR2kxRG9lVVlTUXRkSng4emxuZlZhdndzSitFc0xSUUt4T3RaTlRUZ0VBemJNVHZ1N1YiLCJtYWMiOi
JiMWRhZmNiMWE3NzNiZTkyNDcwNDRmODk5NjRjOGQ0Zjk5ODA3YmRlZWZhZTU3OTMzMzc3MzFmYzlmNWE4MjU1In0%3D; expires=Thu, 02-Dec-
2021 03:36:35 GMT; Max-Age=7200; path=/; samesite=lax
Set-Cookie:
caru_session=eyJpdiI6ImpraVNYZUJTS1lpUXFnWFY3RUt4d0E9PSIsInZhbHVlIjoiMmlpdVBlYjlwTmk5UkVkMWFsQnBZY1dibnBpd0xuUmdiQWFtellkV0NET
WtLczdWeGxkQmNBNXRWMzNmRkhnT1djVE9yQkNXSFFWSzk1RUk5S2RTNm5aUVdjNHYxT2dXRDdQc05RcjhBNnRRRTJCdGtrWW9PQmpRQVVjYWQ
wbU4iLCJtYWMiOiIzMGExZGFjZmZhNDZhMTJlMDkwMTEwMTc3YzQ0YmRjNjNjODg3ZWJjZDQzODI3MDhkYjQ2OTQ2ZDA0MjdhMjdiIn0%3D;
expires=Thu, 02-Dec-2021 03:36:35 GMT; Max-Age=7200; path=/; httponly; samesite=lax
Content-Length: 394

<!DOCTYPE html>
<html>
```


2.4. https://test-caru.welcometw.com/login

Previous Next

Summary

Severity:	**Medium**
Confidence:	**Firm**
Host:	**https://test-caru.welcometw.com**
Path:	**/login**

Issue detail

The following cookies were issued by the application and do not have the secure flag set:

- **XSRF-TOKEN**
- **caru_session**

The cookies appear to contain session tokens, which may increase the risk associated with this issue. You should review the contents of the cookies to determine their function.

Request 1


```
POST /login HTTP/1.1
Host: test-caru.welcometw.com
Cookie: XSRF-
TOKEN=eyJpdiI6IkY4OUM3M0V6REt4QmZWd3VJRVAwbVE9PSIsInZhbHVlIjoiS3hEa05MUTlYajRSUVhKeHN0cmtCQ2hYb2xqUkdHZ01HVk9UaTUwdU1C
c2dTRFhqM3RlSVkydU50eGpxMnJON2lwdUt3QmpDbkJya3pSK2RKOXVqS2hSWkFvYm80d0FPenFtUFphZWJvOFRtU3YxeG9OTmZ3ZWVDMmZGVm93
NiAiLCJtYWMiOiJlNDc3YTY1YzQwNzBiOTJlOWFjZDI1Nzk1NWE4MjBjMjU4ZWZjYWFlODQzZWFjM2I2M2MzMzVkMGZlYWJhMDdkIn0%3D;
caru_session=eyJpdiI6IkR1RXczazFZdk05S2RlQTVKSGtrNEE9PSIsInZhbHVlIjoiV3crcUp5OE5yNDI4S09Rd2xkUEVGNjV1U1IUR0ITMXRzRENMeVpiS3Fu
MnBBKzMxUCtkYjFvcCtGMWVPcmNMVUZoeDMrMkRjbzhaMS9LZzFrclpLS0pYUDczN1A5M2tLYnp3dFlSRnd1UU9td0EwbWJaZEdDLzduRTYwRmo3YnliL
CJtYWMiOiI0ZTNhNGJjODk0MzFiZjNlOGQ4YmE3OTc3YmFhOTJlNzdlNjgyNWFhMmRkOGExMThlYjc1MWUyZTg2NzA3N2YyIn0%3D
Content-Length: 113
Cache-Control: max-age=0
Sec-Ch-Ua: " Not A;Brand";v="99", "Chromium";v="96", "Google Chrome";v="96"
Sec-Ch-Ua-Mobile: ?0
Sec-Ch-Ua-Platform: "Windows"
Dnt: 1
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/96.0.4664.45 Safari/537.36
Origin: https://test-caru.welcometw.com
Content-Type: application/x-www-form-urlencoded
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
Sec-Fetch-Site: same-origin
```


Response 1


```
HTTP/1.1 302 Found
Server: nginx/1.21.3
Content-Type: text/html; charset=UTF-8
Connection: close
Cache-Control: no-cache, private
Date: Thu, 02 Dec 2021 01:32:14 GMT
Location: https://test-caru.welcometw.com/admin
Set-Cookie: XSRF-
TOKEN=eyJpdiI6IkpDcVU2Q2pqOGJlYWRySTFUTGpjWHc9PSIsInZhbHVlIjoiWnBMMkJTY3U0d2F6UEtYUFlGWmthVTRlMU5LNFlhS2s0R2k2dEd6ekJkel
EybVVrUUFXdkVOWFRkNzlCRHRZNkt6a29FMm9MN3J4a0MranpWcjI3MjZaZEx6Q2p3dnJOb1kwQ2I2UjU1R3hLNGpaM2RWYkFhRmc2bXlLbFZOSkYiLC
JtYWMiOiI0ZTE4NGM1MWQzNjljYTFiYTMyNmEyZGI1MzI0MjFlZWQ5ZWNlNjczNDIxNGI2YzFlZjM1NDlhYzU5MzQwYmE1In0%3D; expires=Thu, 02-Dec-
2021 03:32:14 GMT; Max-Age=7200; path=/; samesite=lax
Set-Cookie:
caru_session=eyJpdiI6IlpLbVpVM0s5TlVVQVFyOVBzZ3NSUkE9PSIsInZhbHVlIjoiSFoxVXRJQWlUOVoxWjhjaWNNR1VUMzI0OXg5cHB3MkNPT3puUzhmb
0YwT3QyK2hDa0VMVUtzYXRHQWFLckkzL3VweXh2K20zZ203UVBBcU10L3gyMnFqdDc4akhzbDJKRnkwRlYvWUxveGE5VElzd1dHS0dzMGtETFV0MjNjU
```

```
<!DOCTYPE html>
<html>
```

2.5. https://test-caru.welcometw.com/login

Previous Next

Summary

Severity:	**Information**
Confidence:	**Certain**
Host:	**https://test-caru.welcometw.com**
Path:	**/login**

Issue detail

The following cookie was issued by the application and does not have the secure flag set:

- remember_web_59ba36addc2b2f9401580f014c7f58ea4e30989d

The cookie does not appear to contain a session token, which may reduce the risk associated with this issue. You should review the contents of the cookie to determine its function.

Request 1

```
POST /login HTTP/1.1
Host: test-caru.welcometw.com
Cookie: XSRF-
TOKEN=eyJpdiI6IkZWQ0h5K1JldWFHQ28rY25sSzlrVlE9PSIsInZhbHVlIjoiaWxxT3FIQTE0WUZEazcrRVE4SUhNSDVTZllrRnJHMVcwalRZelVoQ3hibFFTVH
p4OUt6Q3k1S2YxVE1FT25uRzJ3aWlkRExsRXdCV0Rib0FKbDhVOTI5NExseXNGTzZSRmMwSHM0L0kyRzVJcC9ZWmNRdkd6WjBnMDgwMVRyUzgiLCJt
YWMiOiJhMmU1ZjI0MzUwMTM4MzkwYzE5MDI4NGRhOTEyNGQwMmMwYTdmMTVhMjNjNzliOWMxNTMzM2EwY2Q3NDdjMDdhIn0%3D;
caru_session=eyJpdiI6IlJQc2pPNzdYZ0V2L1lURDRIM0VGVGc9PSIsInZhbHVlIjoiZ0dzUkJHS0hueXUwbWQxZ2VPMGpmdWNCdlhaR1RQaHhFSlFXeTlwV
zQyS0h2a0lrUWtpYXl0cTQxaFJ6Rzdycng0azA5VWt5TmpWRngyelB2dWZNcEY1c1JOSDdHbSsxV3pramdmNnZ5N2hRejdnNW8yWlNZWHNPWnBMTmhU
ZXYiLCJtYWMiOiIxYWM0MjFkNTRlYzI5MDA1MWI0ZDg0NjFiZTgxYWNiZjgyY2ExMjVjNTM5ZTc4ZDVhYmM0ODc5OTBkNWIwMzU3In0%3D
Content-Length: 113
Cache-Control: max-age=0
Sec-Ch-Ua: " Not A;Brand";v="99", "Chromium";v="96", "Google Chrome";v="96"
Sec-Ch-Ua-Mobile: ?0
Sec-Ch-Ua-Platform: "Windows"
Origin: https://test-caru.welcometw.com
Upgrade-Insecure-Requests: 1
Dnt: 1
Content-Type: application/x-www-form-urlencoded
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/96.0.4664.45 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
Sec-Fetch-Site: same-origin
```

Response 1

```
HTTP/1.1 302 Found
Server: nginx/1.21.3
Content-Type: text/html; charset=UTF-8
Connection: close
Cache-Control: no-cache, private
Date: Thu, 02 Dec 2021 01:37:48 GMT
Location: https://test-caru.welcometw.com/admin
Set-Cookie: XSRF-
TOKEN=eyJpdiI6Ik5sUjJZQWQxeWs1aWpNQkVFbnovRmc9PSIsInZhbHVlIjoiTnVWcFhqSWxRM2VyeDlvVUlWZFk1WlFDTW5PWW8yZ0h4UVFpMU55MW
NBN2JXTlJ2OUZKeDR2T0pzSDkwVU5PYUUxcGhPc1FEMlZMOVo5VHNDSFR2VmkxRUF6QnZTZHNGVFRQTVB5blkrRHFyZnJMelNmbU9VRTFTbWg2M
nA1UG8iLCJtYWMiOiI0OTdlYjM4YmM3NjQ2YzUxZTVkNzU0NzFlNjM0MDAyNjY2YWFmYTVlYTk4N2I2M2JiOGM5OTEyYzdlMGYxMWIzIn0%3D;
expires=Thu, 02-Dec-2021 03:37:48 GMT; Max-Age=7200; path=/; samesite=lax
Set-Cookie:
caru_session=eyJpdiI6IklxZ3VSVTZLZEs1QmFkSHRvSERranc9PSIsInZhbHVlIjoiZk9TY3ZRMVg3WHNCV1ZZYkRmYjBLbUkvVFJZOGdpMk1SN1hINUpIY1
VzNmFNMDEzQ3F6K1lBZjRINEsycytLSHlzcjUvQTBMaExxRZGsxRGMxdEhWejFjTEgwY1lBMUVtYWxVY1A5VzVqRktSUlloN28vSHBCMDZSQXptT0pYZGEi
LCJtYWMiOiI3NDJmNThlODZhZjVkNTFhYzJjOWU3ZTQyYWM0ZTI0ZDA4ODM4Yjc4NjYwN2E4ZmM3ZTUyYTQyZmU2ZjRmMzdkIn0%3D; expires=Thu,
02-Dec-2021 03:37:48 GMT; Max-Age=7200; path=/; httponly; samesite=lax
Set-Cookie:
remember_web_59ba36addc2b2f9401580f014c7f58ea4e30989d=eyJpdiI6Im1jNWltZERONURQYUc5SzI0SXowN2c9PSIsInZhbHVlIjoiUi95RHp6RTh1S0RW
d0dCTkRrZWUvd0hPb1lSb0E3a0oybStuR2dVT3dIdnpqbjRsUzVMYTdWVUN0U0libjE2OXp4Q2dIUG1ER3JhZjY1WXJTZG9XYldhNG5UU0FFUUZNRDJNV
```

3. Cookie without HttpOnly flag set

Previous Next

There are 3 instances of this issue:

- /
- /admin
- /login

Issue background

If the HttpOnly attribute is set on a cookie, then the cookie's value cannot be read or set by client-side JavaScript. This measure makes certain client-side attacks, such as cross-site scripting, slightly harder to exploit by preventing them from trivially capturing the cookie's value via an injected script.

Issue remediation

There is usually no good reason not to set the HttpOnly flag on all cookies. Unless you specifically require legitimate client-side scripts within your application to read or set a cookie's value, you should set the HttpOnly flag by including this attribute within the relevant Set-cookie directive.

You should be aware that the restrictions imposed by the HttpOnly flag can potentially be circumvented in some circumstances, and that numerous other serious attacks can be delivered by client-side script injection, aside from simple cookie stealing.

References

- Web Security Academy: Exploiting XSS vulnerabilities
- HttpOnly effectiveness

Vulnerability classifications

- CWE-16: Configuration
- CAPEC-31: Accessing/Intercepting/Modifying HTTP Cookies

3.1. https://test-caru.welcometw.com/

Previous Next

Summary

Severity:	**Low**
Confidence:	**Firm**
Host:	**https://test-caru.welcometw.com**
Path:	**/**

Issue detail

The following cookie was issued by the application and does not have the HttpOnly flag set:

- **XSRF-TOKEN**

The cookie appears to contain a session token, which may increase the risk associated with this issue. You should review the contents of the cookie to determine its function.This issue was found in multiple locations under the reported path.

Request 1

```
GET /facebook/auth HTTP/1.1
Host: test-caru.welcometw.com
Accept-Encoding: gzip, deflate
Accept: */*
Accept-Language: en
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/95.0.4638.54 Safari/537.36
Connection: close
```

Response 1

```
HTTP/1.1 302 Found
Server: nginx/1.21.3
Content-Type: text/html; charset=UTF-8
```

```
Date: Thu, 02 Dec 2021 02:29:12 GMT
Location: https://www.facebook.com/v3.3/dialog/oauth?client_id=1438080078283348&redirect_uri=https%3A%2F%2Ftest-caru.welcometw.com%2Ffacebook%2Fauthcallback&scope=email&response_type=code&state=HAQptkGrfQl0IFLtEhOQBVybIB57SbFs0Vb7ZuoV
Set-Cookie: XSRF-TOKEN=eyJpdiI6InNnMDJyRmU3TnlKU0ZYa0FzYVprbWc9PSIsInZhbHVlIjoiOFhwbENmSHo0a29Wc3lSNXRkVmhTRkptQ1FJaDJlVU0vcTlEaVE2RWtseGJDVnFEUHZJUHZ6L1c2cG8vUG5yQUs0Vk9hUDQrZDdjaUUzbHo4eXAzd1FNRHg0eEZXWGhDVlZqcWpjUDY4UlJCdkdCNld1WVNodmtHOThtVERTd20iLCJtYWMiOiJlZDdmMTZkYTA4MzZlM2IwMGY1Nzk1ZTJhZDlmZDcwYzFmOWVkZGViZDIzYjEyOGE3YmNmNzlyMWYwZGU3YTU5In0%3D; expires=Thu, 02-Dec-2021 04:29:12 GMT; Max-Age=7200; path=/; samesite=lax
Set-Cookie: caru_session=eyJpdiI6IkdtTUZvVU1sdVBlomlSR2VTZmY0SVE9PSIsInZhbHVlIjoidStGR1IndFZnUjVlQ2NjMkMzVlBiYWpnT3A5Z0dCZERwbWlzR0RrSmNiZG56SkZEdmlVak5xejhORE1aQ0VWL1doSjFFQnZzOWovU2tSelM5WXpKSVNaYXZvaEpKSCtKQ1hEVXpjSjlpYnd2VUQ4eFdUN0pNYVo2SkUxOENQZ0ciLCJtYWMiOiJiZTMxNTVkMjc2OTU1YTdlMjlxMmQ5ZjQ2NzY0MmQ4OTkzOGQ2NzcxMGFiNzM5NWZmYzgzYTMxOTJhYzc4ZTI5In0%3D; expires=Thu, 02-Dec-2021 04:29:12 GMT; Max-Age=7200; path=/; httponly; samesite=lax
Content-Length: 1202

<!DOCTYPE html>
```

Request 2

```
POST /login HTTP/1.1
Host: test-caru.welcometw.com
Cookie: XSRF-TOKEN=eyJpdiI6IkZWQ0h5K1JldWFHQ28rY25sSzlrVlE9PSIsInZhbHVlIjoiaWxxT3FIQTE0WUZEazcrRVE4SUhNSDVTZllrRnJHMVcwalRZelVoQ3hibFFTVHp4OUt6Q3k1S2YxVE1FT25uRzJ3aWlkRExsRXdCV0Rib0FKbDhVOTI5NExseXNGTzZSRmMwSHM0L0kyRzVJcC9ZWmNRdkd6WjBnMDgwMVRyUzgiLCJtYWMiOiJhMmU1ZjI0MzUwMTM4MzkwYzE5MDI4NGRhOTEyNGQwMmMwYTdmMTVhMjNjNzliOWMxNTMzM2EwY2Q3NDdjMDdhIn0%3D; caru_session=eyJpdiI6IlJQc2pPNzdYZ0V2L1lURDRlM0VGVGc9PSIsInZhbHVlIjoiZ0dzUkJHS0hueXUwbWQxZ2VPMGpmdWNCdlhaR1RQaHhFSlFXeTlwVzQyS0h2a0lrUWtpYXl0cTQxaFJ6Rzdycng0azA5VWt5TmpWRngyelB2dWZNcEY1c1JOSDdHbSsxV3pramdmNnZ5N2hRejdnNW8yWlNZWHNPWnBMTmhUZXYiLCJtYWMiOilxYWM0MjFkNTRlYzI5MDA1MWI0ZDg0NjFiZTgxYWNiZjgyY2ExMjVjNTM5ZTc4ZDVhYmM0ODc5OTBkNWIwMzU3In0%3D
Content-Length: 113
Cache-Control: max-age=0
Sec-Ch-Ua: " Not A;Brand";v="99", "Chromium";v="96", "Google Chrome";v="96"
Sec-Ch-Ua-Mobile: ?0
Sec-Ch-Ua-Platform: "Windows"
Origin: https://test-caru.welcometw.com
Upgrade-Insecure-Requests: 1
Dnt: 1
Content-Type: application/x-www-form-urlencoded
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/96.0.4664.45 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
Sec-Fetch-Site: same-origin
```

Response 2

```
HTTP/1.1 302 Found
Server: nginx/1.21.3
Content-Type: text/html; charset=UTF-8
Connection: close
Cache-Control: no-cache, private
Date: Thu, 02 Dec 2021 01:37:48 GMT
Location: https://test-caru.welcometw.com/admin
Set-Cookie: XSRF-TOKEN=eyJpdiI6Ik5sUjJZQWQxeWs1aWpNQkVFbnovRmc9PSIsInZhbHVlIjoiTnVWcFhqSWxRM2VyeDlvVUlWZFk1WlFDTW5PWW8yZ0h4UVFpMU55MWNBN2JXTlJ2OUZKeDR2T0pzSDkwVU5PYUUxcGhPc1FEMlZMOVo5VHNDSFR2VmkxRUF6QnZTZHNGVFRQTVB5blkrRHFyZnJMelNmbU9VRTFTbWg2MnA1UG8iLCJtYWMiOiI0OTdlYjM4YmM3NjQ2YzUxZTVkNzU0NzFlNjM0MDAyNjY2YWFmYTVlYTk4N2I2M2JiOGM5OTEyYzdlMGYxMWIzIn0%3D; expires=Thu, 02-Dec-2021 03:37:48 GMT; Max-Age=7200; path=/; samesite=lax
Set-Cookie: caru_session=eyJpdiI6IklxZ3VSVTZLZEs1QmFkSHRvSERranc9PSIsInZhbHVlIjoiZk9TY3ZRMVg3WHNCV1ZZYkRmYjBLbUkvVFJZOGdpMk1SN1hlNUplY1VzNmFNMDEzQ3F6K1lBZjRINEsycytLSHlzcjUvQTBMaExxRZGsxRGMxdEhWejFjTEgwY1lBMUVtYWxVYlA5VzVqRktSUlloN28vSHBCMDZSQXptT0pYZGEiLCJtYWMiOiI3NDJmNThlODZhZjVkNTFhYzJjOWU3ZTQyYWM0ZTI0ZDA4ODM4Yjc4NjYwN2E4ZmM3ZTUyYTQyZmU2ZjRmMzdkIn0%3D; expires=Thu, 02-Dec-2021 03:37:48 GMT; Max-Age=7200; path=/; httponly; samesite=lax
Set-Cookie: remember_web_59ba36addc2b2f9401580f014c7f58ea4e30989d=eyJpdiI6Im1jNWltZERONURQYUc5SzI0SXowN2c9PSIsInZhbHVlIjoiUi95RHp6RTh1S0RWd0dCTkRrZWUvd0hPb1lSb0E3a0oybStuR2dVT3dldnpqbjRsUzVMYTdWVUN0U0libjE2OXp4Q2dlUG1ER3JhZjY1WXJTZG9XYldhNG5UU0FFUUZNRDJNVk9rdWhSakqvMEZLUWFn4M3BtZGpqRHd1clB0alFrNmtXTGFOVnhqbkl5cDh1Y0VpVWzV3BRdzVnbGRiL09xVk9mWTl0NXRJRExaQVpieHpnRUFVTZwh2h
```

Request 3

```
POST /login HTTP/1.1
Host: test-caru.welcometw.com
Cookie: XSRF-TOKEN=eyJpdiI6IkY4OUM3M0V6REt4QmZWd3VJRVAwbVE9PSIsInZhbHVlIjoiS3hEa05MUTlYajRSUVhKeHN0cmtCQ2hYb2xqUkdHZ01HVk9UaTUwdU1Cc2dTRFhqM3RlSVkydU50eGpxMnJON2lwdUt3QmpDbkJya3pSK2RKOXVqS2hSWkFvYm80d0FPenFtUFphZWJvOFRtU3YxeG9OTmZ3ZWVDMmZGVm93NlAiLCJtYWMiOiJlNDc3YTY1YzQwNzBiOTJlOWFjZDI1Nzk1NWE4MjBjMjU4ZWZjYWFlODQzZWFjM2I2M2MzMzVkMGZlYWJhMDdkIn0%3D; caru_session=eyJpdiI6IkR1RXczazFZdk05S2RlQTVKSGtrNEE9PSIsInZhbHVlIjoiV3crcUp5OE5yNDI4S09Rd2xkUEVGNjV1U1lUR0lTMXRzRENMeVpiS3FuMnBBKzMxUCtkYjFvcCtGMWVPcmNMVUZoeDMrMkRjbzhaMS9LZzFrclpLS0pYUDczN1A5M2tLYnp3dFlSRnd1UU9td0EwbWJaZEdDLzduRTYwRmo3YnliIiwibWFjIjoiOTBiZTNhNGJjODk0MzFiZjNlOGQ4YmE3OTc3YmFhOTJlNzdlNjgyNWFhMmRkOGExMThlYjc1MWUyZTg2NzA3N2YyIn0%3D
Content-Length: 113
Cache-Control: max-age=0
Sec-Ch-Ua: " Not A;Brand";v="99", "Chromium";v="96", "Google Chrome";v="96"
Sec-Ch-Ua-Mobile: ?0
Sec-Ch-Ua-Platform: "Windows"
```

Response 1

```
HTTP/1.1 302 Found
Server: nginx/1.21.3
Content-Type: text/html; charset=UTF-8
Connection: close
Cache-Control: no-cache, private
Date: Thu, 02 Dec 2021 01:36:35 GMT
Location: https://test-caru.welcometw.com/login
Set-Cookie: XSRF-
TOKEN=eyJpdiI6IklkVVNncnRhQXprbHNtbGhHa3FUblE9PSIsInZhbHVlIjoiTUkyTWdDcUlZWUhKVWJXdk40bHltN29pVlBiajMzVXlyZFBtRVRGWi9zSS9NYV
BNbEVubGhpRUEwV3NIcitwb1FYaE5KMjZHUExrcGlNR2kxRG9IVVlTUXRkSng4emxuZlZhdndzSitFc0xSUUt4T3RaTlRUZ0VBemJNVHZ1N1YiLCJtYWMiOi
JiMWRhZmNiMWE3NzNiZTkyNDcwNDRmODk5NjRjOGQ0Zjk5ODA3YmRlZWZhZTU3OTMzMzc3MzFmYzlmNWE4MjU1In0%3D; expires=Thu, 02-Dec-
2021 03:36:35 GMT; Max-Age=7200; path=/; samesite=lax
Set-Cookie:
caru_session=eyJpdiI6ImpraVNYZUJTS1lpUXFnWFY3RUt4d0E9PSIsInZhbHVlIjoiMmlpdVBIYjlwTmk5UkVkMWFsQnBZY1dibnBpd0xuUmdiQWFtellkV0NET
WtLczdWeGxkQmNBNXRWMzNmRkhnT1djVE9yQkNXSFFWSzk1RUk5S2RTNm5aUVdjNHYxT2dXRDdQc05RcjhBNnRRRTJCdGtrWW9PQmpRQVVjYWQ
wbU4iLCJtYWMiOiIzMGExZGFjZmZhNDZhMTJlMDkwMTEwMTc3YzQ0YmRjNjNjODg3ZWJjZDQzODI3MDhkYjQ2OTQ2ZDA0MjdhMjdiIn0%3D;
expires=Thu, 02-Dec-2021 03:36:35 GMT; Max-Age=7200; path=/; httponly; samesite=lax
Content-Length: 394

<!DOCTYPE html>
<html>
```

3.3. https://test-caru.welcometw.com/login

Previous Next

Summary

!	Severity:	**Low**
	Confidence:	**Firm**
	Host:	**https://test-caru.welcometw.com**
	Path:	**/login**

Issue detail

The following cookie was issued by the application and does not have the HttpOnly flag set:

- **XSRF-TOKEN**

The cookie appears to contain a session token, which may increase the risk associated with this issue. You should review the contents of the cookie to determine its function.

Request 1

```
POST /login HTTP/1.1
Host: test-caru.welcometw.com
Cookie: XSRF-
TOKEN=eyJpdiI6IkY4OUM3M0V6REt4QmZWd3VJRVAwbVE9PSIsInZhbHVlIjoiS3hEa05MUTlYajRSUVhKeHN0cmtCQ2hYb2xqUkdHZ01HVk9UaTUwdU1C
c2dTRFhqM3RISVkydU50eGpxMnJON2lwdUt3QmpDbkJya3pSK2RKOXVqS2hSWkFvYm80d0FPenFtUFphZWJvOFRtU3YxeG9OTmZ3ZWVDMmZGVm93
NlAiLCJtYWMiOiJlNDc3YTY1YzQwNzBiOTJlOWFjZDI1Nzk1NWE4MjBjMjU4ZWZjYWFlODQzZWFjM2I2M2MzMzVkMGZlYWJhMDdkIn0%3D;
caru_session=eyJpdiI6IkR1RXczazFZdk05S2RIQTVKSGtrNEE9PSIsInZhbHVlIjoiV3crcUp5OE5yNDI4S09Rd2xkUEVGNjV1U1lUR0lTMXRzRENMeVpiS3Fu
MnBBKzMxUCtkYjFvcCtGMWVPcmNMVUZoeDMrMkRjbzhaMS9LZzFrclpLS0pYUDczN1A5M2tLYnp3dFlSRnd1UU9td0EwbWJaZEdDLzduRTYwRmo3YnliL
CJtYWMiOiI0ZTNhNGJjODk0MzFiZjNlOGQ4YmE3OTc3YmFhOTJlNzdlNjgyNWFhMmRkOGExMThlYjc1MWUyZTg2NzA3N2YyIn0%3D
Content-Length: 113
Cache-Control: max-age=0
Sec-Ch-Ua: " Not A;Brand";v="99", "Chromium";v="96", "Google Chrome";v="96"
Sec-Ch-Ua-Mobile: ?0
Sec-Ch-Ua-Platform: "Windows"
Dnt: 1
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/96.0.4664.45 Safari/537.36
Origin: https://test-caru.welcometw.com
Content-Type: application/x-www-form-urlencoded
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
Sec-Fetch-Site: same-origin
```

Response 1

```
HTTP/1.1 302 Found
Server: nginx/1.21.3
Content-Type: text/html; charset=UTF-8
```

```
Set-Cookie: XSRF-
TOKEN=eyJpdiI6IkpDcVU2Q2pqOGJlYWRySTFUTGpjWHc9PSIsInZhbHVlIjoiWnBMMkJTY3U0d2F6UEtYUFlGWmthVTRIMU5LNFlhS2s0R2k2dEd6ekJkel
EybVVrUUFXdkVOWFRkNzlCRHRZNkt6a29FMm9MN3J4a0MranpWcji3MjZaZEx6Q2p3dnJOb1kwQ2l2UjU1R3hLNGpaM2RWYkFhRmc2bXlLbFZOSkYiLC
JtYWMiOiI0ZTE4NGM1MWQzNjljYTFiYTMyNmEyZGI1MzI0MjFlZWQ5ZWNlNjczNDIxNGI2YzFlZjM1NDlhYzU5MzQwYmE1In0%3D; expires=Thu, 02-Dec-
2021 03:32:14 GMT; Max-Age=7200; path=/; samesite=lax
Set-Cookie:
caru_session=eyJpdiI6IlpLbVpVM0s5TlVVQVFyOVBzZ3NSUkE9PSIsInZhbHVlIjoiSFoxVXRJQWlUOVoxWjhjaWNNR1VUMzI0OXg5cHB3MkNPT3puUzhmb
0YwT3QyK2hDa0VMVUtzYXRHQWFLckkzL3VweXh2K20zZ203UVBBcU10L3gyMnFqdDc4akhzbDJKRnkwRlYvWUxveGE5VEIzd1dHS0dzMGtETFV0MjNjU
0YiLCJtYWMiOiI1YmQ4OTRkZTBjNjU0N2U0MDUxNTM1NTBlMGEwZTIzZWUxYTNjY2RkYTA0N2M1NDBhNmNmMDI5NjE5ZDA5MTEyIn0%3D;
expires=Thu, 02-Dec-2021 03:32:14 GMT; Max-Age=7200; path=/; httponly; samesite=lax
Content-Length: 394

<!DOCTYPE html>
<html>
```

4. Password field with autocomplete enabled

Previous Next

Summary

Severity:	Low
Confidence:	Certain
Host:	https://test-caru.welcometw.com
Path:	/login

Issue detail

The page contains a form with the following action URL:

- https://test-caru.welcometw.com/login

The form contains the following password field with autocomplete enabled:

- password

Issue background

Most browsers have a facility to remember user credentials that are entered into HTML forms. This function can be configured by the user and also by applications that employ user credentials. If the function is enabled, then credentials entered by the user are stored on their local computer and retrieved by the browser on future visits to the same application.

The stored credentials can be captured by an attacker who gains control over the user's computer. Further, an attacker who finds a separate application vulnerability such as cross-site scripting may be able to exploit this to retrieve a user's browser-stored credentials.

Issue remediation

To prevent browsers from storing credentials entered into HTML forms, include the attribute **autocomplete="off"** within the FORM tag (to protect all form fields) or within the relevant INPUT tags (to protect specific individual fields).

Please note that modern web browsers may ignore this directive. In spite of this there is a chance that not disabling autocomplete may cause problems obtaining PCI compliance.

Vulnerability classifications

- CWE-200: Information Exposure

Request 1

```
GET /login HTTP/1.1
Host: test-caru.welcometw.com
Cookie: XSRF-
TOKEN=eyJpdiI6IkFVTlBWYjYyeVJUbW5waC9rZktBM2c9PSIsInZhbHVlIjoiOUY5bkdhaEVCTUdoempxNXczK2RIRXlSNGpXK3NVdjVCUVVzdWFOcnVyMX
JpTER2RCs2aDJJbEhITWM3S2RzeVNPZGpCNERzVjdPOGRWZFNWRUc1ZUU1cTVvOHZXQ2NEOWk4WjlwNXRmeFpLYks4Zkd0Snp4RWlYVjR2YXNU
MGkiLCJtYWMiOiI2OWQ1Mzc3OWUwNTBkMDE3ZjVjY2QzMmI3N2UwZTc2NjVhMTBhMGNjNzVhYjZhMDA3MDJhNDEzYzdjNmNkZmNlIn0%3D;
caru_session=eyJpdiI6IlU2NEFTcWNsbFNudjluODhlTU8xdFE9PSIsInZhbHVlIjoicEptRDFwWnhHQ216dHpBVHZ3MzR0ZTVaT1VUbFQxZXJsNVJVaDFWS2
gyQ2FNZ2k5RVljZ2plT2JEZ0tdFFDKzErZUpkeFFMK2pmVFVkWlRNSERwTUYvSkVPK3M4NXZhWFZRZy9pLzhqNyszaEwrSmhxa29XMFloalFyS1Z6MWEi
LCJtYWMiOiJiMmY2ODY2NjQ1OWEyMTM5MTQ3NzYxODM5NjA2ZmFmZWZmY2M4OTQ1NDM3Y2NjZjVjNzIzOWE4YzFmNjc4N2YyIn0%3D
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
Dnt: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/96.0.4664.45 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: navigate
```

```
Sec-Fetch-User: ?1
Sec-Fetch-Dest: document
Sec-Ch-Ua: " Not A;Brand";v="99", "Chromium";v="96", "Google Chrome";v="96"
Sec-Ch-Ua-Mobile: ?0
Sec-Ch-Ua-Platform: "Windows"
```

Response 1

```
HTTP/1.1 200 OK
Server: nginx/1.21.3
Content-Type: text/html; charset=UTF-8
Connection: close
Cache-Control: no-cache, private
Date: Thu, 02 Dec 2021 01:36:38 GMT
Set-Cookie: XSRF-
TOKEN=eyJpdiI6IkZWQ0h5K1JldWFHQ28rY25sSzlrVlE9PSIsInZhbHVlIjoiaWxoT3FIQTE0WUZEazcrRVE4SUhNSDVTZlIrRnJHMVcwalRZelVoQ3hibFFTVHp4OUt6Q3k1S2YxVE1FT25uRzJ3aWlkRExsRXdCV0Rib0FKbDhVOTI5NExseXNGTzZSRmMwSHM0L0kyRzVJcC9ZWmNRdkd6WjBnMDgwMVRyUzgiLCJtYWMiOiJhMmU1ZjI0MzUwMTM4MzkwYzE5MDI4NGRhOTEyNGQwMmMwYTdmMTVhMjNjNzliOWMxNTMzM2EwY2Q3NDdjMDdhIn0%3D; expires=Thu, 02-Dec-2021 03:36:38 GMT; Max-Age=7200; path=/; samesite=lax
Set-Cookie:
caru_session=eyJpdiI6IlJQc2pPNzdYZ0V2L1lURDRIM0VGVGc9PSIsInZhbHVlIjoiZ0dzUkJHS0hueXUwbWQxZ2VPMGpmdWNCdlhaR1RQaHhFSlFXeTlwVzQyS0h2a0lrUWtpYXl0cTQxaFJ6Rzdycng0azA5VWt5TmpWRngyelB2dWZNcEY1c1JOSDdHbSsxV3pramdmNnZ5N2hRejdnNW8yWlNZWHNPWnBMTmhUZXYiLCJtYWMiOiIxYWM0MjFkNTRlYzI5MDA1MWI0ZDg0NjFiZTgxYWNiZjgyY2ExMjVjNTM5ZTc4ZDVhYmM0ODc5OTBkNWIwMzU3In0%3D; expires=Thu, 02-Dec-2021 03:36:38 GMT; Max-Age=7200; path=/; httponly; samesite=lax
Content-Length: 3427

<!doctype html>
<html lang="zh-hant">
<head>
```

5. Ajax request header manipulation (DOM-based)

Previous Next

Summary

Severity:	**Low**
Confidence:	**Firm**
Host:	**https://test-caru.welcometw.com**
Path:	**/**

Issue detail

The application may be vulnerable to DOM-based Ajax request header manipulation. Data is read from **document.cookie** and passed to **xhr.setRequestHeader.value**.

Issue background

DOM-based vulnerabilities arise when a client-side script reads data from a controllable part of the DOM (for example, the URL) and processes this data in an unsafe way.

Ajax request header manipulation arises when a script writes controllable data into a header of an Ajax request that is issued using XmlHttpRequest. An attacker may be able to use the vulnerability to construct a URL that, if visited by another application user, will set an arbitrary header in the subsequent Ajax request.

The potential impact of the vulnerability depends on the role of specific HTTP headers in the server-side application's processing of the Ajax request. If the header is used to control the behavior that results from the Ajax request, then the attacker may be able to cause the user to perform unintended actions by manipulating the header.

Burp Suite automatically identifies this issue using static code analysis, which may lead to false positives that are not actually exploitable. The relevant code and execution paths should be reviewed to determine whether this vulnerability is indeed present, or whether mitigations are in place that would prevent exploitation.

Issue remediation

The most effective way to avoid DOM-based Ajax request header manipulation vulnerabilities is not to dynamically set Ajax request headers using data that originated from any untrusted source. This behavior should never be implemented for headers that have any role in controlling the effects of privileged actions within the application.

References

- Web Security Academy: Ajax request header manipulation (DOM-based)

Vulnerability classifications

- CWE-116: Improper Encoding or Escaping of Output
- CAPEC-6: Argument Injection

Request 1

```
GET / HTTP/1.1
Host: test-caru.welcometw.com
Accept-Encoding: gzip, deflate
Accept: */*
Accept-Language: en
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/95.0.4638.54 Safari/537.36
Connection: close
```

Response 1

```
HTTP/1.1 200 OK
Server: nginx/1.21.3
Content-Type: text/html; charset=UTF-8
Connection: close
Cache-Control: no-cache, private
Date: Thu, 02 Dec 2021 02:29:12 GMT
Set-Cookie: XSRF-
TOKEN=eyJpdiI6InR1YnhEaGIzcWN5d3JDd2ozQ0NlQ3c9PSIsInZhbHVlIjoiWGxZNm9Tb2pnVFlQM20vQ3dNejdSbTVNdU02c0liRDYxdmZRRUhTSWMyZF
VRYkxOeU0rSUk3NitWV2tKYlFjZUFRdG1JUXZEcWdhSC91MW5UaHFqdmJsQmVoQnBUZk1OekoyL3N2cDMzNzRMcHNNczRpTGhFYnB2dlpnTVMvb1ciL
CJtYWMiOiI1NzBiNGI5OTMxNmE4M2FhNDZkNDc2NmFhNjQ4YjlkZDhjYjA4ZGQwNTY2YjEzYjQxMTBlMGMzN2YxNzJiNGFmIn0%3D; expires=Thu, 02-
Dec-2021 04:29:12 GMT; Max-Age=7200; path=/; samesite=lax
Set-Cookie:
caru_session=eyJpdiI6InZhd3YzUS9vNGI4aDVoYTJtS3RCc0E9PSIsInZhbHVlIjoiMzN5U1dYV1Y3OGZrV24vdTVsKy9NcEpYZkJTU3orSHg0ZnNhbXEwWjZ
LUTBTcEg0TGVieENiMjFuaXRTSCtFSWUzd2ZCQzdUR1kwczBlbUZUT2RXbjRnUitzdFVWYmZuNEJieE1qMkl0eFFBUlF2MDNOdndUMnl0V0lzd1ROR2wiL
CJtYWMiOiI1YWEwZTAxNGQ3NWMyMjYyZmRmODc2MmQzZGMwZjQzMTJmYWFlZGJlODRiZmRjNzhhYTgxNml1ZjIxY2JkMjlmIn0%3D; expires=Thu, 02-
Dec-2021 04:29:12 GMT; Max-Age=7200; path=/; httponly; samesite=lax
Content-Length: 7873

<!doctype html>
<html lang="zh-hant">
<head>
```

Dynamic analysis

Data is read from **document.cookie** and passed to **xhr.setRequestHeader.value**.

The following value was injected into the source:

```
d95s1a9c9c%2527%2522`'"/d95s1a9c9c/><d95s1a9c9c/\>blr1rxhdjj&
```

The previous value reached the sink as:

```
d95s1a9c9c%27%22`'"/d95s1a9c9c/><d95s1a9c9c/\>blr1rxhdjj&
```

The stack trace at the source was:

```
at Object.VazNf (<anonymous>:1:181933)
at Object.hrNdT (<anonymous>:1:572090)
at HTMLDocument.Object.<computed>.get (<anonymous>:1:589232)
at Object.read (https://test-caru.welcometw.com/js/app.js:7461:32)
at dispatchXhrRequest (https://test-caru.welcometw.com/js/app.js:6389:17)
at new Promise (<anonymous>)
at xhrAdapter (https://test-caru.welcometw.com/js/app.js:6291:10)
at dispatchRequest (https://test-caru.welcometw.com/js/app.js:6937:10)
```

The stack trace at the sink was:

```
at Object.UInmG (<anonymous>:1:180817)
at Object.llarH (<anonymous>:1:574598)
at _0x5dfed6 (<anonymous>:1:592957)
at XMLHttpRequest._0x40ae7d.XMLHttpRequest.<computed>.<computed> [as setRequestHeader] (<anonymous>:1:492665)
at setRequestHeader (https://test-caru.welcometw.com/js/app.js:6405:19)
at Object.forEach (https://test-caru.welcometw.com/js/app.js:7963:12)
at dispatchXhrRequest (https://test-caru.welcometw.com/js/app.js:6399:13)
at new Promise (<anonymous>)
at xhrAdapter (https://test-caru.welcometw.com/js/app.js:6291:10)
at dispatchRequest (https://test-caru.welcometw.com/js/app.js:6937:10)
```

This was triggered by a **load** event.

6. Link manipulation (reflected DOM-based)

Previous Next

There are 3 instances of this issue:

- /loginbgoydjwd7u [URL path filename]
- /loginn7mn4v6bek [URL path filename]
- /loginyztjz2hz7e [URL path filename]

Issue background

Reflected DOM-based vulnerabilities arise when data is copied from a request and echoed into the application's immediate response within a part of the DOM that is then processed in an unsafe way by a client-side script. An attacker can leverage the reflection to control a part of the response (for example, a JavaScript string) that can be used to trigger the DOM-based vulnerability.

DOM-based link manipulation arises when a script writes controllable data to a navigation target within the current page, such as a clickable link or the submission URL of a form. An attacker may be able to use the vulnerability to construct a URL that, if visited by another application user, will modify the target of links within the response. An attacker may be able to leverage this to perform various attacks, including:

- Causing the user to redirect to an arbitrary external URL, to facilitate a phishing attack.
- Causing the user to submit sensitive form data to a server controlled by the attacker.
- Causing the user to perform an unintended action within the application, by changing the file or query string associated with a link.
- Bypassing browser anti-XSS defenses by injecting on-site links containing XSS exploits, since browser anti-XSS defenses typically do not operate on on-site links.

Burp Suite automatically identifies this issue using static code analysis, which may lead to false positives that are not actually exploitable. The relevant code and execution paths should be reviewed to determine whether this vulnerability is indeed present, or whether mitigations are in place that would prevent exploitation.

Issue remediation

The most effective way to avoid DOM-based link manipulation vulnerabilities is not to dynamically set the target URLs of links or forms using data that originated from any untrusted source. If the desired functionality of the application means that this behavior is unavoidable, then defenses must be implemented within the client-side code to prevent malicious data from introducing an arbitrary URL as a link target. In general, this is best achieved by using a whitelist of URLs that are permitted link targets, and strictly validating the target against this list before setting the link target.

References

- Web Security Academy: Link manipulation (DOM-based)

Vulnerability classifications

- CWE-20: Improper Input Validation
- CAPEC-153: Input Data Manipulation

6.1. https://test-caru.welcometw.com/loginbgoydjwd7u [URL path filename]

Previous Next

Summary

Severity:	**Low**
Confidence:	**Firm**
Host:	**https://test-caru.welcometw.com**
Path:	**/loginbgoydjwd7u**

Issue detail

The application may be vulnerable to reflected DOM-based link manipulation.

The value of the URL path filename is copied into a JavaScript string literal. The payload **bgoydjwd7u** was submitted in the URL path filename.

The string containing the payload is then passed to **element.setAttribute.href**.

Request 1

```
POST /loginbgoydjwd7u HTTP/1.1
Host: test-caru.welcometw.com
Cookie: XSRF-
TOKEN=eyJpdiI6IkZWQ0h5K1JldWFHQ28rY25sSzlrVlE9PSIsInZhbHVlIjoiaWxoT3FIQTE0WUZEazcrRVE4SUhNSDVTZlIrRnJHMVcwalRZelVoQ3hibFFTVH
p4OUt6Q3k1S2YxVE1FT25uRzJ3aWlkRExsRXdCV0Rib0FKbDhVOTI5NExseXNGTzZSRmMwSHM0L0kyRzVJcC9ZWmNRdkd6WjBnMDgwMVRyUzgiLCJt
YWMiOiJhMmU1ZjI0MzUwMTM4MzkwYzE5MDI4NGRhOTEyNGQwMmMwYTdmMTVhMjNjNzliOWMxNTMzM2EwY2Q3NDdjMDdhIn0%3D;
caru_session=eyJpdiI6IlJQc2pPNzdYZ0V2L1IURDRIM0VGVGc9PSIsInZhbHVlIjoiZ0dzUkJHS0hueXUwbWQxZ2VPMGpmdWNCdlhaR1RQaHhFSlFXeTlwV
zQyS0h2a0IrUWtpYXl0cTQxaFJ6Rzdycng0azA5VWt5TmpWRngyelB2dWZNcEY1c1JOSDdHbSsxV3pramdmNnZ5N2hRejdnNW8yWlNZWHNPWnBMTmhU
ZXYiLCJtYWMiOiIxYWM0MjFkNTRlYzI5MDA1MWI0ZDg0NjFiZTgxYWNiZjgyY2ExMjVjNTM5ZTc4ZDVhYmM0ODc5OTBkNWIwMzU3In0%3D
Content-Length: 113
Cache-Control: max-age=0
Sec-Ch-Ua: " Not A;Brand";v="99", "Chromium";v="96", "Google Chrome";v="96"
Sec-Ch-Ua-Mobile: ?0
Sec-Ch-Ua-Platform: "Windows"
Origin: https://test-caru.welcometw.com
Upgrade-Insecure-Requests: 1
Dnt: 1
Content-Type: application/x-www-form-urlencoded
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/96.0.4664.45 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
Sec-Fetch-Site: same-origin
```

Response 1

```
HTTP/1.1 405 Method Not Allowed
Server: nginx/1.21.3
Content-Type: text/html; charset=UTF-8
Connection: close
allow: GET, HEAD
Cache-Control: no-cache, private
date: Thu, 02 Dec 2021 02:50:44 GMT
Content-Length: 572626

<!doctype html>
<html class="theme-light">
<!--
Symfony\Component\HttpKernel\Exception\MethodNotAllowedHttpException: The POST method is not supported for this route. Supported methods: GET, HEAD.
in
...[SNIP]...
```

Dynamic analysis

The value of the URL path filename is copied into a JavaScript string literal. The payload **bgoydjwd7u** was submitted in the URL path filename.

The string containing the payload is then passed to **element.setAttribute.href**.

The previous value reached the sink as:

```
https://test-caru.welcometw.com/loginxrar2hhq2c
```

The stack trace at the source was:

```
at Object.NdoOX (<anonymous>:1:128317)
at _0x3124b3 (<anonymous>:1:322777)
at Object.sveaB (<anonymous>:1:182488)
at Object.bxgXv (<anonymous>:1:573767)
at _0x5dfed6 (<anonymous>:1:592917)
at Object.UKouh (<anonymous>:1:170365)
at _0x4d375b (<anonymous>:1:508395)
at Object.TgdHu (<anonymous>:1:175531)
at Object.DRoaf (<anonymous>:1:479191)
at HTMLAnchorElement.setAttribute (<anonymous>:1:509426)
at yr (https://test-caru.welcometw.com/login:95:44171)
at _r (https://test-caru.welcometw.com/login:95:43910)
at Array.br (https://test-caru.welcometw.com/login:95:43501)
at v (https://test-caru.welcometw.com/login:95:57584)
at f (https://test-caru.welcometw.com/login:95:56878)
at h (https://test-caru.welcometw.com/login:95:57340)
at f (https://test-caru.welcometw.com/login:95:56863)
at h (https://test-caru.welcometw.com/login:95:57340)
at f (https://test-caru.welcometw.com/login:95:56863)
at a.__patch__ (https://test-caru.welcometw.com/login:95:60891)
at a.t._update (https://test-caru.welcometw.com/login:95:34419)
at a.r (https://test-caru.welcometw.com/login:95:68170)
```

```
at a.Tn.$mount (https://test-caru.welcometw.com/login:95:68341)
at a.Tn.$mount (https://test-caru.welcometw.com/login:95:93802)
at init (https://test-caru.welcometw.com/login:95:19438)
at https://test-caru.welcometw.com/login:95:56472
at f (https://test-caru.welcometw.com/login:95:56749)
```

The stack trace at the sink was:

```
at Object.UInmG (<anonymous>:1:180817)
at Object.llarH (<anonymous>:1:574598)
at _0x5dfed6 (<anonymous>:1:592957)
at Object.UKouh (<anonymous>:1:170365)
at _0x4d375b (<anonymous>:1:508395)
at Object.TgdHu (<anonymous>:1:175531)
at Object.DRoaf (<anonymous>:1:479191)
at HTMLAnchorElement.setAttribute (<anonymous>:1:509426)
at yr (https://test-caru.welcometw.com/login:95:44171)
at _r (https://test-caru.welcometw.com/login:95:43910)
at Array.br (https://test-caru.welcometw.com/login:95:43501)
at v (https://test-caru.welcometw.com/login:95:57584)
at f (https://test-caru.welcometw.com/login:95:56878)
at h (https://test-caru.welcometw.com/login:95:57340)
at f (https://test-caru.welcometw.com/login:95:56863)
at h (https://test-caru.welcometw.com/login:95:57340)
at f (https://test-caru.welcometw.com/login:95:56863)
at a.__patch__ (https://test-caru.welcometw.com/login:95:60891)
at a.t._update (https://test-caru.welcometw.com/login:95:34419)
at a.r (https://test-caru.welcometw.com/login:95:68170)
at mn.get (https://test-caru.welcometw.com/login:95:26728)
at new mn (https://test-caru.welcometw.com/login:95:26646)
at https://test-caru.welcometw.com/login:95:68194
at a.Tn.$mount (https://test-caru.welcometw.com/login:95:68341)
at a.Tn.$mount (https://test-caru.welcometw.com/login:95:93802)
at init (https://test-caru.welcometw.com/login:95:19438)
at https://test-caru.welcometw.com/login:95:56472
at f (https://test-caru.welcometw.com/login:95:56749)
at h (https://test-caru.welcometw.com/login:95:57340)
at f (https://test-caru.welcometw.com/login:95:56863)
```

6.2. https://test-caru.welcometw.com/loginn7mn4v6bek [URL path filename]

Previous Next

Summary

Severity:	Low
Confidence:	Firm
Host:	https://test-caru.welcometw.com
Path:	/loginn7mn4v6bek

Issue detail

The application may be vulnerable to reflected DOM-based link manipulation.

The value of the URL path filename is copied into a JavaScript string literal. The payload **n7mn4v6bek** was submitted in the URL path filename.

The string containing the payload is then passed to **element.setAttribute.href**.

Request 1

```
POST /loginn7mn4v6bek HTTP/1.1
Host: test-caru.welcometw.com
Cookie: XSRF-
TOKEN=eyJpdiI6IlNXNHJsMVBlMW9OdFlZUGdJd0NuNUE9PSIsInZhbHVlIjoiT2x3MTRScmRyTHJacWxXWHFGVlZRK2xDL1hRNzh6TGhqUmY1Q3RUYXd
KNVE3a0RBb2xhMjRsTlBTK0Jqd3ZtZnI4amVCbk10MUNSL1V4a2FsN1AxbkI5Qi9neEZLbzdOWHlFOGRodWVOdmREZEdRbHhJKzVkWms2azAxN09CR2
YiLCJtYWMiOiJlNzQ3YmIyMzVmMzY5MWQ4MzZhYzIxZGU2OTNiNDgyZGE1MDMwMzMxNjQ4YTliZjM2ODRmMzc4YjBhMjE2NGQ3In0%3D;
caru_session=eyJpdiI6ImJpT3Y1QURDRUxJK3padk03UVpLeVE9PSIsInZhbHVlIjoibkpRcTFBKzZsUVdKUitlK25sVUpnRWxtL0pzbU43Q1QyWXNCWlo3a2o
1VGxaSVpkUzZ3TlFMTEZQVGVsTmwrMVhUZVBCQnoxRS9xMzRMc3YxZldsN0xCM0syMlVwWkdLQ3E3VFBmWHFONE9Jdm53Z1djRHZvQ09UQVh1VzJ
WbGYiLCJtYWMiOiJmMTViMTg5ZmQ0NDE5OWRlODUxOGRmYjZjYThhOTIjM2YxMWQ5MzdhZjg2ODY4OTI3MTZhZTg5MWUzYWIzNzQ4In0%3D
Content-Length: 111
Cache-Control: max-age=0
Sec-Ch-Ua: " Not A;Brand";v="99", "Chromium";v="96", "Google Chrome";v="96"
Sec-Ch-Ua-Mobile: ?0
Sec-Ch-Ua-Platform: "Windows"
Origin: https://test-caru.welcometw.com
Upgrade-Insecure-Requests: 1
```

```
Content-Type: application/x-www-form-urlencoded
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/96.0.4664.45 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
Sec-Fetch-Site: same-origin
```

Response 1

```
HTTP/1.1 405 Method Not Allowed
Server: nginx/1.21.3
Content-Type: text/html; charset=UTF-8
Connection: close
allow: GET, HEAD
Cache-Control: no-cache, private
date: Thu, 02 Dec 2021 02:50:44 GMT
Content-Length: 572625

<!doctype html>
<html class="theme-light">
<!--
Symfony\Component\HttpKernel\Exception\MethodNotAllowedHttpException: The POST method is not supported for this route. Supported methods: GET, HEAD.
in
...[SNIP]...
```

Dynamic analysis

The value of the URL path filename is copied into a JavaScript string literal. The payload **n7mn4v6bek** was submitted in the URL path filename.

The string containing the payload is then passed to **element.setAttribute.href**.

The previous value reached the sink as:

```
https://test-caru.welcometw.com/loginn40dz5r5tr
```

The stack trace at the source was:

```
at Object.NdoOX (<anonymous>:1:128317)
at _0x3124b3 (<anonymous>:1:322777)
at Object.sveaB (<anonymous>:1:182488)
at Object.bxgXv (<anonymous>:1:573767)
at _0x5dfed6 (<anonymous>:1:592917)
at Object.UKouh (<anonymous>:1:170365)
at _0x4d375b (<anonymous>:1:508395)
at Object.TgdHu (<anonymous>:1:175531)
at Object.DRoaf (<anonymous>:1:479191)
at HTMLAnchorElement.setAttribute (<anonymous>:1:509426)
at yr (https://test-caru.welcometw.com/login:95:44171)
at _r (https://test-caru.welcometw.com/login:95:43910)
at Array.br (https://test-caru.welcometw.com/login:95:43501)
at v (https://test-caru.welcometw.com/login:95:57584)
at f (https://test-caru.welcometw.com/login:95:56878)
at h (https://test-caru.welcometw.com/login:95:57340)
at f (https://test-caru.welcometw.com/login:95:56863)
at h (https://test-caru.welcometw.com/login:95:57340)
at f (https://test-caru.welcometw.com/login:95:56863)
at a.__patch__ (https://test-caru.welcometw.com/login:95:60891)
at a.t._update (https://test-caru.welcometw.com/login:95:34419)
at a.r (https://test-caru.welcometw.com/login:95:68170)
at mn.get (https://test-caru.welcometw.com/login:95:26728)
at new mn (https://test-caru.welcometw.com/login:95:26646)
at https://test-caru.welcometw.com/login:95:68194
at a.Tn.$mount (https://test-caru.welcometw.com/login:95:68341)
at a.Tn.$mount (https://test-caru.welcometw.com/login:95:93802)
at init (https://test-caru.welcometw.com/login:95:19438)
at https://test-caru.welcometw.com/login:95:56472
at f (https://test-caru.welcometw.com/login:95:56749)
```

The stack trace at the sink was:

```
at Object.UInmG (<anonymous>:1:180817)
at Object.llarH (<anonymous>:1:574598)
at _0x5dfed6 (<anonymous>:1:592957)
at Object.UKouh (<anonymous>:1:170365)
at _0x4d375b (<anonymous>:1:508395)
```

```
at a.t._update (https://test-caru.welcometw.com/login:95:34419)
at a.r (https://test-caru.welcometw.com/login:95:68170)
at mn.get (https://test-caru.welcometw.com/login:95:26728)
at new mn (https://test-caru.welcometw.com/login:95:26646)
at https://test-caru.welcometw.com/login:95:68194
at a.Tn.$mount (https://test-caru.welcometw.com/login:95:68341)
at a.Tn.$mount (https://test-caru.welcometw.com/login:95:93802)
at init (https://test-caru.welcometw.com/login:95:19438)
at https://test-caru.welcometw.com/login:95:56472
at f (https://test-caru.welcometw.com/login:95:56749)
at h (https://test-caru.welcometw.com/login:95:57340)
at f (https://test-caru.welcometw.com/login:95:56863)
```

6.3. https://test-caru.welcometw.com/loginyztjz2hz7e [URL path filename]

Previous Next

Summary

Severity:	Low
Confidence:	Firm
Host:	https://test-caru.welcometw.com
Path:	/loginyztjz2hz7e

Issue detail

The application may be vulnerable to reflected DOM-based link manipulation.

The value of the URL path filename is copied into a JavaScript string literal. The payload **yztjz2hz7e** was submitted in the URL path filename.

The string containing the payload is then passed to **element.setAttribute.href**.

Request 1

```
POST /loginyztjz2hz7e HTTP/1.1
Host: test-caru.welcometw.com
Cookie: XSRF-
TOKEN=eyJpdiI6IkY4OUM3M0V6REt4QmZWd3VJRVAwbVE9PSIsInZhbHVlIjoiS3hEa05MUTlYajRSUVhKeHN0cmtCQ2hYb2xqUkdHZ01HVk9UaTUwdU1C
c2dTRFhqM3RlSVkydU50eGpxMnJON2lwdUt3QmpDbkJya3pSK2RKOXVqS2hSWkFvYm80d0FPenFtUFphZWJvOFRtU3YxeG9OTmZ3ZWVDMmZGVm93
NlAiLCJtYWMiOiJlNDc3YTY1YzQwNzBiOTJlOWFjZDI1Nzk1NWE4MjBjMjU4ZWZjYWFlODQzZWFjM2I2M2MzMzVkMGZlYWJhMDdkIn0%3D;
caru_session=eyJpdiI6IkR1RXczazFZdk05S2RlQTVKSGtrNEE9PSIsInZhbHVlIjoiV3crcUp5OE5yNDl4S09Rd2xkUEVGNjV1U1lUR0lTMXRzRENMeVpiS3Fu
MnBBKzMxUCtkYjFvcCtGMWVPcmNMVUZoeDMrMkRjbzhaMS9LZzFrclpLS0pYUDczN1A5M2tLYnp3dFlSRnd1UU9td0EwbWJaZEdDLzduRTYwRmo3YnliL
CJtYWMiOiI0ZTNhNGJjODk0MzFiZjNlOGQ4YmE3OTc3YmFhOTJlNzdlNjgyNWFhMmRkOGExMThlYjc1MWUyZTg2NzA3N2YyIn0%3D
Content-Length: 113
Cache-Control: max-age=0
Sec-Ch-Ua: " Not A;Brand";v="99", "Chromium";v="96", "Google Chrome";v="96"
Sec-Ch-Ua-Mobile: ?0
Sec-Ch-Ua-Platform: "Windows"
Dnt: 1
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/96.0.4664.45 Safari/537.36
Origin: https://test-caru.welcometw.com
Content-Type: application/x-www-form-urlencoded
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
Sec-Fetch-Site: same-origin
```

Response 1

```
HTTP/1.1 405 Method Not Allowed
Server: nginx/1.21.3
Content-Type: text/html; charset=UTF-8
Connection: close
allow: GET, HEAD
Cache-Control: no-cache, private
date: Thu, 02 Dec 2021 02:50:43 GMT
Content-Length: 572625

<!doctype html>
<html class="theme-light">
<!--
Symfony\Component\HttpKernel\Exception\MethodNotAllowedHttpException: The POST method is not supported for this route. Supported methods: GET, HEAD.
in
...[SNIP]...
```

Dynamic analysis

The string containing the payload is then passed to **element.setAttribute.href**.

The previous value reached the sink as:

```
https://test-caru.welcometw.com/loginam2hrmk62u
```

The stack trace at the source was:

```
at Object.NdoOX (<anonymous>:1:128317)
at _0x3124b3 (<anonymous>:1:322777)
at Object.sveaB (<anonymous>:1:182488)
at Object.bxgXv (<anonymous>:1:573767)
at _0x5dfed6 (<anonymous>:1:592917)
at Object.UKouh (<anonymous>:1:170365)
at _0x4d375b (<anonymous>:1:508395)
at Object.TgdHu (<anonymous>:1:175531)
at Object.DRoaf (<anonymous>:1:479191)
at HTMLAnchorElement.setAttribute (<anonymous>:1:509426)
at yr (https://test-caru.welcometw.com/login:95:44171)
at _r (https://test-caru.welcometw.com/login:95:43910)
at Array.br (https://test-caru.welcometw.com/login:95:43501)
at v (https://test-caru.welcometw.com/login:95:57584)
at f (https://test-caru.welcometw.com/login:95:56878)
at h (https://test-caru.welcometw.com/login:95:57340)
at f (https://test-caru.welcometw.com/login:95:56863)
at h (https://test-caru.welcometw.com/login:95:57340)
at f (https://test-caru.welcometw.com/login:95:56863)
at a.__patch__ (https://test-caru.welcometw.com/login:95:60891)
at a.t._update (https://test-caru.welcometw.com/login:95:34419)
at a.r (https://test-caru.welcometw.com/login:95:68170)
at mn.get (https://test-caru.welcometw.com/login:95:26728)
at new mn (https://test-caru.welcometw.com/login:95:26646)
at https://test-caru.welcometw.com/login:95:68194
at a.Tn.$mount (https://test-caru.welcometw.com/login:95:68341)
at a.Tn.$mount (https://test-caru.welcometw.com/login:95:93802)
at init (https://test-caru.welcometw.com/login:95:19438)
at https://test-caru.welcometw.com/login:95:56472
at f (https://test-caru.welcometw.com/login:95:56749)
```

The stack trace at the sink was:

```
at Object.UInmG (<anonymous>:1:180817)
at Object.llarH (<anonymous>:1:574598)
at _0x5dfed6 (<anonymous>:1:592957)
at Object.UKouh (<anonymous>:1:170365)
at _0x4d375b (<anonymous>:1:508395)
at Object.TgdHu (<anonymous>:1:175531)
at Object.DRoaf (<anonymous>:1:479191)
at HTMLAnchorElement.setAttribute (<anonymous>:1:509426)
at yr (https://test-caru.welcometw.com/login:95:44171)
at _r (https://test-caru.welcometw.com/login:95:43910)
at Array.br (https://test-caru.welcometw.com/login:95:43501)
at v (https://test-caru.welcometw.com/login:95:57584)
at f (https://test-caru.welcometw.com/login:95:56878)
at h (https://test-caru.welcometw.com/login:95:57340)
at f (https://test-caru.welcometw.com/login:95:56863)
at h (https://test-caru.welcometw.com/login:95:57340)
at f (https://test-caru.welcometw.com/login:95:56863)
at a.__patch__ (https://test-caru.welcometw.com/login:95:60891)
at a.t._update (https://test-caru.welcometw.com/login:95:34419)
at a.r (https://test-caru.welcometw.com/login:95:68170)
at mn.get (https://test-caru.welcometw.com/login:95:26728)
at new mn (https://test-caru.welcometw.com/login:95:26646)
at https://test-caru.welcometw.com/login:95:68194
at a.Tn.$mount (https://test-caru.welcometw.com/login:95:68341)
at a.Tn.$mount (https://test-caru.welcometw.com/login:95:93802)
at init (https://test-caru.welcometw.com/login:95:19438)
at https://test-caru.welcometw.com/login:95:56472
at f (https://test-caru.welcometw.com/login:95:56749)
at h (https://test-caru.welcometw.com/login:95:57340)
at f (https://test-caru.welcometw.com/login:95:56863)
```

7. Source code disclosure

Previous Next

Summary

Severity:	Low
Confidence:	Tentative
Host:	https://test-caru.welcometw.com
Path:	/js/app.js

Issue detail

The application appears to disclose some server-side source code written in ASP.

Issue background

Source code intended to be kept server-side can sometimes end up being disclosed to users. Such code may contain sensitive information such as database passwords and secret keys, which may help malicious users formulate attacks against the application.

Issue remediation

Server-side source code is normally disclosed to clients as a result of typographical errors in scripts or because of misconfiguration, such as failing to grant executable permissions to a script or directory. Review the cause of the code disclosure and prevent it from happening.

References

- Web Security Academy: Information disclosure

Vulnerability classifications

- CWE-18: Source Code
- CWE-200: Information Exposure
- CWE-388: Error Handling
- CWE-540: Information Exposure Through Source Code
- CWE-541: Information Exposure Through Include Source Code
- CWE-615: Information Exposure Through Comments
- CAPEC-37: Retrieve Embedded Sensitive Data

Request 1

```
GET /js/app.js HTTP/1.1
Host: test-caru.welcometw.com
Accept-Encoding: gzip, deflate
Accept: */*
Accept-Language: en-US,en-GB;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/95.0.4638.54 Safari/537.36
Connection: close
Cache-Control: max-age=0
```

Response 1

```
HTTP/1.1 200 OK
Server: nginx/1.21.3
Date: Thu, 02 Dec 2021 02:14:47 GMT
Content-Type: application/javascript
Content-Length: 2963603
Last-Modified: Thu, 02 Dec 2021 01:57:23 GMT
Connection: close
ETag: "61a82803-2d3893"
Accept-Ranges: bytes

/******/ (function(modules) { // webpackBootstrap
/******/ 	// The module cache
/******/ 	var installedModules = {};
/******/
/******/ 	// The require function
/******/ 	function __webpack_require__(m
...[SNIP]...
</li>'
*
* // Use the internal `print` function in "evaluate" delimiters.
* var compiled = _.template('<% print("hello " + user); %>!');
```

8. Strict transport security not enforced

Previous Next

There are 3 instances of this issue:

- /
- /admin
- /login

Issue background

The application fails to prevent users from connecting to it over unencrypted connections. An attacker able to modify a legitimate user's network traffic could bypass the application's use of SSL/TLS encryption, and use the application as a platform for attacks against its users. This attack is performed by rewriting HTTPS links as HTTP, so that if a targeted user follows a link to the site from an HTTP page, their browser never attempts to use an encrypted connection. The sslstrip tool automates this process.

To exploit this vulnerability, an attacker must be suitably positioned to intercept and modify the victim's network traffic.This scenario typically occurs when a client communicates with the server over an insecure connection such as public Wi-Fi, or a corporate or home network that is shared with a compromised computer. Common defenses such as switched networks are not sufficient to prevent this. An attacker situated in the user's ISP or the application's hosting infrastructure could also perform this attack. Note that an advanced adversary could potentially target any connection made over the Internet's core infrastructure.

Issue remediation

The application should instruct web browsers to only access the application using HTTPS. To do this, enable HTTP Strict Transport Security (HSTS) by adding a response header with the name 'Strict-Transport-Security' and the value 'max-age=expireTime', where expireTime is the time in seconds that browsers should remember that the site should only be accessed using HTTPS. Consider adding the 'includeSubDomains' flag if appropriate.

Note that because HSTS is a "trust on first use" (TOFU) protocol, a user who has never accessed the application will never have seen the HSTS header, and will therefore still be vulnerable to SSL stripping attacks. To mitigate this risk, you can optionally add the 'preload' flag to the HSTS header, and submit the domain for review by browser vendors.

References

- HTTP Strict Transport Security
- sslstrip
- HSTS Preload Form

Vulnerability classifications

- CWE-523: Unprotected Transport of Credentials
- CAPEC-94: Man in the Middle Attack
- CAPEC-157: Sniffing Attacks

8.1. https://test-caru.welcometw.com/

Previous Next

Summary

Severity:	Low
Confidence:	Certain
Host:	https://test-caru.welcometw.com
Path:	/

Issue detail

This issue was found in multiple locations under the reported path.

Request 1

```
GET /admin HTTP/1.1
Host: test-caru.welcometw.com
Cookie: XSRF-
TOKEN=eyJpdiI6IkpDcVU2Q2pqOGJlYWRySTFUTGpjWHc9PSIsInZhbHVlIjoiWnBMMkJTY3U0d2F6UEtYUFlGWmthVTRlMU5LNFlhS2s0R2k2dEd6ekJkel
EybVVrUUFXdkVOWFRkNzlCRHRZNkt6a29FMm9MN3J4a0MranpWcjI3MjZaZEx6Q2p3dnJOb1kwQ2I2UjU1R3hLNGpaM2RWYkFhRmc2bXlLbFZOSkYiLC
JtYWMiOiI0ZTE4NGM1MWQzNjljYTFiYTMyNmEyZGI1MzI0MjFlZWQ5ZWNlNjczNDIxNGI2YzFlZjM1NDlhYzU5MzQwYmE1In0%3D;
```

```
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Sec-Fetch-Dest: document
Sec-Ch-Ua: " Not A;Brand";v="99", "Chromium";v="96", "Google Chrome";v="96"
Sec-Ch-Ua-Mobile: ?0
Sec-Ch-Ua-Platform: "Windows"
```

Response 1

```
HTTP/1.1 302 Found
Server: nginx/1.21.3
Content-Type: text/html; charset=UTF-8
Connection: close
Cache-Control: no-cache, private
Date: Thu, 02 Dec 2021 01:36:35 GMT
Location: https://test-caru.welcometw.com/login
Set-Cookie: XSRF-
TOKEN=eyJpdiI6IklkVVNncnRhQXprbHNtbGhHa3FUblE9PSIsInZhbHVlIjoiTUkyTWdDcUlZWUhKVWJXdk40bHltN29pVlBiajMzVXlyZFBtRVRGWi9zSS9NYVBNbEVubGhpRUEwV3Nlcitwb1FYaE5KMjZHUExrcGlNR2kxRG9lVVlTUXRkSng4emxuZlZhdndzSitFc0xSUUt4T3RaTlRUZ0VBemJNVHZ1N1YiLCJtYWMiOiJiMWRhZmNiMWE3NzNiZTkyNDcwNDRmODk5NjRjOGQ0Zjk5ODA3YmRlZWZhZTU3OTMzMzc3MzFmYzlmNWE4MjU1In0%3D; expires=Thu, 02-Dec-
2021 03:36:35 GMT; Max-Age=7200; path=/; samesite=lax
Set-Cookie:
caru_session=eyJpdiI6ImpraVNYZUJTS1IpUXFnWFY3RUt4d0E9PSIsInZhbHVlIjoiMmlpdVBlYjlwTmk5UkVkMWFsQnBZY1dibnBpd0xuUmdiQWFtellkV0NETWtLczdWeGxkQmNBNXRWMzNmRkhnT1djVE9yQkNXSFFWSzk1RUk5S2RTNm5aUVdjNHYxT2dXRDdQc05RcjhBNnRRRTJCdGtrWW9PQmpRQVVjYWQwbU4iLCJtYWMiOiIzMGExZGFjZmZhNDZhMTJlMDkwMTEwMTc3YzQ0YmRjNjNjODg3ZWJjZDQzODI3MDhkYjQ2OTQ2ZDA0MjdhMjdiIn0%3D;
expires=Thu, 02-Dec-2021 03:36:35 GMT; Max-Age=7200; path=/; httponly; samesite=lax
Content-Length: 394

<!DOCTYPE html>
<html>
```

8.2. https://test-caru.welcometw.com/admin

Previous Next

Summary

Severity:	**Low**
Confidence:	**Certain**
Host:	**https://test-caru.welcometw.com**
Path:	**/admin**

Request 1

```
GET /admin HTTP/1.1
Host: test-caru.welcometw.com
Cookie: XSRF-
TOKEN=eyJpdiI6IkpDcVU2Q2pqOGJlYWRySTFUTGpjWHc9PSIsInZhbHVlIjoiWnBMMkJTY3U0d2F6UEtYUFlGWmthVTRlMU5LNFlhS2s0R2k2dEd6ekJkelEybVVrUUFXdkVOWFRkNzlCRHRZNkt6a29FMm9MN3J4a0MranpWcjl3MjZaZEx6Q2p3dnJOb1kwQ2l2UjU1R3hLNGpaM2RWYkFhRmc2bXlLbFZOSkYiLCJtYWMiOiI0ZTE4NGM1MWQzNjljYTFiYTMyNmEyZGI1Mzl0MjFlZWQ5ZWNlNjczNDIxNGI2YzFlZjM1NDlhYzU5MzQwYmE1In0%3D;
caru_session=eyJpdiI6IlpLbVpVM0s5TlVVQVFyOVBzZ3NSUkE9PSIsInZhbHVlIjoiSFoxVXRJQWlUOVoxWjhjaWNNR1VUMzl0OXg5cHB3MkNPT3puUzhmb0YwT3QyK2hDa0VMVUtzYXRHQWFLckkzL3VweXh2K20zZ203UVBBcU10L3gyMnFqdDc4akhzbDJKRnkwRlYvWUxveGE5VElzd1dHS0dzMGtETFV0MjNjU0YiLCJtYWMiOiI1YmQ4OTRkZTBjNjU0N2U0MDUxNTM1NTBlMGEwZTIzZWUxYTNjY2RkYTA0N2M1NDBhNmNmMDI5NjE5ZDA5MTEyIn0%3D
Cache-Control: max-age=0
Dnt: 1
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/96.0.4664.45 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Sec-Fetch-Dest: document
Sec-Ch-Ua: " Not A;Brand";v="99", "Chromium";v="96", "Google Chrome";v="96"
Sec-Ch-Ua-Mobile: ?0
Sec-Ch-Ua-Platform: "Windows"
```

Response 1

```
HTTP/1.1 302 Found
Server: nginx/1.21.3
Content-Type: text/html; charset=UTF-8
Connection: close
Cache-Control: no-cache, private
Date: Thu, 02 Dec 2021 01:36:35 GMT
```

```
Set-Cookie: XSRF-
TOKEN=eyJpdiI6IklkVVNncnRhQXprbHNtbGhHa3FUblE9PSIsInZhbHVlIjoiTUkyTWdDcUlZWUhKVWJXdk40bHltN29pVlBiajMzVXlyZFBtRVRGWi9zSS9NYV
BNbEVubGhpRUEwV3Nlcitwb1FYaE5KMjZHUExrcGlNR2kxRG9lVVITUXRkSng4emxuZlZhdndzSitFc0xSUUt4T3RaTlRUZ0VBemJNVHZ1N1YiLCJtYWMiOi
JiMWRhZmNiMWE3NzNlZTkyNDcwNDRmODk5NjRjOGQ0Zjk5ODA3YmRlZWZhZTU3OTMzMzc3MzFmYzlmNWE4MjU1In0%3D; expires=Thu, 02-Dec-
2021 03:36:35 GMT; Max-Age=7200; path=/; samesite=lax
Set-Cookie:
caru_session=eyJpdiI6ImpraVNYZUJTS1lpUXFnWFY3RUt4d0E9PSIsInZhbHVlIjoiMmlpdVBlYjlwTmk5UkVkMWFsQnBZY1dibnBpd0xuUmdiQWFtellkV0NET
WtLczdWeGxkQmNBNXRWMzNmRkhnT1djVE9yQkNXSFFWSzk1RUk5S2RTNm5aUVdjNHYxT2dXRDdQc05RcjhBNnRRRTJCdGtrWW9PQmpRQVVjYWQ
wbU4iLCJtYWMiOiIzMGExZGFjZmZhNDZhMTJlMDkwMTEwMTc3YzQ0YmRjNjNjODg3ZWJjZDQzODI3MDhkYjQ2OTQ2ZDA0MjdhMjdiIn0%3D;
expires=Thu, 02-Dec-2021 03:36:35 GMT; Max-Age=7200; path=/; httponly; samesite=lax
Content-Length: 394

<!DOCTYPE html>
<html>
```

8.3. https://test-caru.welcometw.com/login

Previous Next

Summary

Severity:	Low
Confidence:	Certain
Host:	https://test-caru.welcometw.com
Path:	/login

Request 1

```
POST /login HTTP/1.1
Host: test-caru.welcometw.com
Cookie: XSRF-
TOKEN=eyJpdiI6IkY4OUM3M0V6REt4QmZWd3VJRVAwbVE9PSIsInZhbHVlIjoiS3hEa05MUTlYajRSUVhKeHN0cmtCQ2hYb2xqUkdHZ01HVk9UaTUwdU1C
c2dTRFhqM3RlSVkydU50eGpxMnJON2lwdUt3QmpDbkJya3pSK2RKOXVqS2hSWkFvYm80d0FPenFtUFphZWJvOFRtU3YxeG9OTmZ3ZWVDMmZGVm93
NlAiLCJtYWMiOiJlNDc3YTY1YzQwNzBiOTJlOWFjZDI1Nzk1NWE4MjBjMjU4ZWZjYWFlODQzZWFjM2I2M2MzMzVkMGZlYWJhMDdkIn0%3D;
caru_session=eyJpdiI6IkR1RXczazFZdk05S2RlQTVKSGtrNEE9PSIsInZhbHVlIjoiV3crcUp5OE5yNDI4S09Rd2xkUEVGNjV1U1lUR0lTMXRzRENMeVpiS3Fu
MnBBKzMxUCtkYjFvcCtGMWVPcmNMVUZoeDMrMkRjbzhaMS9LZzFrclpLS0pYUDczN1A5M2tLYnp3dFlSRnd1UU9td0EwbWJaZEdDLzduRTYwRmo3YnliL
CJtYWMiOiI0ZTNhNGJjODk0MzFiZjNlOGQ4YmE3OTc3YmFhOTJlNzdlNjgyNWFhMmRkOGExMThlYjc1MWUyZTg2NzA3N2YyIn0%3D
Content-Length: 113
Cache-Control: max-age=0
Sec-Ch-Ua: " Not A;Brand";v="99", "Chromium";v="96", "Google Chrome";v="96"
Sec-Ch-Ua-Mobile: ?0
Sec-Ch-Ua-Platform: "Windows"
Dnt: 1
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/96.0.4664.45 Safari/537.36
Origin: https://test-caru.welcometw.com
Content-Type: application/x-www-form-urlencoded
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
Sec-Fetch-Site: same-origin
```

Response 1

```
HTTP/1.1 302 Found
Server: nginx/1.21.3
Content-Type: text/html; charset=UTF-8
Connection: close
Cache-Control: no-cache, private
Date: Thu, 02 Dec 2021 01:32:14 GMT
Location: https://test-caru.welcometw.com/admin
Set-Cookie: XSRF-
TOKEN=eyJpdiI6IkpDcVU2Q2pqOGJlYWRySTFUTGpjWHc9PSIsInZhbHVlIjoiWnBMMkJTY3U0d2F6UEtYUFlGWmthVTRIMU5LNFlhS2s0R2k2dEd6ekJkel
EybVVrUUFXdkVOWFRkNzlCRHRZNkt6a29FMm9MN3J4a0MranpWcjl3MjZaZEx6Q2p3dnJOb1kwQ2I2UjU1R3hLNGpaM2RWYkFhRmc2bXlLbFZOSkYiLC
JtYWMiOiI0ZTE4NGM1MWQzNjljYTFiYTMyNmEyZGI1MzI0MjFlZWQ5ZWNlNjczNDIxNGI2YzFlZjM1NDlhYzU5MzQwYmE1In0%3D; expires=Thu, 02-Dec-
2021 03:32:14 GMT; Max-Age=7200; path=/; samesite=lax
Set-Cookie:
caru_session=eyJpdiI6IlpLbVpVM0s5TlVVQVFyOVBzZ3NSUkE9PSIsInZhbHVlIjoiSFoxVXRJQWlUOVoxWjhjaWNNR1VUMzI0OXg5cHB3MkNPT3puUzhmb
0YwT3QyK2hDa0VMVUtzYXRHQWFLckkzL3VweXh2K20zZ203UVBBcU10L3gyMnFqdDo4akhzbDJKRnkwRlYvWUxveGE5VElzd1dHS0dzMGtETFV0MjNjU
0YiLCJtYWMiOiI1YmQ4OTRkZTBjNjU0N2U0MDUxNTM1NTBlMGEwZTIzZWUxYTNjY2RkYTA0N2M1NDBhNmNmMDI5NjE5ZDA5MTEyIn0%3D;
expires=Thu, 02-Dec-2021 03:32:14 GMT; Max-Age=7200; path=/; httponly; samesite=lax
Content-Length: 394

<!DOCTYPE html>
<html>
```

9. Input returned in response (reflected)

Previous Next

There are 4 instances of this issue:

- /admin [XSRF-TOKEN cookie]
- /admin [caru_session cookie]
- /admin [remember_web_59ba36addc2b2f9401580f014c7f58ea4e30989d cookie]
- /login [URL path filename]

Issue background

Reflection of input arises when data is copied from a request and echoed into the application's immediate response.

Input being returned in application responses is not a vulnerability in its own right. However, it is a prerequisite for many client-side vulnerabilities, including cross-site scripting, open redirection, content spoofing, and response header injection. Additionally, some server-side vulnerabilities such as SQL injection are often easier to identify and exploit when input is returned in responses. In applications where input retrieval is rare and the environment is resistant to automated testing (for example, due to a web application firewall), it might be worth subjecting instances of it to focused manual testing.

Vulnerability classifications

- CWE-20: Improper Input Validation
- CWE-116: Improper Encoding or Escaping of Output

9.1. https://test-caru.welcometw.com/admin [XSRF-TOKEN cookie]

Previous Next

Summary

Severity:	**Information**
Confidence:	**Certain**
Host:	**https://test-caru.welcometw.com**
Path:	**/admin**

Issue detail

The value of the **XSRF-TOKEN** cookie is copied into the application's response.

Request 1

```
POST /admin HTTP/1.1
Host: test-caru.welcometw.com
Cookie: XSRF-
TOKEN=eyJpdiI6Ik5sUjJZQWQxeWs1aWpNQkVFbnovRmc9PSIsInZhbHVlIjoiTnVWcFhqSWxRM2VyeDlvVUlWZFk1WlFDTW5PWW8yZ0h4UVFpMU55MW
NBN2JXTlJ2OUZKeDR2T0pzSDkwVU5PYUUxcGhPc1FEMlZMOVo5VHNDSFR2VmkxRUF6QnZTZHNGVFRQTVB5blkrRHFyZnJMelNmbU9VRTFTbWg2M
nA1UG8iLCJtYWMiOiI0OTdlYjM4YmM3NjQ2YzUxZTVkNzU0NzFlNjM0MDAyNjY2YWFmYTVlYTk4N2I2M2JiOGM5OTEyYzdlMGYxMWIzIn0%3dkejz7xgtep;
caru_session=eyJpdiI6IklxZ3VSVTZLZEs1QmFkSHRvSERranc9PSIsInZhbHVlIjoiZk9TY3ZRMVg3WHNCV1ZZYkRmYjBLbUkvVFJZOGdpMk1SN1hlNUplY1
VzNmFNMDEzQ3F6K1lBZjRlNEsycytLSHlzcjUvQTBMaExRZGsxRGMxdEhWejFjTEgwY1lBMUVtYWxVYlA5VzVqRktSUlloN28vSHBCMDZSQXptT0pYZGEi
LCJtYWMiOiI3NDJmNThlODZhZjVkNTFhYzJjOWU3ZTQyYWM0ZTI0ZDA4ODM4Yjc4NjYwN2E4ZmM3ZTUyYTQyZmU2ZjRmMzdkIn0%3D;
remember_web_59ba36addc2b2f9401580f014c7f58ea4e30989d=eyJpdiI6Im1jNWltZERONURQYUc5Szl0SXowN2c9PSIsInZhbHVlIjoiUi95RHp6RTh1S0RW
d0dCTkRrZWUvd0hPb1lSb0E3a0oybStuR2dVT3dldnpqbjRsUzVMYTdWVUN0U0libjE2OXp4Q2dlUG1ER3JhZjY1WXJTZG9XYldhNG5UU0FFUUZNRDJNV
k9rdWhSakgvMEZUWFp4M3BtZGpoRHd1clB0alErNmtXTGFOVnhqbklrcDh1Y0VoVWlzV3BRdzVnbGRjL09xVk9mWTI0NXRJRExaQVpieHppRlJEVTZwb2h
2bnViSzZOQlzZPK3cwZzBnZTFDbG1ySld3RXM3SkZCeitOeXhvV0s3TUtKeDdtTT0iLCJtYWMiOiI1ZWY1NDNhNjJkOGI0ZDFhYmQyMzJjMjAzZWMwZGJlZj
hlNGNmNzEzNzk5NDI5MjU4Y2ExNTI5YzkyY2Y5OTdiIn0%3D
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
Dnt: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/96.0.4664.45 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: navigate
```

Response 1

```
HTTP/1.1 405 Method Not Allowed
```

```
allow: GET, HEAD
Cache-Control: no-cache, private
date: Thu, 02 Dec 2021 02:03:55 GMT
Content-Length: 572448

<!doctype html>
<html class="theme-light">
<!--
Symfony\Component\HttpKernel\Exception\MethodNotAllowedHttpException: The POST method is not supported for this route. Supported methods: GET, HEAD. in
...[SNIP]...
0pzSDkwVU5PYUUxcGhPc1FEMlZMOVo5VHNDSFR2VmkxRUF6QnZTZHNGVFRQTVB5blkrRHFyZnJMelNmbU9VRTFTbWg2MnA1UG8iLCJtYWMiOiI0OTdlYjM4YmM3NjQ2YzUxZTVkNzU0NzFlNjM0MDAyNjY2YWFmYTVlYTk4N2I2M2JiOGM5OTEyYzdlMGYxMWIzIn0%3dkejz7xgtep;
caru_session=eyJpdiI6IklxZ3VSVTZLZEs1QmFkSHRvSERranc9PSIsInZhbHVlIjoiZk9TY3ZRMVg3WHNCV1ZZYkRmYjBLbUkvVFJZOGdpMk1SN1hlNUplY1VzNmFNMDEzQ3F6K1lBZjRINEsycytLSHIzcjUvQTBMaExRZGsxRGMxdEhWejFjTEgwY1lBMUVtYW
...[SNIP]...
2T0pzSDkwVU5PYUUxcGhPc1FEMlZMOVo5VHNDSFR2VmkxRUF6QnZTZHNGVFRQTVB5blkrRHFvZnJMelNmbU9VRTFTbWo2MnA1UG8iLCJtYWMiOiI0
```

9.2. https://test-caru.welcometw.com/admin [caru_session cookie]

Previous Next

Summary

Severity:	**Information**
Confidence:	**Certain**
Host:	**https://test-caru.welcometw.com**
Path:	**/admin**

Issue detail

The value of the **caru_session** cookie is copied into the application's response.

Request 1

```
POST /admin HTTP/1.1
Host: test-caru.welcometw.com
Cookie: XSRF-TOKEN=eyJpdiI6Ik5sUjJZQWQxeWs1aWpNQkVFbnovRmc9PSIsInZhbHVlIjoiTnVWcFhqSWxRM2VyeDlvVUlWZFk1WlFDTW5PWW8yZ0h4UVFpMU55MWNBN2JXTlJ2OUZKeDR2T0pzSDkwVU5PYUUxcGhPc1FEMlZMOVo5VHNDSFR2VmkxRUF6QnZTZHNGVFRQTVB5blkrRHFyZnJMelNmbU9VRTFTbWg2MnA1UG8iLCJtYWMiOiI0OTdlYjM4YmM3NjQ2YzUxZTVkNzU0NzFlNjM0MDAyNjY2YWFmYTVlYTk4N2I2M2JiOGM5OTEyYzdlMGYxMWIzIn0%3D; caru_session=eyJpdiI6IklxZ3VSVTZLZEs1QmFkSHRvSERranc9PSIsInZhbHVlIjoiZk9TY3ZRMVg3WHNCV1ZZYkRmYjBLbUkvVFJZOGdpMk1SN1hlNUplY1VzNmFNMDEzQ3F6K1lBZjRINEsycytLSHIzcjUvQTBMaExRZGsxRGMxdEhWejFjTEgwY1lBMUVtYWxVYlA5VzVqRktSUlloN28vSHBCMDZSQXptT0pYZGEiLCJtYWMiOiI3NDJmNThlODZhZjVkNTFhYzJjOWU3ZTQyYWM0ZTI0ZDA4ODM4Yjc4NjYwN2E4ZmM3ZTUyYTQyZmU2ZjRmMzdkIn0%3d26ju6teu9p; remember_web_59ba36addc2b2f9401580f014c7f58ea4e30989d=eyJpdiI6Im1jNWltZERONURQYUc5Szl0SXowN2c9PSIsInZhbHVlIjoiUi95RHp6RTh1S0RWd0dCTkRrZWUvd0hPb1lSb0E3a0oybStuR2dVT3dldnpqbjRsUzVMYTdWVUN0U0libjE2OXp4Q2dlUG1ER3JhZjY1WXJTZG9XYldhNG5UU0FFUUZNRDJNVk9rdWhSakgvMEZUWFp4M3BtZGpoRHd1clB0alErNmtXTGFOVnhqbkl5cDh1Y0VoVWlzV3BRdzVnbGRjL09xVk9mWTI0NXRJREExaQVpieHppRlJEVTZwb2h2bnViSzZOQzZPK3owZzBnZTFDbG1ySld3RXM3SkZCeitOeXhvV0s3TUtKeDdtT0iLCJtYWMiOiI1ZWY1NDNhNjJkOGI0ZDFhYmQyMzJjMjAzZWMwZGJlZjhlNGNmNzEzNzk5NDI5MjU4Y2ExNTI5YzkyY2Y5OTdiIn0%3D
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
Dnt: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/96.0.4664.45 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: navigate
```

Response 1

```
HTTP/1.1 405 Method Not Allowed
Server: nginx/1.21.3
Content-Type: text/html; charset=UTF-8
Connection: close
allow: GET, HEAD
Cache-Control: no-cache, private
date: Thu, 02 Dec 2021 02:09:25 GMT
Content-Length: 572448

<!doctype html>
<html class="theme-light">
<!--
Symfony\Component\HttpKernel\Exception\MethodNotAllowedHttpException: The POST method is not supported for this route. Supported methods: GET, HEAD. in
...[SNIP]...
jRINEsycytLSHIzcjUvQTBMaExRZGsxRGMxdEhWejFjTEgwY1lBMUVtYWxVYlA5VzVqRktSUlloN28vSHBCMDZSQXptT0pYZGEiLCJtYWMiOiI3NDJmNThlODZhZjVkNTFhYzJjOWU3ZTQyYWM0ZTI0ZDA4ODM4Yjc4NjYwN2E4ZmM3ZTUyYTQyZmU2ZjRmMzdkIn0%3d26ju6teu9p;
```

9.3. https://test-caru.welcometw.com/admin [remember_web_59ba36addc2b2f9401580f014c7f58ea4e30989d cookie]

Previous Next

Summary

Severity:	**Information**
Confidence:	**Certain**
Host:	**https://test-caru.welcometw.com**
Path:	**/admin**

Issue detail

The value of the **remember_web_59ba36addc2b2f9401580f014c7f58ea4e30989d** cookie is copied into the application's response.

Request 1


```
POST /admin HTTP/1.1
Host: test-caru.welcometw.com
Cookie: XSRF-
TOKEN=eyJpdiI6Ik5sUjJZQWQxeWs1aWpNQkVFbnovRmc9PSIsInZhbHVlIjoiTnVWcFhqSWxRM2VyeDlvVUlWZFk1WlFDTW5PWW8yZ0h4UVFpMU55MW
NBN2JXTlJ2OUZKeDR2T0pzSDkwVU5PYUUxcGhPc1FEMlZMOVo5VHNDSFR2VmkxRUF6QnZTZHNGVFRQTVB5blkrRHFyZnJMelNmbU9VRTFTbWg2M
nA1UG8iLCJtYWMiOiI0OTdlYjM4YmM3NjQ2YzUxZTVkNzU0NzFlNjM0MDAyNjY2YWFmYTVlYTk4N2I2M2JiOGM5OTEyYzdlMGYxMWIzIn0%3D;
caru_session=eyJpdiI6IkIxZ3VSVTZLZEs1QmFkSHRvSERranc9PSIsInZhbHVlIjoiZk9TY3ZRMVg3WHNCV1ZZYkRmYjBLbUkvVFJZOGdpMk1SN1hlNUplY1
VzNmFNMDEzQ3F6K1lBZjRlNEsycytLSHIzcjUvQTBMaExRZGsxRGMxdEhWejFjTEgwY1lBMUVtYWxVYlA5VzVqRktSUlloN28vSHBCMDZSQXptT0pYZGEi
LCJtYWMiOiI3NDJmNThlODZhZjVkNTFhYzJjOWU3ZTQyYWM0ZTI0ZDA4ODM4Yjc4NjYwN2E4ZmM3ZTUyYTQyZmU2ZjRmMzdkIn0%3D;
remember_web_59ba36addc2b2f9401580f014c7f58ea4e30989d=eyJpdiI6Im1jNWltZERONURQYUc5SzI0SXowN2c9PSIsInZhbHVlIjoiUi95RHp6RTh1S0RW
d0dCTkRrZWUvd0hPb1ISb0E3a0oybStuR2dVT3dldnpqbjRsUzVMYTdWVUN0U0libjE2OXp4Q2dlUG1ER3JhZjY1WXJTZG9XYldhNG5UU0FFUUZNRDJNV
k9rdWhSakgvMEZUWFp4M3BtZGpoRHd1clB0alErNmtXTGFOVnhqbkl5cDh1Y0VoVWlzV3BRdzVnbGRjL09xVk9mWTI0NXRJREexaQVpieHppRlJEVTZwb2h
2bnViSzZOQzZPK3cwZzBnZTFDbG1ySld3RXM3SkZCeitOeXhvV0s3TUtKeDdtT0iLCJtYWMiOiI1ZWY1NDNhNjJkOGI0ZDFhYmQyMzJjMjAzZWMwZGJlZj
hlNGNmNzEzNzk5NDI5MjU4Y2ExNTI5YzkyY2Y5OTdiIn0%3drc7xtzrh49
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
Dnt: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/96.0.4664.45 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: navigate
```


Response 1


```
HTTP/1.1 405 Method Not Allowed
Server: nginx/1.21.3
Content-Type: text/html; charset=UTF-8
Connection: close
allow: GET, HEAD
Cache-Control: no-cache, private
date: Thu, 02 Dec 2021 02:14:26 GMT
Content-Length: 572448

<!doctype html>
<html class="theme-light">
<!--
Symfony\Component\HttpKernel\Exception\MethodNotAllowedHttpException: The POST method is not supported for this route. Supported methods: GET, HEAD. in
...[SNIP]...
k9mWTI0NXRJREExaQVpieHppRlJEVTZwb2h2bnViSzZOQzZPK3cwZzBnZTFDbG1ySld3RXM3SkZCeitOeXhvV0s3TUtKeDdtT0iLCJtYWMiOiI1ZWY1NDN
hNjJkOGI0ZDFhYmQyMzJjMjAzZWMwZGJlZjhlNGNmNzEzNzk5NDI5MjU4Y2ExNTI5YzkyY2Y5OTdiIn0%3drc7xtzrh49"],"host":["test-
caru.welcometw.com"]},"cookies":{"XSRF-
TOKEN":"eyJpdiI6Ik5sUjJZQWQxeWs1aWpNQkVFbnovRmc9PSIsInZhbHVlIjoiTnVWcFhqSWxRM2VyeDlvVUlWZFk1WlFDTW5PWW8yZ0h4UVFpMU55M
WNBN2JXTlJ2OUZKeDR2T0pzSDkwV
...[SNIP]
```

9.4. https://test-caru.welcometw.com/login [URL path filename]

Previous Next

Summary

Severity:	Information
Confidence:	Certain
Host:	https://test-caru.welcometw.com
Path:	/login

Issue detail

The value of the URL path filename is copied into the application's response.

Request 1

```
POST /logintf8xdrvgr6 HTTP/1.1
Host: test-caru.welcometw.com
Cookie: XSRF-
TOKEN=eyJpdiI6IkY4OUM3M0V6REt4QmZWd3VJRVAwbVE9PSIsInZhbHVlIjoiS3hEa05MUTlYajRSUVhKeHN0cmtCQ2hYb2xqUkdHZ01HVk9UaTUwdU1C
c2dTRFhqM3RlSVkydU50eGpxMnJON2lwdUt3QmpDbkJya3pSK2RKOXVqS2hSWkFvYm80d0FPenFtUFphZWJvOFRtU3YxeG9OTmZ3ZWVDMmZGVm93
NlAiLCJtYWMiOiJlNDc3YTY1YzQwNzBiOTJlOWFjZDI1Nzk1NWE4MjBjMjU4ZWZjYWFlODQzZWFjM2I2M2MzMzVkMGZlYWJhMDdkIn0%3D;
caru_session=eyJpdiI6IkR1RXczazFZdk05S2RlQTVKSGtrNEE9PSIsInZhbHVlIjoiV3crcUp5OE5yNDl4S09Rd2xkUEVGNjV1U1lUR0lTMXRzRENMeVpiS3Fu
MnBBKzMxUCtkYjFvcCtGMWVPcmNMVUZoeDMrMkRjbzhaMS9LZzFrclpLS0pYUDczN1A5M2tLYnp3dFlSRnd1UU9td0EwbWJaZEdDLzduRTYwRmo3YnliL
CJtYWMiOiI0ZTNhNGJjODk0MzFiZjNlOGQ4YmE3OTc3YmFhOTJlNzdlNjgyNWFhMmRkOGExMThlYjc1MWUyZTg2NzA3N2YyIn0%3D
Content-Length: 113
Cache-Control: max-age=0
Sec-Ch-Ua: " Not A;Brand";v="99", "Chromium";v="96", "Google Chrome";v="96"
Sec-Ch-Ua-Mobile: ?0
Sec-Ch-Ua-Platform: "Windows"
Dnt: 1
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/96.0.4664.45 Safari/537.36
Origin: https://test-caru.welcometw.com
Content-Type: application/x-www-form-urlencoded
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
Sec-Fetch-Site: same-origin
```

Response 1

```
HTTP/1.1 405 Method Not Allowed
Server: nginx/1.21.3
Content-Type: text/html; charset=UTF-8
Connection: close
allow: GET, HEAD
Cache-Control: no-cache, private
date: Thu, 02 Dec 2021 02:46:42 GMT
Content-Length: 572625

<!doctype html>
<html class="theme-light">
<!--
Symfony\Component\HttpKernel\Exception\MethodNotAllowedHttpException: The POST method is not supported for this route. Supported methods: GET, HEAD.
in
...[SNIP]...
nate($request, $response);","61":""},"file":"\/var\/www\/test-caru.welcometw.com\/public\/index.php","is_application_frame":false}],"context":{"request":
{"url":"https:\/\/test-caru.welcometw.com\/logintf8xdrvgr6","ip":null,"method":"POST","useragent":"Mozilla\/5.0 (Windows NT 10.0; Win64; x64)
AppleWebKit\/537.36 (KHTML, like Gecko) Chrome\/96.0.4664.45 Safari\/537.36"},"request_data":{"queryString":[],"body"
...[SNIP]...
```

10. Cross-domain script include

Previous Next

There are 2 instances of this issue:

- /
- /admin

Issue background

When an application includes a script from an external domain, this script is executed by the browser within the security context of the invoking application. The script can therefore do anything that the application's own scripts can do, such as accessing application data and performing actions within the context of the current user.

If you include a script from an external domain, then you are trusting that domain with the data and functionality of your application, and you are trusting the domain's own security to prevent an attacker from modifying the script to perform malicious actions within your application.

Issue remediation

Issue remediation

Scripts should ideally not be included from untrusted domains. Applications that rely on static third-party scripts should consider using Subresource Integrity to make browsers verify them, or copying the contents of these scripts onto their own domain and including them from there. If that is not possible (e.g. for licensing reasons) then consider reimplementing the script's functionality within application code.

References

- Subresource Integrity

Vulnerability classifications

- CWE-829: Inclusion of Functionality from Untrusted Control Sphere

---

10.1. https://test-caru.welcometw.com/

Previous Next

Summary

Severity:	**Information**
Confidence:	**Certain**
Host:	**https://test-caru.welcometw.com**
Path:	**/**

Issue detail

The response dynamically includes the following script from another domain:

- https://www.googletagmanager.com/gtag/js?id=G-WW3MTCGQNN

Request 1

```
GET / HTTP/1.1
Host: test-caru.welcometw.com
Accept-Encoding: gzip, deflate
Accept: */*
Accept-Language: en
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/95.0.4638.54 Safari/537.36
Connection: close
```

Response 1

```
HTTP/1.1 200 OK
Server: nginx/1.21.3
Content-Type: text/html; charset=UTF-8
Connection: close
Cache-Control: no-cache, private
Date: Thu, 02 Dec 2021 02:29:12 GMT
Set-Cookie: XSRF-
TOKEN=eyJpdiI6InR1YnhEaGlzcWN5d3JDd2ozQ0NlQ3c9PSIsInZhbHVlIjoiWGxZNm9Tb2pnVFlQM20vQ3dNejdSbTVNdU02c0liRDYxdmZRRUhTSWMyZF
VRYkxOeU0rSUk3NitWV2tKYlFjZUFRdG1JUXZEcWdhSC91MW5UaHFqdmJsQmVoQnBUZk1OekoyL3N2cDMzNzRMcHNNczRpTGhFYnB2dlpnTVMvb1ciL
CJtYWMiOiI1NzBiNGI5OTMxNmE4M2FhNDZkNDc2NmFhNjQ4YjlkZDhjYjA4ZGQwNTY2YjEzYjQxMTBlMGMzN2YxNzJiNGFmIn0%3D; expires=Thu, 02-
Dec-2021 04:29:12 GMT; Max-Age=7200; path=/; samesite=lax
Set-Cookie:
caru_session=eyJpdiI6InZhd3YzUS9vNGI4aDVoYTJtS3RCc0E9PSIsInZhbHVlIjoiMzN5U1dYV1Y3OGZrV24vdTVsKy9NcEpYZkJTU3orSHg0ZnNhbXEwWjZ
LUTBTcEg0TGVieENiMjFuaXRTSCtFSWUzd2ZCQzdUR1kwczBlbUZUT2RXbjRnUitzdFVWYmZuNEJieE1qMkl0eFFBUlF2MDNOdndUMnI0V0lzd1ROR2wiL
CJtYWMiOiI1YWEwZTAxNGQ3NWMyMjYyZmRmODc2MmQzZGMwZjQzMTJmYWFlZGJlODRiZmRjNzhhYTgxNml1ZjIxY2JkMjlmIn0%3D; expires=Thu, 02-
Dec-2021 04:29:12 GMT; Max-Age=7200; path=/; httponly; samesite=lax
Content-Length: 7873

<!doctype html>
<html lang="zh-hant">
<head>
```

10.2. https://test-caru.welcometw.com/admin

Previous Next

Summary

Severity:	Information
Confidence:	Certain
Host:	https://test-caru.welcometw.com
Path:	/admin

Issue detail

The response dynamically includes the following script from another domain:

- https://cdnjs.cloudflare.com/ajax/libs/select2/4.0.3/js/select2.min.js

Request 1


```
GET /admin HTTP/1.1
Host: test-caru.welcometw.com
Cookie: XSRF-
TOKEN=eyJpdiI6Ik5sUjJZQWQxeWs1aWpNQkVFbnovRmc9PSIsInZhbHVlIjoiTnVWcFhqSWxRM2VyeDlvVUlWZFk1WlFDTW5PWW8yZ0h4UVFpMU55MWNBN2JXTlJ2OUZKeDR2T0pzSDkwVU5PYUUxcGhPc1FEMlZMOVo5VHNDSFR2VmkxRUF6QnZTZHNGVFRQTVB5blkrRHFyZnJMelNmbU9VRTFTbWg2MnA1UG8iLCJtYWMiOiI0OTdlYjM4YmM3NjQ2YzUxZTVkNzU0NzFlNjM0MDAyNjY2YWFmYTVlYTk4N2I2M2JiOGM5OTEyYzdlMGYxMWIzIn0%3D;
caru_session=eyJpdiI6IklxZ3VSVTZLZEs1QmFkSHRvSERranc9PSIsInZhbHVlIjoiZk9TY3ZRMVg3WHNCV1ZZYkRmYjBLbUkvVFJZOGdpMk1SN1hlNUplY1VzNmFNMDEzQ3F6K1lBZjRINEsycytLSHlzcjUvQTBMaExRZGsxRGMxdEhWejFjTEgwY1lBMUVtYWxVYlA5VzVqRktSUlloN28vSHBCMDZSQXptT0pYZGEiLCJtYWMiOiI3NDJmNThlODZhZjVkNTFhYzJjOWU3ZTQyYWM0ZTI0ZDA4ODM4Yjc4NjYwN2E4ZmM3ZTUyYTQyZmU2ZjRmMzdkIn0%3D;
remember_web_59ba36addc2b2f9401580f014c7f58ea4e30989d=eyJpdiI6Im1jNWltZERONURQYUc5Szl0SXowN2c9PSIsInZhbHVlIjoiUi95RHp6RTh1S0RWd0dCTkRrZWUvd0hPb1lSb0E3a0oybStuR2dVT3dldnpqbjRsUzVMYTdWVUN0U0libjE2OXp4Q2dlUG1ER3JhZjY1WXJTZG9XYldhNG5UU0FFUUZNRDJNVk9rdWhSakgvMEZUWFp4M3BtZGpoRHd1clB0alErNmtXTGFOVnhqbkl5cDh1Y0VoVWlzV3BRdzVnbGRjL09xVk9mWTI0NXRJRExaQlVpieHppRlJEVTZwb2h2bnViSzZOQzZPK3cwZzBnZTFDbG1ySld3RXM3SkZCeitOeXhvV0s3TUtKeDdtT0iLCJtYWMiOiI1ZWY1NDNhNjJkOGI0ZDFhYmQyMzJjMjAzZWMwZGJlZjhlNGNmNzEzNzk5NDI5MjU4Y2ExNTI5YzkyY2Y5OTdiIn0%3D
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
Dnt: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/96.0.4664.45 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: navigate
```


Response 1


```
HTTP/1.1 200 OK
Server: nginx/1.21.3
Content-Type: text/html; charset=UTF-8
Connection: close
Cache-Control: no-cache, private
Date: Thu, 02 Dec 2021 01:41:32 GMT
Set-Cookie: XSRF-
TOKEN=eyJpdiI6ImNtQUxNd3o1VUNFQlg0ams3K04rK0E9PSIsInZhbHVlIjoiNndKSGNCOGpieUhQT0FtTnRrdURWOS9CVmR0NGdTWmMyOWJMVmVMc3l4YmFpTytlaHg3NTRyM1NnRmU5ZGhZaUxCb0JUNVlwMkhSNExkSnh0d2k5dHlqS3FDK295SGpDRUxLZlZlcmtEam9sT3NMTEFJSDhuc0cySk1mcjlwM1AiLCJtYWMiOiI4MjhmOWVjNmFkZjg1ODVmZTRlNDVhZjRkNzM4NTdmOTM2Mjg4M2Q3YzZjNzlxNWYwZTk0YzY2NmUxZTQ1YTA2In0%3D; expires=Thu, 02-Dec-2021 03:41:32 GMT; Max-Age=7200; path=/; samesite=lax
Set-Cookie:
caru_session=eyJpdiI6IjBIL21NZVJUb0NWVldnRlFCMk5qU2c9PSIsInZhbHVlIjoicWZGQkJycHFzTEtUeUd5OFQwUmV2bUYwOTAvQmEwV1VTMUNiUkd2Ly9SL0JCeVlQQW9rVnRpS0lRc1NwR3cvWXRNd3lSREhVTkZEelBWWWdOdlVWZURoVlczUysxV0dKWXNNdkRndnZ1R25LaHZSZ0s2aHNDNlVZT0w4U0RhdjQiLCJtYWMiOiJmZWFlYjg3MzZhMDU3Yzc4ODM5YTk2MTcwZTQ0MjhhYzI3MzEyOGZjMDQyMzc5ZGQ0NTcwYzM3YjRhZjYxMWY4In0%3D; expires=Thu, 02-Dec-2021 03:41:32 GMT; Max-Age=7200; path=/; httponly; samesite=lax
Content-Length: 8260

<!DOCTYPE html>
<html lang="zh-hant">
```


11. Frameable response (potential Clickjacking)

Previous Next

There are 4 instances of this issue:

- /
- /admin
- /login
- /password/reset

Issue description

If a page fails to set an appropriate X-Frame-Options or Content-Security-Policy HTTP header, it might be possible for a page controlled by an attacker to load it within an iframe. This may enable a clickjacking attack, in which the attacker's page overlays the target application's interface with a different interface provided by the attacker. By inducing victim users to perform actions such as mouse clicks and keystrokes, the attacker can cause them to unwittingly carry out actions within the application that is being targeted. This technique allows the attacker to circumvent defenses against cross-site request forgery, and may result in unauthorized actions.

Note that some applications attempt to prevent these attacks from within the HTML page itself, using "framebusting" code. However, this type of defense is normally ineffective and can usually be circumvented by a skilled attacker.

You should determine whether any functions accessible within frameable pages can be used by application users to perform any sensitive actions within the application.

Issue remediation

To effectively prevent framing attacks, the application should return a response header with the name **X-Frame-Options** and the value **DENY** to prevent framing altogether, or the value **SAMEORIGIN** to allow framing only by pages on the same origin as the response itself. Note that the SAMEORIGIN header can be partially bypassed if the application itself can be made to frame untrusted websites.

References

- Web Security Academy: Clickjacking
- X-Frame-Options

Vulnerability classifications

- CWE-693: Protection Mechanism Failure
- CAPEC-103: Clickjacking

11.1. https://test-caru.welcometw.com/

Previous Next

Summary

Severity:	**Information**
Confidence:	**Firm**
Host:	**https://test-caru.welcometw.com**
Path:	/

Request 1

```
GET / HTTP/1.1
Host: test-caru.welcometw.com
Accept-Encoding: gzip, deflate
Accept: */*
Accept-Language: en
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/95.0.4638.54 Safari/537.36
Connection: close
```

Response 1

```
HTTP/1.1 200 OK
Server: nginx/1.21.3
Content-Type: text/html; charset=UTF-8
Connection: close
Cache-Control: no-cache, private
Date: Thu, 02 Dec 2021 02:29:12 GMT
Set-Cookie: XSRF-
TOKEN=eyJpdiI6InR1YnhEaGIzcWN5d3JDd2ozQ0NlQ3c9PSIsInZhbHVlIjoiWGxZNm9Tb2pnVFlQM20vQ3dNejdSbTVNdU02c0liRDYxdmZRRUhTSWMyZF
VRYkxOeU0rSUk3NitWV2tKYlFjZUFRdG1JUXZEcWdhSC91MW5UaHFqdmJsQmVoQnBUZk1OekoyL3N2cDMzNzRMcHNNczRpTGhFYnB2dlpnTVMvb1ciL
CJtYWMiOiI1NzBiNGI5OTMxNmE4M2FhNDZkNDc2NmFhNjQ4YjlkZDhjYjA4ZGQwNTY2YjEzYjQxMTBlMGMzN2YxNzJiNGFmIn0%3D; expires=Thu, 02-
Dec-2021 04:29:12 GMT; Max-Age=7200; path=/; samesite=lax
Set-Cookie:
caru_session=eyJpdiI6InZhd3YzUS9vNGI4aDVoYTJtS3RCc0E9PSIsInZhbHVlIjoiMzN5U1dYV1Y3OGZrV24vdTVsKy9NcEpYZkJTU3orSHg0ZnNhbXEwWjZ
LUTBTcEg0TGVieENiMjFuaXRTSCtFSWUzd2ZCQzdUR1kwczBlbUZUT2RXbjRnUitzdFVWYmZuNEJieE1qMkl0eFFBUlF2MDNOdndUMnI0V0lzd1ROR2wiL
CJtYWMiOiI1YWEwZTAxNGQ3NWMyMjYyZmRmODc2MmQzZGMwZjQzMTJmYWFlZGJlODRiZmRjNzhhYTgxNml1ZjlxY2JkMjlmIn0%3D; expires=Thu, 02-
Dec-2021 04:29:12 GMT; Max-Age=7200; path=/; httponly; samesite=lax
```

```
<html lang="zh-hant">
<head>
```

11.2. https://test-caru.welcometw.com/admin

Previous Next

Summary

Severity:	Information
Confidence:	Firm
Host:	https://test-caru.welcometw.com
Path:	/admin

Request 1

```
GET /admin HTTP/1.1
Host: test-caru.welcometw.com
Cookie: XSRF-
TOKEN=eyJpdiI6Ik5sUjJZQWQxeWs1aWpNQkVFbnovRmc9PSIsInZhbHVlIjoiTnVWcFhqSWxRM2VyeDlvVUlWZFk1WlFDTW5PWW8yZ0h4UVFpMU55MWNBN2JXTlJ2OUZKeDR2T0pzSDkwVU5PYUUxcGhPc1FEMlZMOVo5VHNDSFR2VmkxRUF6QnZTZHNGVFRQTVB5blkrRHFyZnJMelNmbU9VRTFTbWg2MnA1UG8iLCJtYWMiOiI0OTdlYjM4YmM3NjQ2YzUxZTVkNzU0NzFlNjM0MDAyNjY2YWFmYTVlYTk4N2I2M2JiOGM5OTEyYzdlMGYxMWIzIn0%3D;
caru_session=eyJpdiI6IklxZ3VSVTZLZEs1QmFkSHRvSERranc9PSIsInZhbHVlIjoiZk9TY3ZRMVg3WHNCV1ZZYkRmYjBLbUkvVFJZOGdpMk1SN1hlNUplY1VzNmFNMDEzQ3F6K1IBZjRINEsycytLSHlzojUvQTBMaExRZGsxRGMxdEhWejFjTEgwY1IBMUVtYWxVYlA5VzVqRktSUlloN28vSHBCMDZSQXptT0pYZGEiLCJtYWMiOiI3NDJmNThlODZhZjVkNTFhYzJjOWU3ZTQyYWM0ZTI0ZDA4ODM4Yjc4NjYwN2E4ZmM3ZTUyYTQyZmU2ZjRmMzdkIn0%3D;
remember_web_59ba36addc2b2f9401580f014c7f58ea4e30989d=eyJpdiI6Im1jNWltZERONURQYUc5Szl0SXowN2c9PSIsInZhbHVlIjoiUi95RHp6RTh1S0RWd0dCTkRrZWUvd0hPb1lSb0E3a0oybStuR2dVT3dldnpqbjRsUzVMYTdWVUN0U0libjE2OXp4Q2dlUG1ER3JhZjY1WXJTZG9XYldhNG5UU0FFUUZNRDJNVk9rdWhSakgvMEZUWFp4M3BtZGpoRHd1clB0alErNmtXTGFOVnhqbkl5cDh1Y0VoVWlzV3BRdzVnbGRjL09xVk9mWTI0NXRJREExaQVpieHppRlJEVTZwb2h2bnViSzZOQzZPK3owZzBnZTFDbG1ySld3RXM3SkZCeitOeXhvV0s3TUtKeDdtT0iLCJtYWMiOiI1ZWY1NDNhNjJkOGI0ZDFhYmQyMzJjMjAzZWMwZGJlZjhlNGNmNzEzNzk5NDI5MjU4Y2ExNTI5YzkyY2Y5OTdiIn0%3D
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
Dnt: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/96.0.4664.45 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: navigate
```

Response 1

```
HTTP/1.1 200 OK
Server: nginx/1.21.3
Content-Type: text/html; charset=UTF-8
Connection: close
Cache-Control: no-cache, private
Date: Thu, 02 Dec 2021 01:41:32 GMT
Set-Cookie: XSRF-
TOKEN=eyJpdiI6ImNtQUxNd3o1VUNFQlg0ams3K04rK0E9PSIsInZhbHVlIjoiNndKSGNCOGpieUhQT0FtTnRrdURWOS9CVmR0NGdTWmMyOWJMVmVMc3I4YmFpTytlaHg3NTRyM1NnRmU5ZGhZaUxCb0JUNVlwMkhSNExkSnh0d2k5dHlqS3FDK295SGpDRUxLZlZIcmtEam9sT3NMTEFJSDhuc0cySk1mcjIwM1AiLCJtYWMiOiI4MjhmOWVjNmFkZjg1ODVmZTRlNDVhZjRkNzM4NTdmOTM2Mjg4M2Q3YzZjNzIxNWYwZTk0YzY2NmUxZTQ1YTA2In0%3D; expires=Thu, 02-Dec-2021 03:41:32 GMT; Max-Age=7200; path=/; samesite=lax
Set-Cookie:
caru_session=eyJpdiI6IjBIL21NZVJUb0NWVldnRlFCMk5qU2c9PSIsInZhbHVlIjoicWZGQkJycHFzTEtUeUd5OFQwUmV2bUYwOTAvQmEwV1VTMUNiUkd2Ly9SL0JCeVlQQW9rVnRpS0lRc1NwR3cvWXRNd3lSREhVTkZEelBWWWdOdlVWZURoVlczUysxV0dKWXNNdkRndnZ1R25LaHZSZ0s2aHNDNlVZT0w4U0RhdjQiLCJtYWMiOiJmZWFlYjg3MzZhMDU3Yzc4ODM5YTk2MTcwZTQ0MjhhYzI3MzEyOGZjMDQyMzc5ZGQ0NTcwYzM3YjRhZjYxMWY4In0%3D;
expires=Thu, 02-Dec-2021 03:41:32 GMT; Max-Age=7200; path=/; httponly; samesite=lax
Content-Length: 8260

<!DOCTYPE html>
<html lang="zh-hant">
```

11.3. https://test-caru.welcometw.com/login

Previous Next

Summary

Severity:	Information
Confidence:	Firm
Host:	https://test-caru.welcometw.com

Request 1

```
GET /login HTTP/1.1
Host: test-caru.welcometw.com
Cookie: XSRF-
TOKEN=eyJpdiI6IkFVTlBWYjYyeVJUbW5waC9rZktBM2c9PSIsInZhbHVlIjoiOUY5bkdhaEVCTUdoempxNXczK2RIRXISNGpXK3NVdjVCUVVzdWFOcnVyMX
JpTER2RCs2aDJJbEhITWM3S2RzeVNPZGpCNERzVjdPOGRWZFNWRUc1ZUU1cTVvOHZXQ2NEOWk4WjlwNXRmeFpLYks4Zkd0Snp4RWlYVjR2YXNU
MGkiLCJtYWMiOiI2OWQ1Mzc3OWUwNTBkMDE3ZjVjY2QzMmI3N2UwZTc2NjVhMTBhMGNjNzVhYjZhMDA3MDJhNDEzYzdjNmNkZmNlIn0%3D;
caru_session=eyJpdiI6IlU2NEFTcWNsbFNudjluODhlTU8xdFE9PSIsInZhbHVlIjoicEptRDFwWnhHQ216dHpBVHZ3MzR0ZTVaT1VUbFQxZXJsNVJVaDFWS2
gyQ2FNZ2k5RVljZ2pIT2JEZ0tdFFDKzErZUpkeFFMK2pmVFVkWlRNSERwTUYvSkVPK3M4NXZhWFZRZy9pLzhqNyszaEwrSmhxa29XMFloalFyS1Z6MWEi
LCJtYWMiOiJiMmY2ODY2NjQ1OWEyMTM5MTQ3NzYxODM5NjA2ZmFmZWZmY2M4OTQ1NDM3Y2NjZjVjNzIzOWE4YzFmNjc4N2YyIn0%3D
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
Dnt: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/96.0.4664.45 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Sec-Fetch-Dest: document
Sec-Ch-Ua: " Not A;Brand";v="99", "Chromium";v="96", "Google Chrome";v="96"
Sec-Ch-Ua-Mobile: ?0
Sec-Ch-Ua-Platform: "Windows"
```

Response 1

```
HTTP/1.1 200 OK
Server: nginx/1.21.3
Content-Type: text/html; charset=UTF-8
Connection: close
Cache-Control: no-cache, private
Date: Thu, 02 Dec 2021 01:36:38 GMT
Set-Cookie: XSRF-
TOKEN=eyJpdiI6IkZWQ0h5K1JldWFHQ28rY25sSzlrVlE9PSIsInZhbHVlIjoiaWxoT3FIQTE0WUZEazcrRVE4SUhNSDVTZlIrRnJHMVowalRZelVoQ3hibFFTVH
p4OUt6Q3k1S2YxVE1FT25uRzJ3aWlkRExsRXdCV0Rib0FKbDhVOTI5NExseXNGTzZSRmMwSHM0L0kyRzVJcC9ZWmNRdkd6WjBnMDgwMVRyUzgiLCJt
YWMiOiJhMmU1ZjI0MzUwMTM4MzkwYzE5MDI4NGRhOTEyNGQwMmMwYTdmMTVhMjNjNzliOWMxNTMzM2EwY2Q3NDdjMDdhIn0%3D; expires=Thu,
02-Dec-2021 03:36:38 GMT; Max-Age=7200; path=/; samesite=lax
Set-Cookie:
caru_session=eyJpdiI6IlJQc2pPNzdYZ0V2L1lURDRIM0VGVGc9PSIsInZhbHVlIjoiZ0dzUkJHS0hueXUwbWQxZ2VPMGpmdWNCdlhaR1RQaHhFSlFXeTlwV
zQyS0h2a0lrUWtpYXl0cTQxaFJ6Rzdycng0azA5VWt5TmpWRngyelB2dWZNcEY1c1JOSDdHbSsxV3pramdmNnZ5N2hRejdnNW8yWlNZWHNPWnBMTmhU
ZXYiLCJtYWMiOiIxYWM0MjFkNTRlYzI5MDA1MWI0ZDg0NjFiZTgxYWNiZjgyY2ExMjVjNTM5ZTc4ZDVhYmM0ODc5OTBkNWIwMzU3In0%3D; expires=Thu,
02-Dec-2021 03:36:38 GMT; Max-Age=7200; path=/; httponly; samesite=lax
Content-Length: 3427

<!doctype html>
<html lang="zh-hant">
<head>
```

11.4. https://test-caru.welcometw.com/password/reset

Previous Next

Summary

Severity:	**Information**
Confidence:	**Firm**
Host:	**https://test-caru.welcometw.com**
Path:	**/password/reset**

Request 1

```
GET /password/reset HTTP/1.1
Host: test-caru.welcometw.com
Accept-Encoding: gzip, deflate
Accept: */*
Accept-Language: en
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/95.0.4638.54 Safari/537.36
Connection: close
```

Response 1


```
HTTP/1.1 200 OK
Server: nginx/1.21.3
Content-Type: text/html; charset=UTF-8
Connection: close
Cache-Control: no-cache, private
Date: Thu, 02 Dec 2021 02:29:13 GMT
Set-Cookie: XSRF-
TOKEN=eyJpdiI6IkdtSWhjN1ZRNmh5QVh4dEMrOE1iaVE9PSIsInZhbHVlIjoidTNkYzFjcnhaTUNXbjYzU3ppNkdlY1RKRFErNUxsL2xtUzRxM2VxSWRBb01B
ejVPRHoxUTA3bUlCNUpaYVJQSGlHWmpqejlMdDNyemtVb2VtR3J1ajFqTGNEVW5EcytsVnJOaXFLZ2ppWU6xeHV4ZXNYU1NsTVJFSlNRWDdMc3AiLCJt
YWMiOiJhMDE2MjU4MDg3ZTU4ZjgzN2Y0YTAzNDRiMWJiZTg0NzU4ZTllN2FmZWI3NzY0M2Q3YjE5NjQxOGU5MjM0NWRkIn0%3D; expires=Thu, 02-Dec-
2021 04:29:13 GMT; Max-Age=7200; path=/; samesite=lax
Set-Cookie:
caru_session=eyJpdiI6IldEQlZQWlI0NEVkQnU5RGpnL3dlWE9PSIsInZhbHVlIjoiZHNZcW01N3A2eitROTFSc2FFRExrbGFEbkVaald8NUYrbnp3bjdjWGxyQU
pyWmpSUVZhOUZUSjZ5eWlyNzVLQzNZdE5KRUZEb0ZHYm1ZZlVyR1phS1ZpNkMyNEwrMlhhNEc4VGp2MDIzQUo3S1I2QjU1WUZFWGRoVWVFuRGJCa
WsiLCJtYWMiOiJlNzU2ZTBiN2NhM2ZlZjAxZjBkMGIwNzY5NGMyOTdlZWQ0MjQyNjgwZmNkYjc0NTVlMmMwZjM0YzUzMGEwNDYzIn0%3D; expires=Thu,
02-Dec-2021 04:29:13 GMT; Max-Age=7200; path=/; httponly; samesite=lax
Content-Length: 1621

<!doctype html>
<html lang="zh-hant">
<head>
```


12. Email addresses disclosed

Previous Next

Summary

Severity:	**Information**
Confidence:	**Certain**
Host:	**https://test-caru.welcometw.com**
Path:	**/login**

Issue detail

The following email address was disclosed in the response:

- superadministrator@app.com

Issue background

The presence of email addresses within application responses does not necessarily constitute a security vulnerability. Email addresses may appear intentionally within contact information, and many applications (such as web mail) include arbitrary third-party email addresses within their core content.

However, email addresses of developers and other individuals (whether appearing on-screen or hidden within page source) may disclose information that is useful to an attacker; for example, they may represent usernames that can be used at the application's login, and they may be used in social engineering attacks against the organization's personnel. Unnecessary or excessive disclosure of email addresses may also lead to an increase in the volume of spam email received.

Issue remediation

Consider removing any email addresses that are unnecessary, or replacing personal addresses with anonymous mailbox addresses (such as helpdesk@example.com).

To reduce the quantity of spam sent to anonymous mailbox addresses, consider hiding the email address and instead providing a form that generates the email server-side, protected by a CAPTCHA if necessary.

References

- Web Security Academy: Information disclosure

Vulnerability classifications

- CWE-200: Information Exposure
- CAPEC-37: Retrieve Embedded Sensitive Data

Request 1


```
GET /login HTTP/1.1
Host: test-caru.welcometw.com
Cookie: XSRF-
```

```
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Sec-Fetch-Dest: document
Sec-Ch-Ua: " Not A;Brand";v="99", "Chromium";v="96", "Google Chrome";v="96"
Sec-Ch-Ua-Mobile: ?0
Sec-Ch-Ua-Platform: "Windows"
```

Response 1

```
HTTP/1.1 200 OK
Server: nginx/1.21.3
Content-Type: text/html; charset=UTF-8
Connection: close
Cache-Control: no-cache, private
Date: Thu, 02 Dec 2021 01:36:38 GMT
Set-Cookie: XSRF-
TOKEN=eyJpdiI6IkZWQ0h5K1JldWFHQ28rY25sSzlrVlE9PSIsInZhbHVlIjoiaWxoT3FIQTE0WUZEazcrRVE4SUhNSDVTZlIrRnJHMVcwalRZelVoQ3hibFFTVHp4OUt6Q3k1S2YxVE1FT25uRzJ3aWlkRExsRXdCV0Rib0FKbDhVOTI5NExseXNGTzZSRmMwSHM0L0kyRzVJcC9ZWmNRdkd6WjBnMDgwMVRyUzgiLCJtYWMiOiJhMmU1ZjI0MzUwMTM4MzkwYzE5MDI4NGRhOTEyNGQwMmMwYTdmMTVhMjNjNzliOWMxNTMzM2EwY2Q3NDdjMDdhIn0%3D; expires=Thu, 02-Dec-2021 03:36:38 GMT; Max-Age=7200; path=/; samesite=lax
Set-Cookie:
caru_session=eyJpdiI6IlJQc2pPNzdYZ0V2L1lURDRIM0VGVGc9PSIsInZhbHVlIjoiZ0dzUkJHS0hueXUwbWQxZ2VPMGpmdWNCdlhaR1RQaHhFSlFXeTlwVzQyS0h2a0lrUWtpYXl0cTQxaFJ6Rzdycng0azA5VWt5TmpWRngyelB2dWZNcEY1c1JOSDdHbSsxV3pramdmNnZ5N2hRejdnNW8yWlNZWHNPWnBMTmhUZXYiLCJtYWMiOiIxYWM0MjFkNTRlYzI5MDA1MWI0ZDg0NjFiZTgxYWNiZjgyY2ExMjVjNTM5ZTc4ZDVhYmM0ODc5OTBkNWIwMzU3In0%3D; expires=Thu, 02-Dec-2021 03:36:38 GMT; Max-Age=7200; path=/; httponly; samesite=lax
Content-Length: 3427

<!doctype html>
<html lang="zh-hant">
<head>
```

13. Robots.txt file

Previous Next

Summary

Severity:	**Information**
Confidence:	**Certain**
Host:	**https://test-caru.welcometw.com**
Path:	**/robots.txt**

Issue detail

The web server contains a robots.txt file.

Issue background

The file robots.txt is used to give instructions to web robots, such as search engine crawlers, about locations within the web site that robots are allowed, or not allowed, to crawl and index.

The presence of the robots.txt does not in itself present any kind of security vulnerability. However, it is often used to identify restricted or private areas of a site's contents. The information in the file may therefore help an attacker to map out the site's contents, especially if some of the locations identified are not linked from elsewhere in the site. If the application relies on robots.txt to protect access to these areas, and does not enforce proper access control over them, then this presents a serious vulnerability.

Issue remediation

The robots.txt file is not itself a security threat, and its correct use can represent good practice for non-security reasons. You should not assume that all web robots will honor the file's instructions. Rather, assume that attackers will pay close attention to any locations identified in the file. Do not rely on robots.txt to provide any kind of protection over unauthorized access.

Vulnerability classifications

- CWE-200: Information Exposure

Request 1

```
GET /robots.txt HTTP/1.1
Host: test-caru.welcometw.com
Accept-Encoding: gzip, deflate
```

Response 1

```
HTTP/1.1 200 OK
Server: nginx/1.21.3
Date: Thu, 02 Dec 2021 01:41:32 GMT
Content-Type: text/plain
Content-Length: 24
Last-Modified: Wed, 01 Dec 2021 09:03:16 GMT
Connection: close
ETag: "61a73a54-18"
Accept-Ranges: bytes

User-agent: *
Disallow:
```

14. Cacheable HTTPS response

Previous Next

There are 2 instances of this issue:

- /robots.txt
- /svg/logo.svg

Issue description

Unless directed otherwise, browsers may store a local cached copy of content received from web servers. Some browsers, including Internet Explorer, cache content accessed via HTTPS. If sensitive information in application responses is stored in the local cache, then this may be retrieved by other users who have access to the same computer at a future time.

Issue remediation

Applications should return caching directives instructing browsers not to store local copies of any sensitive data. Often, this can be achieved by configuring the web server to prevent caching for relevant paths within the web root. Alternatively, most web development platforms allow you to control the server's caching directives from within individual scripts. Ideally, the web server should return the following HTTP headers in all responses containing sensitive content:

- Cache-control: no-store
- Pragma: no-cache

References

- Web Security Academy: Information disclosure

Vulnerability classifications

- CWE-524: Information Exposure Through Caching
- CWE-525: Information Exposure Through Browser Caching
- CAPEC-37: Retrieve Embedded Sensitive Data

14.1. https://test-caru.welcometw.com/robots.txt

Previous Next

Summary

Severity:	**Information**
Confidence:	**Certain**
Host:	**https://test-caru.welcometw.com**
Path:	**/robots.txt**

Request 1

```
GET /robots.txt HTTP/1.1
Host: test-caru.welcometw.com
Accept-Encoding: gzip, deflate
Accept: */*
Accept-Language: en
```

```
HTTP/1.1 200 OK
Server: nginx/1.21.3
Date: Thu, 02 Dec 2021 01:41:32 GMT
Content-Type: text/plain
Content-Length: 24
Last-Modified: Wed, 01 Dec 2021 09:03:16 GMT
Connection: close
ETag: "61a73a54-18"
Accept-Ranges: bytes

User-agent: *
Disallow:
```

14.2. https://test-caru.welcometw.com/svg/logo.svg

Previous Next

Summary

Severity:	**Information**
Confidence:	**Certain**
Host:	**https://test-caru.welcometw.com**
Path:	**/svg/logo.svg**

Request 1

```
GET /svg/logo.svg HTTP/1.1
Host: test-caru.welcometw.com
Accept-Encoding: gzip, deflate
Accept: */*
Accept-Language: en
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/95.0.4638.54 Safari/537.36
Connection: close
```

Response 1

```
HTTP/1.1 200 OK
Server: nginx/1.21.3
Date: Thu, 02 Dec 2021 02:29:12 GMT
Content-Type: image/svg+xml
Content-Length: 3329
Last-Modified: Thu, 02 Dec 2021 01:55:34 GMT
Connection: close
ETag: "61a82796-d01"
Accept-Ranges: bytes

<?xml version="1.0" encoding="utf-8"?>
<!-- Generator: Adobe Illustrator 25.0.1, SVG Export Plug-In . SVG Version: 6.00 Build 0) -->
<svg version="1.1" id="....._1" xmlns="http://www.w3.org/2000/svg
...[SNIP]...
```

15. Base64-encoded data in parameter

Previous Next

There are 7 instances of this issue:

- /admin
- /admin
- /login
- /login
- /login
- /login
- /robots.txt

Issue background

Applications sometimes Base64-encode parameters in an attempt to obfuscate them from users or facilitate transport of binary data. The presence of Base64-encoded data may indicate security-sensitive information or functionality that is worthy of further investigation. The data should be reviewed to determine whether it contains any interesting information, or provides any additional entry points for malicious input.

Severity:	Information
Confidence:	Firm
Host:	https://test-caru.welcometw.com
Path:	/admin

Issue detail

The following parameters appear to contain Base64-encoded data:

- **XSRF-TOKEN = {"iv":"JCqU6Cjj8bHadrI1TLjcXw==","value":"ZpL2BScu4wazPKXPYFZkaU4e1NK4YaKk4Gi6tGzzBdzQ2mUkQAWvENXTd79BDtY6KzkoE2oL7rxkC+jzVr9w26ZdLzCjwvrNoY0CivR55GxK4jZ3dVbAaFg6myKIVNJF","mac":"4e184c51d369ca1ba326a2db532421eed9ece6734214b6c1ef3549ac59340ba5"}**
- **caru_session = {"iv":"ZKmZU3K9NUUAQr9PsgsRRA==","value":"HZ1UtlAiT9Z1Z8cicMGUT3249x9ppw2COOznS8foF0Ot2+hCkELUKsatGAaKrl3/upyxv+m3gm7QPAqMt/x22qjt78jHsI2JFy0FV/YLoxa9TB3wWGKGs0kDLUt23cSF","mac":"5bd894de0c6547e405153550e0a0e23ee1a3ccdda047c540a6cf029619d09112"}**

Request 1

```
GET /admin HTTP/1.1
Host: test-caru.welcometw.com
Cookie: XSRF-TOKEN=eyJpdiI6IkpDcVU2Q2pqOGJlYWRySTFUTGpjWHc9PSIsInZhbHVlIjoiWnBMMkJTY3U0d2F6UEtYUFlGWmthVTRIMU5LNFlhS2s0R2k2dEd6ekJkelEybVVrUUFXdkVOWFRkNzlCRHRZNkt6a29FMm9MN3J4a0MranpWcjI3MjZaZEx6Q2p3dnJOb1kwQ2I2UjU1R3hLNGpaM2RWYkFhRmc2bXlLbFZOSkYiLCJtYWMiOiI0ZTE4NGM1MWQzNjljYTFiYTMyNmEyZGI1MzI0MjFlZWQ5ZWNlNjczNDIxNGI2YzFlZjM1NDlhYzU5MzQwYmE1In0%3D; caru_session=eyJpdiI6IlpLbVpVM0s5TlVVQVFyOVBzZ3NSUkE9PSIsInZhbHVlIjoiSFoxVXRJQWlUOVoxWjhjaWNNR1VUMzI0OXg5cHB3MkNPT3puUzhmb0YwT3QyK2hDa0VMVUtzYXRHQWFLckkzL3VweXh2K20zZ203UVBBcU10L3gyMnFqdDc4akhzbDJKRnkwRlYvWUxveGE5VElzd1dHS0dzMGtETFV0MjNjU0YiLCJtYWMiOiI1YmQ4OTRkZTBjNjU0N2U0MDUxNTM1NTBlMGEwZTIzZWUxYTNjY2RkYTA0N2M1NDBhNmNmMDI5NjE5ZDA5MTEyIn0%3D
Cache-Control: max-age=0
Dnt: 1
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/96.0.4664.45 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Sec-Fetch-Dest: document
Sec-Ch-Ua: " Not A;Brand";v="99", "Chromium";v="96", "Google Chrome";v="96"
Sec-Ch-Ua-Mobile: ?0
Sec-Ch-Ua-Platform: "Windows"
```

Response 1

```
HTTP/1.1 302 Found
Server: nginx/1.21.3
Content-Type: text/html; charset=UTF-8
Connection: close
Cache-Control: no-cache, private
Date: Thu, 02 Dec 2021 01:36:35 GMT
Location: https://test-caru.welcometw.com/login
Set-Cookie: XSRF-TOKEN=eyJpdiI6IklkVVNncnRhQXprbHNtbGhHa3FUblE9PSIsInZhbHVlIjoiTUkyTWdDcUlZWUhKVWJXdk40bHltN29pVlBiajMzVXlyZFBtRVRGWi9zSS9NYVBNbEVubGhpRUEwV3Nlcitwb1FYaE5KMjZHUExrcGlNR2kxRG9lVVlTUXRkSng4emxuZlZhdndzSitFc0xSUUt4T3RaTlRUZ0VBemJNVHZ1N1YiLCJtYWMiOiJiMWRhZmNiMWE3NzNiZTkyNDcwNDRmODk5NjRjOGQ0Zjk5ODA3YmRlZWZhZTU3OTMzMzc3MzFmYzlmNWE4MjU1In0%3D; expires=Thu, 02-Dec-2021 03:36:35 GMT; Max-Age=7200; path=/; samesite=lax
Set-Cookie: caru_session=eyJpdiI6ImpraVNYZUJTS1lpUXFnWFY3RUt4d0E9PSIsInZhbHVlIjoiMmlpdVBlYjlwTmk5UkVkMWFsQnBZY1dibnBpd0xuUmdiQWFtellkV0NETWtLczdWeGxkQmNBNXRWMzNmRkhnT1djVE9yQkNXSFFWSzk1RUk5S2RTNm5aUVdjNHYxT2dXRDdQc05RcjhBNnRRRTJCdGtrWW9PQmpRQVVjYWQwbU4iLCJtYWMiOiIzMGExZGFjZmZhNDZhMTJlMDkwMTEwMTc3YzQ0YmRjNjNjODg3ZWJjZDQzODI3MDhkYjQ2OTQ2ZDA0MjdhMjdiIn0%3D; expires=Thu, 02-Dec-2021 03:36:35 GMT; Max-Age=7200; path=/; httponly; samesite=lax
Content-Length: 394

<!DOCTYPE html>
<html>
```

15.2. https://test-caru.welcometw.com/admin

Previous Next

Summary

Severity:	Information

Request 1

```
GET /admin HTTP/1.1
Host: test-caru.welcometw.com
Cookie: XSRF-
TOKEN=eyJpdiI6Ik5sUjJZQWQxeWs1aWpNQkVFbnovRmc9PSIsInZhbHVlIjoiTnVWcFhqSWxRM2VyeDlvVUlWZFk1WlFDTW5PWW8yZ0h4UVFpMU55MWNBN2JXTlJ2OUZKeDR2T0pzSDkwV5PYUUxcGhPc1FEMlZMOVo5VHNDSFR2VmkxRUF6QnZTZHNGVFRQTVB5blkrRHFyZnJMelNmbU9VRTFTbWg2MnA1UG8iLCJtYWMiOiI0OTdlYjM4YmM3NjQ2YzUxZTVkNzU0NzFlNjM0MDAyNjY2YWFmYTVlYTk4N2I2M2JiOGM5OTEyYzdlMGYxMWIzIn0%3D;
caru_session=eyJpdiI6IklxZ3VSVTZLZEs1QmFkSHRvSERranc9PSIsInZhbHVlIjoiZk9TY3ZRMVg3WHNCV1ZZYkRmYjBLbUkvVFJZOGdpMk1SN1hlNUplY1VzNmFNMDEzQ3F6K1lBZjRlNEsycytLSHIzcjUvQTBMaExRZGsxRGMxdEhWejFjTEgwY1lBMUVtYWxVYlA5VzVqRktSUlloN28vSHBCMDZSQXptT0pYZGEiLCJtYWMiOiI3NDJmNThlODZhZjVkNTFhYzJjOWU3ZTQyYWM0ZTI0ZDA4ODM4Yjc4NjYwN2E4ZmM3ZTUyYTQyZmU2ZjRmMzdkIn0%3D;
remember_web_59ba36addc2b2f9401580f014c7f58ea4e30989d=eyJpdiI6Im1jNWltZERONURQYUc5SzI0SXowN2c9PSIsInZhbHVlIjoiUi95RHp6RTh1S0RWd0dCTkRrZWUvd0hPb1lSb0E3a0oybStuR2dVT3dldnpqbjRsUzVMYTdWVUN0U0libjE2OXp4Q2dlUG1ER3JhZjY1WXJTZG9XYldhNG5UU0FFUUZNRDJNVk9rdWhSakgvMEZUWFp4M3BtZGpoRHd1clB0alErNmtXTGFOVnhqbkl5cDh1Y0VoVWlzV3BRdzVnbGRjL09xVk9mWTI0NXRJREexaQVpieHppRlJEVTZwb2h2bnViSzZOQzZPK3cwZzBnZTFDbG1ySld3RXM3SkZCeitOeXhvV0s3TUtKeDdtTT0iLCJtYWMiOiI1ZWY1NDNhNjJkOGI0ZDFhYmQyMzJjMjAzZWMwZGJlZjhlNGNmNzEzNzk5NDI5MjU4Y2ExNTI5YzkyY2Y5OTdiIn0%3D
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
Dnt: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/96.0.4664.45 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: navigate
```

Response 1

```
HTTP/1.1 200 OK
Server: nginx/1.21.3
Content-Type: text/html; charset=UTF-8
Connection: close
Cache-Control: no-cache, private
Date: Thu, 02 Dec 2021 01:41:32 GMT
Set-Cookie: XSRF-
TOKEN=eyJpdiI6ImNtQUxNd3o1VUNFQlg0ams3K04rK0E9PSIsInZhbHVlIjoiNndKSGNCOGpieUhQT0FtTnRrdURWOS9CVmR0NGdTWmMyOWJMVmVMc3l4YmFpTytlaHg3NTRyM1NnRmU5ZGhZaUxCb0JUNVlwMkhSNExkSnh0d2k5dHlqS3FDK295SGpDRUxLZlZIcmtEam9sT3NMTEFJSDhuc0cySk1mcjlwM1AiLCJtYWMiOiI4MjhmOWVjNmFkZjg1ODVmZTRlNDVhZjRkNzM4NTdmOTM2Mjg4M2Q3YzZjNzIxNWYwZTk0YzY2NmUxZTQ1YTA2In0%3D; expires=Thu, 02-Dec-2021 03:41:32 GMT; Max-Age=7200; path=/; samesite=lax
Set-Cookie:
caru_session=eyJpdiI6IjBIL21NZVJUb0NWVldnRlFCMk5qU2c9PSIsInZhbHVlIjoicWZGQkJycHFzTEtUeUd5OFQwUmV2bUYwOTAvQmEwV1VTMUNiUkd2Ly9SL0JCeVlQQW9rVnRpS0lRc1NwR3cvWXRNd3lSREhVTkZEelBWWWdOdlVWZURoVlczUysxV0dKWXNNdkRndnZ1R25LaHZSZ0s2aHNDNlVZT0w4U0RhdjQiLCJtYWMiOiJmZWFlYjg3MzZhMDU3Yzc4ODM5YTk2MTcwZTQ0MjhhYzI3MzEyOGZjMDQyMzc5ZGQ0NTcwYzM3YjRhZjYxMWY4In0%3D;
expires=Thu, 02-Dec-2021 03:41:32 GMT; Max-Age=7200; path=/; httponly; samesite=lax
Content-Length: 8260

<!DOCTYPE html>
<html lang="zh-hant">
```

15.3. https://test-caru.welcometw.com/login

Previous Next

Summary

Severity:	Information
Confidence:	Firm
Host:	https://test-caru.welcometw.com
Path:	/login

Issue detail

The following parameters appear to contain Base64-encoded data:

- **XSRF-TOKEN =**
  {"iv":"F89C73EzDKxBfVwuIEP0mQ==","value":"KxDkNLQ9Xj4RQXJxstrkBChXoljRGGgMGVOTi50uMBsgSDXj3telY2uNtxjq2rN7b0uKwBjCnBrkzR+dJ9ujKhRZAobo4wAOzqmPZaebo8TmSv1xoNNfweeC2fFVow6P","mac":"e477a65c4070b92e9acd257955a820c258efcaae843eac3b63c335d0feaba07d"}
- **caru_session =**
  {"iv":"DuEw3k1YvM9KdeA5JHkk4A==","value":"Ww+qJy8Nr49xKOQwIdPEF65uSYTGIS1tsDCLyZbKqn2pA+31P+db1op+F1eOrcLUFhx3+2Dco8Z1/Kg1krZKKJXP737P93kKbzwtYRFwuQOmwA0mbZdGC/7nE60Fj7br","mac":"4e3a4bc89431bf3e8d8ba7977baa92e77e6825aa2dd8a118eb751e2e867077f2"}

```
Connection: close

email=superadministrator%40app.com&password=+tripgds0&remember=on&_token=KN01TC6ZKzBKgXmhchZB5NxwCexoABqSO8SA4qqp
```

Response 1

```
HTTP/1.1 302 Found
Server: nginx/1.21.3
Content-Type: text/html; charset=UTF-8
Connection: close
Cache-Control: no-cache, private
Date: Thu, 02 Dec 2021 01:32:14 GMT
Location: https://test-caru.welcometw.com/admin
Set-Cookie: XSRF-
TOKEN=eyJpdiI6IkpDcVU2Q2pqOGJlYWRySTFUTGpjWHc9PSIsInZhbHVlIjoiWnBMMkJTY3U0d2F6UEtYUFlGWmthVTRlMU5LNFlhS2s0R2k2dEd6ekJkelEybVVrUUFXdkVOWFRkNzlCRHRZNkt6a29FMm9MN3J4a0MranpWcjl3MjZaZEx6Q2p3dnJOb1kwQ2l2UjU1R3hLNGpaM2RWYkFhRmc2bXlLbFZOSkYiLCJtYWMiOiI0ZTE4NGM1MWQzNjljYTFiYTMyNmEyZGI1MzI0MjFlZWQ5ZWNlNjczNDIxNGI2YzFlZjM1NDlhYzU5MzQwYmE1In0%3D; expires=Thu, 02-Dec-2021 03:32:14 GMT; Max-Age=7200; path=/; samesite=lax
Set-Cookie:
caru_session=eyJpdiI6IlpLbVpVM0s5TlVVQVFyOVBzZ3NSUkE9PSIsInZhbHVlIjoiSFoxVXRJQWlUOVoxWjhjaWNNR1VUMzI0OXg5cHB3MkNPT3puUzhmb0YwT3QyK2hDa0VMVUtzYXRHQWFLckkzL3VweXh2K20zZ203UVBBcU10L3gyMnFqdDc4akhzbDJKRnkwRlYvWUxveGE5VElzd1dHS0dzMGtETFV0MjNjU0YiLCJtYWMiOiI1YmQ4OTRkZTBjNjU0N2U0MDUxNTM1NTBlMGEwZTIzZWUxYTNjY2RkYTA0N2M1NDBhNmNmMDI5NjE5ZDA5MTEyIn0%3D; expires=Thu, 02-Dec-2021 03:32:14 GMT; Max-Age=7200; path=/; httponly; samesite=lax
Content-Length: 394

<!DOCTYPE html>
<html>
```

15.4. https://test-caru.welcometw.com/login

Previous Next

Summary

Severity:	**Information**
Confidence:	**Firm**
Host:	**https://test-caru.welcometw.com**
Path:	**/login**

Issue detail

The following parameters appear to contain Base64-encoded data:

- **XSRF-TOKEN = {"iv":"AUNPVb62yRTmnph/kfKA3g==","value":"9F9nGahEBMGhzjq5w3+dHEyR4jW+sUv5BQUsuaNrur1riLDvD+6h2lIHHMc7KdsySOdjB4DsV7O8dVdSVEG5eE5q5o8vWCcD9i8Z205tfxZKbK8fGtJzxEiXV4vasT0i","mac":"69d53779e050d017f5ccd32b77e0e7665a10a0cc75ab6a00702a413c7c6cdfce"}**
- **caru_session = {"iv":"U64ASqcIISnv9n88eMO1tQ==","value":"pJmD1pZxGCmztzATvw34te5ZOUTIT1erl5RUh1VKh2CaMgi9EYcgjeObDglmtQC+1+eJdxQL+jfTUdZTMHDpMF/JEO+s85vaXVQg/i/8j7+3hL+JhqkoW0YhjQrKVz1a","mac":"b2f68666459a2139147761839606fafeffcc8945437cccf5c7239a8c1f6787f2"}**

Request 1

```
GET /login HTTP/1.1
Host: test-caru.welcometw.com
Cookie: XSRF-
TOKEN=eyJpdiI6IkFVTlBWYjYyeVJUbW5waC9rZktBM2c9PSIsInZhbHVlIjoiOUY5bkdhaEVCTUdoempxNXczK2RlRXlSNGpXK3NVdjVCUVVzdWFOcnVyMXJpTER2RCs2aDJJbEhlTWM3S2RzeVNPZGpCNERzVjdPOGRWZFNWRUc1ZUU1cTVvOHZXQ2NEOWk4WjlwNXRmeFpLYks4Zkd0Snp4RWlYVjR2YXNUMGkiLCJtYWMiOiI2OWQ1Mzc3OWUwNTBkMDE3ZjVjY2QzMml3N2UwZTc2NjVhMTBhMGNjNzVhYjZhMDA3MDJhNDEzYzdjNmNkZmNlIn0%3D; caru_session=eyJpdiI6IlU2NEFTcWNsbFNudjluODhlTU8xdFE9PSIsInZhbHVlIjoicEptRDFwWnhHQ216dHpBVHZ3MzR0ZTVaT1VUbFQxZXJsNVJVaDFWS2gyQ2FNZ2k5RVljZ2plT2JEZ0ltdFFDKzErZUpkeFFMK2pmVFVkWlRNSERwTUYvSkVPK3M4NXZhWFZRZy9pLzhqNyszaEwrSmhxa29XMFloalFyS1Z6MWEiLCJtYWMiOiJiMmY2ODY2NjQ1OWEyMTM5MTQ3NzYxODM5NjA2ZmFmZWZmY2M4OTQ1NDM3Y2NjZjVjNzIzOWE4YzFmNjc4N2YyIn0%3D
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
Dnt: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/96.0.4664.45 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Sec-Fetch-Dest: document
Sec-Ch-Ua: " Not A;Brand";v="99", "Chromium";v="96", "Google Chrome";v="96"
Sec-Ch-Ua-Mobile: ?0
Sec-Ch-Ua-Platform: "Windows"
```

```
<!doctype html>
<html lang="zh-hant">
<head>
```

15.5. https://test-caru.welcometw.com/login

Previous Next

Summary

Severity:	**Information**
Confidence:	**Firm**
Host:	**https://test-caru.welcometw.com**
Path:	**/login**

Issue detail

The following parameters appear to contain Base64-encoded data:

- **XSRF-TOKEN = {"iv":"FVCHy+ReuaGCo+cnIK9kVQ==","value":"ilqOqHA14YFDk7+EQ8lHMH5SfR+FrG1W0jTYzUhCxbIQSTzx9KzCy5Kf1TMEOnnG2wiidDLIEwBWDboAJI8U9294LIysFO6RFc0Hs4/I2G5Ip/YZcQvGzZ0g0801TrS8","mac":"a2e5f24350138390c190284da9124d02c0a7f15a23c79b9c15333a0cd747c07a"}**
- **caru_session = {"iv":"RPsjO77XgEv/YTD4H3EFTg==","value":"gGsRBGKHnyu0md1geO0jfucBvXZGTPhxEJQWy9pW42KHvkB+Qkiaytq41hRzG7rrx4k09UkyNjVFx2zPvufMpF5sRNH7Gm+1Wzkjgf6vy7hQz7g5o2ZSYXsOZpLNhTev","mac":"1ac421d54ec290051b4d8461be81acbf82ca125c539e78d5abc487990d5b0357"}**

Request 1

```
POST /login HTTP/1.1
Host: test-caru.welcometw.com
Cookie: XSRF-
TOKEN=eyJpdiI6IkZWQ0h5K1JldWFHQ28rY25sSzlrVlE9PSIsInZhbHVlIjoiaWxxT3FIQTE0WUZEazcrRVE4SUhNSDVTZlIrRnJHMVcwalRZelVoQ3hibFFTVHp4OUt6Q3k1S2YxVE1FT25uRzJ3aWlkRExsRXdCV0Rib0FKbDhVOTI5NExseXNGTzZSRmMwSHM0L0kyRzVJcC9ZWmNRdkd6WjBnMDgwMVRyUzgiLCJtYWMiOiJhMmU1ZjI0MzUwMTM4MzkwYzE5MDI4NGRhOTEyNGQwMmMwYTdmMTVhMjNjNzliOWMxNTMzM2EwY2Q3NDdjMDdhIn0%3D;
caru_session=eyJpdiI6IlJQc2pPNzdYZ0V2L1IURDRlM0VGVGc9PSIsInZhbHVlIjoiZ0dzUkJHS0hueXUwbWQxZ2VPMGpmdWNCdlhaR1RQaHhFSlFXeTlwVzQyS0h2a0lrUWtpYXI0cTQxaFJ6Rzdycng0azA5VWt5TmpWRngyelB2dWZNcEY1c1JOSDdHbSsxV3pramdmNnZ5N2hRejdnNW8yWlNZWHNPWnBMTmhUZXYiLCJtYWMiOiIxYWM0MjFkNTRlYzI5MDA1MWI0ZDg0NjFiZTgxYWNiZjgyY2ExMjVjNTM5ZTc4ZDVhYmM0ODc5OTBkNWIwMzU3In0%3D
Content-Length: 113
Cache-Control: max-age=0
Sec-Ch-Ua: " Not A;Brand";v="99", "Chromium";v="96", "Google Chrome";v="96"
Sec-Ch-Ua-Mobile: ?0
Sec-Ch-Ua-Platform: "Windows"
Origin: https://test-caru.welcometw.com
Upgrade-Insecure-Requests: 1
Dnt: 1
Content-Type: application/x-www-form-urlencoded
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/96.0.4664.45 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
Sec-Fetch-Site: same-origin
```

Response 1

```
HTTP/1.1 302 Found
Server: nginx/1.21.3
Content-Type: text/html; charset=UTF-8
Connection: close
Cache-Control: no-cache, private
Date: Thu, 02 Dec 2021 01:37:48 GMT
Location: https://test-caru.welcometw.com/admin
Set-Cookie: XSRF-
TOKEN=eyJpdiI6Ik5sUjJZQWQxeWs1aWpNQkVFbnovRmc9PSIsInZhbHVlIjoiTnVWcFhqSWxRM2VyeDlvVUlWZFk1WlFDTW5PWW8yZ0h4UVFpMU55MWNBN2JXTlJ2OUZKeDR2T0pzSDkwVU5PYUUxcGhPc1FEMlZMOVo5VHNDSFR2VmkxRUF6QnZTZHNGVFRQTVB5blkrRHFyZnJMelNmbU9VRTFTbWg2MnA1UG8iLCJtYWMiOiI0OTdlYjM4YmM3NjQ2YzUxZTVkNzU0NzFlNjM0MDAyNjY2YWFmYTVlYTk4N2I2M2JiOGM5OTEyYzdlMGYxMWIzIn0%3D;
expires=Thu, 02-Dec-2021 03:37:48 GMT; Max-Age=7200; path=/; samesite=lax
Set-Cookie:
caru_session=eyJpdiI6IklxZ3VSVTZLZEs1QmFkSHRvSERranc9PSIsInZhbHVlIjoiZk9TY3ZRMVg3WHNCV1ZZYkRmYjBLbUkvVFJZOGdpMk1SN1hlNUplY1VzNmFNMDEzQ3F6K1IBZjRINEsycytLSHlzcjUvQTBMaExRZGsxRGMxdEhWejFjTEgwY1IBMUVtYWxVYlA5VzVqRktSUlloN28vSHBCMDZSQXptT0pYZGEiLCJtYWMiOiI3NDJmNThlODZhZjVkNTFhYzJjOWU3ZTQyYWM0ZTI0ZDA4ODM4Yjc4NjYwN2E4ZmM3ZTUyYTQyZmU2ZjRmMzdkIn0%3D; expires=Thu,
02-Dec-2021 03:37:48 GMT; Max-Age=7200; path=/; httponly; samesite=lax
Set-Cookie:
remember_web_59ba36addc2b2f9401580f014c7f58ea4e30989d=eyJpdiI6Im1jNWltZERONURQYUc5SzI0SXowN2c9PSIsInZhbHVlIjoiUi95RHp6RTh1S0RWd0dCTkRrZWUvd0hPb1ISb0E3a0oybStuR2dVT3dIdnpqbjRsUzVMYTdWVUN0U0libjE2OXp4Q2dlUG1ER3JhZjY1WXJTZG9XYldhNG5UU0FFUUZNRDJNV
```

The following parameters appear to contain Base64-encoded data:

- **XSRF-TOKEN = {"iv":"SW4rI1Pe1oNtYYPgIwCn5A==","value":"Olw14RrdrLrZqIWXqFVVQ+IC/XQ78zLhjRf5CtTawJ5Q7kDAola24INPS+Bjwvmfr8jeBnMt1CR/Uxkal7P1nB9B/gxFKo7NXyE8dhueNvdDdGQlxl+5dZk6k017OBGf","mac":"e747bb235f3691d836ac21de693b482da5030331648a9bf3684f378b0a2164d7"}**
- **caru_session = {"iv":"biOv5ADCELI+zZvM7QZKyQ==","value":"nJQq1A+6lQWJR+e+nlUJgElm/JsmN7CT2YsBZZ7kj5TlZlZdS6wNQLLFPTeINI+1XTePBBz1E/q34Ls v1fWI7LB3K22UpZGKCq7TPfXqN4OlvnwgWcDvoCOTAXuW2Vlf","mac":"f15b189fd44199de8518dfb6ca8a99c3f11d937af8686892716ae891e3ab374 8"}**

Request 1

```
POST /login HTTP/1.1
Host: test-caru.welcometw.com
Cookie: XSRF-
TOKEN=eyJpdiI6IlNXNHJsMVBlMW9OdFlZUGdJd0NuNUE9PSIsInZhbHVlIjoiT2x3MTRScmRyTHJacWxXWHFGVlZRK2xDL1hRNzh6TGhqUmY1Q3RUYXd
KNVE3a0RBb2xhMjRsTlBTK0Jqd3ZtZnI4amVCbk10MUNSL1V4a2FsN1AxbkI5Qi9neEZLbzdOWHlFOGRodWVOdmREZEdRbHhJKzVkWms2azAxN09CR2
YiLCJtYWMiOiJlNzQ3YmIyMzVmMzY5MWQ4MzZhYzIxZGU2OTNiNDgyZGE1MDMwMzMxNjQ4YTliZjM2ODRmMzc4YjBhMjE2NGQ3In0%3D;
caru_session=eyJpdiI6ImJpT3Y1QURDRUxJK3padk03UVpLeVE9PSIsInZhbHVlIjoibkpRcTFBKzZsUVdKUitlK25sVUpnRWxtL0pzbU43Q1QyWXNCWlo3a2o
1VGxaSVpkUzZ3TlFMTEZQVGVsTmwrMVhUZVBCQnoxRS9xMzRMc3YxZldsN0xCM0syMlVwWkdLQ3E3VFBmWHFONE9Jdm53Z1djRHZvQ09UQVh1VzJ
WbGYiLCJtYWMiOiJmMTViMTg5ZmQ0NDE5OWRlODUxOGRmYjZjYThhOTIjM2YxMWQ5MzdhZjg2ODY4OTI3MTZhZTg5MWUzYWIzNzQ4In0%3D
Content-Length: 111
Cache-Control: max-age=0
Sec-Ch-Ua: " Not A;Brand";v="99", "Chromium";v="96", "Google Chrome";v="96"
Sec-Ch-Ua-Mobile: ?0
Sec-Ch-Ua-Platform: "Windows"
Origin: https://test-caru.welcometw.com
Upgrade-Insecure-Requests: 1
Dnt: 1
Content-Type: application/x-www-form-urlencoded
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/96.0.4664.45 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
Sec-Fetch-Site: same-origin
```

Response 1

```
HTTP/1.1 302 Found
Server: nginx/1.21.3
Content-Type: text/html; charset=UTF-8
Connection: close
Cache-Control: no-cache, private
Date: Thu, 02 Dec 2021 01:36:35 GMT
Location: https://test-caru.welcometw.com/login
Set-Cookie: XSRF-
TOKEN=eyJpdiI6IkFVTlBWYjYyeVJUbW5waC9rZktBM2c9PSIsInZhbHVlIjoiOUY5bkdhaEVCTUdoempxNXczK2RIRXISNGpXK3NVdjVCUVVzdWFOcnVyMX
JpTER2RCs2aDJJbEhITWM3S2RzeVNPZGpCNERzVjdPOGRWZFNWRUc1ZUU1cTVvOHZXQ2NEOWk4WjlwNXRmeFpLYks4Zkd0Snp4RWlYVjR2YXNU
MGkiLCJtYWMiOiI2OWQ1Mzc3OWUwNTBkMDE3ZjVjY2QzMml3N2UwZTc2NjVhMTBhMGNjNzVhYjZhMDA3MDJhNDEzYzdjNmNkZmNlIn0%3D;
expires=Thu, 02-Dec-2021 03:36:35 GMT; Max-Age=7200; path=/; samesite=lax
Set-Cookie:
caru_session=eyJpdiI6IlU2NEFTcWNsbFNudjluODhlTU8xdFE9PSIsInZhbHVlIjoicEptRDFwWnhHQ216dHpBVHZ3MzR0ZTVaT1VUbFQxZXJsNVJVaDFWS2
gyQ2FNZ2k5RVljZ2plT2JEZ0ltdFFDKzErZUpkeFFMK2pmVFVkWlRNSERwTUYvSkVPK3M4NXZhWFZRZy9pLzhqNyszaEwrSmhxa29XMFloalFyS1Z6MWEi
LCJtYWMiOiJiMmY2ODY2NjQ1OWEyMTM5MTQ3NzYxODM5NjA2ZmFmZWZmY2M4OTQ1NDM3Y2NjZjVjNzIzOWE4YzFmNjc4N2YyIn0%3D;
expires=Thu, 02-Dec-2021 03:36:35 GMT; Max-Age=7200; path=/; httponly; samesite=lax
Content-Length: 394

<!DOCTYPE html>
<html>
```

15.7. https://test-caru.welcometw.com/robots.txt

Previous

Summary

Severity:	**Information**
Confidence:	**Firm**
Host:	**https://test-caru.welcometw.com**
Path:	**/robots.txt**

Issue detail

The following parameters appear to contain Base64-encoded data:

- **XSRF-TOKEN = {"iv":"NIR2YAd1vk5iiMBEEnz/Fg==","value":"NuVpXiIIQ3erx9oUlVdY5ZQCMnOYo2gHxQQi1Nv1cA7bWNRv9FJx4vOJsH90UNOaE1phOsQD2VL9Z**

```
Connection: close
Cookie: XSRF-
TOKEN=eyJpdiI6Ik5sUjJZQWQxeWs1aWpNQkVFbnovRmc9PSIsInZhbHVlIjoiTnVWcFhqSWxRM2VyeDlvVUlWZFk1WlFDTW5PWW8yZ0h4UVFpMU55MWNB
N2JXTlJ2OUZKeDR2T0pzSDkwVU5PYUUxcGhPc1FEMlZMOVo5VHNDSFR2VmkxRUF6QnZTZHNGVFRQTVB5blkrRHFyZnJMelNmbU9VRTFTbWg2MnA1UG
8iLCJtYWMiOiI0OTdlYjM4YmM3NjQ2YzUxZTVkNzU0NzFlNjM0MDAyNjY2YWFmYTVlYTk4N2I2M2JiOGM5OTEyYzdlMGYxMWIzIn0%3D;
caru_session=eyJpdiI6IklxZ3VSVTZLZEs1QmFkSHRvSERranc9PSIsInZhbHVlIjoiZk9TY3ZRMVg3WHNCV1ZZYkRmYjBLbUkvVFJZOGdpMk1SN1hlNUplY1Vz
NmFNMDEzQ3F6K1IBZjRINEsycytLSHlzcjUvQTBMaExRZGsxRGMxdEhWejFjTEgwY1lBMUVtYWxVYlA5VzVqRktSUllcN28vSHBCMDZSQXptT0pYZGEiLCJtY
WMiOiI3NDJmNThlODZhZjVkNTFhYzJjOWU3ZTQyYWM0ZTI0ZDA4ODM4Yjc4NjYwN2E4ZmM3ZTUyYTQyZmU2ZjRmMzdkIn0%3D;
remember_web_59ba36addc2b2f9401580f014c7f58ea4e30989d=eyJpdiI6Im1jNWltZERONURQYUc5Szl0SXowN2c9PSIsInZhbHVlIjoiUl95RHp6RTh1S0RWd0d
CTkRrZWUvd0hPb1lSb0E3a0oybStuR2dVT3dldnpqbjRsUzVMYTdWVUN0U0libjE2OXp4Q2dlUG1ER3JhZjY1WXJTZG9XYldhNG5UU0FFUUZNRDJNVk9rdWh
SakgvMEZUWFp4M3BtZGpoRHd1clB0alErNmtXTGFOVnhqbkl5cDh1Y0VoVWlzV3BRdzVnbGRjL09xVk9mWTI0NXRJREexaQVpieHppRlJEVTZwb2h2bnViSzZO
QzZPK3cwZzBnZTFDbG1ySld3RXM3SkZCeitOeXhvV0s3TUtKeDdtTT0iLCJtYWMiOiI1ZWY1NDNhNjJkOGI0ZDFhYmQyMzJjMjAzZWMwZGJlZjhlNGNmNzEzN
zk5NDI5MjU4Y2ExNTI5YzkyY2Y5OTdiIn0%3D
```

Response 1

```
HTTP/1.1 200 OK
Server: nginx/1.21.3
Date: Thu, 02 Dec 2021 01:41:32 GMT
Content-Type: text/plain
Content-Length: 24
Last-Modified: Wed, 01 Dec 2021 09:03:16 GMT
Connection: close
ETag: "61a73a54-18"
Accept-Ranges: bytes

User-agent: *
Disallow:
```

16. TLS certificate

Previous

Summary

Severity:	**Information**
Confidence:	**Certain**
Host:	**https://test-caru.welcometw.com**
Path:	/

Issue detail

The server presented a valid, trusted TLS certificate. This issue is purely informational.

The server presented the following certificates:

Server certificate

Issued to: *.welcometw.com, welcometw.com
Issued by: Sectigo RSA Domain Validation Secure Server CA
Valid from: Thu Aug 26 08:00:00 GMT+08:00 2021
Valid to: Tue Sep 27 07:59:59 GMT+08:00 2022

Certificate chain #1

Issued to: Sectigo RSA Domain Validation Secure Server CA
Issued by: USERTrust RSA Certification Authority
Valid from: Fri Nov 02 08:00:00 GMT+08:00 2018
Valid to: Wed Jan 01 07:59:59 GMT+08:00 2031

Certificate chain #2

Issued to: USERTrust RSA Certification Authority
Issued by: AAA Certificate Services
Valid from: Tue Mar 12 08:00:00 GMT+08:00 2019
Valid to: Mon Jan 01 07:59:59 GMT+08:00 2029

Certificate chain #3

Issued to: AAA Certificate Services
Issued by: AAA Certificate Services
Valid from: Thu Jan 01 08:00:00 GMT+08:00 2004
Valid to: Mon Jan 01 07:59:59 GMT+08:00 2029

Certificate chain #4

Issued to:	AAA Certificate Services
Issued by:	AAA Certificate Services
Valid from:	Thu Jan 01 08:00:00 GMT+08:00 2004
Valid to:	Mon Jan 01 07:59:59 GMT+08:00 2029

Issue background

TLS (or SSL) helps to protect the confidentiality and integrity of information in transit between the browser and server, and to provide authentication of the server's identity. To serve this purpose, the server must present an TLS certificate that is valid for the server's hostname, is issued by a trusted authority and is valid for the current date. If any one of these requirements is not met, TLS connections to the server will not provide the full protection for which TLS is designed.

It should be noted that various attacks exist against TLS in general, and in the context of HTTPS web connections in particular. It may be possible for a determined and suitably-positioned attacker to compromise TLS connections without user detection even when a valid TLS certificate is used.

References

- SSL/TLS Configuration Guide

Vulnerability classifications

- CWE-295: Improper Certificate Validation
- CWE-326: Inadequate Encryption Strength
- CWE-327: Use of a Broken or Risky Cryptographic Algorithm

Report generated by Burp Suite web vulnerability scanner v2021.9.1, at Thu Dec 02 12:13:29 GMT+08:00 2021.

附件五 易用性測試

評分標準

評分層級
1 - 有效
2 - 有些狀況
3 - 出問題

使用性問題嚴重程度分級表

	情境描述	測試情境一：消費者租車(自駕)				
使用者	你計畫要和朋友們出去玩，需要租代步工具。	步驟 1 註冊帳號並登入	步驟 2 搜尋自駕租車產品	步驟 3 填寫時間、內容	步驟 4 訂購商品	步驟 5 付款
Tester 1/消費者1(米)	評分	1 - 有效	2 - 找不到搜尋	2 - 重複按了填	1 - 有效	1 - 有效
Tester 2/消費者2(鐘)	評分	1 - 有效	2 - 多次查無商	2 - 重複按了填	1 - 有效	1 - 有效
Tester 3/消費者3(朱)	評分	1 - 有效	1 - 有效	3 - 多次重覆按	1 - 有效	2 - 付款失敗還
Tester 4/消費者4(李)	評分	1 - 有效	1 - 有效	2 - 重複按了填	2 - 註冊後填寫	1 - 有效
Tester 5/消費者5(T)	評分	2 - 不知道密碼	1 - 有效	2 - 重覆按「立	2 - 註冊後填寫	1 - 有效
Tester 6/消費者6(L)	評分	2 - 不知道密碼	2 - 無法搜尋指	2 - 重覆按「立	2 - 註冊後填寫	2 - 付款成功，
Tester 7/車商1(裳X)	評分	1 - 有效	1 - 有效	2 - 重複按了填	1 - 有效	3 - 跑不出付款
Tester 8/車商2(水X)	評分	1 - 有效	2 - 多次查無商	2 - 重複按了填	2 - 註冊後填寫	1 - 有效
Tester 9/車商3(上X)	評分	2 - 不知道密碼	1 - 有效	2 - 重覆按「立	2 - 註冊後填寫	2 - 未填寫信箱
Tester 10/車商4(裕X)	評分					

	情境描述	測試情境二：消費者取車(自駕)、車商核銷		
使用者	你計畫要和朋友們出去玩，需要租代步工具。	步驟 6 消費者出示QRcode	步驟 7 消費者取車拍照上傳	步驟 8 車商核銷(掃碼/人工)
Tester 1/消費者1(米)	評分	3 - 找不到	2 - 找不到現場	2 - 找不到核銷
Tester 2/消費者2(鐘)	評分	2 - 找了很久才	3 - 上傳速度過	3 - 網頁版相機
Tester 3/消費者3(朱)	評分	3 - 無法載入訂	1 - 有效	3 - 網頁版相機
Tester 4/消費者4(李)	評分	3 - 找不到	1 - 有效	3 - 相機無法使
Tester 5/消費者5(T)	評分	3 -訂單無顯示	2 - 上傳速度慢	2 - 找不到核銷
Tester 6/消費者6(L)	評分	3 - 訂單無顯示	1 - 有效	2 - 核銷後未顯
Tester 7/車商1(裳X)	評分	2 - 找了很久才	1 - 有效	2 - 找不到核銷
Tester 8/車商2(水X)	評分	3 - 找不到	1 - 有效	1 - 有效
Tester 9/車商3(上X)	評分	3 - 找不到	3 - 上傳速度過	1 - 有效
Tester 10/車商4(裕X)	評分			

	情境描述	測試情境三：消費者租車(附駕)、取車(附駕)、司機核銷					
使用者	你計畫要和朋友們出去玩，需要租代步工具。	步驟 9 搜尋附駕租車產品	步驟 10 填寫時間、內容	步驟 11 訂購商品	步驟 12 司機核銷 QRcode	步驟 13 司機開始任務	步驟 14 司機結束任務
Tester 1/消費者1(米)	評分	2 - 多次點選附	1 - 有效	1 - 有效	1 - 有效	1 - 有效	3 - 找不到結束
Tester 2/消費者2(鐘)	評分	2 - 改變搜尋條	2 - 忘記剛剛填	1 - 有效	1 - 有效	1 - 有效	3 - 找不到結束
Tester 3/消費者3(朱)	評分	1 - 有效	2 - 一直按「立	3 - 未勾選「附	1 - 有效	1 - 有效	3 - 找不到結束
Tester 4/消費者4(李)	評分	1 - 有效	1 - 有效	1 - 有效	3 - 相機無法使	3 - 無法使用	3 - 找不到結束
Tester 5/消費者5(T)	評分	3 - 未找到附駕	1 - 有效	1 - 有效	1 - 有效	3 - 不知道要開	3 - 找不到結束
Tester 6/消費者6(L)	評分	3 - 未找到附駕	1 - 有效	3 - 未勾選「附	1 - 有效	1 - 有效	3 - 找不到結束
Tester 7/車商1(裳X)	評分						
Tester 8/車商2(水X)	評分						
Tester 9/車商3(上X)	評分	2 - 點選附駕租	1 - 有效	3 - 未勾選「附	1 - 有效	1 - 有效	3 - 找不到結束
Tester 10/車商4(裕X)	評分						

	情境描述	測試情境四：車商主管派車、上架車輛					
使用者	你計畫要和朋友們出去玩，需要租代步工具。	步驟 15 從CarU後台查看付款狀態	步驟 16 查看庫存量	步驟 17 上架車輛	步驟 18 查看今日訂單	步驟 19 進行派車	備註
Tester 1/消費者1(米)	評分	2 - 與前台顯示	1 - 有效	3 - 找不到從哪	2 - 找不到過濾	2 - 以為儲存即	
Tester 2/消費者2(鐘)	評分						
Tester 3/消費者3(朱)	評分						
Tester 4/消費者4(李)	評分						
Tester 5/消費者5(T)	評分	1 - 有效	1 - 有效	2 - 不知道是否	2 - 找不到過濾	1 - 有效	
Tester 6/消費者6(L)	評分	1 - 有效	1 - 有效	2 - 不知道怎麼	2 - 找不到過濾	1 - 有效	
Tester 7/車商1(裳X)	評分	1 - 有效	1 - 有效	2 - 不知道怎麼	1 - 有效	1 - 有效	
Tester 8/車商2(水X)	評分	1 - 有效	1 - 有效	2 - 上架後看不	1 - 有效	1 - 有效	
Tester 9/車商3(上X)	評分	3 - 看不到內容	1 - 有效	3 - 看不到內容	3 - 看不到內容	3 - 看不到內容	
Tester 10/車商4(裕X)	評分						測試失敗(較年長，不會操作網站)

排序後分級表

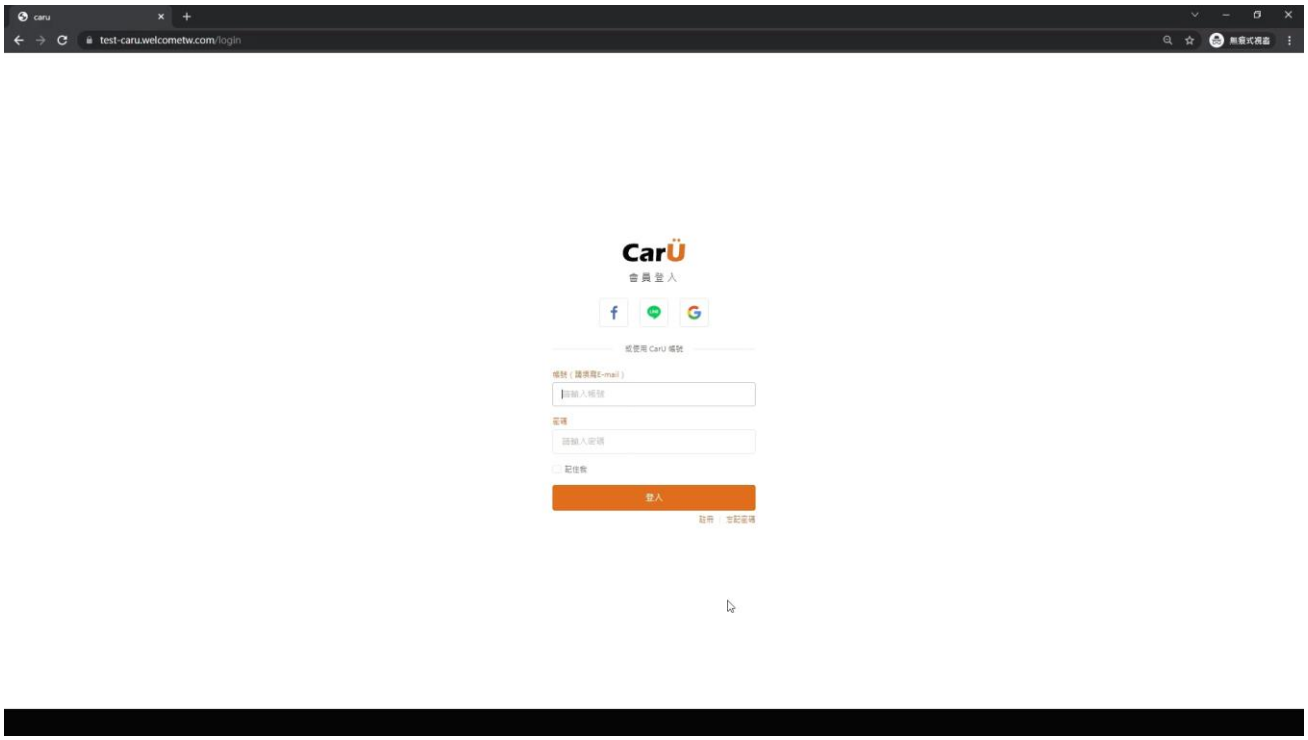
測試情境一：消費者租車(自駕)					測試情境二：消費者取車(自駕)、車商核銷		
步驟 1 註冊帳號並登入	步驟 2 搜尋自駕租車產品	步驟 3 填寫時間、內容	步驟 4 訂購商品	步驟 5 付款	步驟 6 消費者出示QRcode	步驟 7 消費者取車拍照上傳	步驟 8 車商核銷(掃碼/人工)
2 - 不知道密碼不能少於8字元，註冊後選項被清除	2 - 找不到搜尋結果	3 - 多次重覆按填寫時間還是無效	2 - 註冊後填寫內容被清除	3 - 跑不出付款頁面	3 - 找不到QRcode位置	3 - 上傳速度過慢，以為沒有成功	3 - 相機無法使用
2 - 不知道密碼不能少於8字元	2 - 多次查無商品	2 - 重複按了填寫日期的地方	2 - 註冊後填寫內容被清除	2 - 未填寫信箱	3 - 找不到QRcode位置	3 - 上傳速度過慢，以為沒有成功	3 - 網頁版相機無法使用，用app開才可以
2 - 不知道密碼不能少於8字元，註冊後選項被清除	2 - 無法搜尋指定車商	2 - 重覆按「立即訂購」，沒有填寫取還車時間、重複點選日期欄	1 - 有效	2 - 付款失敗還是有QRcode，不知道要不要重新付款	3 - 無法載入訂單內容	2 - 上傳速度慢	3 - 網頁版相機無法使用，用app開才可以
1 - 有效	2 - 多次查無商品	2 - 重複按了填寫日期的地方	2 - 註冊後填寫內容被清除	2 - 付款成功，卻顯示「已確認，待付款」，以為要重新付款	3 - 找不到QRcode位置	2 - 找不到現場拍攝之相機位置	2 - 找不到核銷位置
1 - 有效	1 - 有效	2 - 重覆按「立即訂購」和日期欄位	2 - 註冊後填寫內容被清除	1 - 有效	3 -訂單無顯示QRcode	1 - 有效	2 - 找不到核銷位置
1 - 有效	1 - 有效	2 - 重覆按「立即訂購」，沒有填寫取還車時間	2 - 註冊後填寫內容被清除	1 - 有效	3 - 訂單無顯示QRcode	1 - 有效	2 - 核銷後未顯示在畫面上
1 - 有效	1 - 有效	2 - 重複按了填寫日期的地方	1 - 有效	1 - 有效	3 - 找不到QRcode位置	1 - 有效	2 - 找不到核銷位置
1 - 有效	1 - 有效	2 - 重複按了填寫日期的地方	1 - 有效	1 - 有效	2 - 找了很久才找到QRcode	1 - 有效	1 - 有效
1 - 有效	1 - 有效	2 - 重複按了填寫日期的地方	1 - 有效	1 - 有效	2 - 找了很久才找到QRcode	1 - 有效	1 - 有效

測試情境三：消費者租車(附駕)、取車(附駕)、司機核銷					
步驟 9 搜尋附駕租車產品	步驟 10 填寫時間、內容	步驟 11 訂購商品	步驟 12 司機核銷 QRcode	步驟 13 司機開始任務	步驟 14 司機結束任務
3 - 未找到附駕包車	2 - 忘記剛剛填寫過的時間	3 - 未勾選「附駕駛」	3 - 相機無法使用	3 - 無法使用	3 - 找不到結束任務功能
3 - 未找到附駕包車	2 - 一直按「立即訂購」而不是「預訂」	3 - 未勾選「附駕駛」	1 - 有效	3 - 不知道要開啟定位	3 - 找不到結束任務功能
2 - 多次點選附駕租車，頁面仍顯示自駕租車	1 - 有效	3 - 未勾選「附駕駛」	1 - 有效	1 - 有效	3 - 找不到結束任務功能
2 - 改變搜尋條件以為搜尋結果會跟著變，等了一下才發現沒有	1 - 有效	1 - 有效	1 - 有效	1 - 有效	3 - 找不到結束任務功能
2 - 點選附駕租車，頁面仍顯示自駕租車，重複點選	1 - 有效	1 - 有效	1 - 有效	1 - 有效	3 - 找不到結束任務功能
1 - 有效	1 - 有效	1 - 有效	1 - 有效	1 - 有效	3 - 找不到結束任務功能
1 - 有效	1 - 有效	1 - 有效	1 - 有效	1 - 有效	3 - 找不到結束任務功能

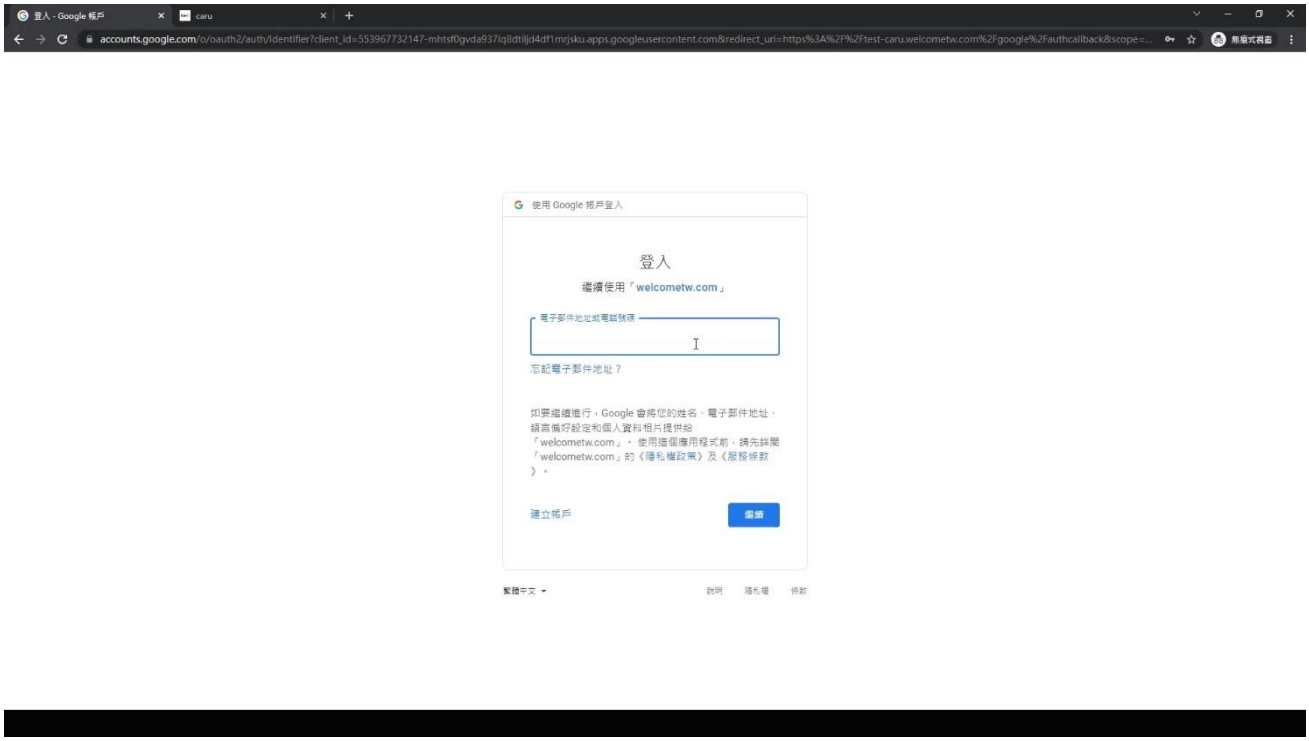
測試情境四：車商主管派車、上架車輛				
步驟 15 從CarU後台查看付款狀態	步驟 16 查看庫存量	步驟 17 上架車輛	步驟 18 查看今日訂單並其狀態	步驟 19 進行派車
3 - 看不到內容(手機)	1 - 有效	3 - 看不到內容(手機)	3 - 看不到內容(手機)	3 - 看不到內容(手機)
2 - 與前台顯示狀態不一致	1 - 有效	3 - 找不到從哪裏上架	2 - 找不到過濾訂單時間功能	2 - 以為儲存即會關閉頁面
1 - 有效	1 - 有效	2 - 不知道是否上架成功，重複上架	2 - 找不到過濾訂單時間功能	1 - 有效
1 - 有效	1 - 有效	2 - 不知道怎麼上架	1 - 有效	1 - 有效
1 - 有效	1 - 有效	2 - 不知道怎麼上架	1 - 有效	1 - 有效
1 - 有效	1 - 有效	2 - 上架後看不到數量改變，重複上架	1 - 有效	1 - 有效

附件六 符合性驗證相關截圖

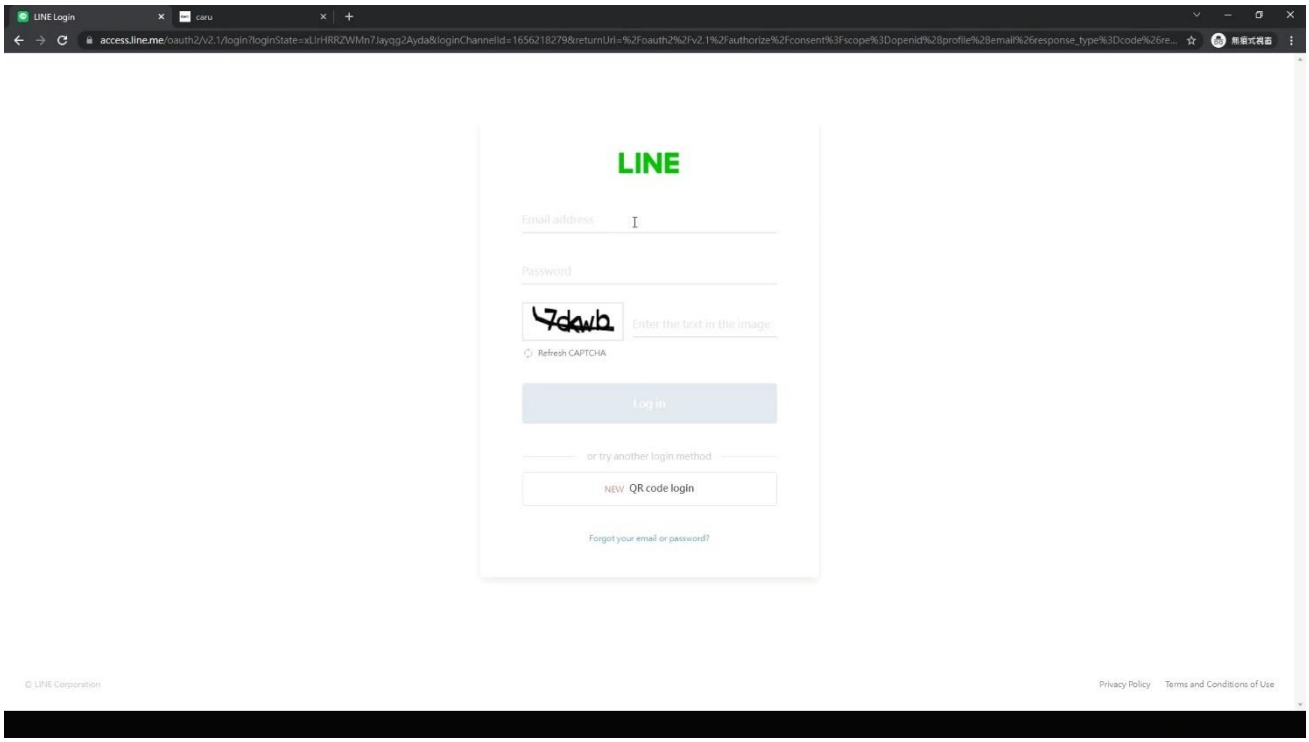
A-01-01：



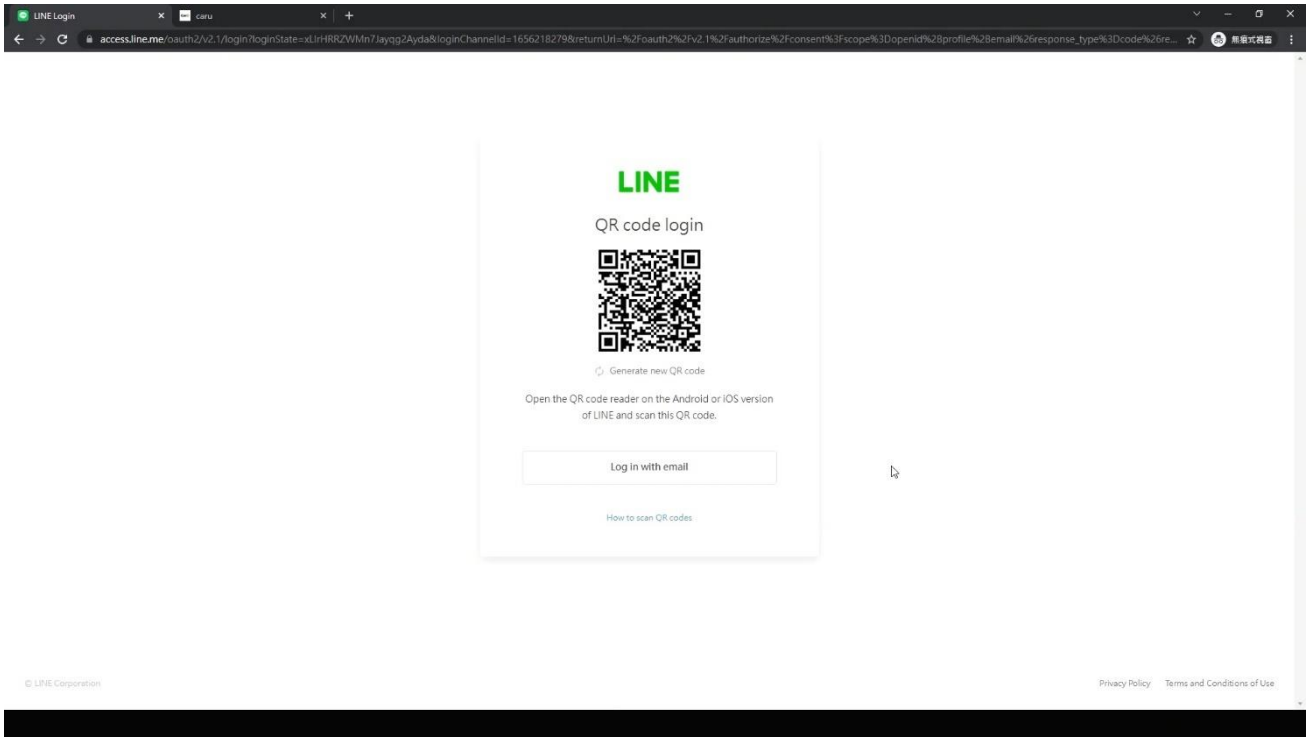
A-02-01：



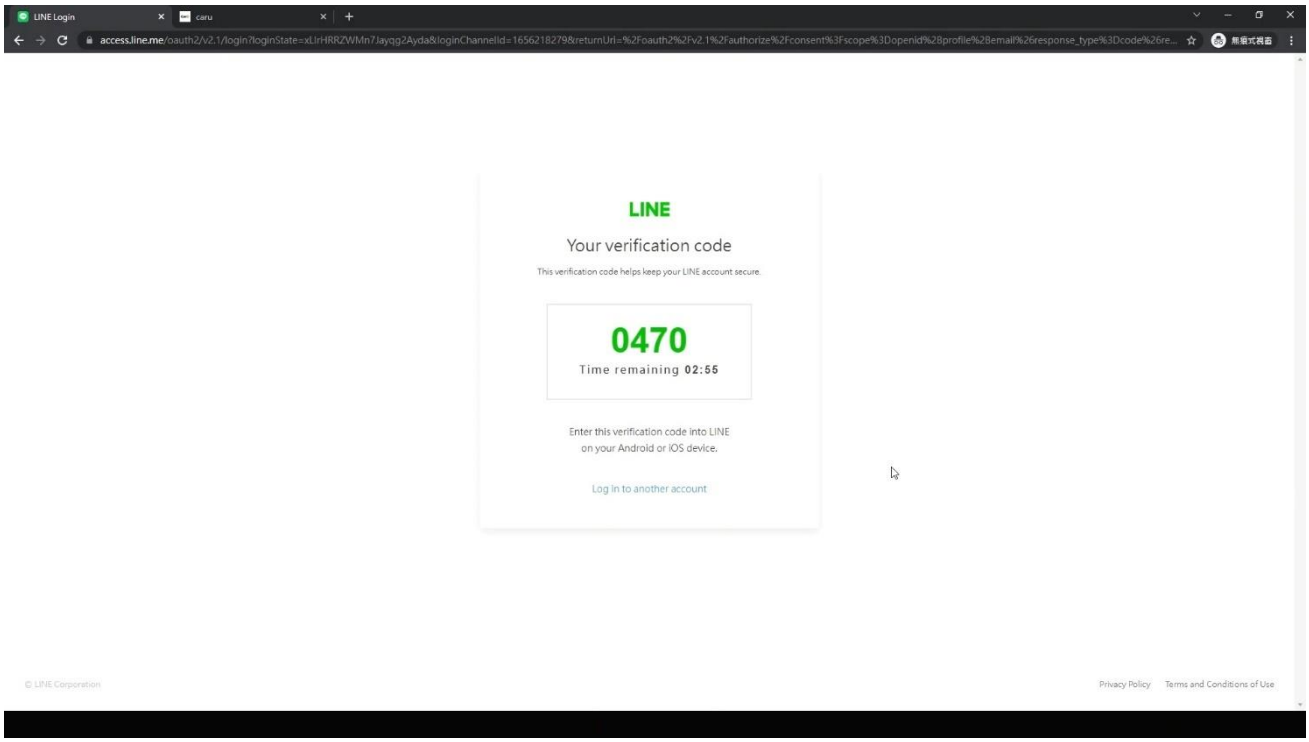
A-03-01


LINE Login
caru
access.line.me/oauth2/v2.1/login?loginState=xLIrHRRZWMn7Jayqg2Ayda&loginChannelId=1656218279&returnUri=%2Foauth2%2Fv2.1%2Fauthorize%2Fconsent%3Fscope%3Dopenid%28profile%28email%26response_type%3Dcode%26re...
LINE
Email address
Password
Enter the text in the image
Refresh CAPTCHA
Log in
or try another login method
NEW QR code login
Forgot your email or password?
© LINE Corporation
Privacy Policy
Terms and Conditions of Use

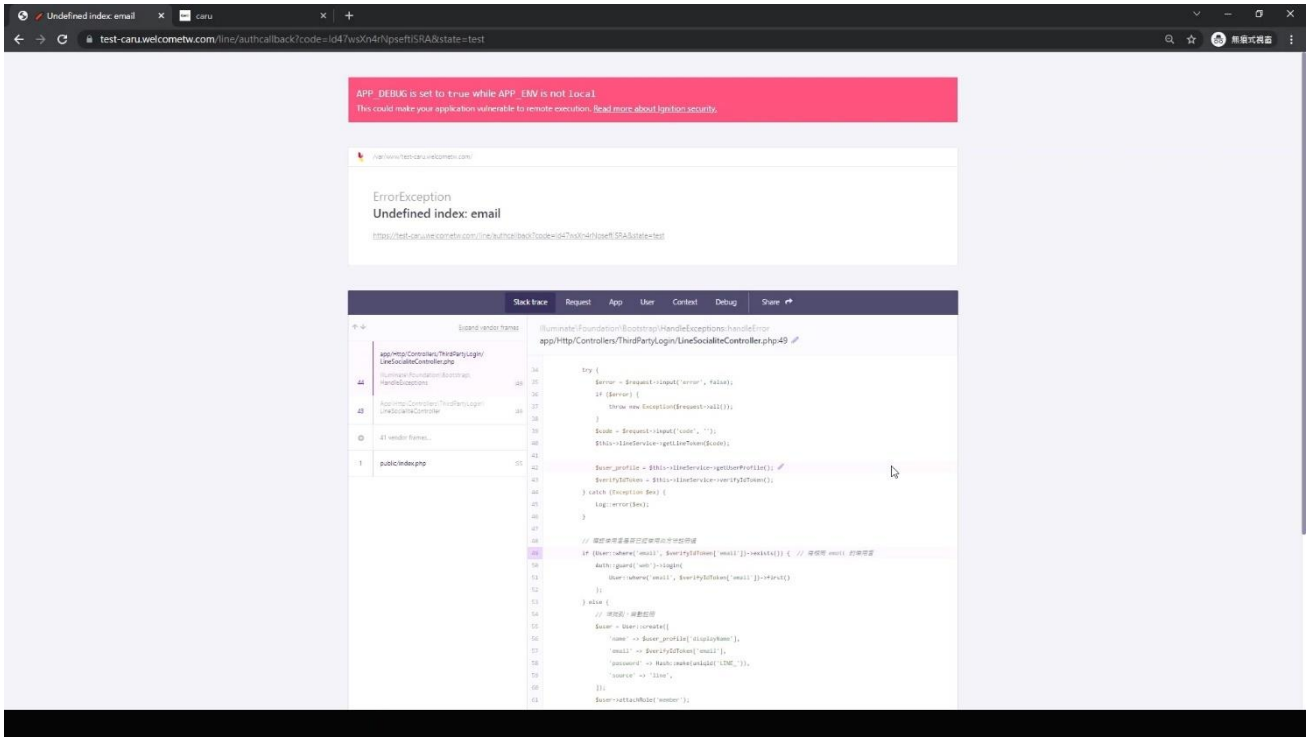
A-03-02


LINE Login
caru
access.line.me/oauth2/v2.1/login?loginState=xLIrHRRZWMn7Jayqg2Ayda&loginChannelId=1656218279&returnUri=%2Foauth2%2Fv2.1%2Fauthorize%2Fconsent%3Fscope%3Dopenid%28profile%28email%26response_type%3Dcode%26re...
LINE
QR code login
Generate new QR code
Open the QR code reader on the Android or iOS version of LINE and scan this QR code.
Log in with email
How to scan QR codes
© LINE Corporation
Privacy Policy
Terms and Conditions of Use

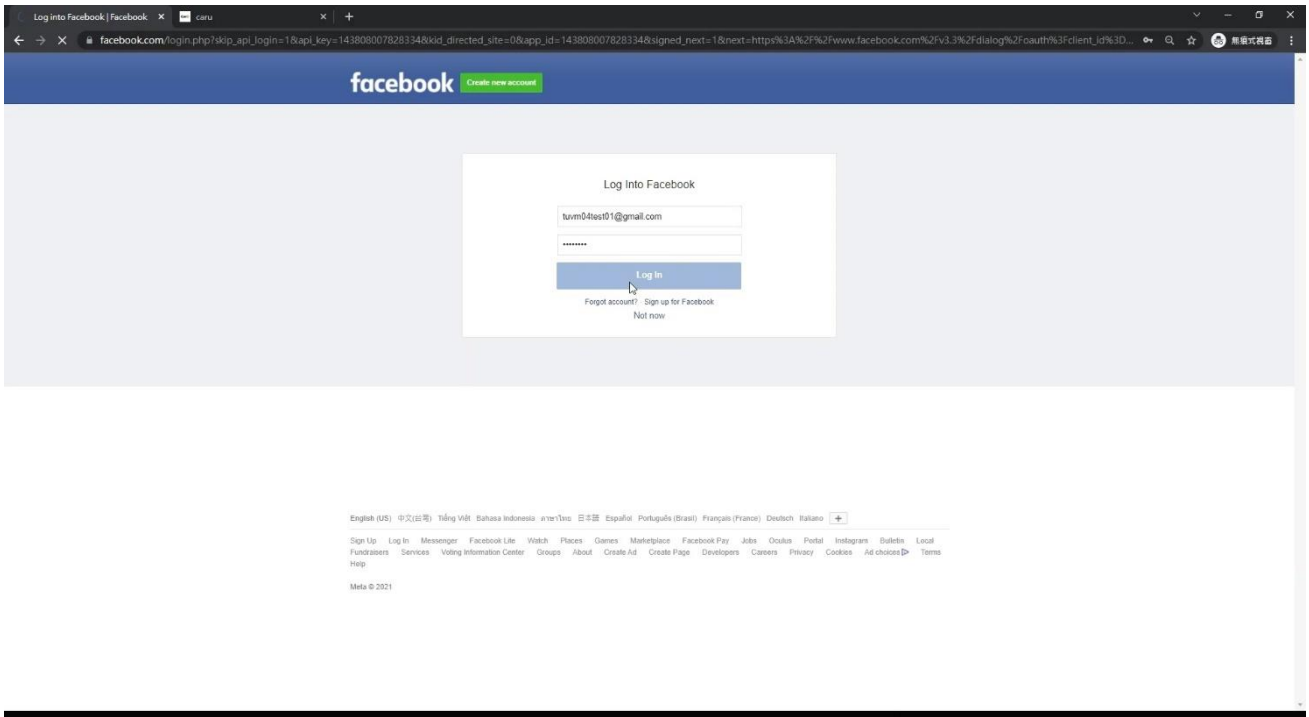
A-03-03


LINE Login
caru
access.line.me/oauth2/v2.1/login?loginState=xLlrHRRZWMn7Jayqg2Ayda&loginChannelId=1656218279&returnUri=%2Foauth%2Fv2.1%2Fauthorize%2Fconsent%3Fscope%3Dopenid%28profile%28email%26response_type%3Dcode%26re...
LINE
Your verification code
This verification code helps keep your LINE account secure.
0470
Time remaining 02:55
Enter this verification code into LINE on your Android or iOS device.
Log in to another account
© LINE Corporation
Privacy Policy
Terms and Conditions of Use

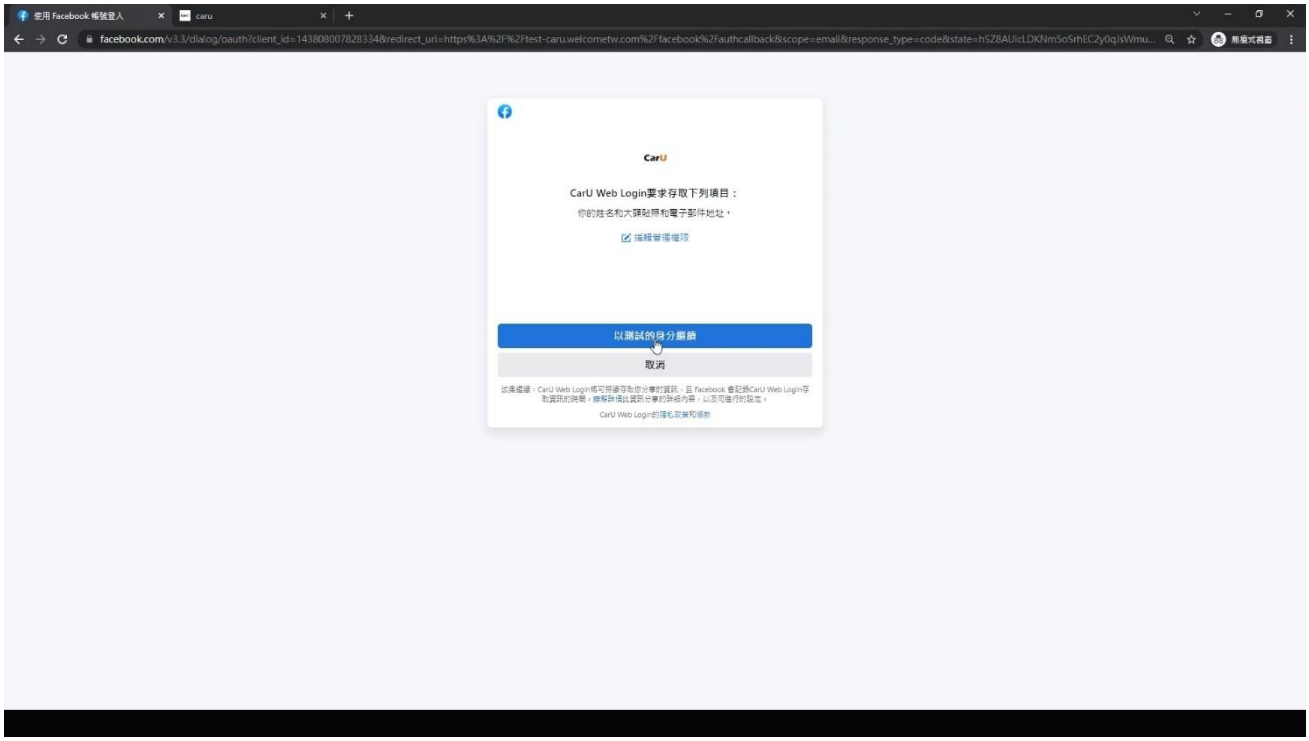
A-03-04


Undefined index: email
caru
test-caru.welcometw.com/line/authcallback?code=ld47wsXn4rNpseftISRA&state=test
APP_DEBUG is set to true while APP_ENV is not local
This could make your application vulnerable to remote execution. Read more about Ignition security.
ErrorException
Undefined index: email
Stack trace
Request
App
User
Context
Debug
Share
app/Http/Controllers/ThirdPartyLogin/LineSocialiteController.php:49
public/index.php

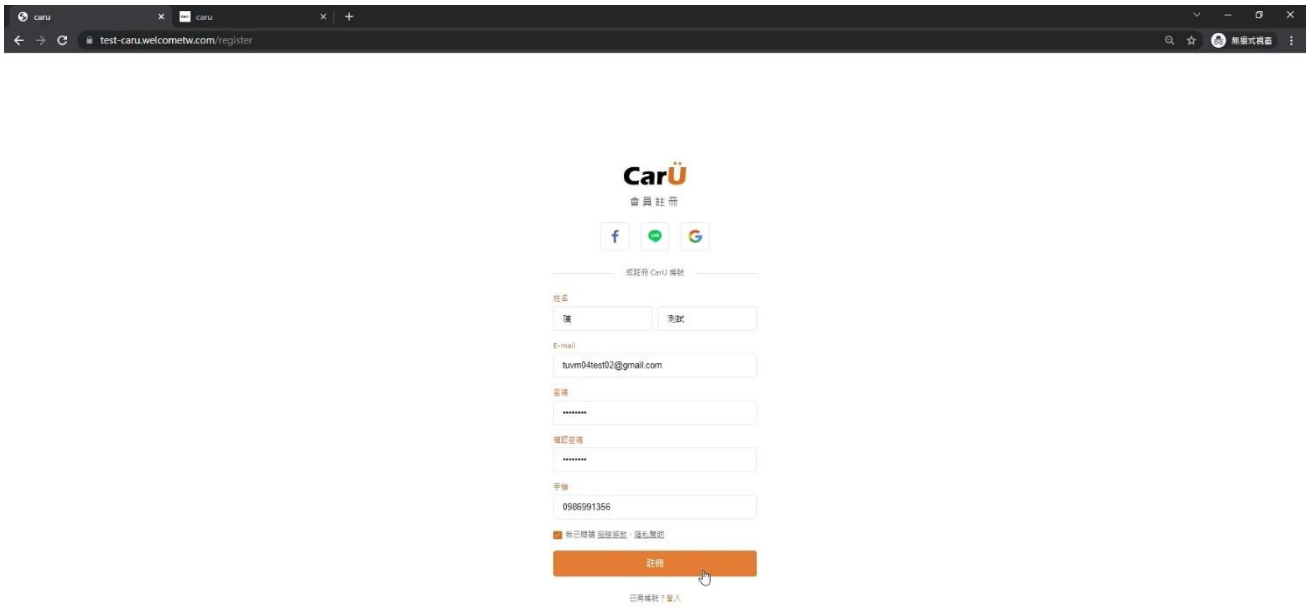
A-04-01


Log into Facebook | Facebook
caru
facebook.com/login.php?skip_api_login=1&api_key=1438080078283348kid_directed_site=0&app_id=1438080078283348signed_next=1&next=https%3A%2F%2Fwww.facebook.com%2Fv3.3%2Fdialog%2Foauth%3Fclient_id%3D...
facebook
Create new account
Log Into Facebook
tuvm04test01@gmail.com
Log In
Forgot account? · Sign up for Facebook
Not now
English (US) 中文(台灣) Tiếng Việt Bahasa Indonesia ภาษาไทย 日本語 Español Português (Brasil) Français (France) Deutsch Italiano
Sign Up Log In Messenger Facebook Lite Watch Places Games Marketplace Facebook Pay Jobs Oculus Portal Instagram Bulletin Local
Fundraisers Services Voting Information Center Groups About Create Ad Create Page Developers Careers Privacy Cookies Ad choices Terms
Help
Meta © 2021

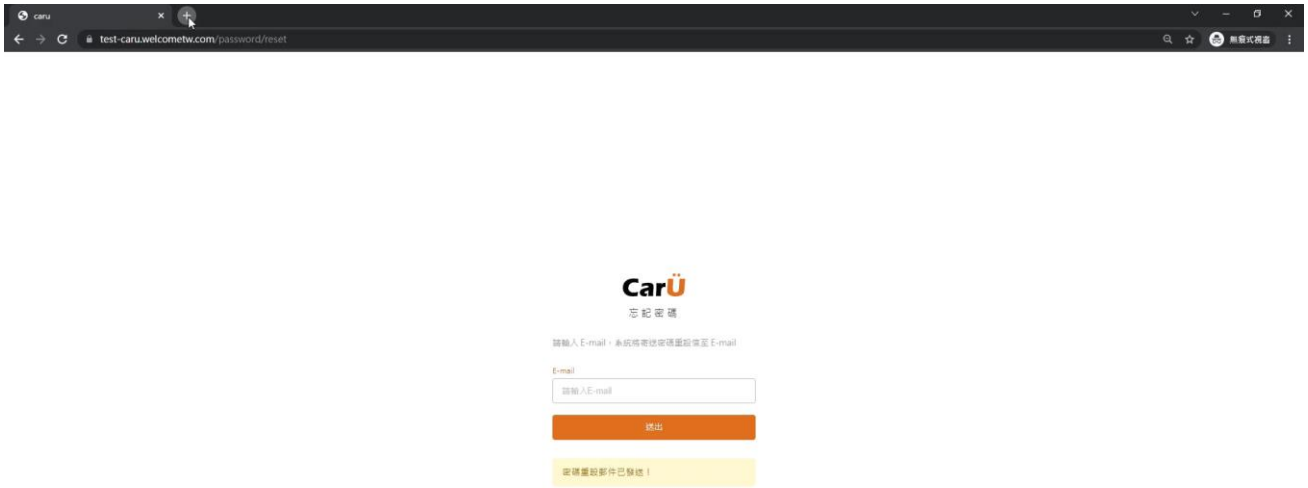
A-04-02


使用 Facebook 帳號登入
caru
facebook.com/v3.3/dialog/oauth?client_id=1438080078283348redirect_uri=https%3A%2F%2Ftest-caru.welcometw.com%2Ffacebook%2Fauthcallback&scope=email&response_type=code&state=h5Z8AUicLDKNm5o5rhEC2y0qJsWmu...
CarU
CarU Web Login要求存取下列項目：
你的姓名和大頭貼照和電子郵件地址。
編輯管理權限
以測試的身分繼續
取消
如果繼續，CarU Web Login將可根據你分享的資訊，且 Facebook 會記錄CarU Web Login存取資訊的時間。瞭解詳情此資訊分享的詳細內容，以及可進行的設定。
CarU Web Login的隱私政策和條款

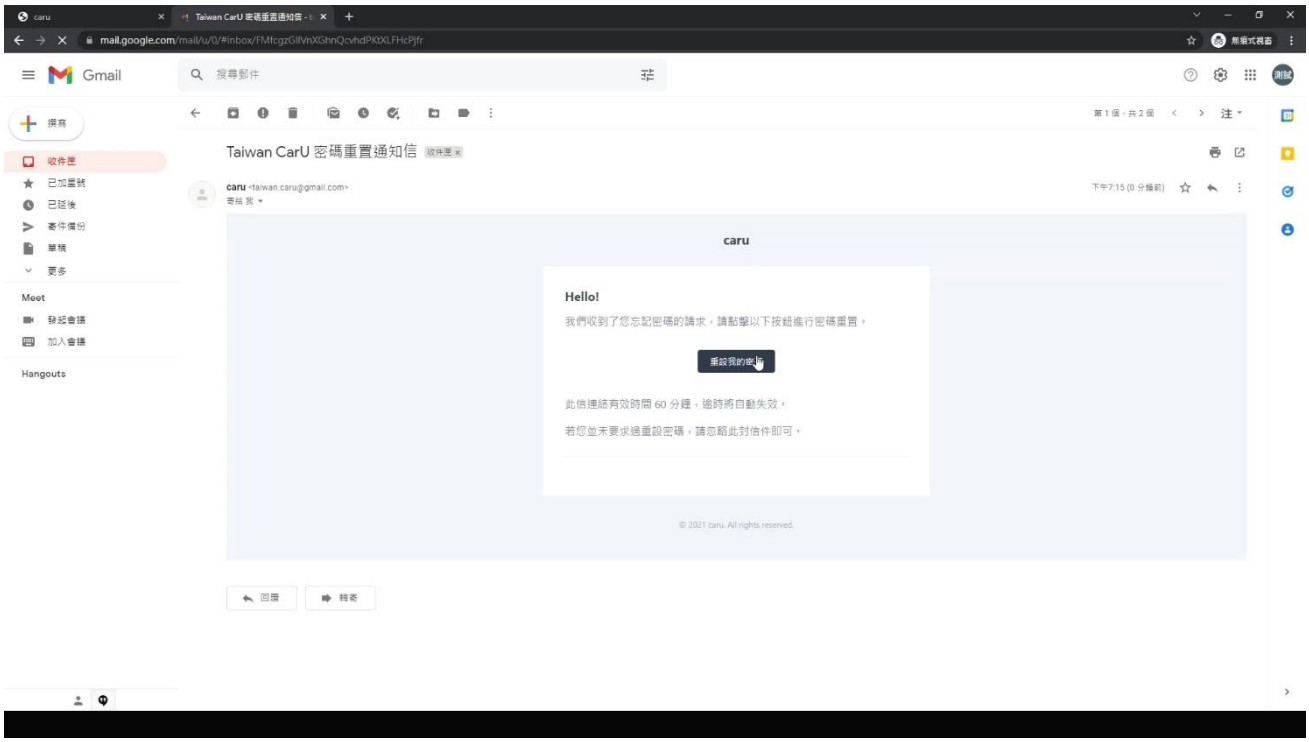
A-05-01


caru
caru
test-caru.welcometw.com/register
CarÜ
會員註冊
或註冊 CarU 帳號
姓名
陳
測試
E-mail
tuvm04test02@gmail.com
密碼
確認密碼
手機
0986991356
註冊
已有帳號？登入

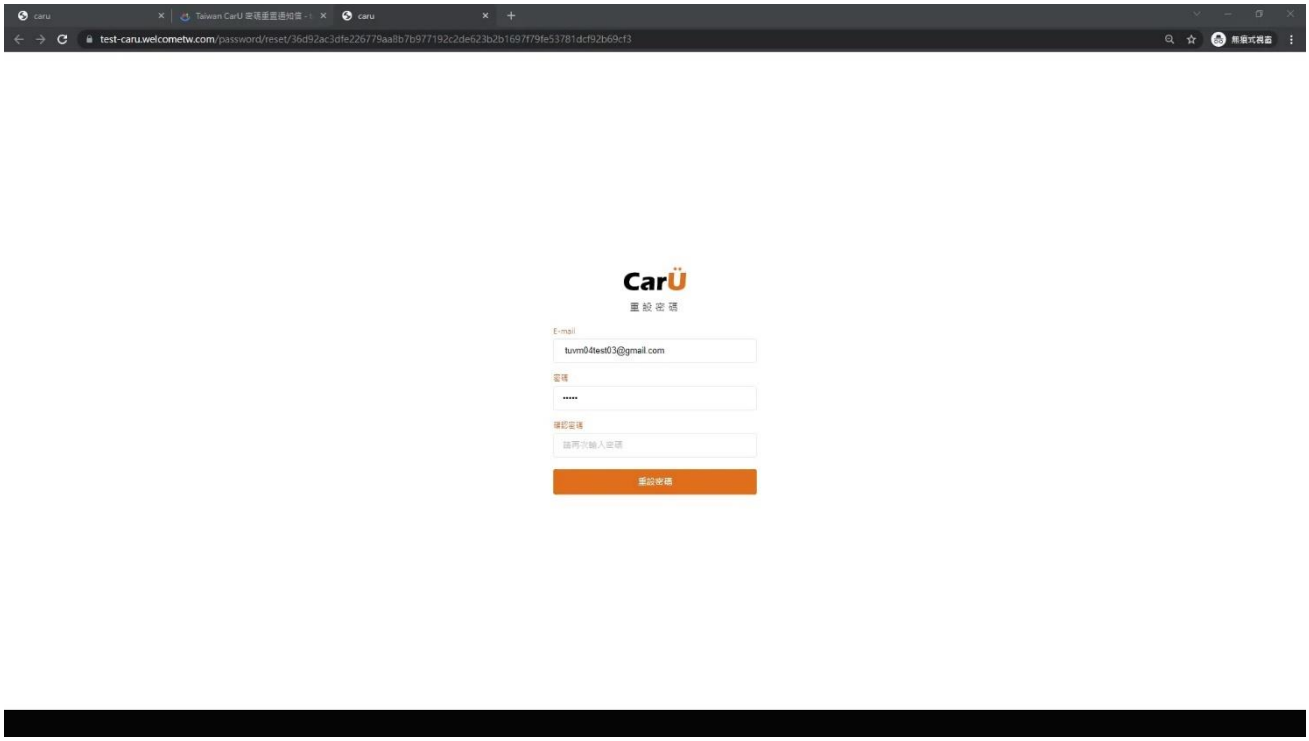
A-06-01


caru
test-caru.welcometw.com/password/reset
CarÜ
忘記密碼
E-mail
送出

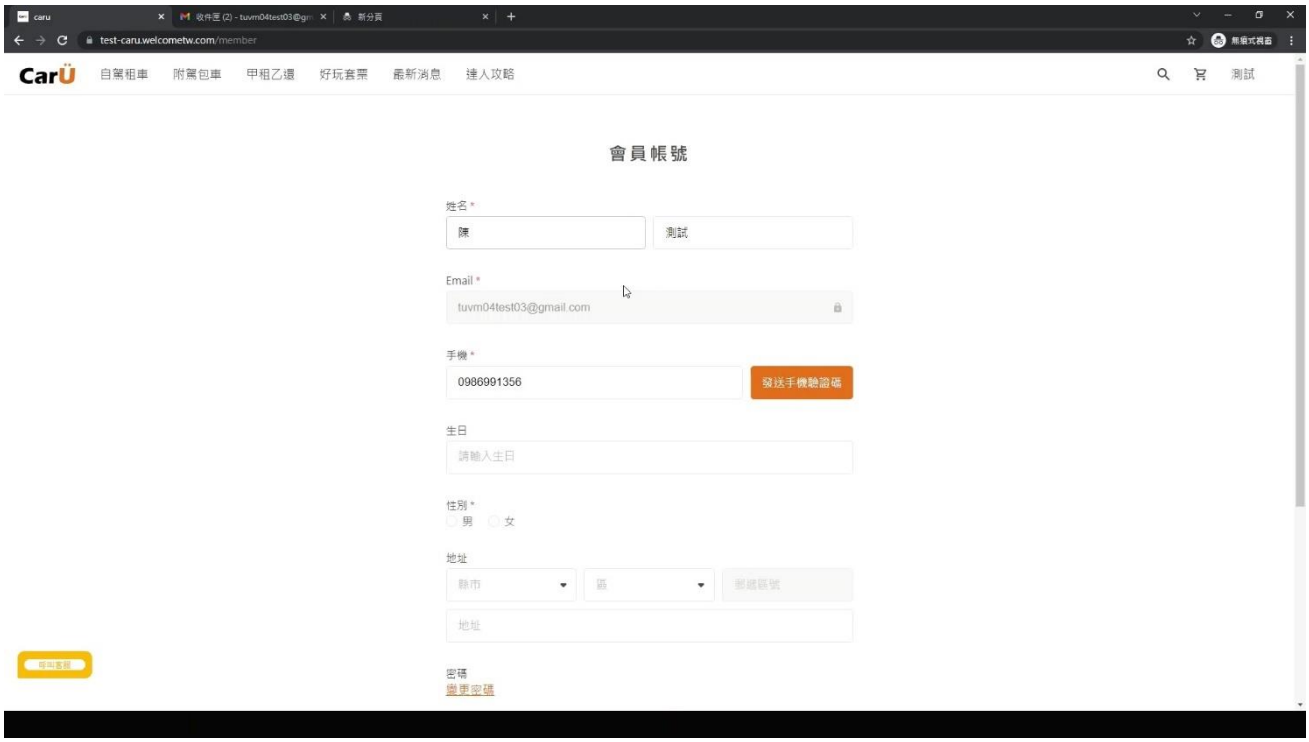
A-06-02


Gmail
Taiwan CarU 密碼重置通知信
caru
Hello!
我們收到了您忘記密碼的請求，請點擊以下按鈕進行密碼重置，
重設我的密碼
此信連結有效時間 60 分鐘，逾時將自動失效，
若您並未要求過重設密碼，請忽略此封信件即可，
© 2021 caru. All rights reserved.

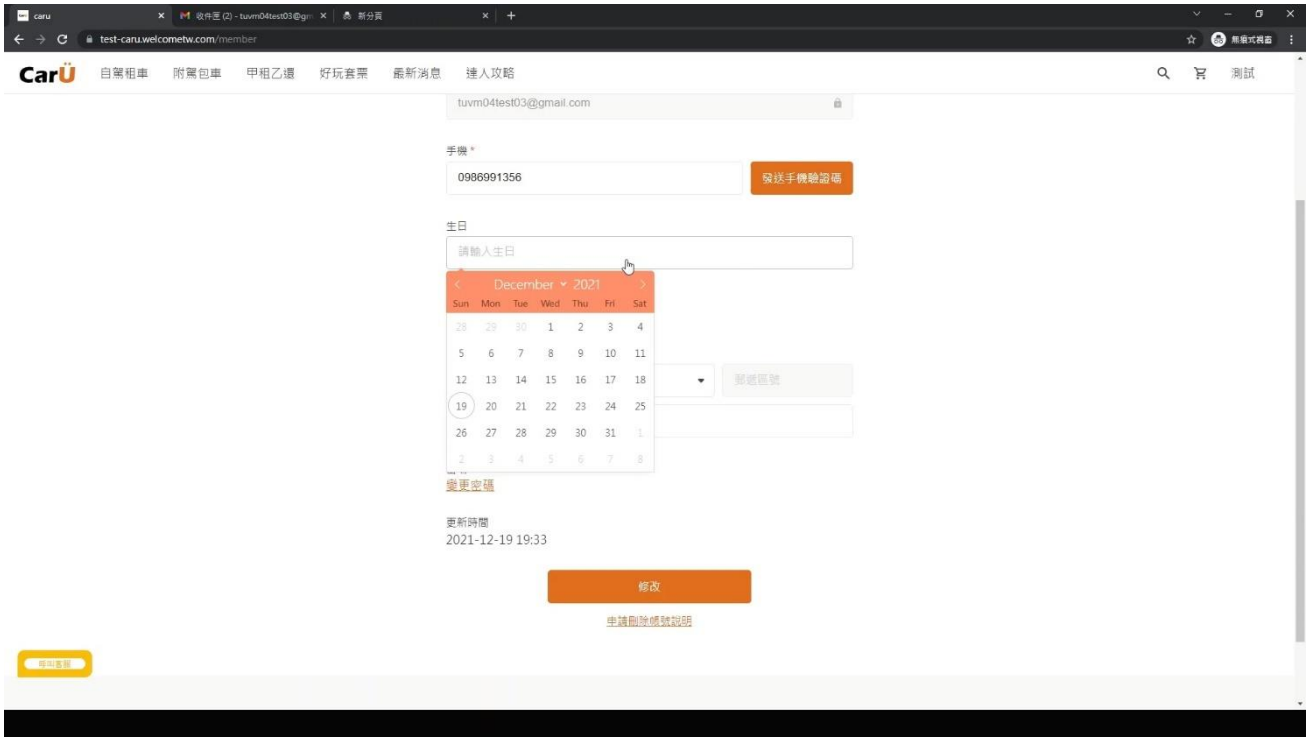
A-06-03


CarÜ
重設密碼
E-mail
tuvm04test03@gmail.com
密碼
確認密碼
重設密碼

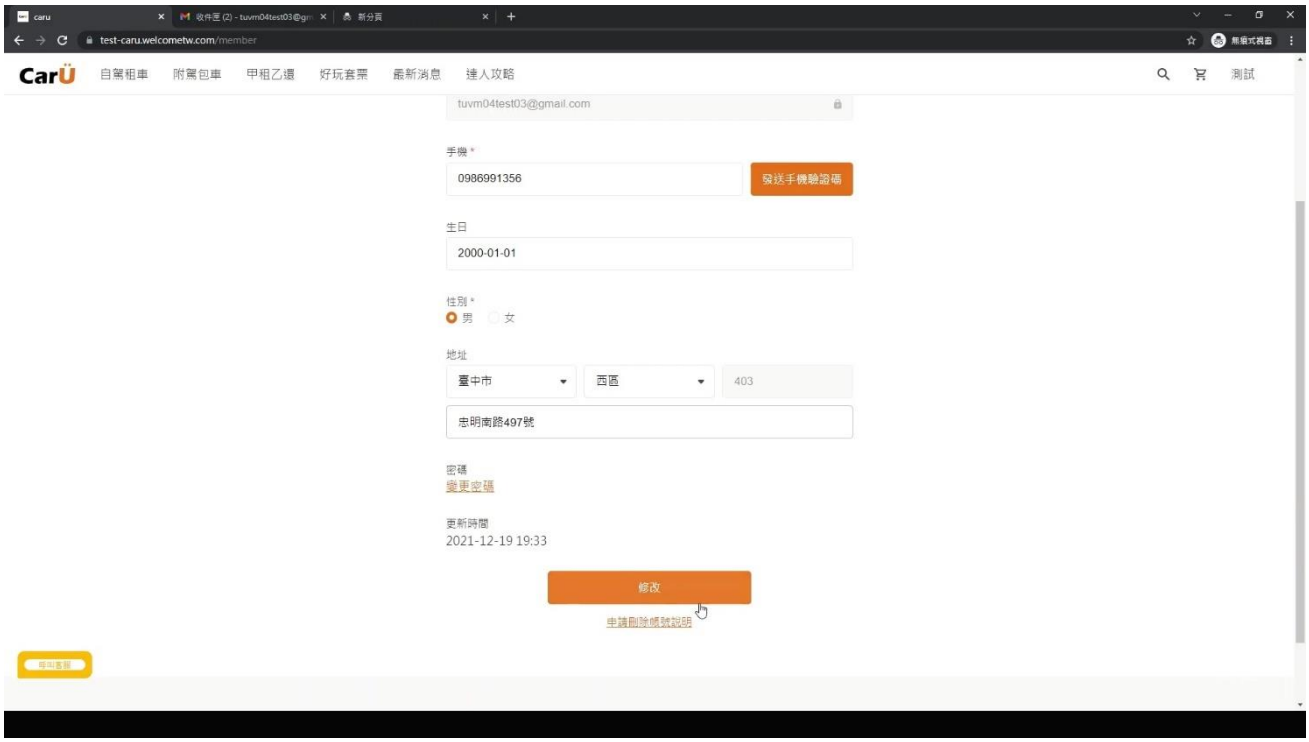
A-07-01


test-caru.welcometw.com/member
CarÜ
自駕租車
附駕包車
甲租乙還
好玩套票
最新消息
達人攻略
測試
會員帳號
姓名 *
陳
測試
Email *
tuvm04test03@gmail.com
手機 *
0986991356
發送手機驗證碼
生日
請輸入生日
性別 *
男
女
地址
縣市
區
郵遞區號
地址
密碼
變更密碼

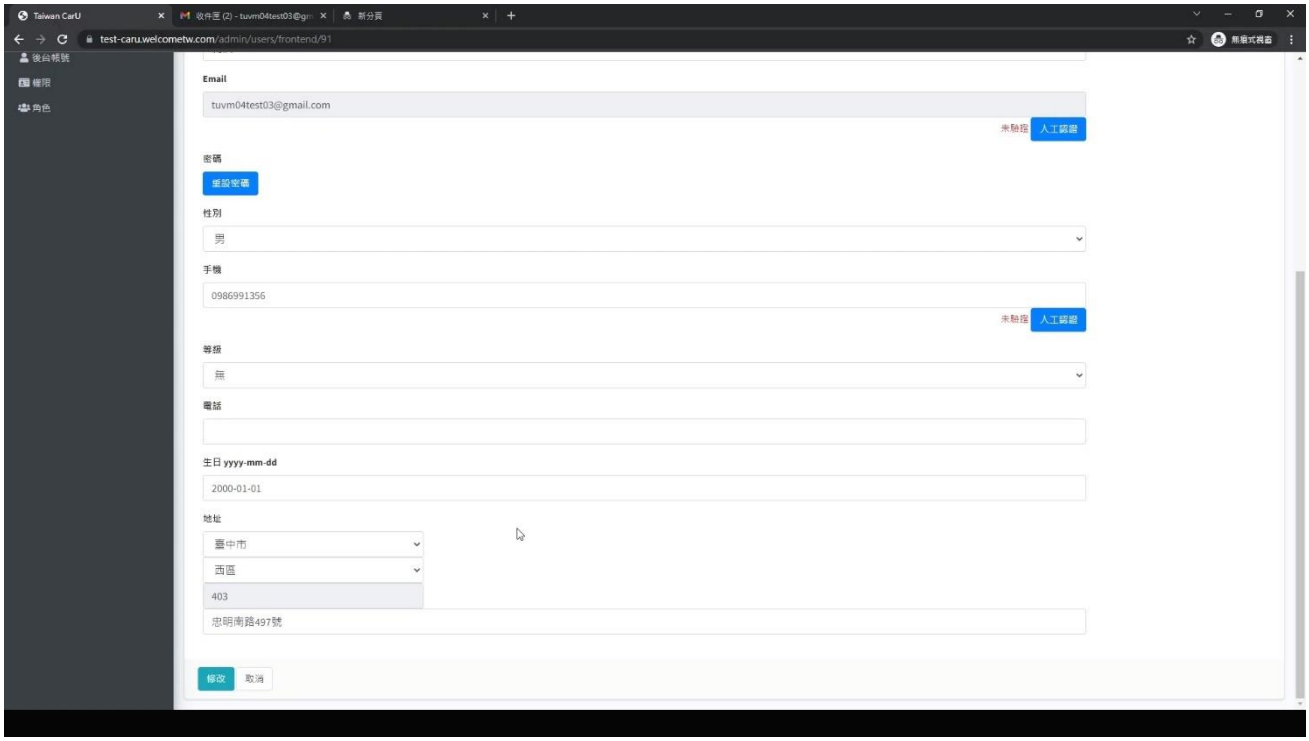
A-07-02


test-caru.welcometw.com/member
CarÜ
自駕租車
附駕包車
甲租乙還
好玩套票
最新消息
達人攻略
測試
tuvm04test03@gmail.com
手機 *
0986991356
發送手機驗證碼
生日
請輸入生日
December 2021
Sun Mon Tue Wed Thu Fri Sat
變更密碼
更新時間
2021-12-19 19:33
修改
申請刪除帳號說明

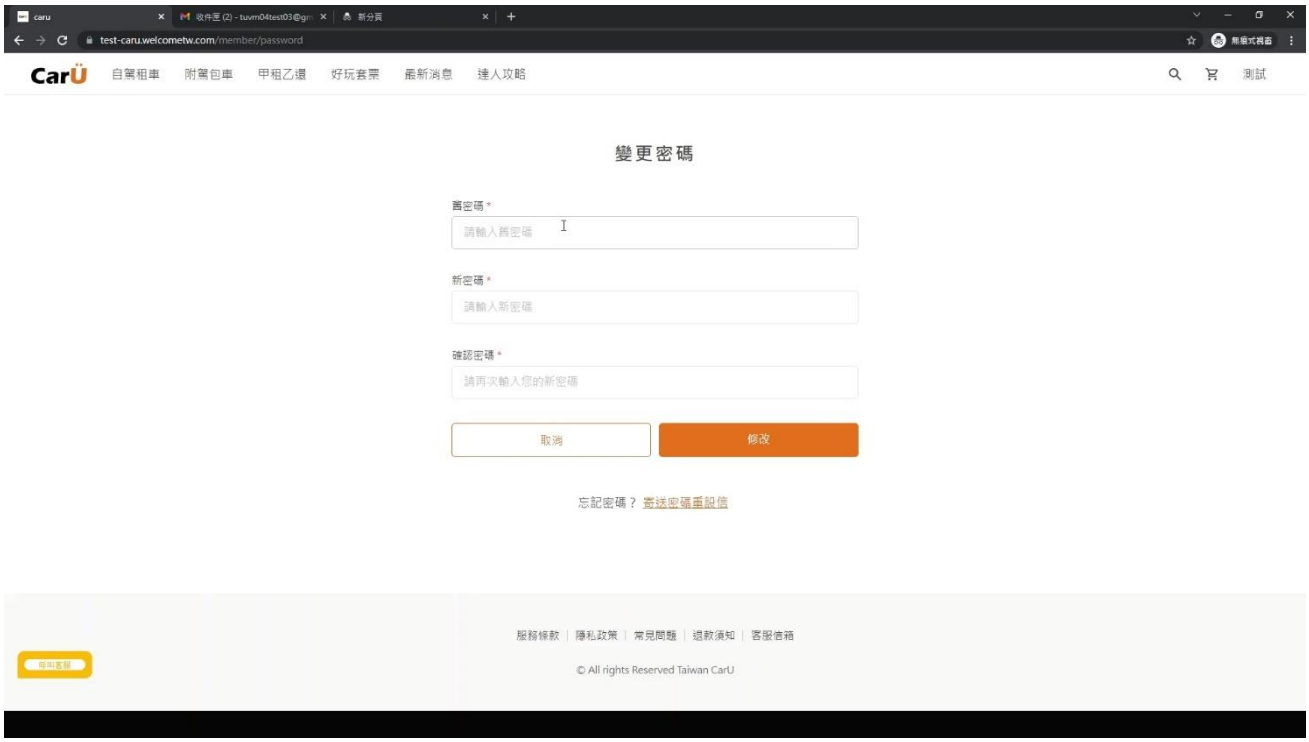
A-07-03


test-caru.welcometw.com/member
CarÜ
自駕租車
附駕包車
甲租乙還
好玩套票
最新消息
達人攻略
測試
tuvm04test03@gmail.com
手機 *
0986991356
發送手機驗證碼
生日
2000-01-01
性別 *
男
女
地址
臺中市
西區
403
忠明南路497號
密碼
變更密碼
更新時間
2021-12-19 19:33
修改
申請刪除帳號說明

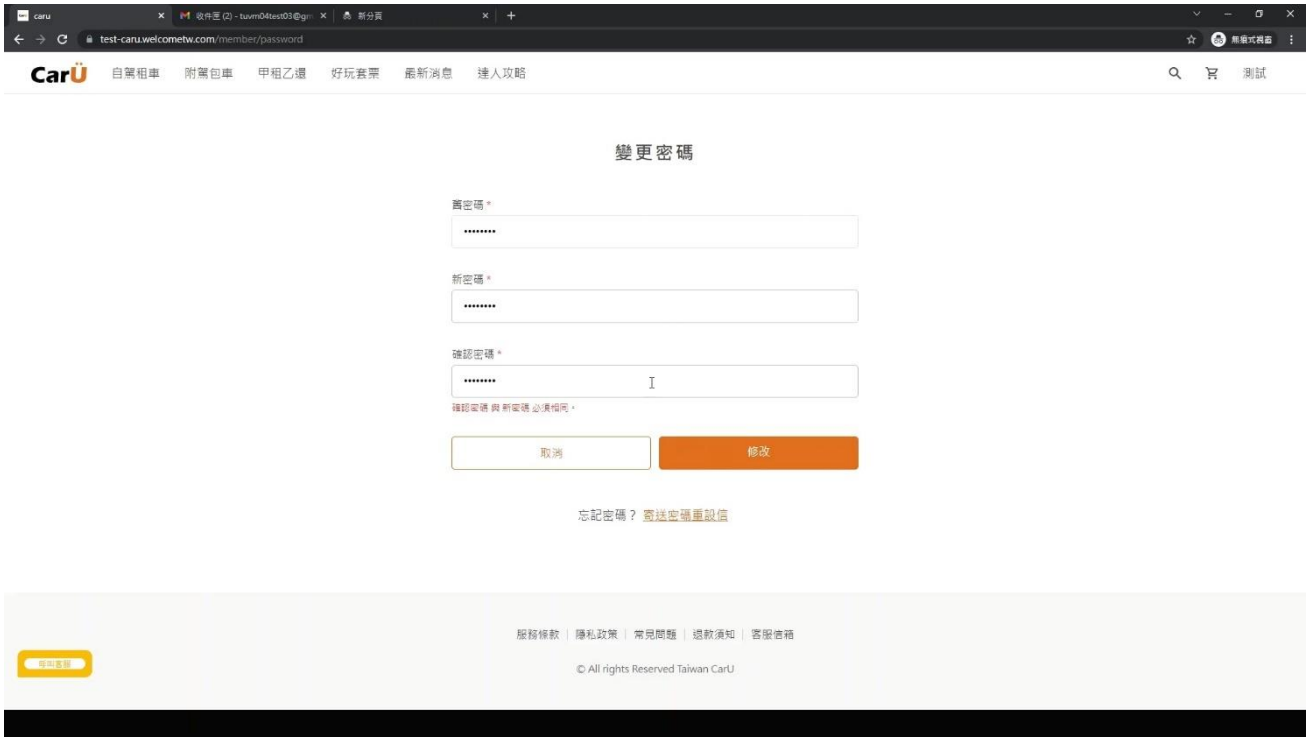
A-07-04


Taiwan CarU
test-caru.welcometw.com/admin/users/frontend/91
後台帳號
權限
角色
Email
tuvm04test03@gmail.com
未驗證
人工認證
密碼
重設密碼
性別
男
手機
0986991356
未驗證
人工認證
等級
無
電話
生日 yyyy-mm-dd
2000-01-01
地址
臺中市
西區
403
忠明南路497號
修改
取消

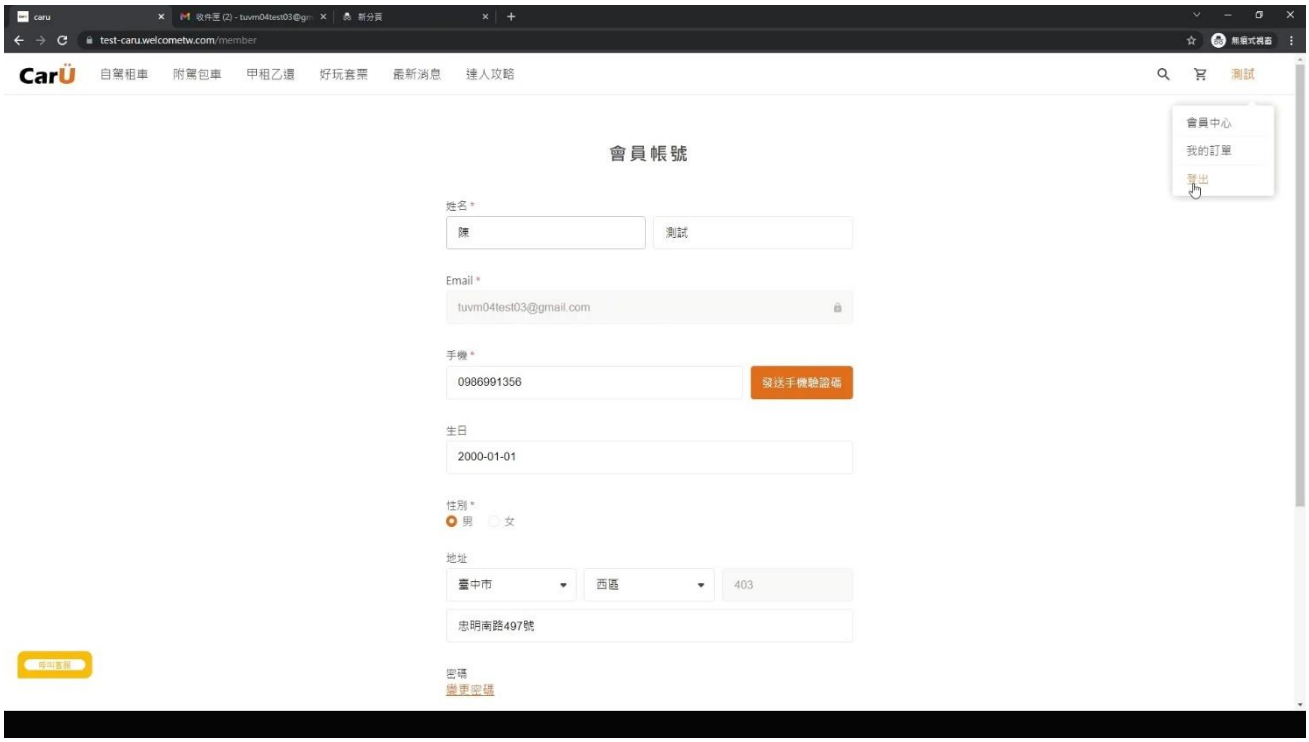
A-08-01


test-caru.welcometw.com/member/password
CarÜ
自駕租車
附駕包車
甲租乙還
好玩套票
最新消息
達人攻略
測試
變更密碼
舊密碼 *
請輸入舊密碼
新密碼 *
請輸入新密碼
確認密碼 *
請再次輸入您的新密碼
取消
修改
忘記密碼？ 寄送密碼重設信
服務條款 | 隱私政策 | 常見問題 | 退款須知 | 客服信箱
© All rights Reserved Taiwan CarU

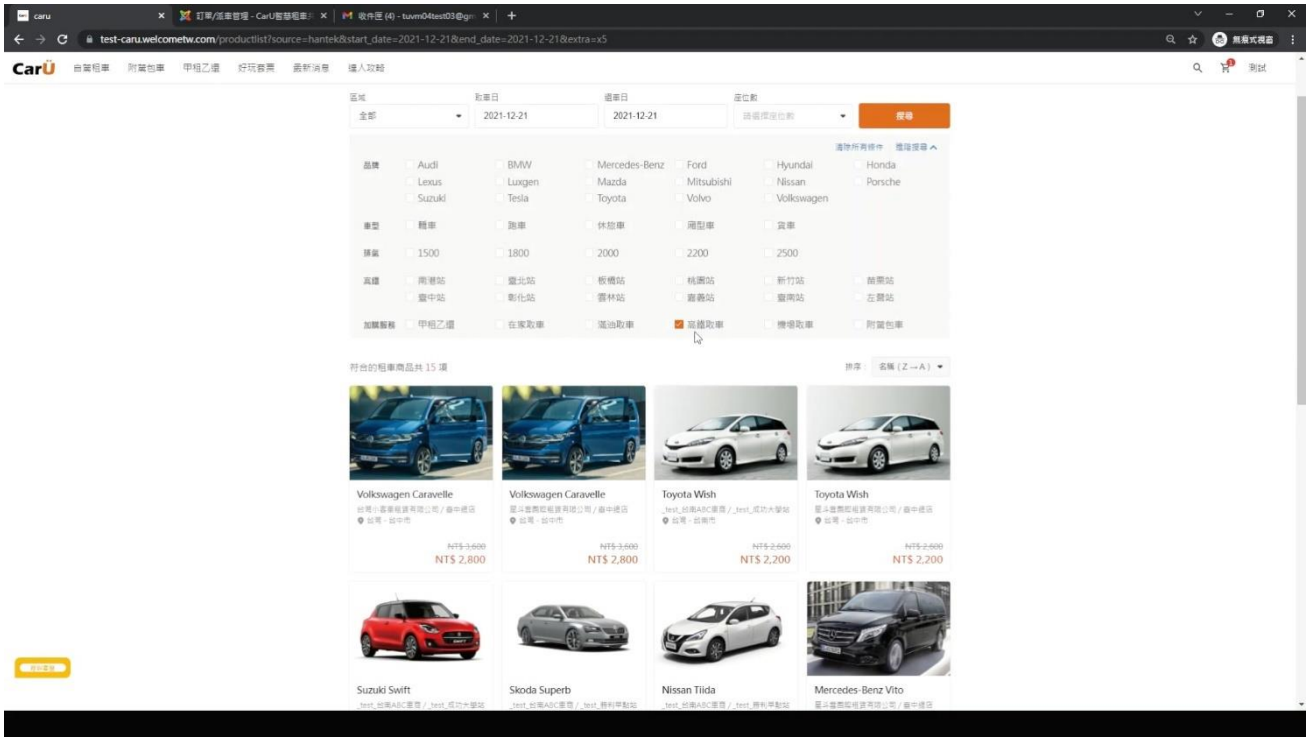
A-08-02


test-caru.welcometw.com/member/password
CarÜ
自駕租車
附駕包車
甲租乙還
好玩套票
最新消息
達人攻略
測試
變更密碼
舊密碼 *
新密碼 *
確認密碼 *
確認密碼與新密碼必須相同。
取消
修改
忘記密碼？ 寄送密碼重設信
服務條款 | 隱私政策 | 常見問題 | 退款須知 | 客服信箱
© All rights Reserved Taiwan CarU

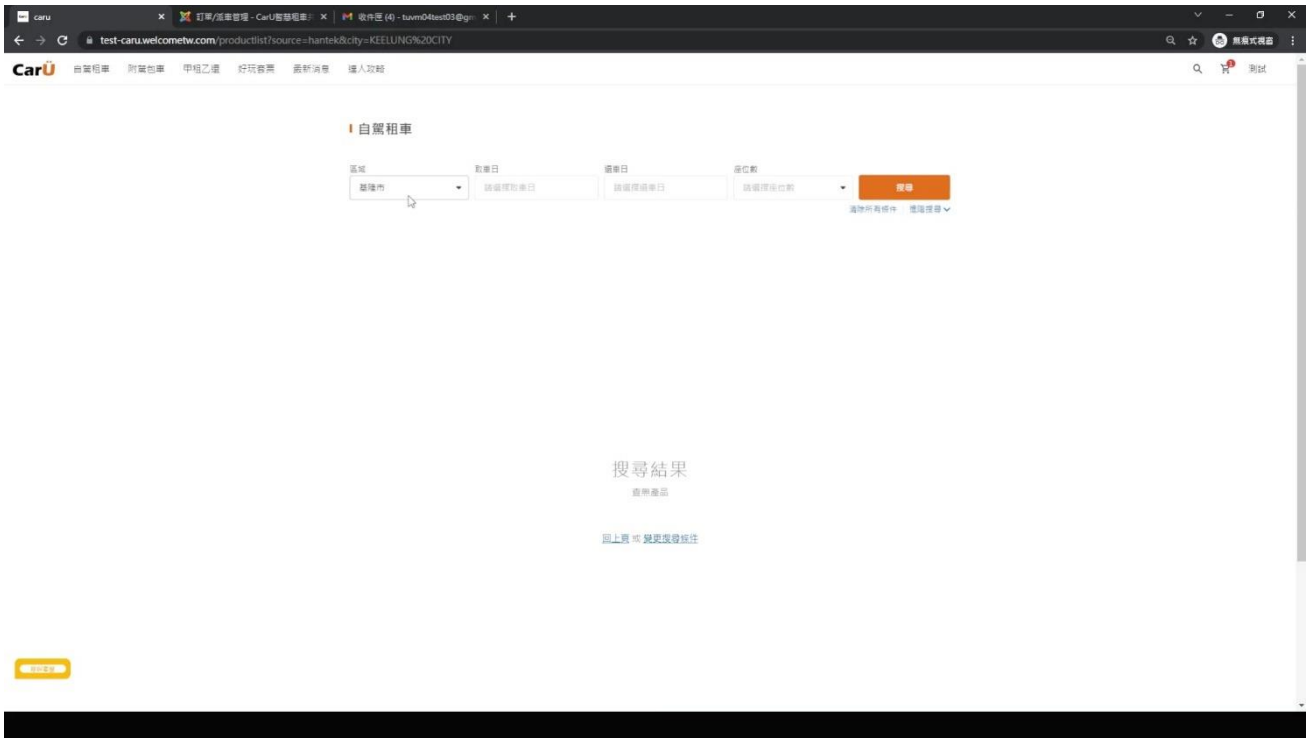
A-10-01


test-caru.welcometw.com/member
CarÜ
自駕租車
附駕包車
甲租乙還
好玩套票
最新消息
達人攻略
測試
會員中心
我的訂單
會員帳號
姓名 *
陳
測試
Email *
tuvm04test03@gmail.com
手機 *
0986991356
發送手機驗證碼
生日
2000-01-01
性別 *
男
女
地址
臺中市
西區
403
忠明南路497號
密碼
變更密碼

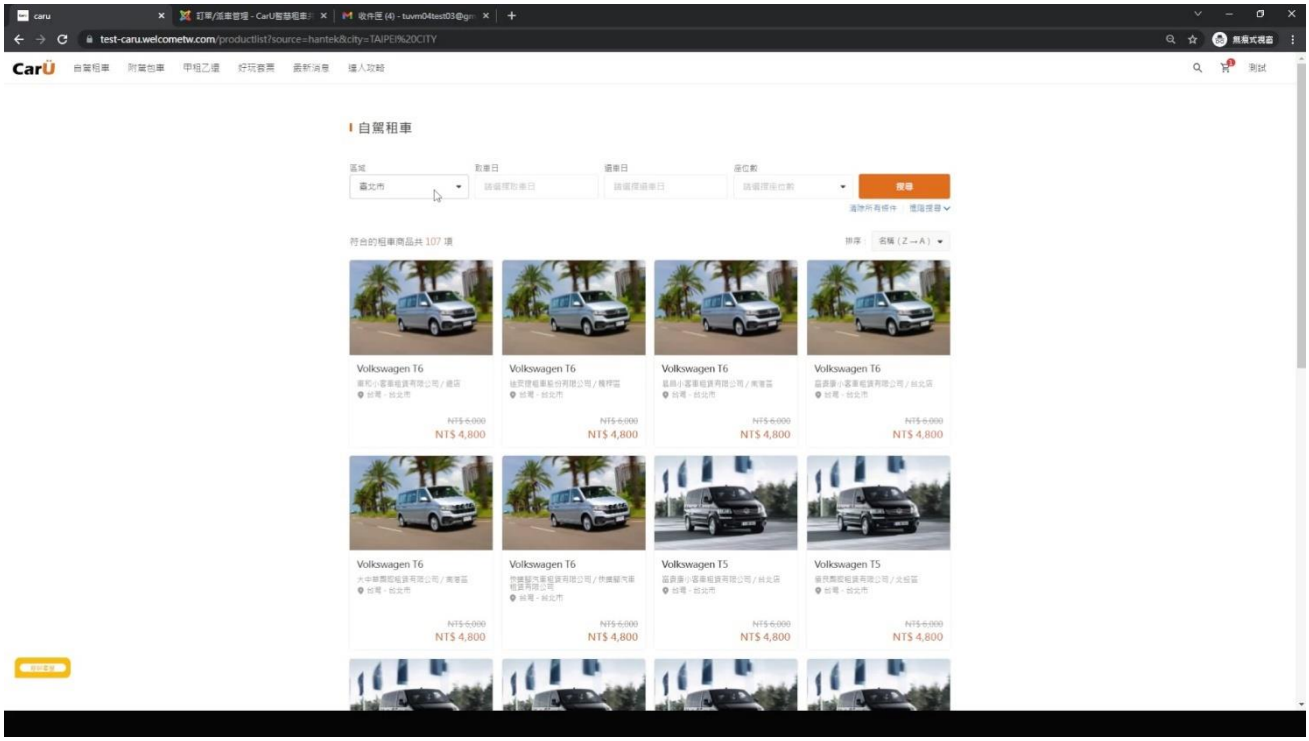
A-11-01


test-caru.welcometw.com/productlist?source=hantek&start_date=2021-12-21&end_date=2021-12-21&extra=x5
CarÜ
自駕租車
附駕包車
甲租乙還
好玩套票
最新消息
達人攻略
測試
2021-12-21
2021-12-21
Audi
BMW
Mercedes-Benz
Ford
Hyundai
Honda
Lexus
Luxgen
Mazda
Mitsubishi
Nissan
Porsche
Suzuki
Tesla
Toyota
Volvo
Volkswagen
1500
1800
2000
2200
2500
Volkswagen Caravelle
NT$ 2,800
Volkswagen Caravelle
NT$ 2,800
Toyota Wish
NT$ 2,200
Toyota Wish
NT$ 2,200
Suzuki Swift
Skoda Superb
Nissan Tiida
Mercedes-Benz Vito

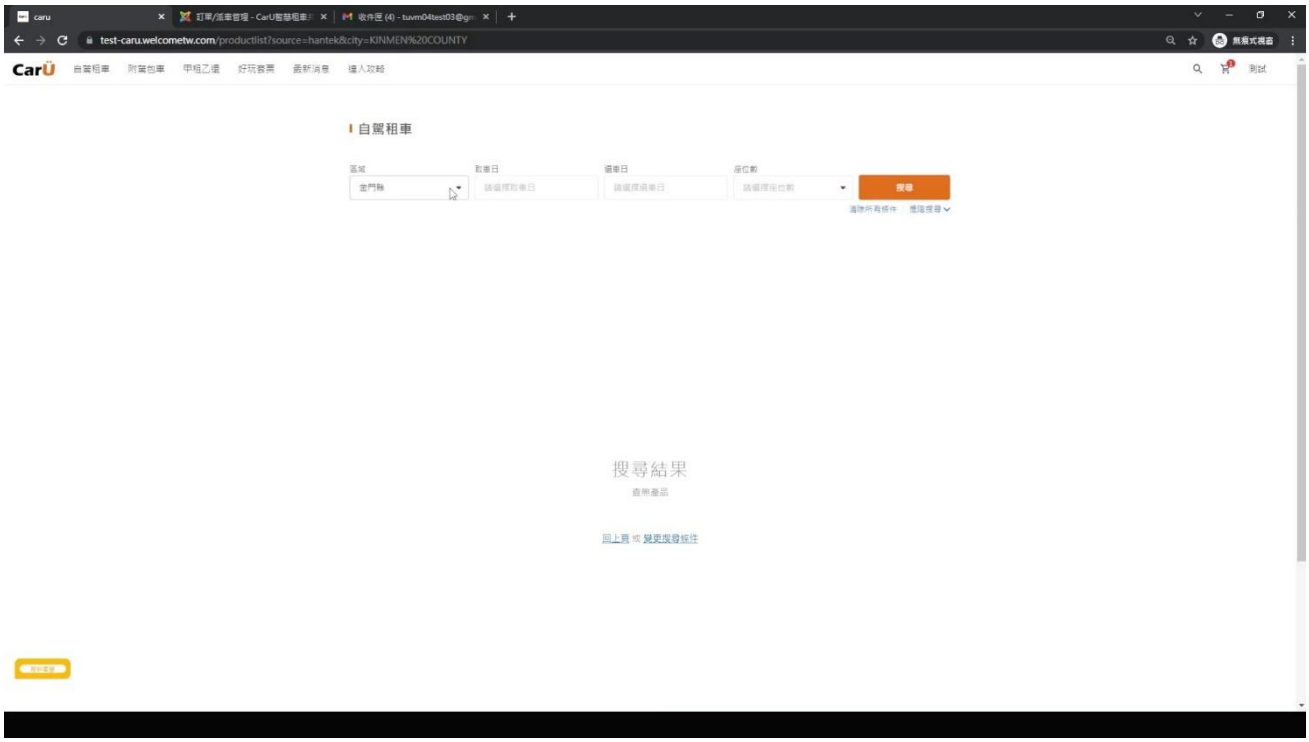
A-11-02


test-caru.welcometw.com/productlist?source=hantek&city=KEELUNG%20CITY
CarÜ
自駕租車
附加包車
甲租乙還
好玩套票
最新消息
達人攻略
測試
自駕租車
區域
基隆市
取車日
還車日
座位數
搜尋
清除所有條件
進階搜尋
搜尋結果
查無產品
回上頁 或 變更搜尋條件

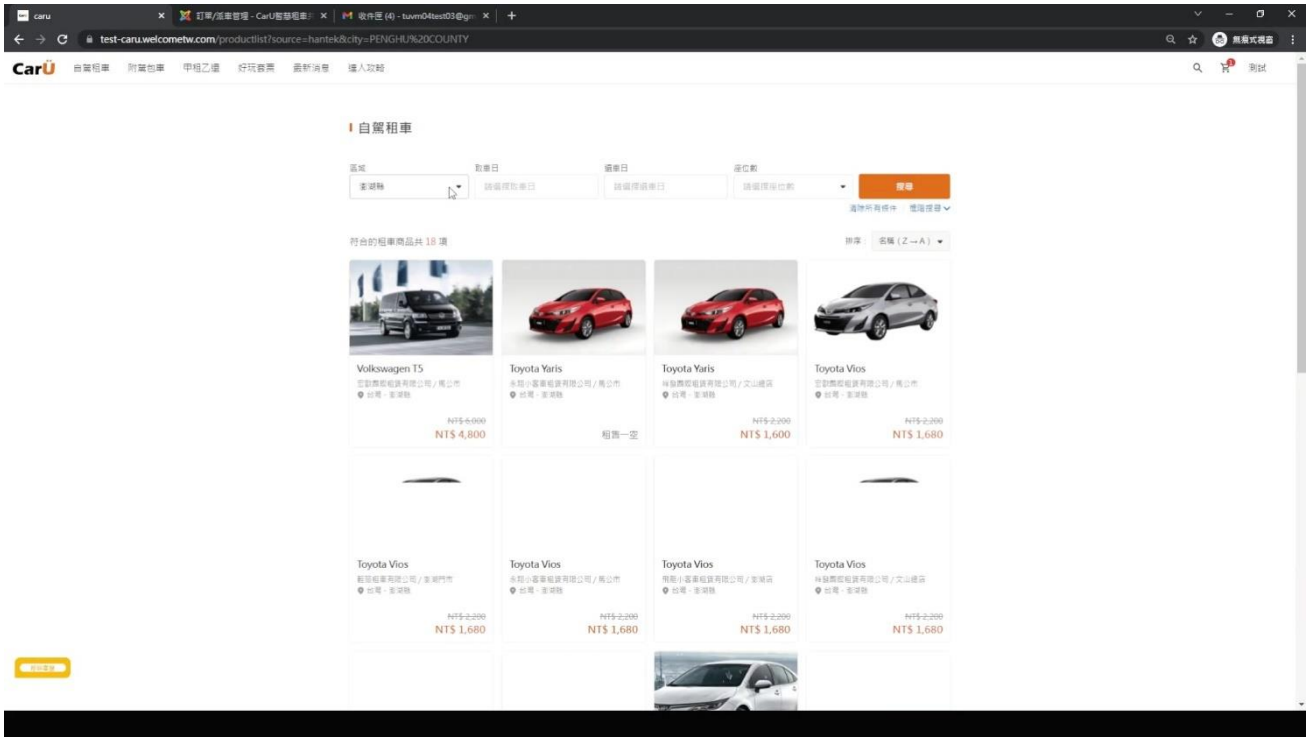
A-11-03


test-caru.welcometw.com/productlist?source=hantek&city=TAIPEI%20CITY
CarÜ
自駕租車
附加包車
甲租乙還
好玩套票
最新消息
達人攻略
測試
自駕租車
區域
臺北市
取車日
還車日
座位數
搜尋
清除所有條件
進階搜尋
符合的租車商品共 107 項
排序
名稱 (Z → A)
Volkswagen T6
Volkswagen T6
Volkswagen T6
Volkswagen T6
NT$ 6,000
NT$ 4,800
Volkswagen T6
Volkswagen T6
Volkswagen T5
Volkswagen T5

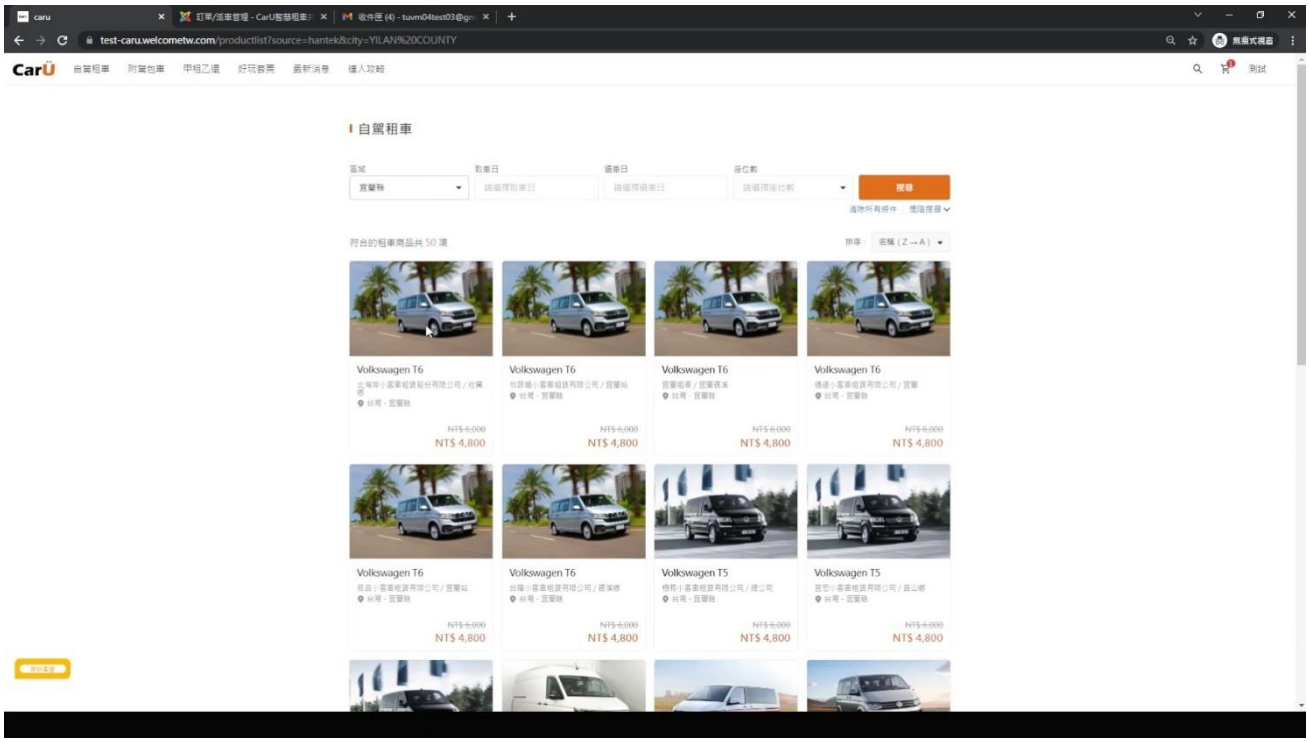
A-11-04


test-caru.welcometw.com/productlist?source=hantek&city=KINMEN%20COUNTY
CarÜ
自駕租車
附贈包車
甲租乙還
好玩套票
最新消息
達人攻略
測試
自駕租車
搜尋
搜尋結果
查無產品
回上頁 或 變更搜尋條件

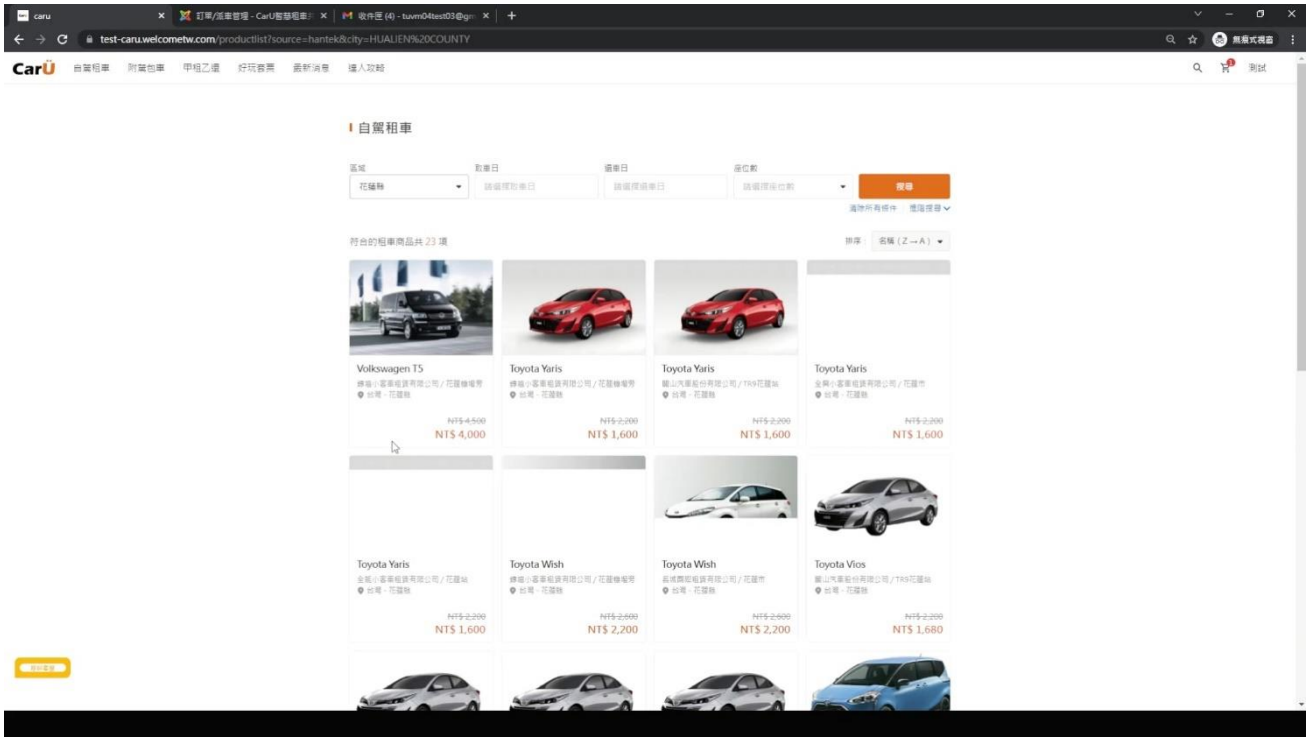
A-11-05


test-caru.welcometw.com/productlist?source=hantek&city=PENGHU%20COUNTY
CarÜ
自駕租車
附贈包車
甲租乙還
好玩套票
最新消息
達人攻略
測試
自駕租車
搜尋
符合的租車商品共 18 項
排序
名稱 (Z → A)
Volkswagen T5
NT$ 6,000
NT$ 4,800
Toyota Yaris
租賃一空
Toyota Yaris
NT$ 2,200
NT$ 1,600
Toyota Vios
NT$ 2,200
NT$ 1,680
Toyota Vios
NT$ 2,200
NT$ 1,680
Toyota Vios
NT$ 2,200
NT$ 1,680
Toyota Vios
NT$ 2,200
NT$ 1,680
Toyota Vios
NT$ 2,200
NT$ 1,680

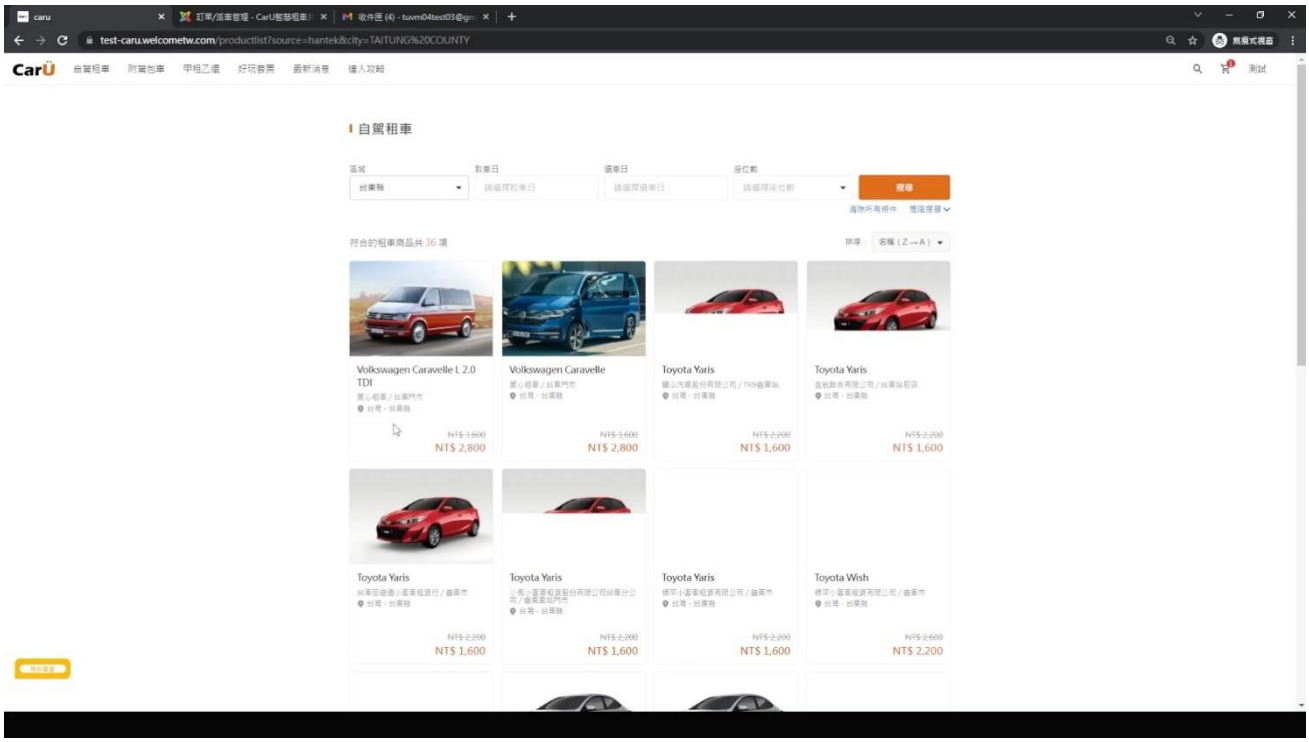
A-11-06


test-caru.welcometw.com/productlist?source=hantek&city=YILAN%20COUNTY
自駕租車
Volkswagen T6
NT$ 4,800
Volkswagen T5

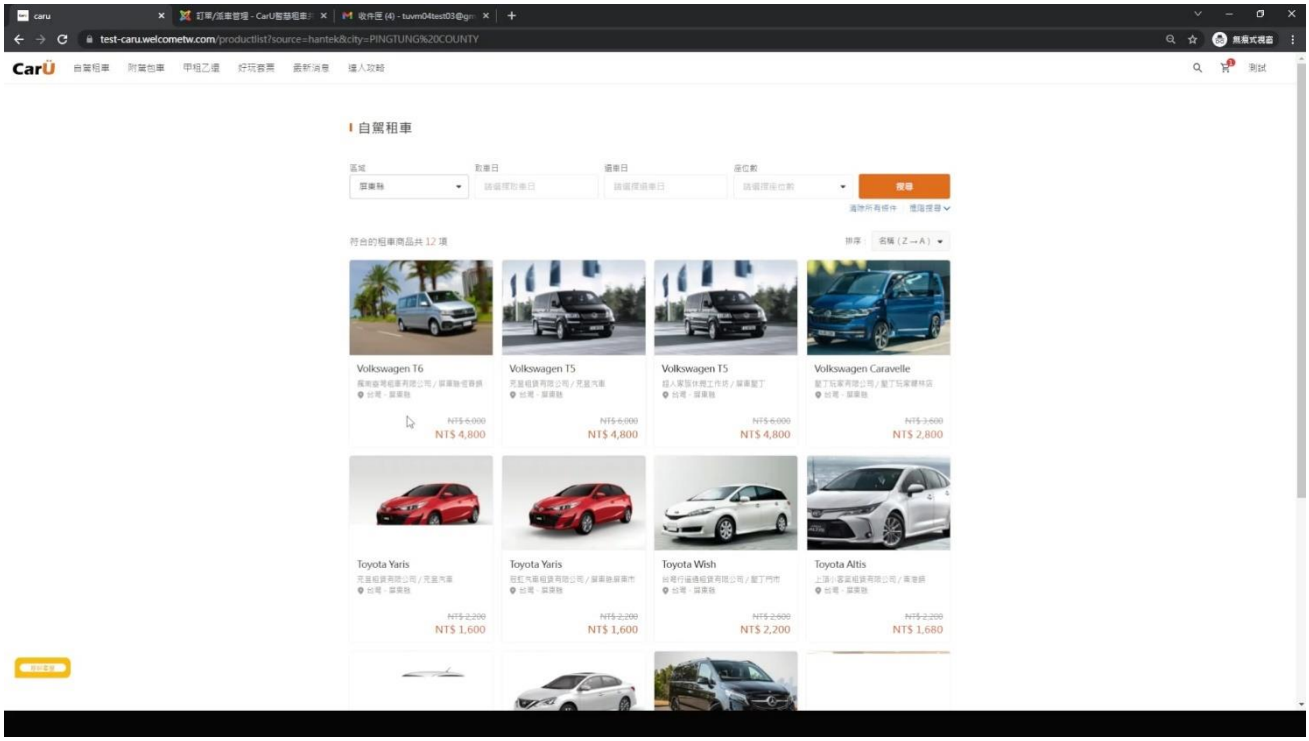
A-11-07


test-caru.welcometw.com/productlist?source=hantek&city=HUALIEN%20COUNTY
自駕租車
Volkswagen T5
NT$ 4,000
Toyota Yaris
NT$ 1,600
Toyota Wish
NT$ 2,200
Toyota Vios
NT$ 1,680

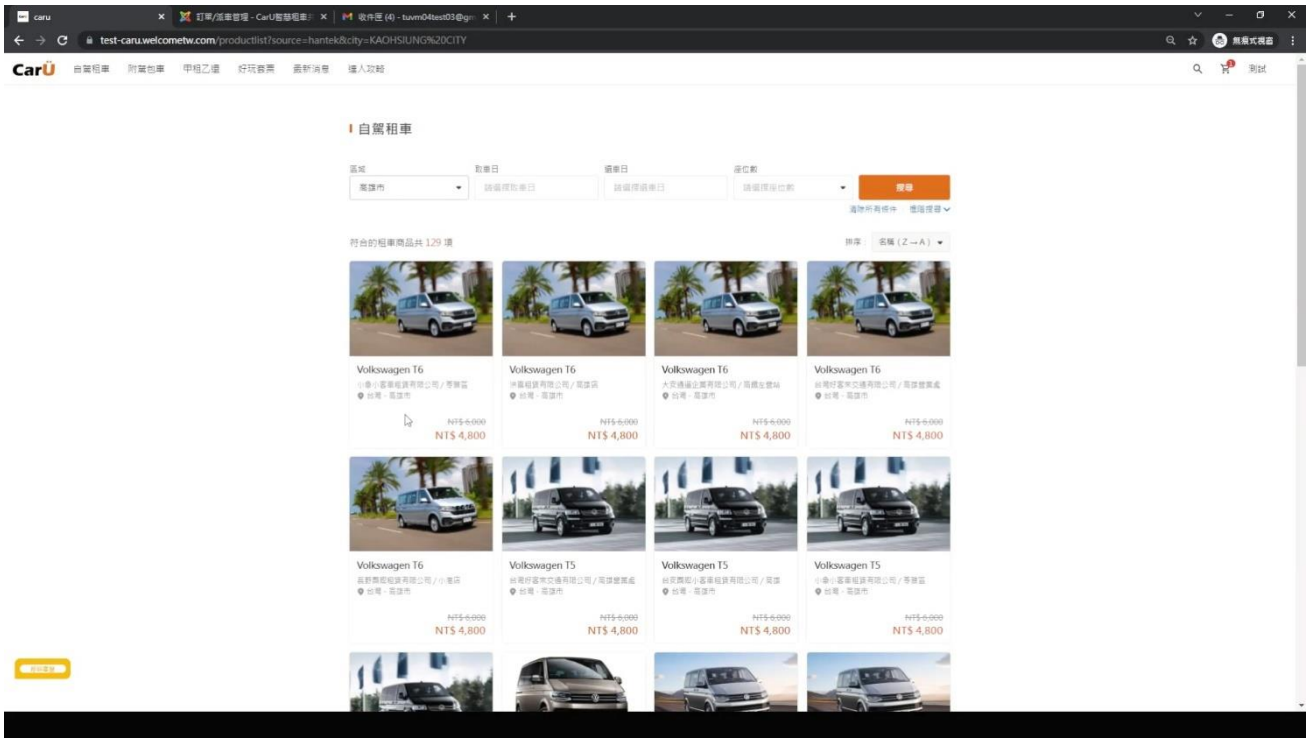
A-11-08


test-caru.welcometw.com/productlist?source=hantek&city=TAITUNG%20COUNTY
CarÜ
自駕租車
區域
取車日
還車日
座位數
搜尋
符合的租車商品共 36 項
Volkswagen Caravelle L 2.0 TDI
NT$ 3,600
NT$ 2,800
Volkswagen Caravelle
NT$ 3,600
NT$ 2,800
Toyota Yaris
NT$ 2,200
NT$ 1,600
Toyota Yaris
NT$ 2,200
NT$ 1,600
Toyota Yaris
NT$ 2,200
NT$ 1,600
Toyota Yaris
NT$ 2,200
NT$ 1,600
Toyota Yaris
NT$ 2,200
NT$ 1,600
Toyota Wish
NT$ 2,600
NT$ 2,200

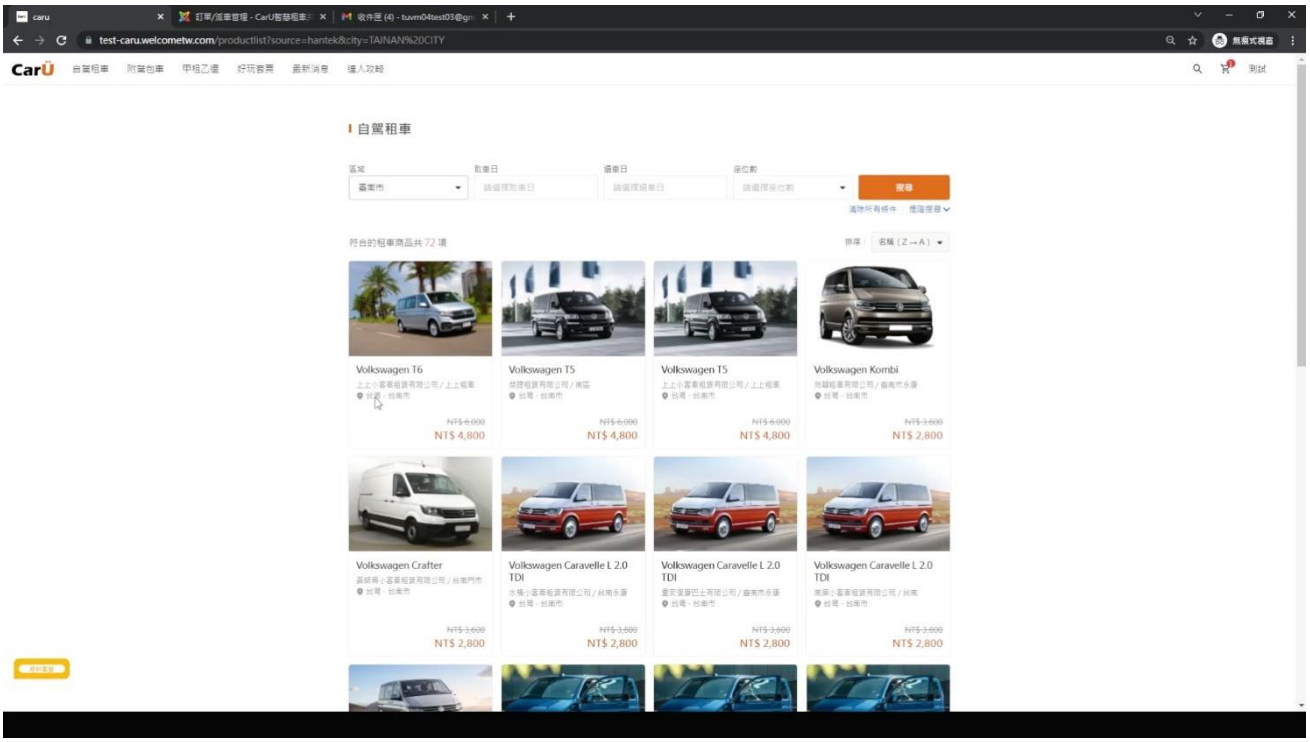
A-11-09


test-caru.welcometw.com/productlist?source=hantek&city=PINGTUNG%20COUNTY
CarÜ
自駕租車
區域
取車日
還車日
座位數
搜尋
符合的租車商品共 12 項
Volkswagen T6
NT$ 6,000
NT$ 4,800
Volkswagen T5
NT$ 6,000
NT$ 4,800
Volkswagen T5
NT$ 6,000
NT$ 4,800
Volkswagen Caravelle
NT$ 3,600
NT$ 2,800
Toyota Yaris
NT$ 2,200
NT$ 1,600
Toyota Yaris
NT$ 2,200
NT$ 1,600
Toyota Wish
NT$ 2,600
NT$ 2,200
Toyota Altis
NT$ 2,200
NT$ 1,680

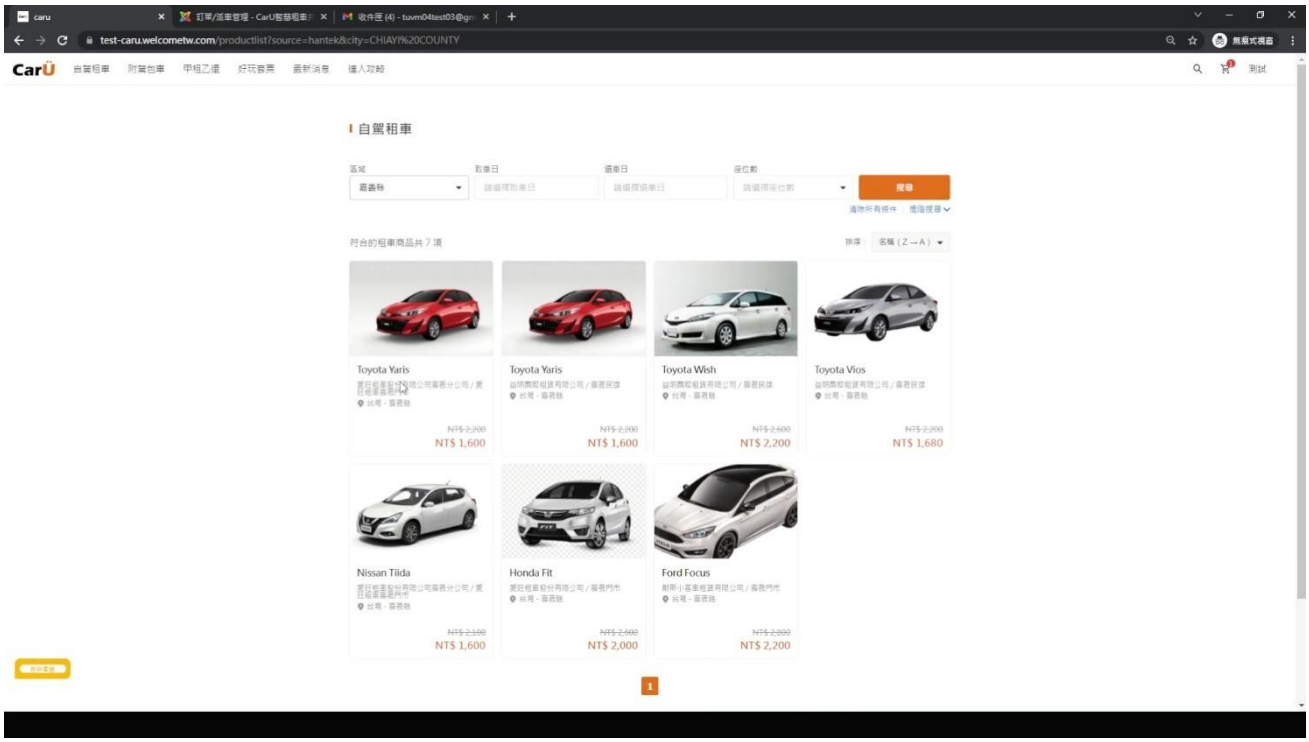
A-11-10


test-caru.welcometw.com/productlist?source=hantek&city=KAOHSIUNG%20CITY
自駕租車
Volkswagen T6
NT$ 4,800
Volkswagen T5
NT$ 4,800

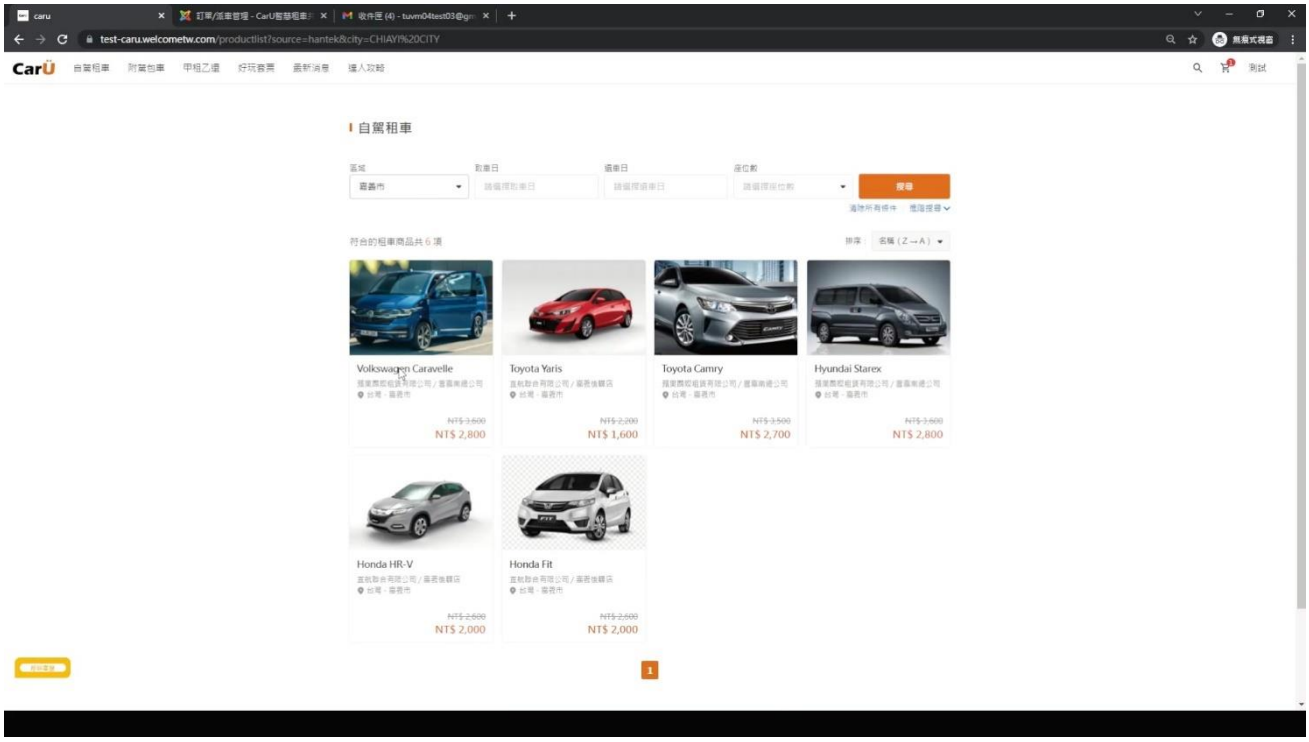
A-11-11


test-caru.welcometw.com/productlist?source=hantek&city=TAINAN%20CITY
自駕租車
Volkswagen T6
NT$ 4,800
Volkswagen T5
NT$ 4,800
Volkswagen Kombi
NT$ 2,800
Volkswagen Crafter
NT$ 2,800
Volkswagen Caravelle L 2.0 TDI
NT$ 2,800

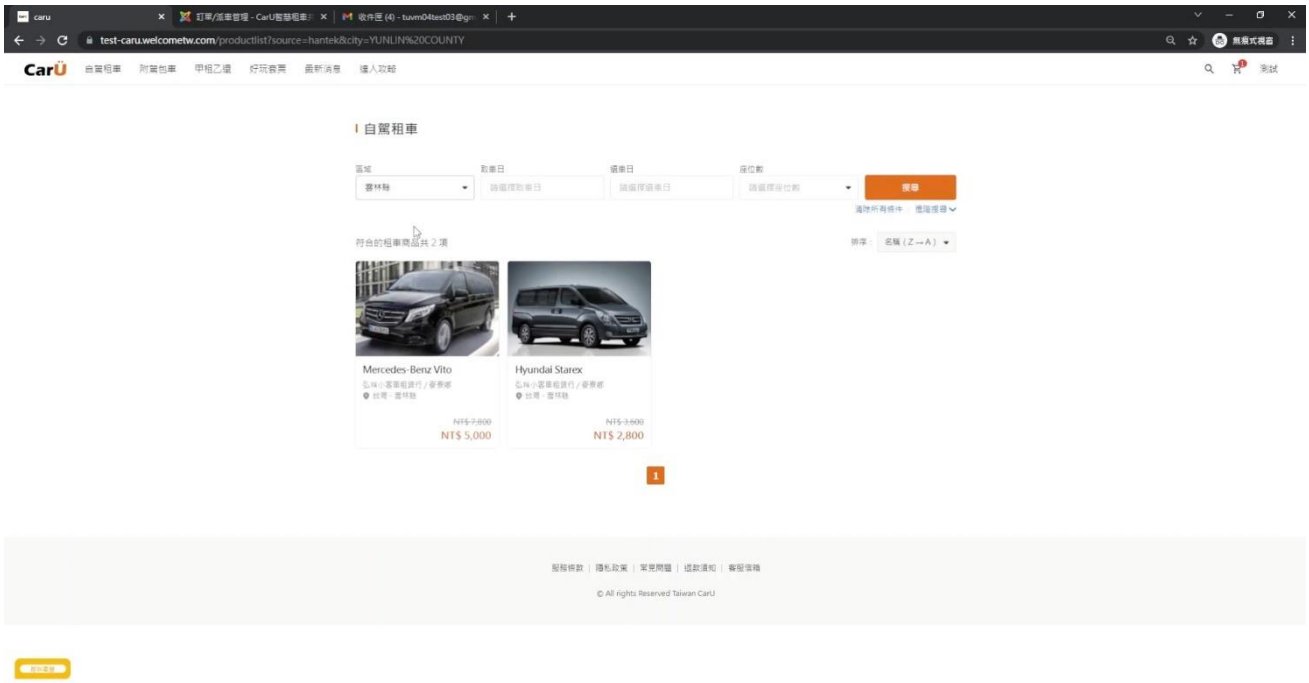
A-11-12


test-caru.welcometw.com/productlist?source=hantek&city=CHIAYI%20COUNTY
自駕租車
Toyota Yaris
NT$ 1,600
Toyota Yaris
NT$ 1,600
Toyota Wish
NT$ 2,200
Toyota Vios
NT$ 1,680
Nissan Tiida
NT$ 1,600
Honda Fit
NT$ 2,000
Ford Focus
NT$ 2,200

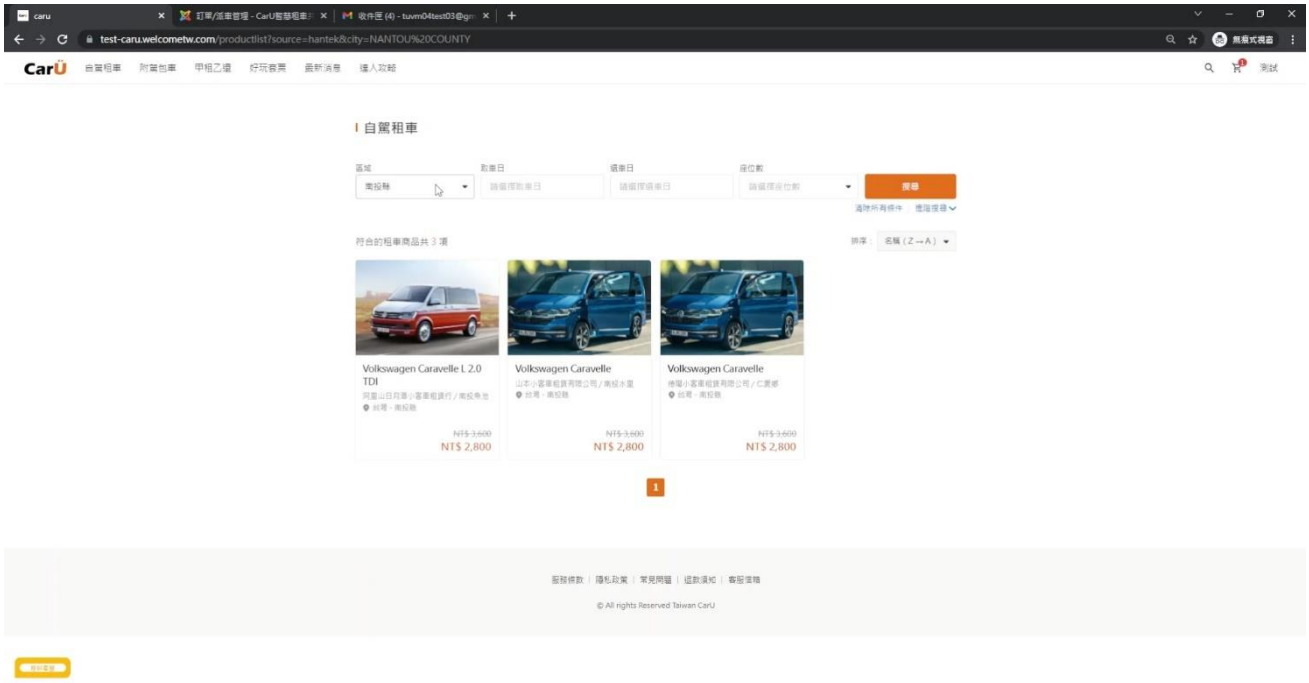
A-11-13


test-caru.welcometw.com/productlist?source=hantek&city=CHIAYI%20CITY
自駕租車
Volkswagen Caravelle
NT$ 2,800
Toyota Yaris
NT$ 1,600
Toyota Camry
NT$ 2,700
Hyundai Starex
NT$ 2,800
Honda HR-V
NT$ 2,000
Honda Fit
NT$ 2,000

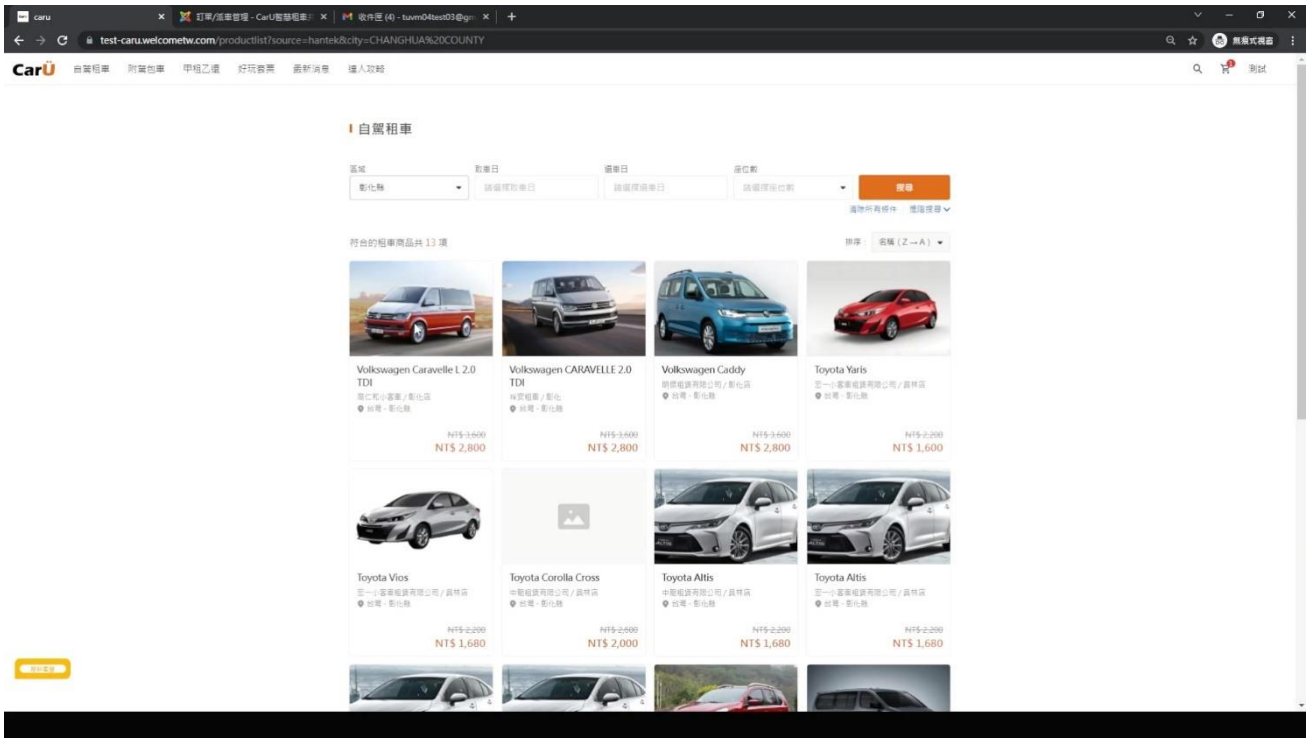
A-11-14


test-caru.welcometw.com/productlist?source=hantek&city=YUNLIN%20COUNTY
CarU
自駕租車
Mercedes-Benz Vito
NT$ 5,000
Hyundai Starex
NT$ 2,800

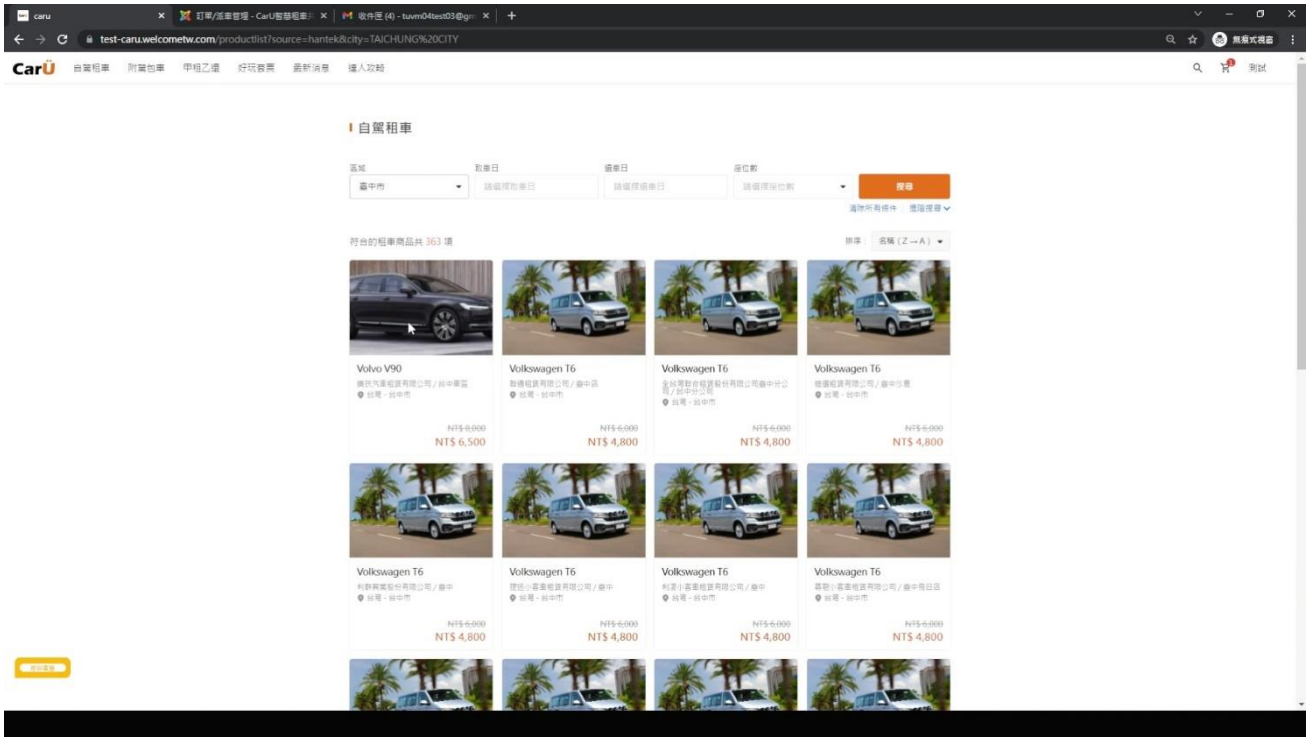
A-11-15


test-caru.welcometw.com/productlist?source=hantek&city=NANTOU%20COUNTY
CarU
自駕租車
Volkswagen Caravelle L 2.0 TDI
NT$ 2,800
Volkswagen Caravelle
NT$ 2,800
Volkswagen Caravelle
NT$ 2,800

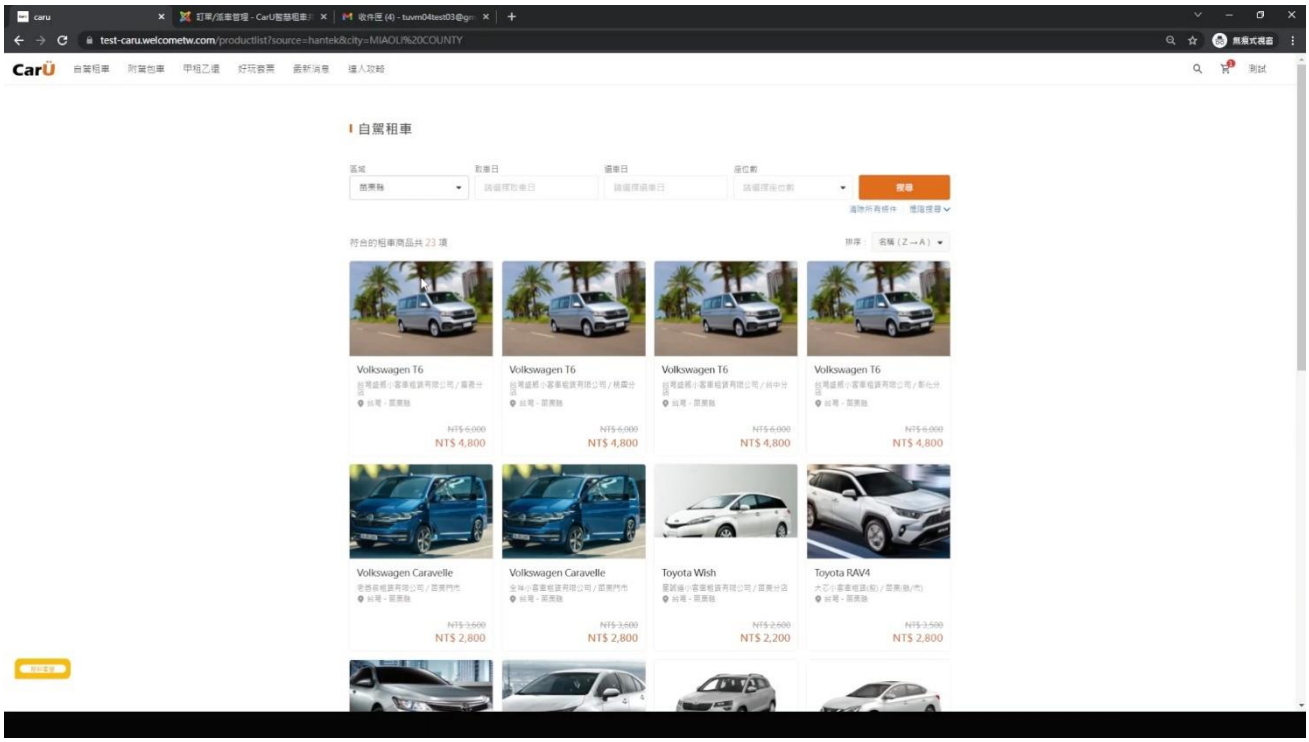
A-11-16


test-caru.welcometw.com/productlist?source=hantek&city=CHANGHUA%20COUNTY
自駕租車
Volkswagen Caravelle L 2.0 TDI
NT$ 2,800
Volkswagen CARAVELLE 2.0 TDI
NT$ 2,800
Volkswagen Caddy
NT$ 2,800
Toyota Yaris
NT$ 1,600
Toyota Vios
NT$ 1,680
Toyota Corolla Cross
NT$ 2,000
Toyota Altis
NT$ 1,680
Toyota Altis
NT$ 1,680

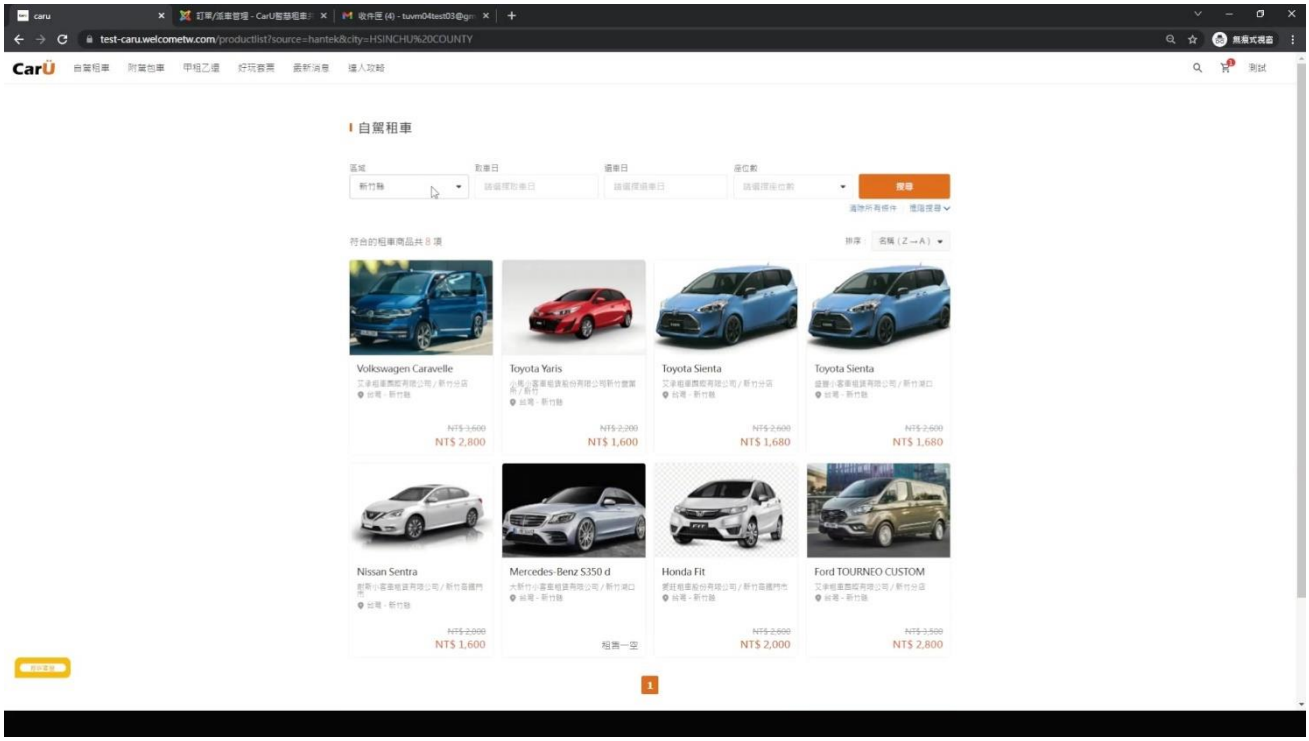
A-11-17


test-caru.welcometw.com/productlist?source=hantek&city=TAICHUNG%20CITY
自駕租車
Volvo V90
NT$ 6,500
Volkswagen T6
NT$ 4,800
Volkswagen T6
NT$ 4,800
Volkswagen T6
NT$ 4,800
Volkswagen T6
NT$ 4,800
Volkswagen T6
NT$ 4,800
Volkswagen T6
NT$ 4,800
Volkswagen T6
NT$ 4,800

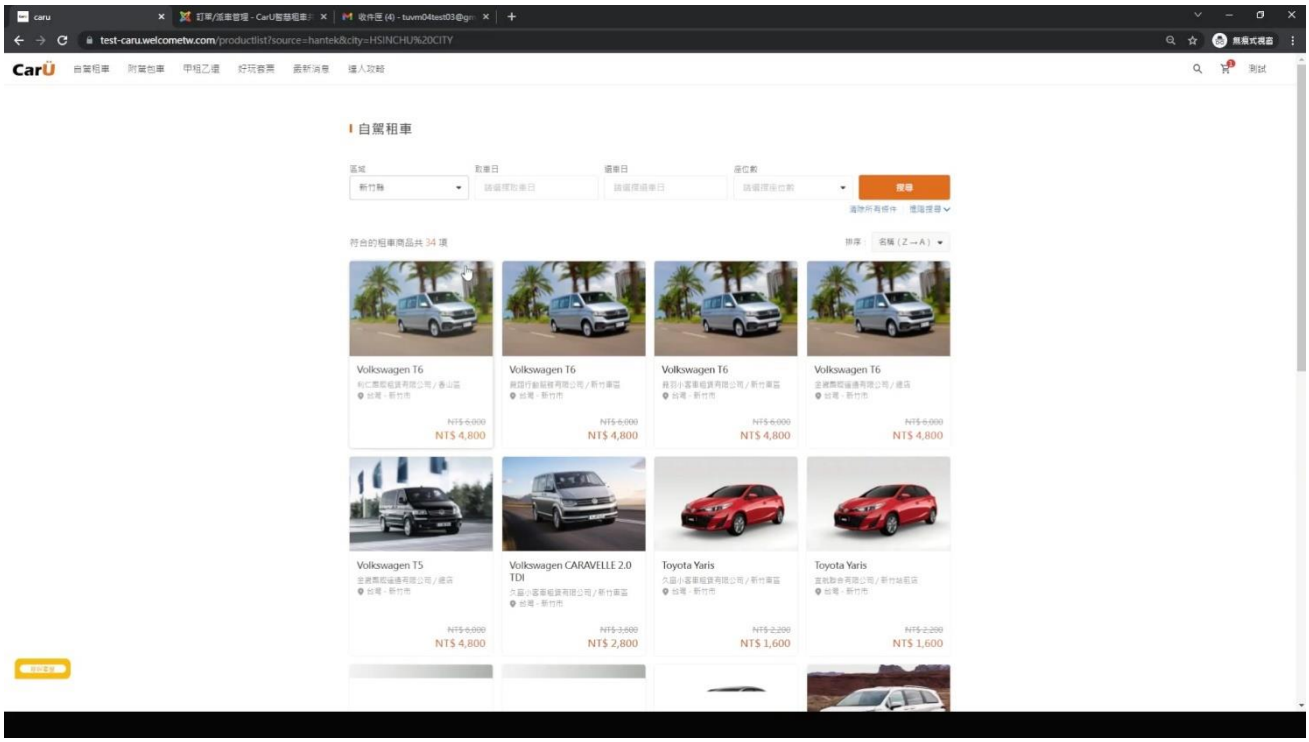
A-11-18


test-caru.welcometw.com/productlist?source=hantek&city=MIAOLI%20COUNTY
CarÜ
自駕租車
附贈包車
甲組乙選
好玩套票
最新消息
達人攻略
測試
自駕租車
區域
取車日
還車日
座位數
搜尋
符合的租車商品共 23 項
排序：
名稱（Z→A）
Volkswagen T6
NT$ 6,000
NT$ 4,800
Volkswagen Caravelle
NT$ 3,600
NT$ 2,800
Toyota Wish
NT$ 2,600
NT$ 2,200
Toyota RAV4
NT$ 3,500
NT$ 2,800

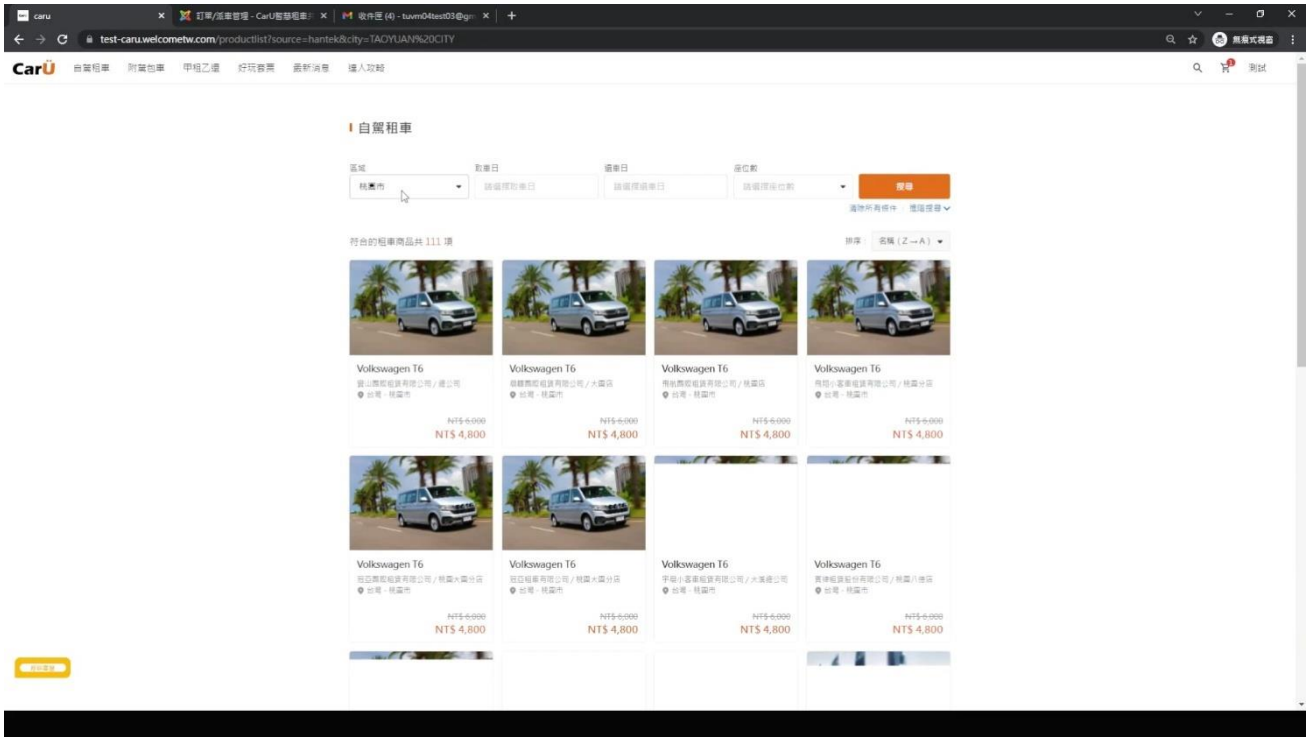
A-11-19


test-caru.welcometw.com/productlist?source=hantek&city=HSINCHU%20COUNTY
CarÜ
自駕租車
附贈包車
甲組乙選
好玩套票
最新消息
達人攻略
測試
自駕租車
區域
取車日
還車日
座位數
搜尋
新竹縣
符合的租車商品共 8 項
排序：
名稱（Z→A）
Volkswagen Caravelle
NT$ 3,600
NT$ 2,800
Toyota Yaris
NT$ 2,200
NT$ 1,600
Toyota Sienta
NT$ 2,600
NT$ 1,680
Toyota Sienta
NT$ 2,600
NT$ 1,680
Nissan Sentra
NT$ 2,000
NT$ 1,600
Mercedes-Benz S350 d
租賃一空
Honda Fit
NT$ 2,600
NT$ 2,000
Ford TOURNEO CUSTOM
NT$ 3,500
NT$ 2,800

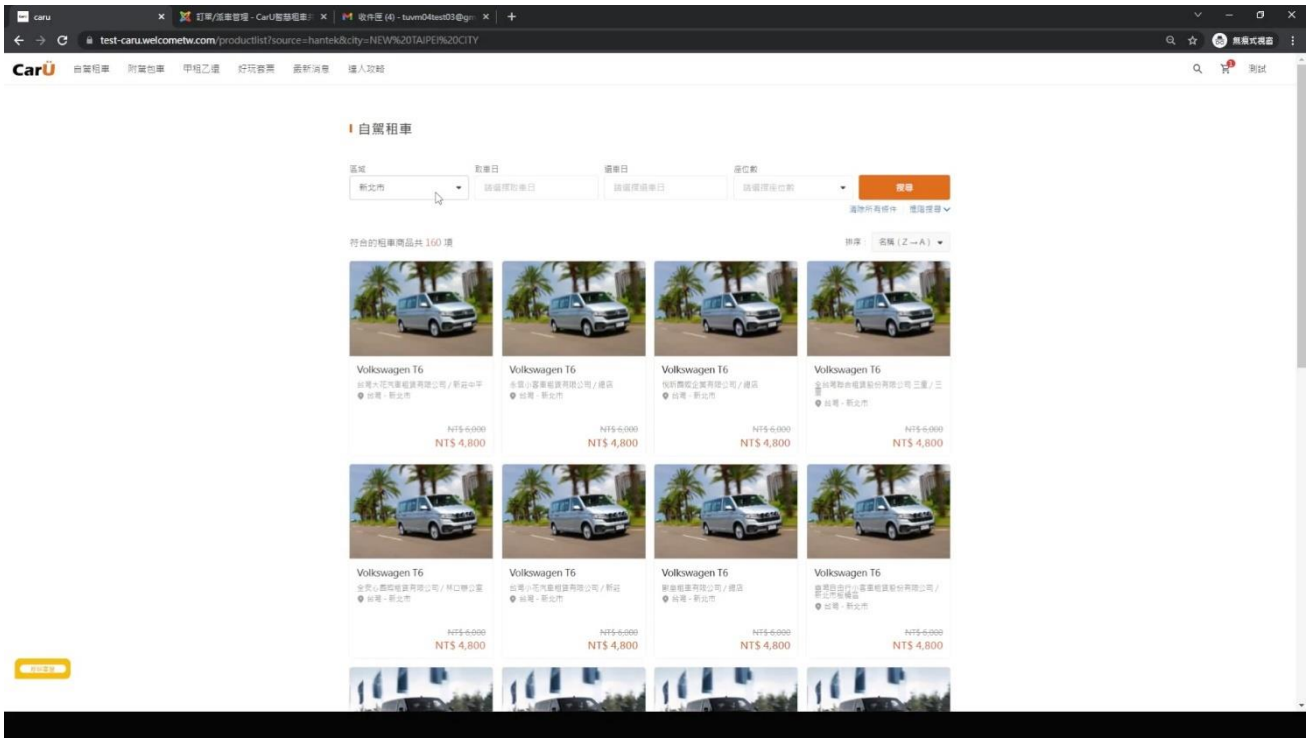
A-11-20


test-caru.welcometw.com/productlist?source=hantek&city=HSINCHU%20CITY
自駕租車
Volkswagen T6
NT$ 4,800
Volkswagen T5
NT$ 4,800
Volkswagen CARAVELLE 2.0 TDI
NT$ 2,800
Toyota Yaris
NT$ 1,600
Toyota Yaris
NT$ 1,600

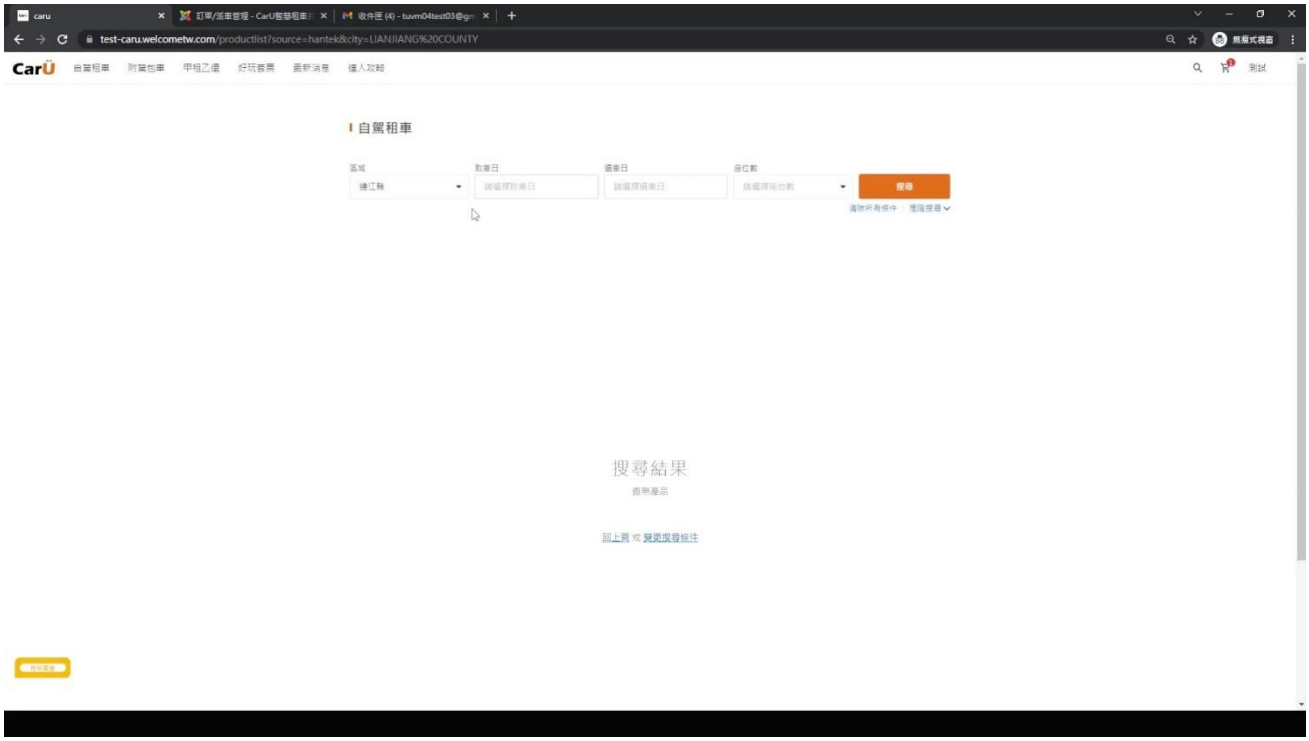
A-11-21


test-caru.welcometw.com/productlist?source=hantek&city=TAOYUAN%20CITY
自駕租車
Volkswagen T6
NT$ 4,800

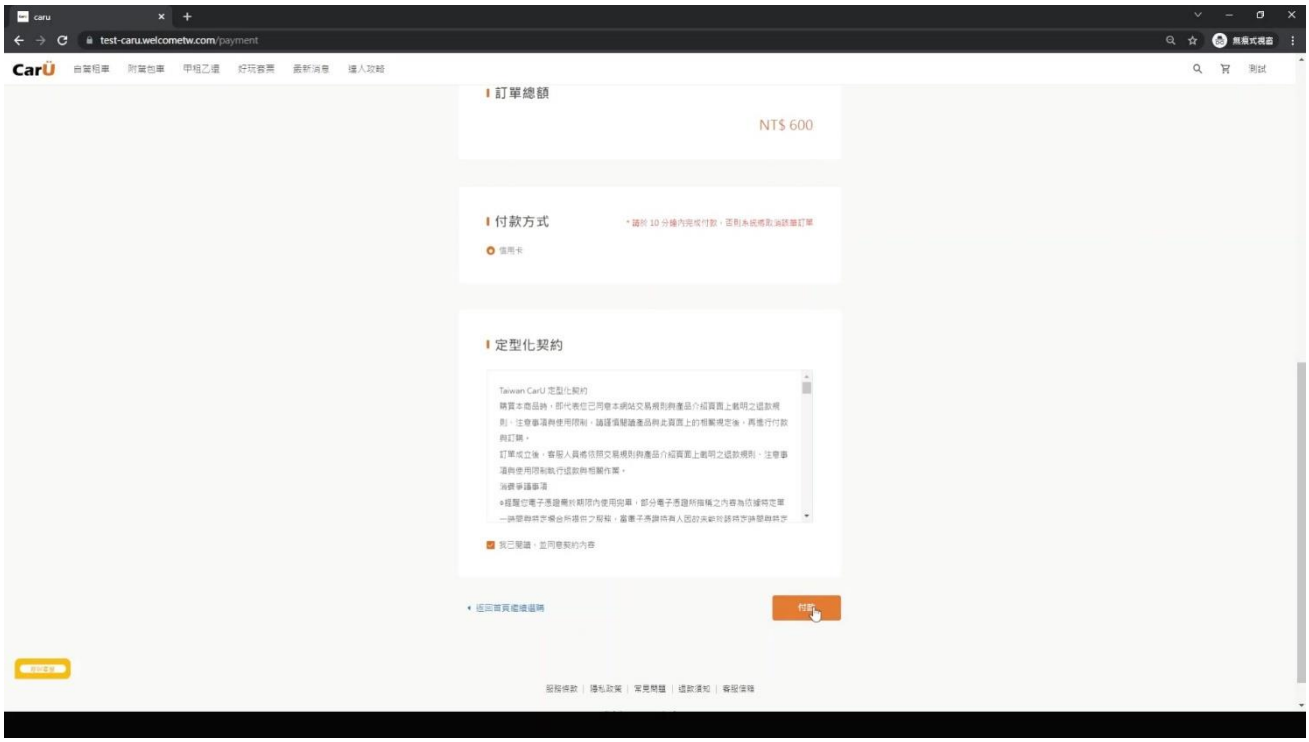
A-11-22


test-caru.welcometw.com/productlist?source=hantek&city=NEW%20TAIPEI%20CITY
CarÜ
自駕租車
附加包車
甲租乙還
好玩套票
最新消息
達人攻略
測試
自駕租車
區域
新北市
取車日
還車日
座位數
搜尋
符合的租車商品共 160 項
排序：名稱（Z→A）
Volkswagen T6
NT$ 6,000
NT$ 4,800

A-11-23


test-caru.welcometw.com/productlist?source=hantek&city=LIANJIANG%20COUNTY
CarÜ
自駕租車
附加包車
甲租乙還
好玩套票
最新消息
達人攻略
測試
自駕租車
區域
連江縣
取車日
還車日
座位數
搜尋
搜尋結果
查無產品
回上頁 或 變更搜尋條件

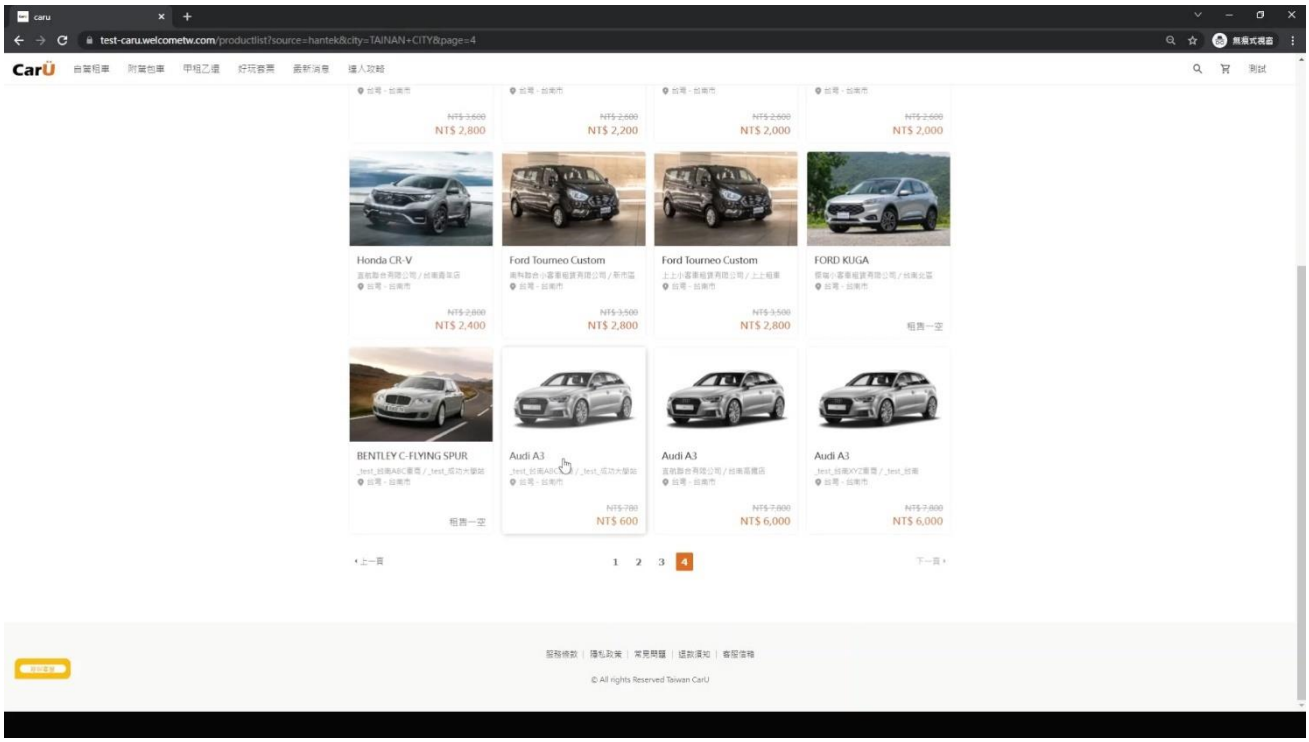
A-12-01


test-caru.welcometw.com/payment
訂單總額
NT$ 600
付款方式
定型化契約
付款

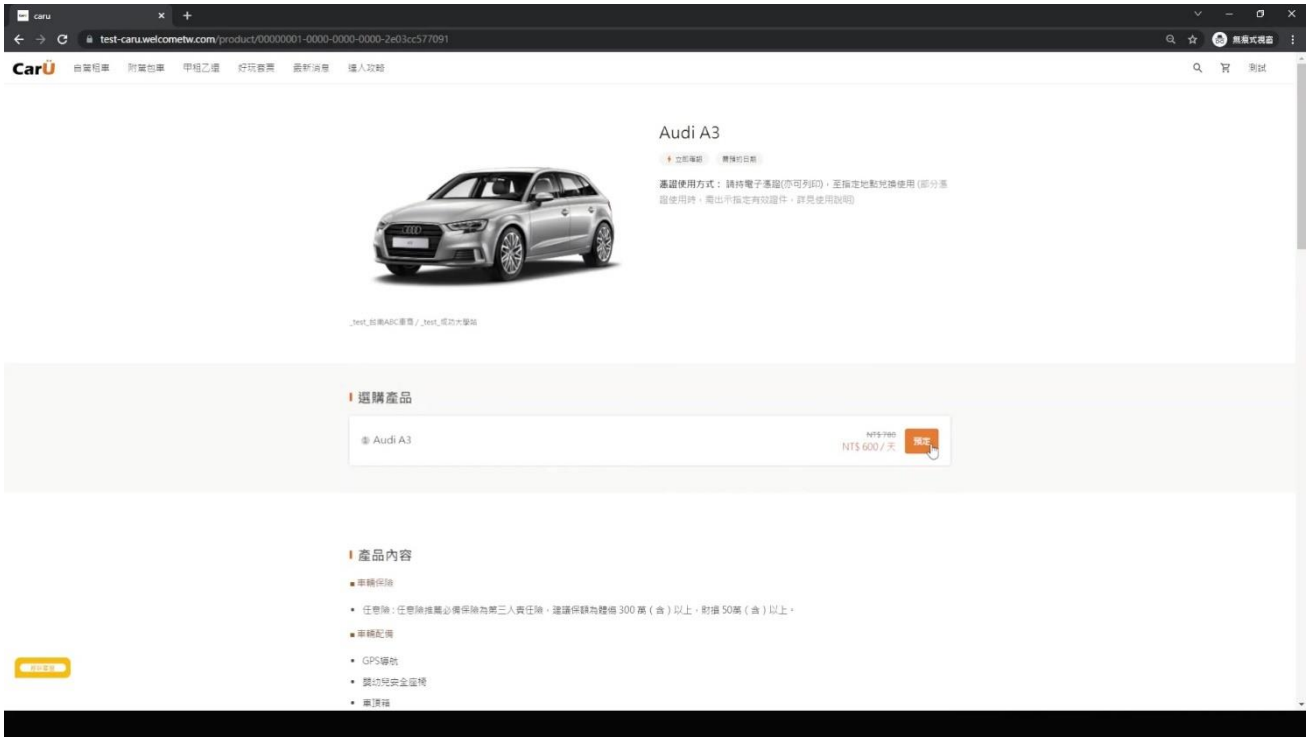
A-14-01

test-caru.welcometw.com/terms
服務條款

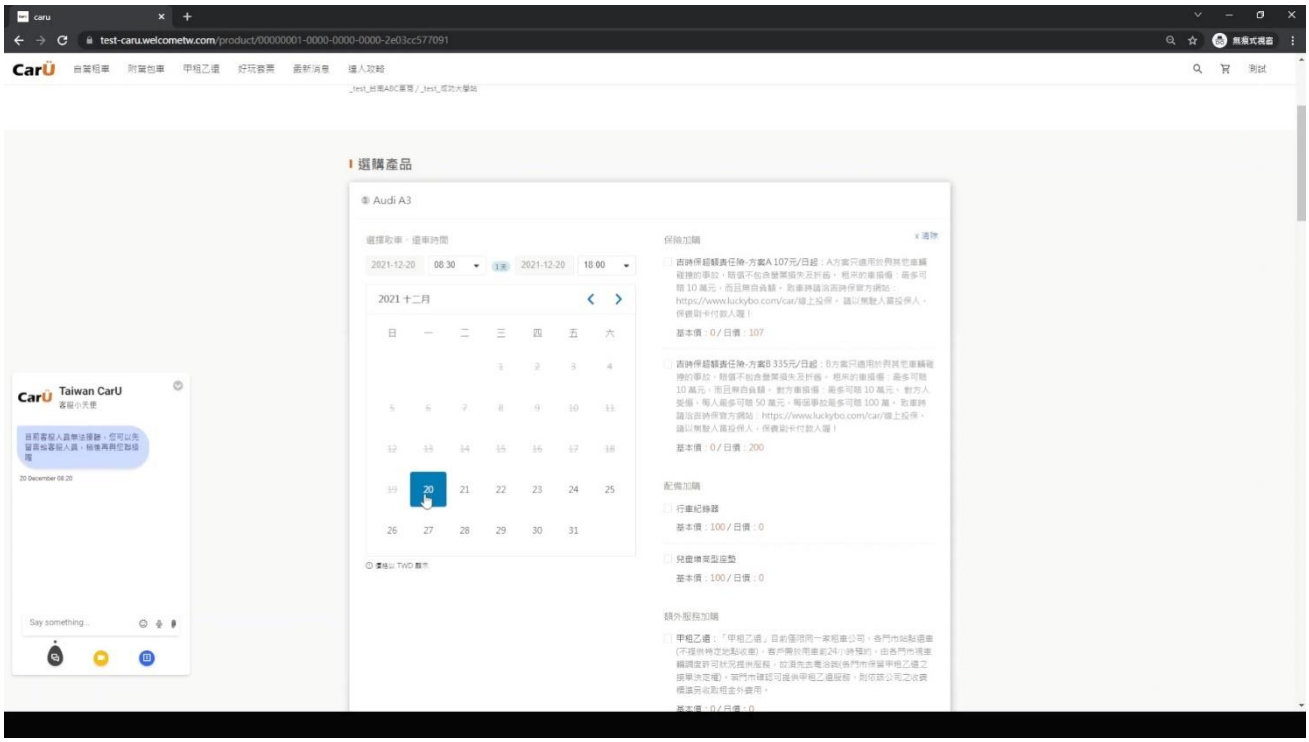
A-15-01


test-caru.welcometw.com/productlist?source=hantek&city=TAINAN+CITY&page=4
CarU
Honda CR-V
NT$ 2,400
Ford Tourneo Custom
NT$ 2,800
Ford Tourneo Custom
NT$ 2,800
FORD KUGA
BENTLEY C-FLYING SPUR
Audi A3
NT$ 600
Audi A3
NT$ 6,000
Audi A3
NT$ 6,000
1 2 3 4
© All rights Reserved Taiwan CarU

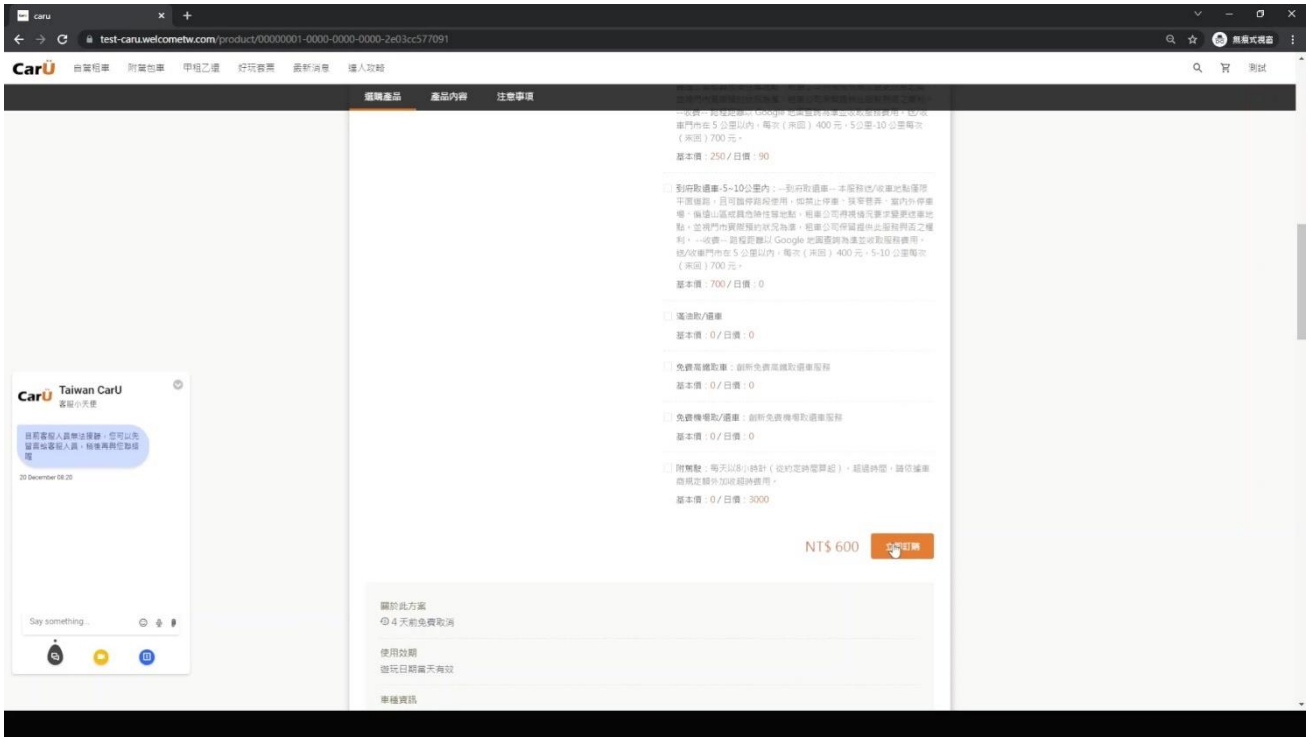
A-15-02


test-caru.welcometw.com/product/00000001-0000-0000-0000-2e03cc577091
CarU
Audi A3
選購產品
Audi A3
NT$ 600 / 天
產品內容

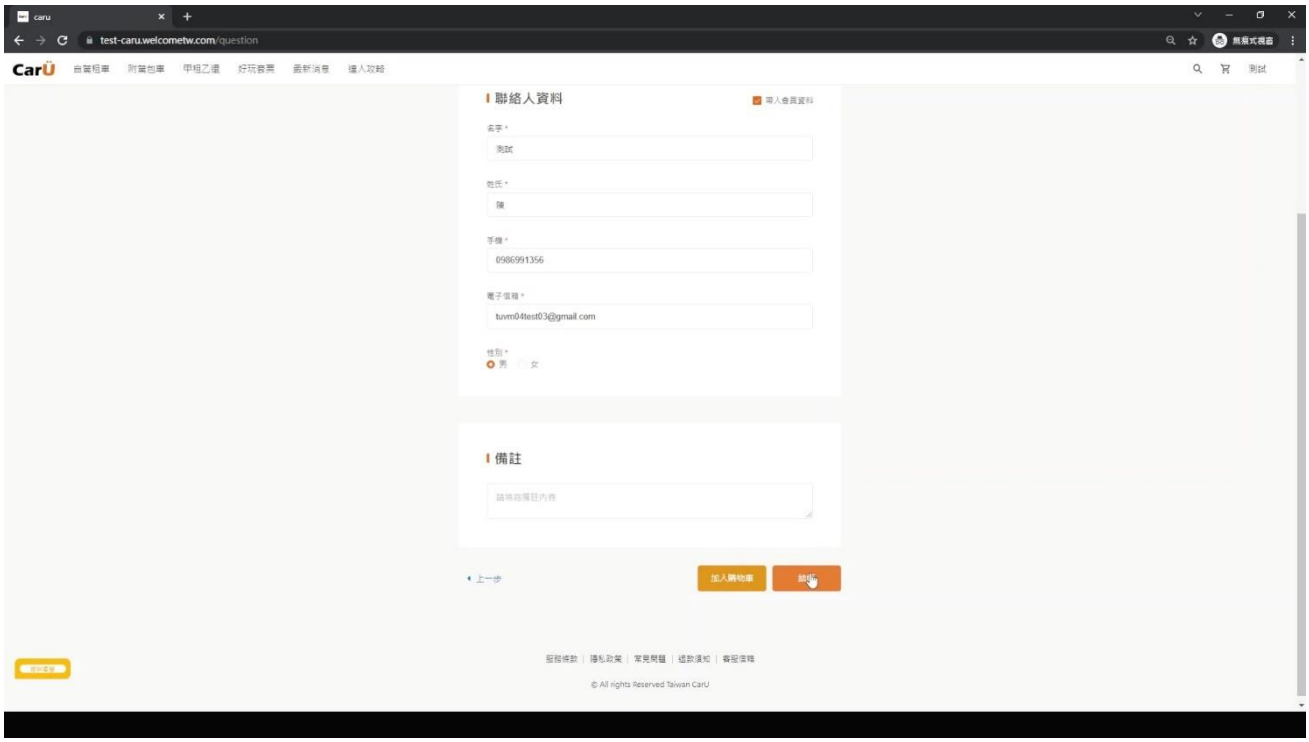
A-15-03


test-caru.welcometw.com/product/00000001-0000-0000-0000-2e03cc577091
CarU
選購產品
Audi A3
Taiwan CarU

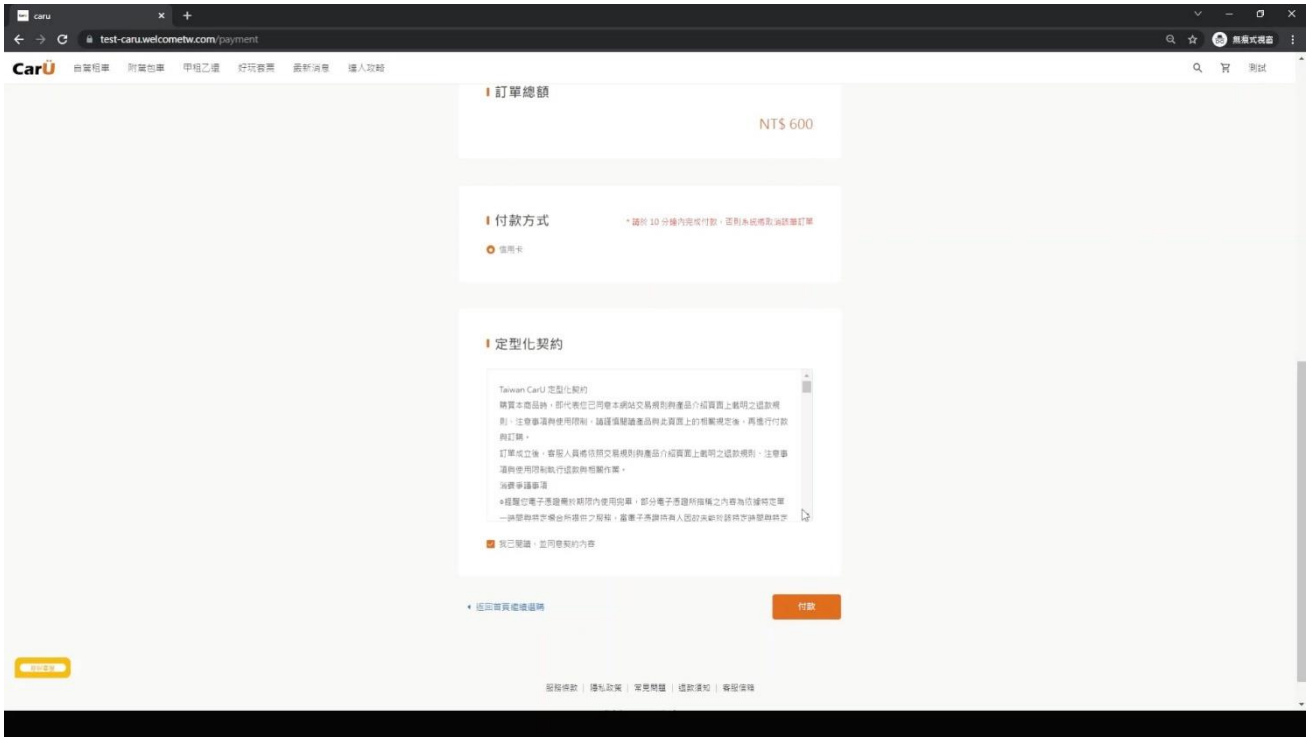
A-15-04


test-caru.welcometw.com/product/00000001-0000-0000-0000-2e03cc577091
CarU
選購產品
產品內容
注意事項
NT$ 600
Taiwan CarU

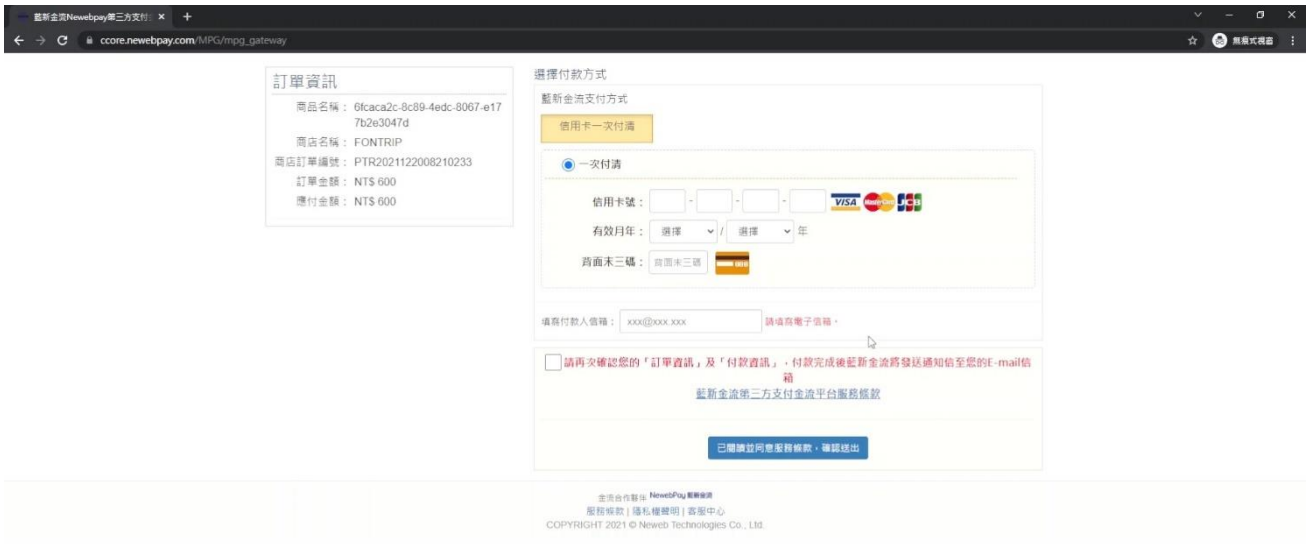
A-15-05


test-caru.welcometw.com/question
CarÜ
聯絡人資料
名字 *
測試
姓氏 *
陳
手機 *
0986991356
電子信箱 *
tuvm04test03@gmail.com
性別 *
男
女
備註
上一步
加入購物車
結帳
服務條款 | 隱私政策 | 常見問題 | 退款須知 | 客服信箱
© All rights Reserved Taiwan CarU

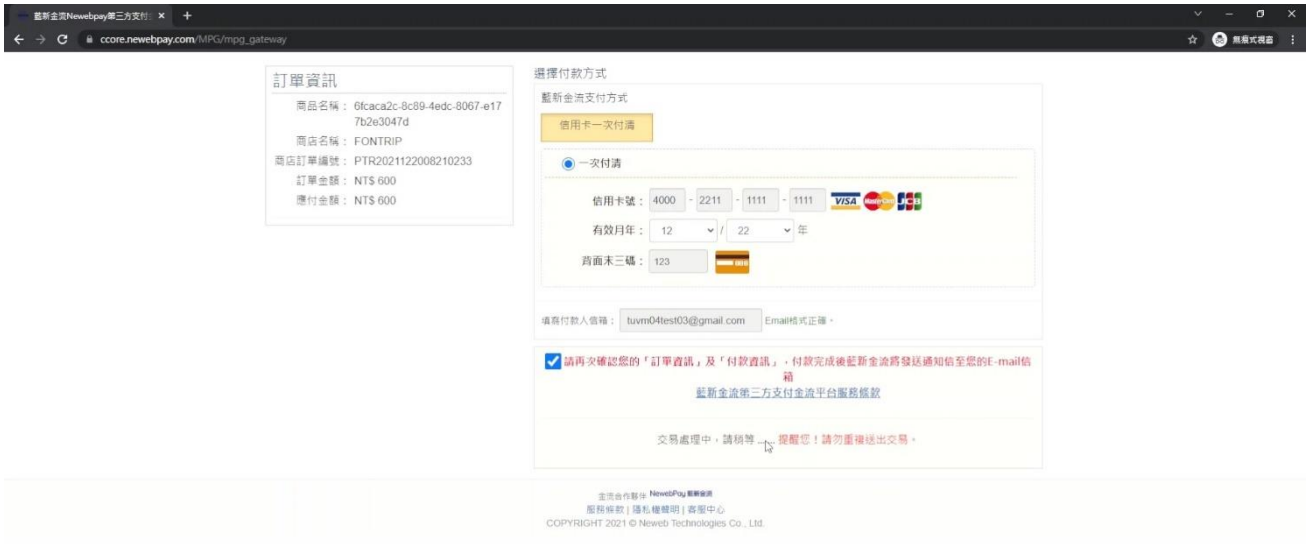
A-15-06


test-caru.welcometw.com/payment
CarÜ
訂單總額
NT$ 600
付款方式
信用卡
定型化契約
Taiwan CarU 定型化契約
我已閱讀，並同意契約內容
返回前頁繼續選購
付款
服務條款 | 隱私政策 | 常見問題 | 退款須知 | 客服信箱

A-15-07


ccore.newebpay.com/MPG/mpg_gateway
訂單資訊
商品名稱： 6fcaca2c-8c89-4edc-8067-e177b2e3047d
商店名稱： FONTRIP
商店訂單編號： PTR2021122008210233
訂單金額： NT$ 600
應付金額： NT$ 600
選擇付款方式
藍新金流支付方式
信用卡一次付清
一次付清
信用卡號：
有效月年：
選擇
年
背面末三碼：
填寫付款人信箱：
xxx@xxx.xxx
請填寫電子信箱。
請再次確認您的「訂單資訊」及「付款資訊」，付款完成後藍新金流將發送通知信至您的E-mail信箱
藍新金流第三方支付金流平台服務條款
已閱讀並同意服務條款，確認送出
服務條款 | 隱私權聲明 | 客服中心
COPYRIGHT 2021 © Neweb Technologies Co., Ltd.

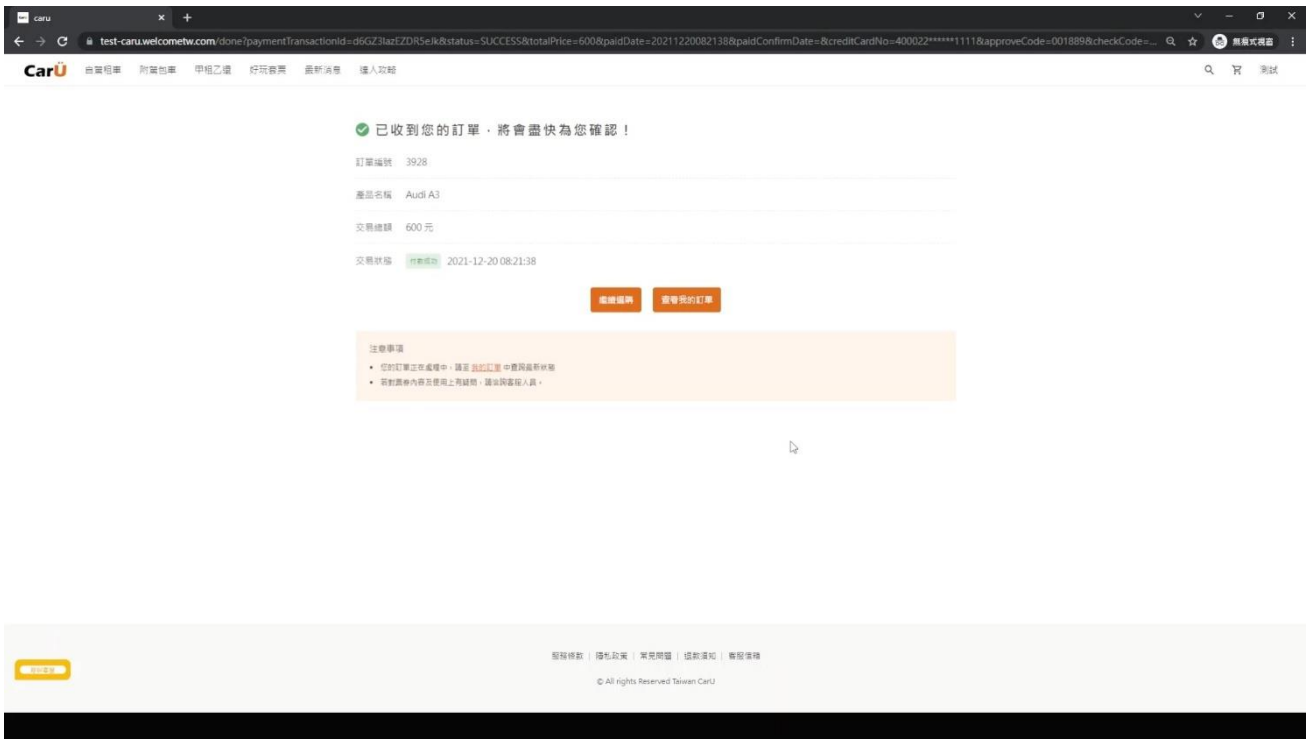
A-15-08


ccore.newebpay.com/MPG/mpg_gateway
訂單資訊
商品名稱： 6fcaca2c-8c89-4edc-8067-e177b2e3047d
商店名稱： FONTRIP
商店訂單編號： PTR2021122008210233
訂單金額： NT$ 600
應付金額： NT$ 600
選擇付款方式
藍新金流支付方式
信用卡一次付清
一次付清
信用卡號： 4000 - 2211 - 1111 - 1111
有效月年： 12 / 22 年
背面末三碼： 123
填寫付款人信箱： tuvm04test03@gmail.com
Email格式正確。
請再次確認您的「訂單資訊」及「付款資訊」，付款完成後藍新金流將發送通知信至您的E-mail信箱
藍新金流第三方支付金流平台服務條款
交易處理中，請稍等...
提醒您！請勿重複送出交易。
服務條款 | 隱私權聲明 | 客服中心
COPYRIGHT 2021 © Neweb Technologies Co., Ltd.

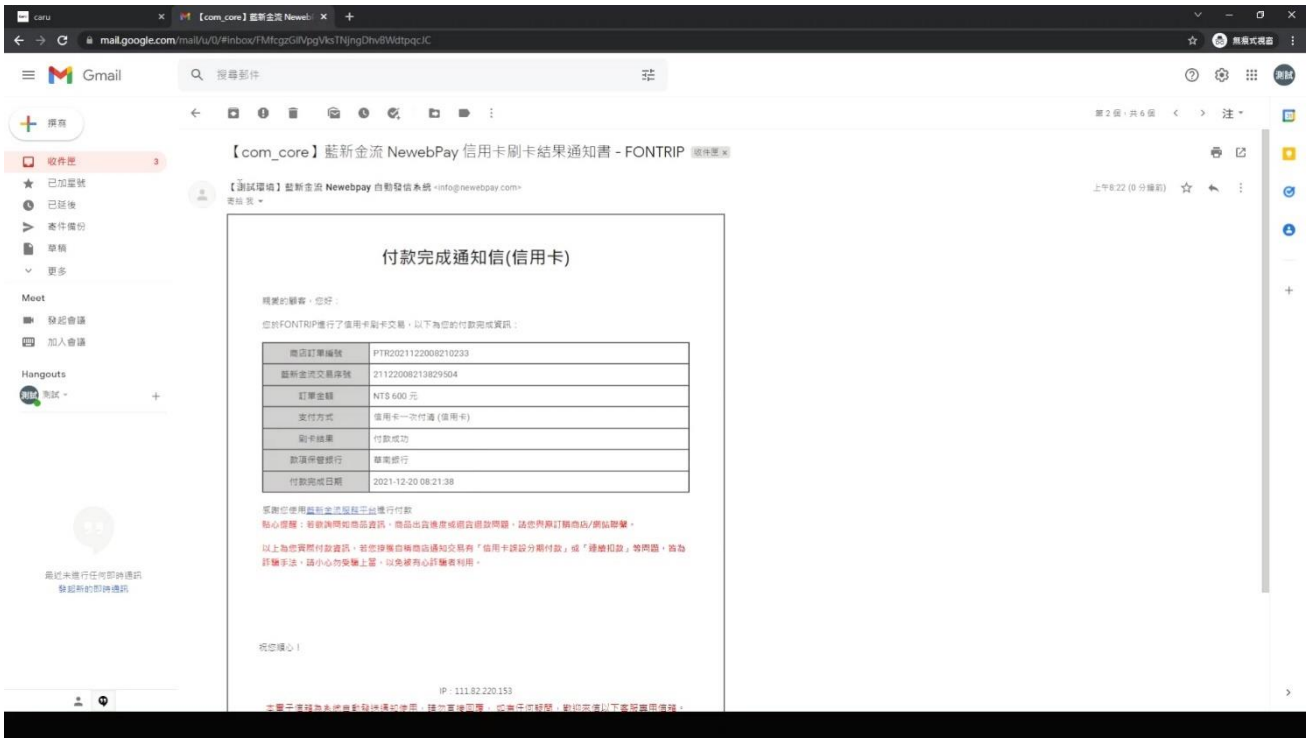
A-15-09

ccore.newebpay.com/MPG/mpg_gateway/payment_info_submit
NewebPay 藍新金流
頁面轉跳中，請稍候...

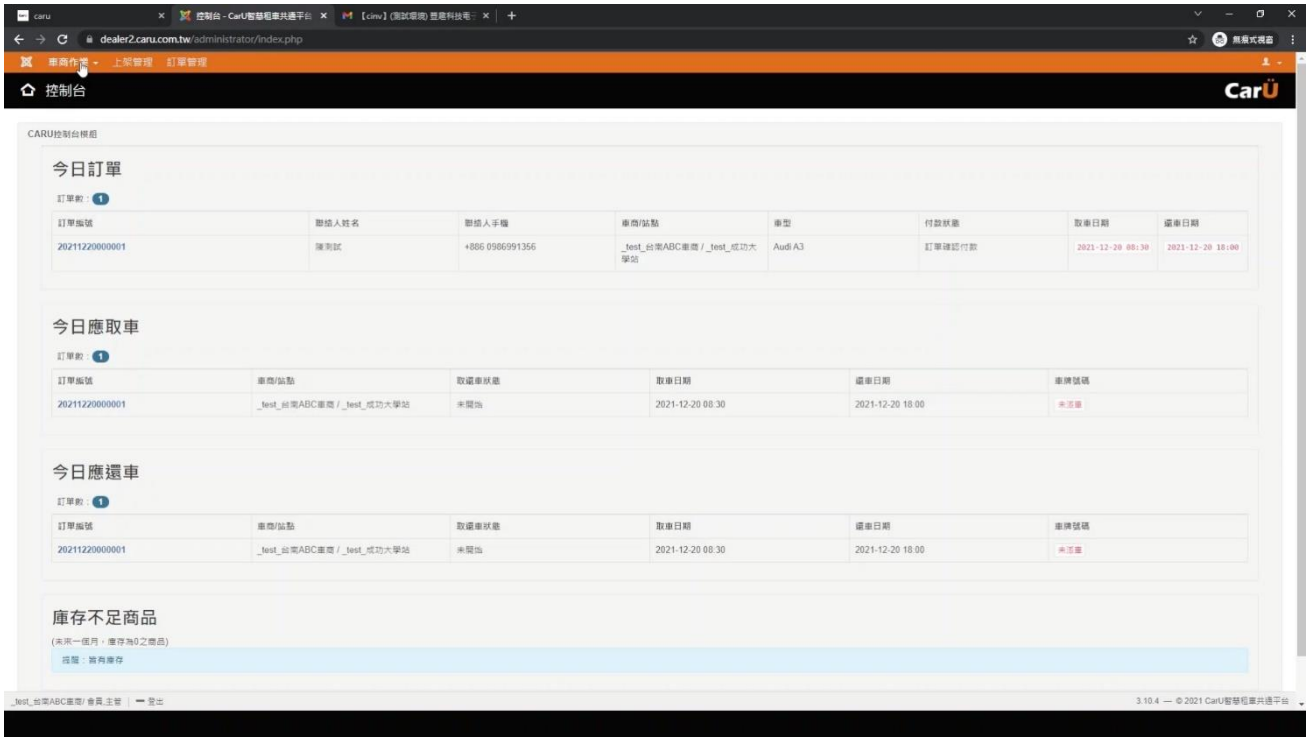
A-15-10


test-caru.welcometw.com/done?paymentTransactionId=d6GZ3lazEZDR5eJk&status=SUCCESS&totalPrice=600&paidDate=20211220082138&paidConfirmDate=&creditCardNo=400022******1111&approveCode=001889&checkCode=...
CarU
已收到您的訂單，將會盡快為您確認！
訂單編號 3928
產品名稱 Audi A3
交易總額 600 元
交易狀態 2021-12-20 08:21:38
繼續選購
查看我的訂單
注意事項
© All rights Reserved Taiwan CarU

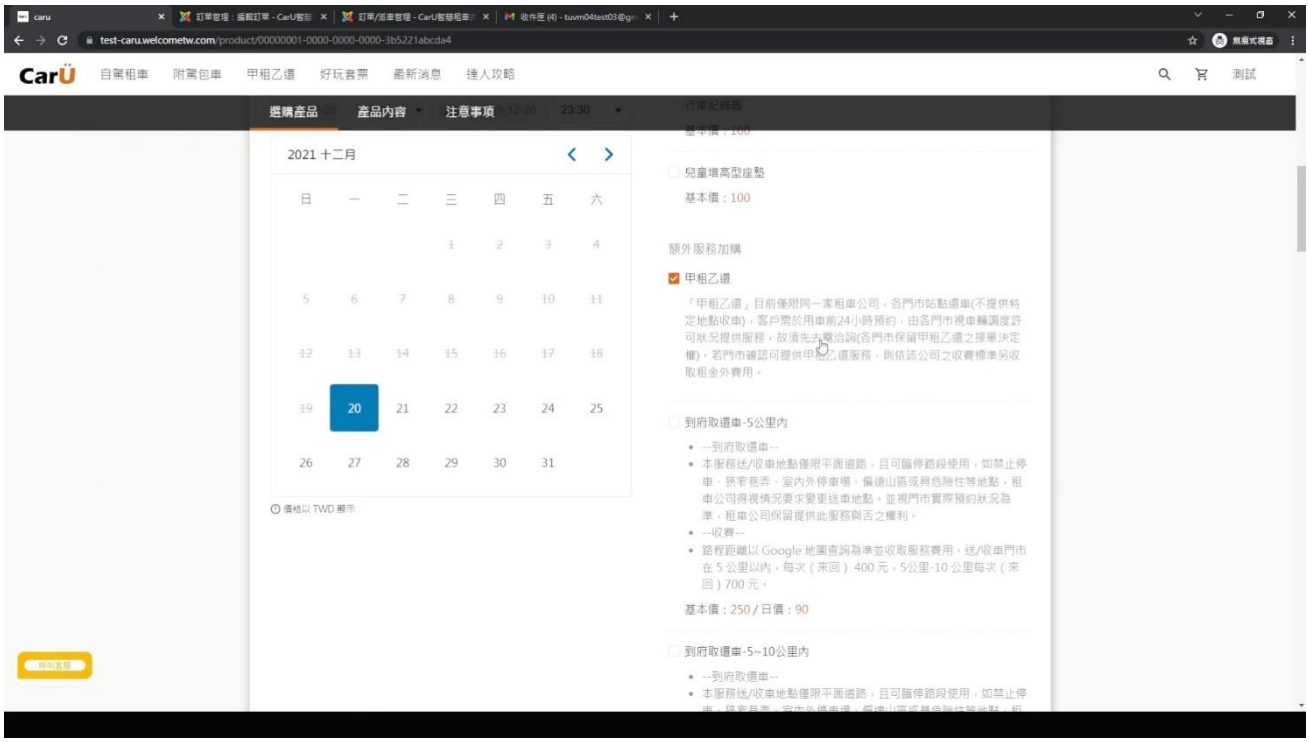
A-15-11


【com_core】藍新金流 NewebPay 信用卡刷卡結果通知書 - FONTRIP
付款完成通知信(信用卡)

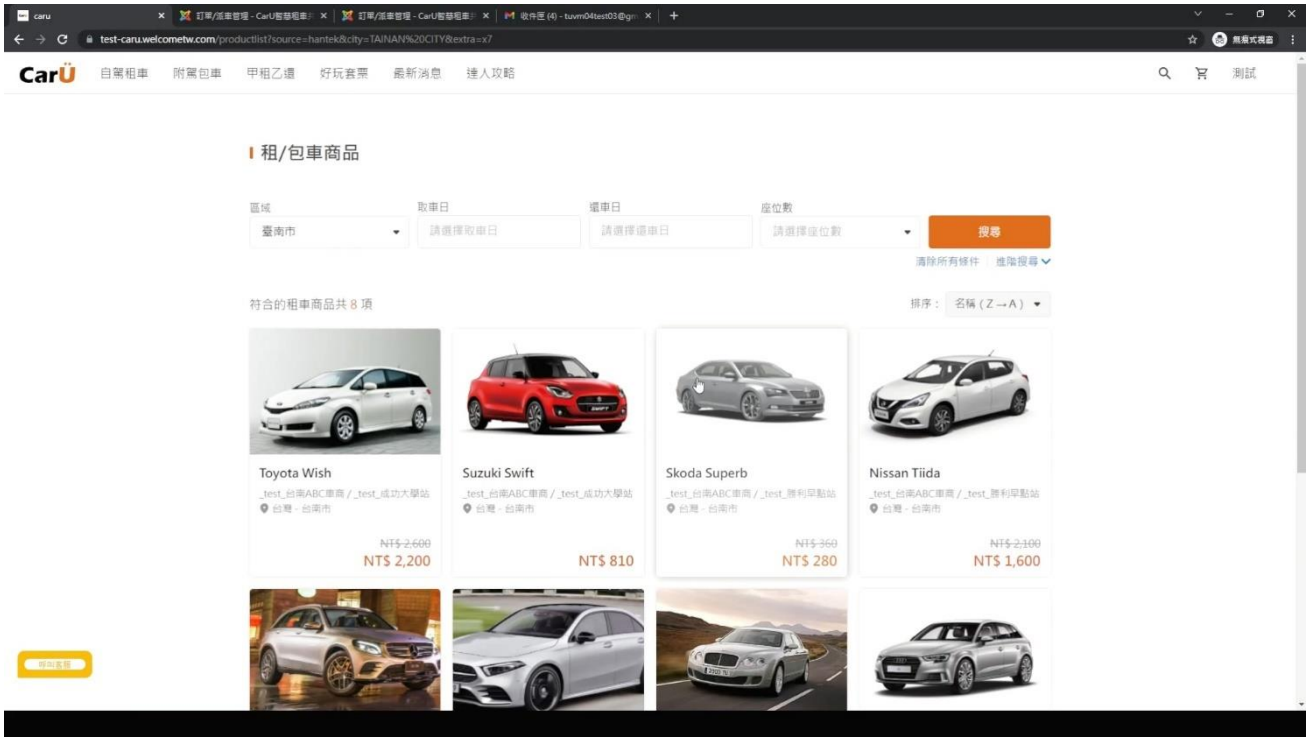
A-15-12


控制台
今日訂單
今日應取車
今日應還車
庫存不足商品

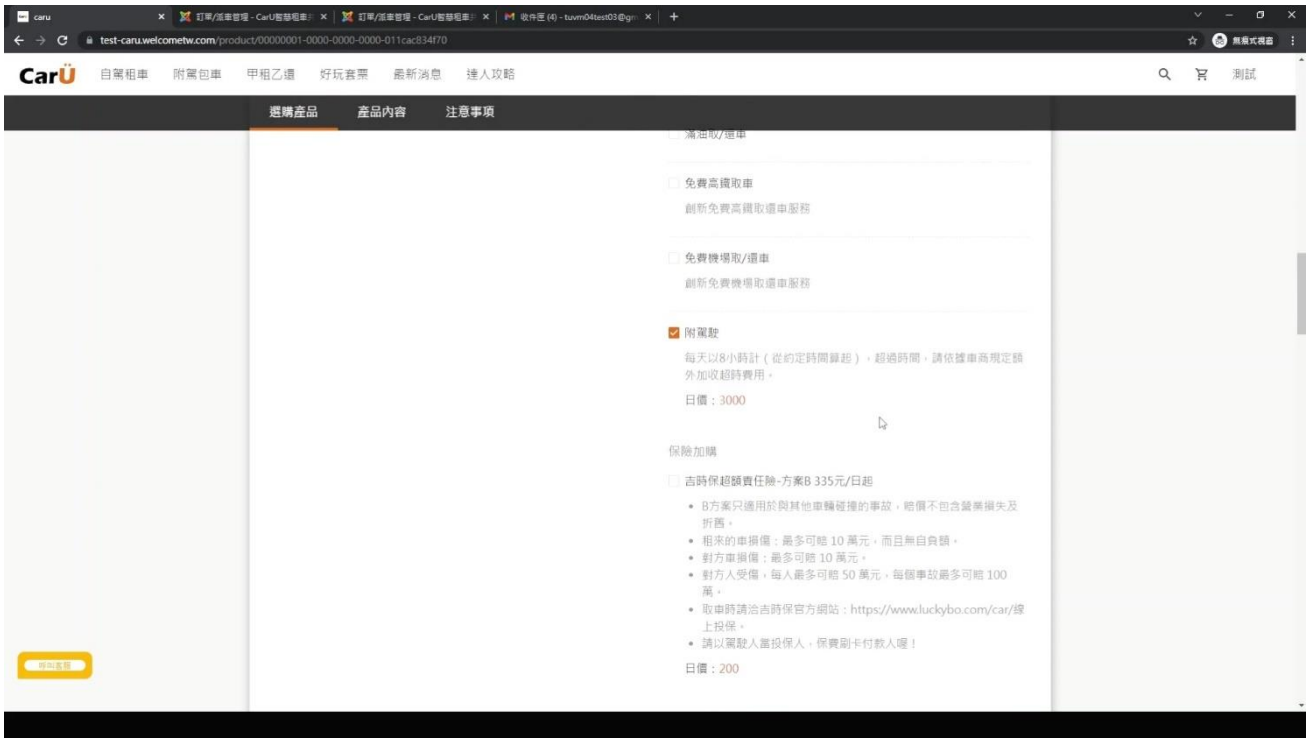
A-16-01


test-caru.welcometw.com/product/00000001-0000-0000-0000-3b5221abcda4
CarÜ
自駕租車
附駕包車
甲租乙還
好玩套票
最新消息
達人攻略
測試
選購產品
產品內容
注意事項
2021 十二月
日 一 二 三 四 五 六
20
價格以 TWD 顯示
兒童增高型座墊
基本價：100
額外服務加購
甲租乙還
「甲租乙還」目前僅限同一家租車公司，各門市站點還車(不提供特定地點收車)，客戶需於用車前24小時預約，由各門市視車輛調度許可狀況提供服務，故須先洽詢(各門市保留甲租乙還之接單決定權)，若門市確認可提供甲租乙還服務，則依該公司之收費標準另收取租金外費用。
到府取還車-5公里內
--到府取還車--
本服務送/收車地點僅限平面道路，且可臨停路段使用，如禁止停車、狹窄巷弄、室內外停車場、偏遠山區或具危險性等地點，租車公司得視情況要求變更送車地點，並視門市實際預約狀況為準，租車公司保留提供此服務與否之權利。
--收費--
路程距離以 Google 地圖查詢為準並收取服務費用，送/收車門市在 5 公里以內，每次（來回）400 元，5公里-10 公里每次（來回）700 元。
基本價：250 / 日價：90
到府取還車-5~10公里內
--到府取還車--
本服務送/收車地點僅限平面道路，且可臨停路段使用，如禁止停

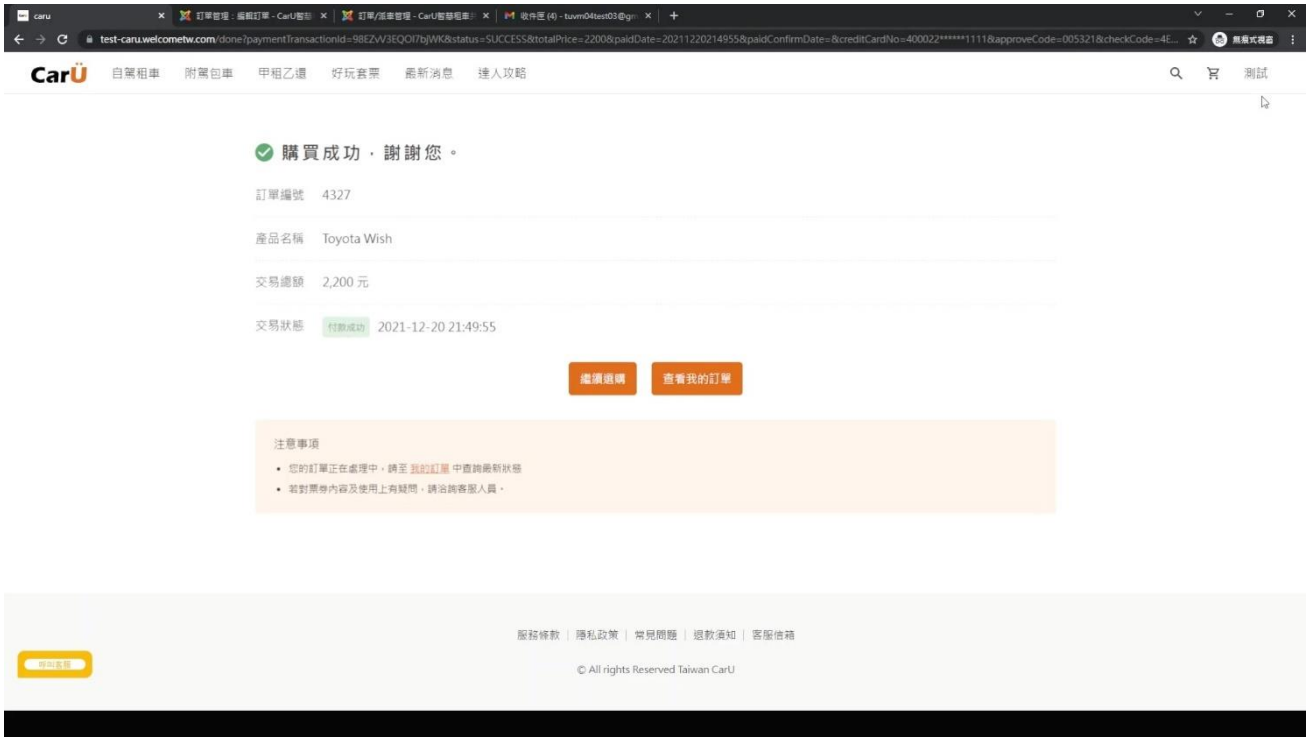
A-17-01


test-caru.welcometw.com/productlist?source=hantek&city=TAINAN%20CITY&extra=x7
CarÜ
自駕租車
附駕包車
甲租乙還
好玩套票
最新消息
達人攻略
測試
租/包車商品
區域
臺南市
取車日
還車日
座位數
搜尋
清除所有條件
進階搜尋
符合的租車商品共 8 項
排序：
名稱（Z→A）
Toyota Wish
_test_台南ABC車商 / _test_成功大學站
台灣 - 台南市
NT$ 2,600
NT$ 2,200
Suzuki Swift
_test_台南ABC車商 / _test_成功大學站
台灣 - 台南市
NT$ 810
Skoda Superb
_test_台南ABC車商 / _test_勝利早點站
台灣 - 台南市
NT$ 360
NT$ 280
Nissan Tiida
_test_台南ABC車商 / _test_勝利早點站
台灣 - 台南市
NT$ 2,100
NT$ 1,600

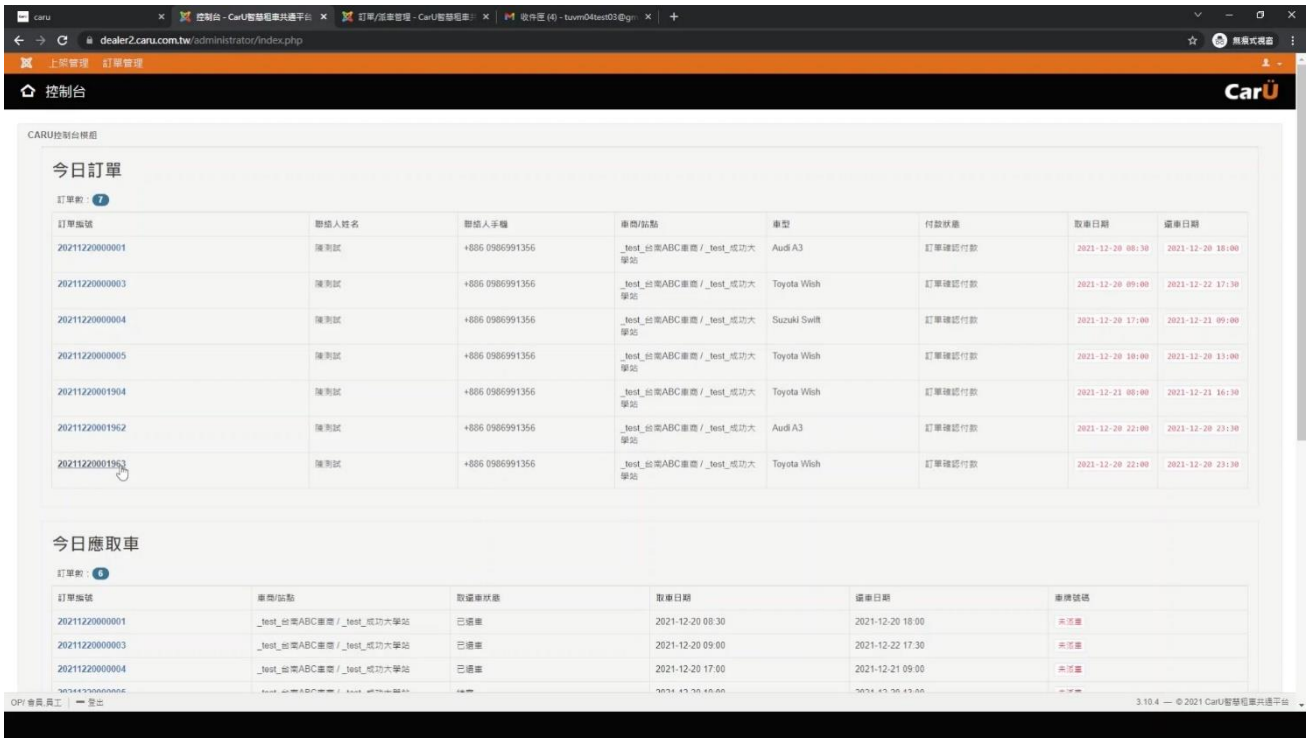
A-17-02


test-caru.welcometw.com/product/00000001-0000-0000-0000-011cac834f70
CarÜ
自駕租車
附駕包車
甲租乙還
好玩套票
最新消息
達人攻略
測試
選購產品
產品內容
注意事項
免費高鐵取車
創新免費高鐵取還車服務
免費機場取/還車
創新免費機場取還車服務
附駕駛
每天以8小時計（從約定時間算起），超過時間，請依據車商規定額外加收超時費用。
日價：3000
保險加購
吉時保超額責任險-方案B 335元/日起
B方案只適用於與其他車輛碰撞的事故，賠償不包含營業損失及折舊。
租來的車損傷：最多可賠 10 萬元，而且無自負額。
對方車損傷：最多可賠 10 萬元。
對方人受傷，每人最多可賠 50 萬元，每個事故最多可賠 100 萬。
取車時請洽吉時保官方網站：https://www.luckybo.com/car/線上投保。
請以駕駛人當投保人，保費刷卡付款人喔！
日價：200

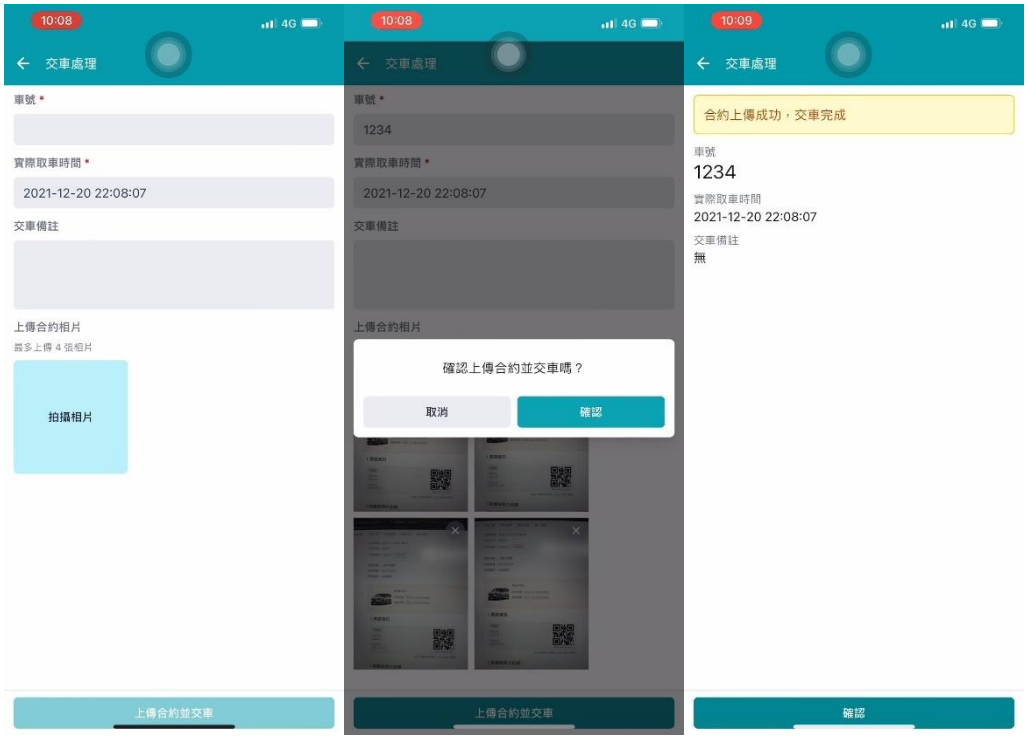
A-18-01


test-caru.welcometw.com/done?paymentTransactionId=98EZW3EQOI7bjWK&status=SUCCESS&totalPrice=2200&paidDate=20211220214955&paidConfirmDate=&creditCardNo=400022******1111&approveCode=005321&checkCode=4E...
CarÜ
自駕租車
附駕包車
甲租乙還
好玩套票
最新消息
達人攻略
測試
購買成功，謝謝您。
訂單編號 4327
產品名稱 Toyota Wish
交易總額 2,200 元
交易狀態 付款成功 2021-12-20 21:49:55
繼續選購
查看我的訂單
注意事項
您的訂單正在處理中，請至 我的訂單 中查詢最新狀態
若對票券內容及使用上有疑問，請洽詢客服人員。
服務條款 | 隱私政策 | 常見問題 | 退款須知 | 客服信箱
© All rights Reserved Taiwan CarU

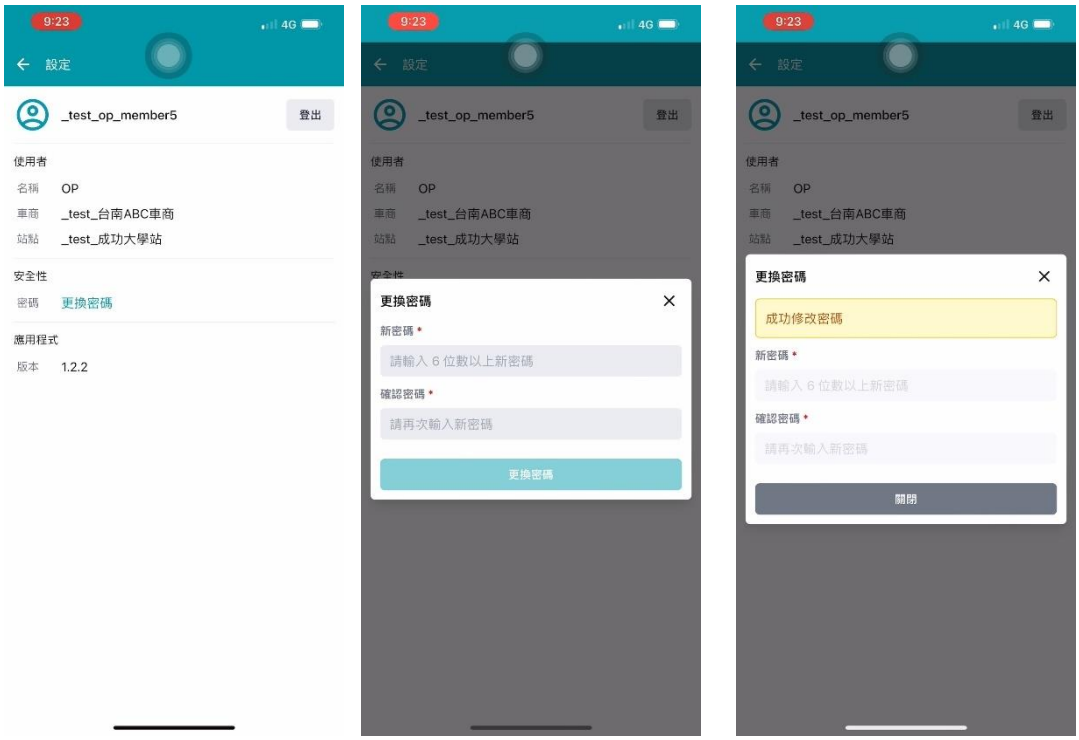
A-18-02


dealer2.caru.com.tw/administrator/index.php
控制台
CarU
CARU控制台模組
今日訂單
訂單數：7
今日應取車
訂單數：6

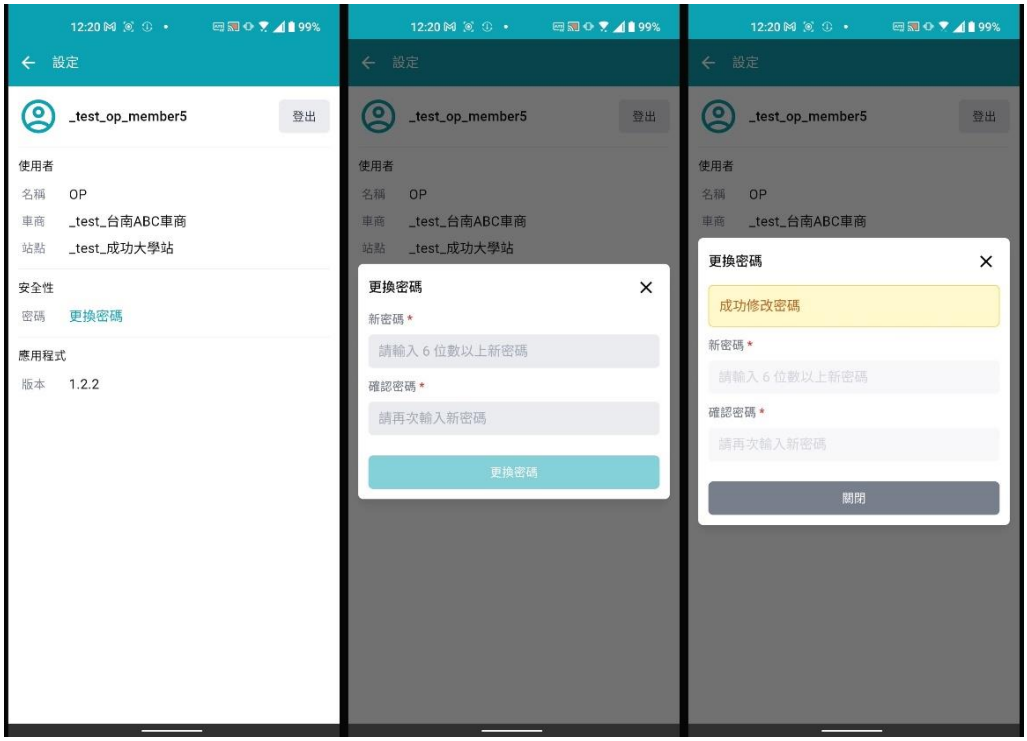
A-44-01


10:08
交車處理
車號 *
實際取車時間 *
2021-12-20 22:08:07
交車備註
上傳合約相片
最多上傳 4 張相片
拍攝相片
上傳合約並交車
1234
確認上傳合約並交車嗎？
取消
確認
10:09
合約上傳成功，交車完成
車號
1234
實際取車時間
2021-12-20 22:08:07
交車備註
無
確認

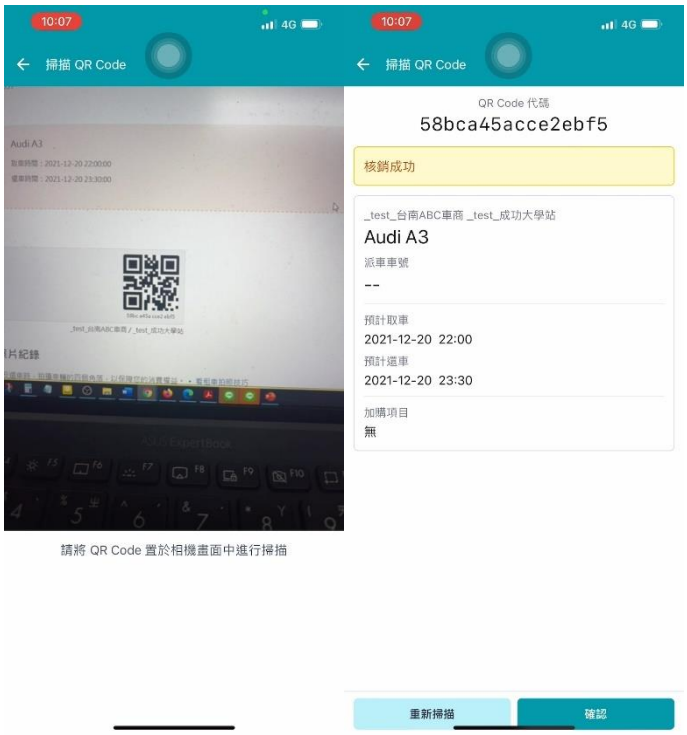
A-45-01


9:23
4G
設定
_test_op_member5
登出
使用者
名稱 OP
車商 _test_台南ABC車商
站點 _test_成功大學站
安全性
密碼 更換密碼
應用程式
版本 1.2.2
更換密碼
新密碼 *
請輸入 6 位數以上新密碼
確認密碼 *
請再次輸入新密碼
更換密碼
成功修改密碼
關閉

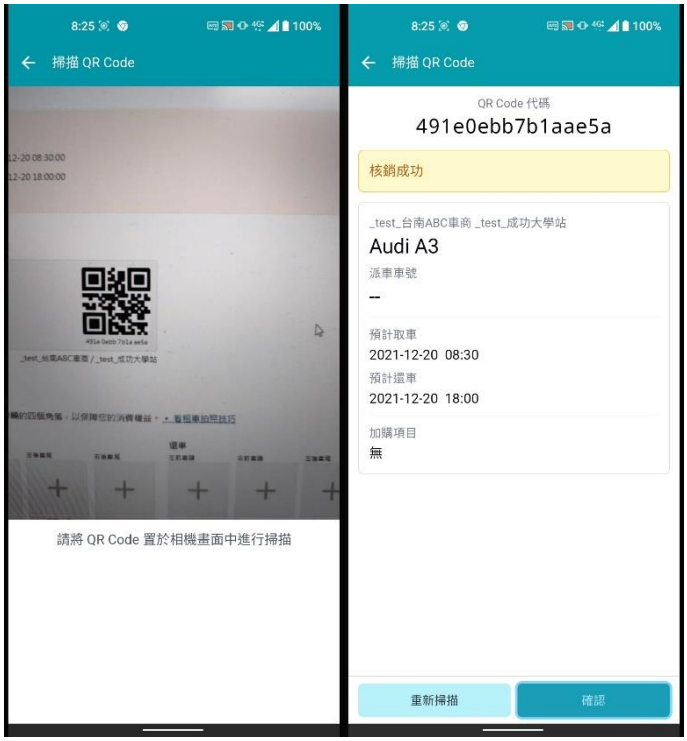
A-45-02


12:20
99%
設定
_test_op_member5
登出
使用者
名稱 OP
車商 _test_台南ABC車商
站點 _test_成功大學站
安全性
密碼 更換密碼
應用程式
版本 1.2.2
更換密碼
新密碼 *
請輸入 6 位數以上新密碼
確認密碼 *
請再次輸入新密碼
更換密碼
成功修改密碼
關閉

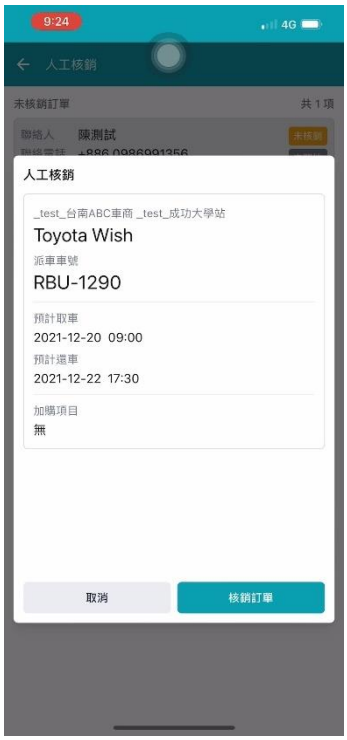
A-46-01


10:07
4G
掃描 QR Code
請將 QR Code 置於相機畫面中進行掃描
10:07
4G
掃描 QR Code
QR Code 代碼
58bca45acce2ebf5
核銷成功
_test_台南ABC車商 _test_成功大學站
Audi A3
派車車號
--
預計取車
2021-12-20 22:00
預計還車
2021-12-20 23:30
加購項目
無
重新掃描
確認

A-46-02


8:25
100%
掃描 QR Code
請將 QR Code 置於相機畫面中進行掃描
8:25
100%
掃描 QR Code
QR Code 代碼
491e0ebb7b1aae5a
核銷成功
_test_台南ABC車商 _test_成功大學站
Audi A3
派車車號
--
預計取車
2021-12-20 08:30
預計還車
2021-12-20 18:00
加購項目
無
重新掃描
確認

A-47-01


9:24
4G
人工核銷
未核銷訂單
共 1 項
聯絡人
陳測試
未核銷
人工核銷
_test_台南ABC車商 _test_成功大學站
Toyota Wish
派車車號
RBU-1290
預計取車
2021-12-20 09:00
預計還車
2021-12-22 17:30
加購項目
無
取消
核銷訂單

9:24
4G
人工核銷
核銷成功
_test_台南ABC車商 _test_成功大學站
Toyota Wish
派車車號
RBU-1290
預計取車
2021-12-20 09:00
預計還車
2021-12-22 17:30
加購項目
無
返回人工核銷
確認

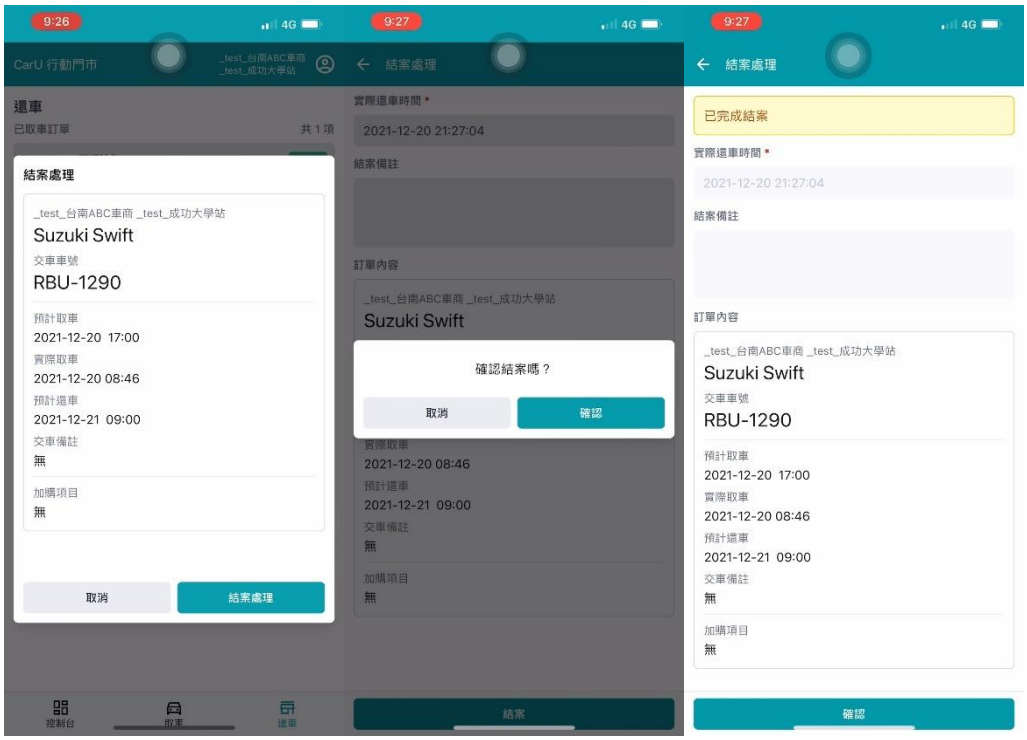
A-48-01

10:08
4G
CarU 行動門市
_test_台南ABC車商
_test_成功大學站
取車
無駕身份驗證
已核銷訂單
共 1 項
交車處理
_test_台南ABC車商 _test_成功大學站
Audi A3
派車車號
--
預計取車
2021-12-20 22:00
預計還車
2021-12-20 23:30
加購項目
無
取消
交車處理
掃描 QR Code 核銷
人工核銷
控制台
取車
還車

10:08
4G
交車處理
車號 *
1234
實際取車時間 *
2021-12-20 22:08:07
交車備註
上傳合約相片
確認上傳合約並交車嗎？
取消
確認
上傳合約並交車

10:09
4G
交車處理
合約上傳成功，交車完成
車號
1234
實際取車時間
2021-12-20 22:08:07
交車備註
無
確認

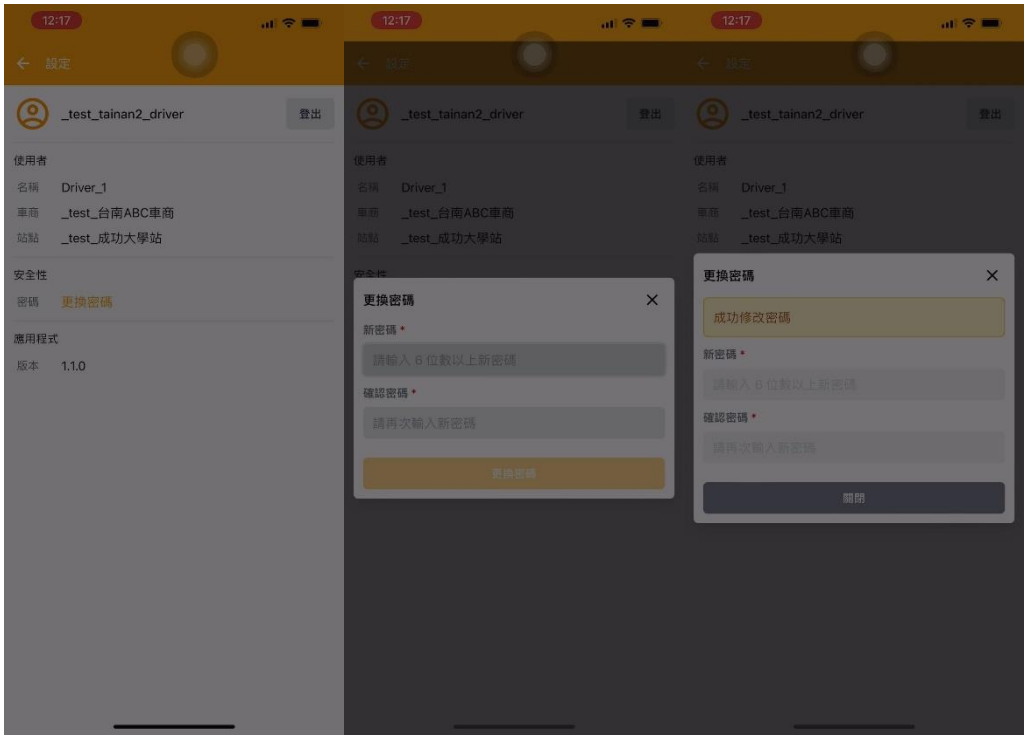
A-49-01


9:26
CarU 行動門市
還車
已取車訂單
共 1 項
結案處理
_test_台南ABC車商 _test_成功大學站
Suzuki Swift
交車車號
RBU-1290
預計取車
2021-12-20 17:00
實際取車
2021-12-20 08:46
預計還車
2021-12-21 09:00
交車備註
無
加購項目
無
取消
結案處理
控制台
取車
還車
9:27
結案處理
實際還車時間 *
2021-12-20 21:27:04
結案備註
訂單內容
_test_台南ABC車商 _test_成功大學站
Suzuki Swift
確認結案嗎？
取消
確認
實際取車
2021-12-20 08:46
預計還車
2021-12-21 09:00
交車備註
無
加購項目
無
結案
9:27
結案處理
已完成結案
實際還車時間 *
2021-12-20 21:27:04
結案備註
訂單內容
_test_台南ABC車商 _test_成功大學站
Suzuki Swift
交車車號
RBU-1290
預計取車
2021-12-20 17:00
實際取車
2021-12-20 08:46
預計還車
2021-12-21 09:00
交車備註
無
加購項目
無
確認

A-51-01

9:23
4G
CarU 行動門市
_test_台南ABC車商
_test_成功大學站
控制台
近日取車
聯絡人 陳測試
聯絡電話 +886 0986991356
派車車號 --
預計取車 2021-12-20 08:30
預計還車 2021-12-20 18:00
已核銷
已還車
聯絡人 陳測試
聯絡電話 +886 0986991356
派車車號 RBU-1290
預計取車 2021-12-20 09:00
預計還車 2021-12-22 17:30
未核銷
未開始
近日還車
聯絡人 陳測試
聯絡電話 +886 0986991356
交車車號 --
預計取車 2021-12-20 10:00
實際取車 2021-12-20 01:11
預計還車 2021-12-20 13:00
已核銷
結案
聯絡人 陳測試
聯絡電話 +886 0986991356
交車車號 ABC-1234
預計取車 2021-12-20 08:30
實際取車 2021-12-20 00:26
已核銷
已還車
控制台
取車
還車

A-54-01

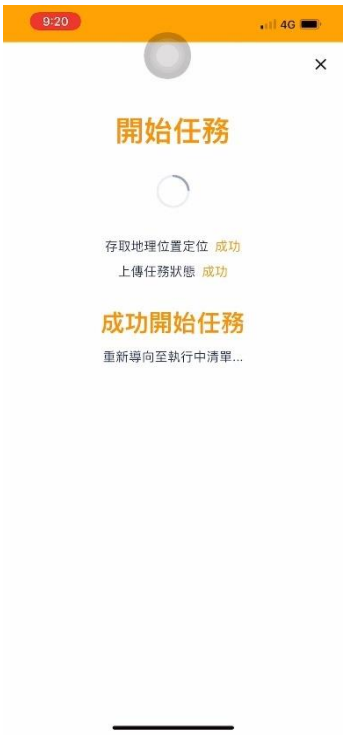

12:17
設定
_test_tainan2_driver
登出
使用者
名稱 Driver_1
車商 _test_台南ABC車商
站點 _test_成功大學站
安全性
密碼 更換密碼
應用程式
版本 1.1.0
更換密碼
新密碼 *
請輸入 6 位數以上新密碼
確認密碼 *
請再次輸入新密碼
成功修改密碼
關閉

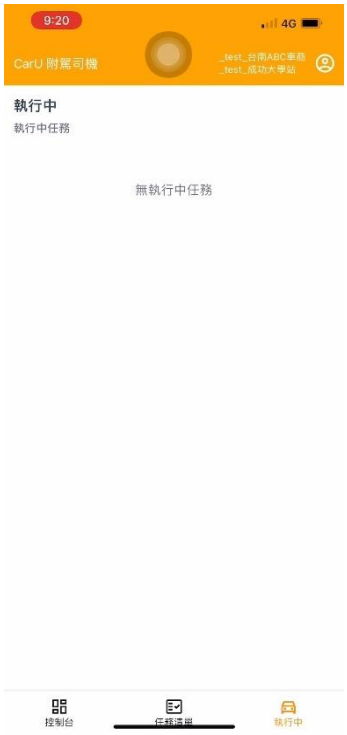
A-55-01

10:44
4G
CarU 附駕司機
_test_台南ABC車廂
_test_成功大學站
控制台
近日任務
無近日任務
控制台
執行中

A-56-01

請將 QR Code 置於相機畫面中進行掃描





A-57-01

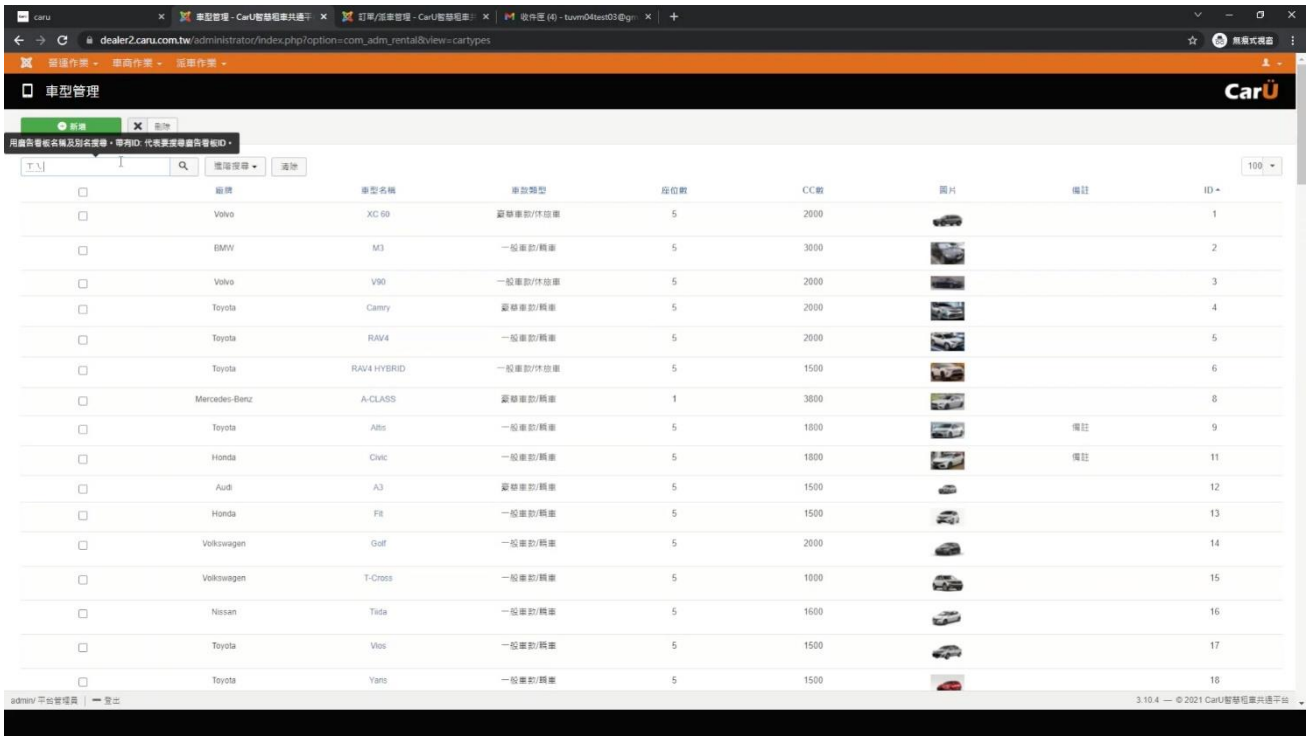
10:27
4G
人工核銷
未核銷任務
共 1 項
聯絡人 陳測試
聯絡電話 +886 0986991356
車號 TTT 9898
取車 2021-12-20 22:00
還車 2021-12-20 23:30
未核銷
未開始

10:27
4G
人工核銷
未核銷任務
共 1 項
聯絡人 陳測試
聯絡電話 +886 0986991356
車號 TTT 9898
人工核銷
_test_台南ABC車商 _test_成功大學站
Mercedes-Benz A-CLASS
車號
TTT 9898
取車時間
2021-12-20 22:00
還車時間
2021-12-20 23:30
加購項目
服務
• 附駕駛
取消
核銷任務

10:27
4G
開始任務
存取地理位置定位 成功
上傳任務狀態 成功
成功開始任務
重新導向至執行中清單...

10:27
4G
CarU 附駕司機
_test_台南ABC車商
_test_成功大學站
執行中
執行中任務
共 1 項
聯絡人 陳測試
聯絡電話 +886 0986991356
車號 TTT 9898
取車 2021-12-20 22:00
還車 2021-12-20 23:30
已核銷
代駕開始
控制台
任務清單
執行中

A-61-01


dealer2.caru.com.tw/administrator/index.php?option=com_adm_rental&view=cartypes
車型管理
CarÜ
新增
刪除
用廣告看板名稱及別名搜尋，帶有ID: 代表要搜尋廣告看板ID。
進階搜尋
清除
100
廠牌 車型名稱 車款類型 座位數 CC數 圖片 備註 ID
Volvo XC 60 豪華車款/休旅車 5 2000 1
BMW M3 一般車款/轎車 5 3000 2
Volvo V90 一般車款/休旅車 5 2000 3
Toyota Camry 豪華車款/轎車 5 2000 4
Toyota RAV4 一般車款/轎車 5 2000 5
Toyota RAV4 HYBRID 一般車款/休旅車 5 1500 6
Mercedes-Benz A-CLASS 豪華車款/轎車 1 3800 8
Toyota Altis 一般車款/轎車 5 1800 備註 9
Honda Civic 一般車款/轎車 5 1800 備註 11
Audi A3 豪華車款/轎車 5 1500 12
Honda Fit 一般車款/轎車 5 1500 13
Volkswagen Golf 一般車款/轎車 5 2000 14
Volkswagen T-Cross 一般車款/轎車 5 1000 15
Nissan Tiida 一般車款/轎車 5 1600 16
Toyota Vios 一般車款/轎車 5 1500 17
Toyota Yaris 一般車款/轎車 5 1500 18
admin/ 平台管理員 登出
3.10.4 — © 2021 CarÜ智慧租車共通平台

附件七 期末審查簡報

01. 計畫背景

小客車租賃業數位轉型發展計畫
商業模式設計與數位轉型推動實務之
專案管理及監督審驗(1/2)

期末報告審查簡報

報告單位： 逢甲大學

報 告 人 ： 黃啟倡 計畫主持人

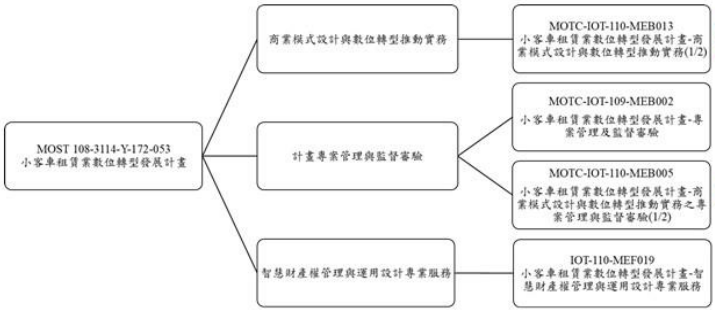
01. 計畫背景

計畫緣起

- 為**積極輔導小客車租賃業數位轉型**，**發展符合臺灣適地性之「智慧租車平台服務」大型建置專案**，藉由新科技與智慧化服務的導入，強化整體交通行動服務網絡以及提升國內小客車租賃相關產業衍生產值，增加產業競爭力，提供民眾優質服務體驗。
- 為使上述平台能有效推廣與執行，**透過第三方專案管理團隊進行計畫品質監督與審驗，以系統測試、文件審查及多面相的專業技術諮詢提升計畫的執行品質與降低風險**。

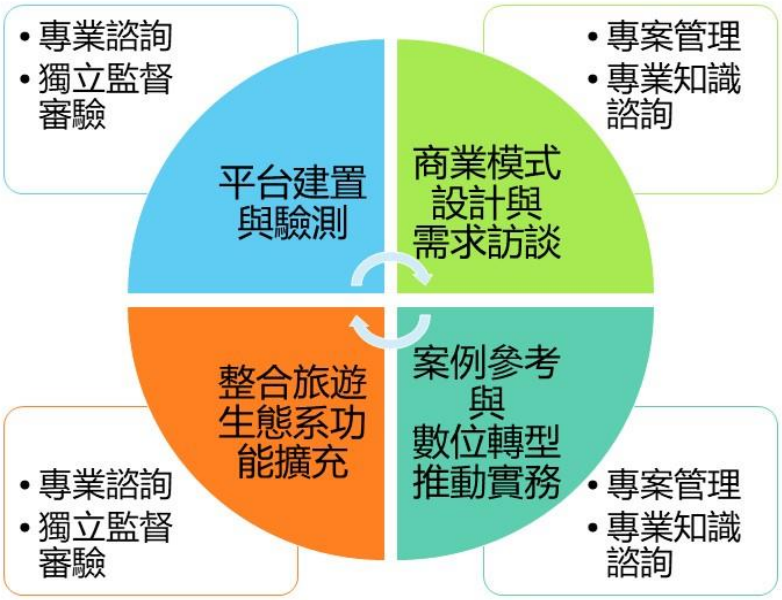
計畫目標

- 為**確保「小客車租賃業數位轉型發展計畫(1/1)」**系統規劃建置、技術發展、服務推廣、營運模式、策略研擬等之完善，並**有效掌握成果品質，符合專案設定服務水準**，而辦理本計畫之**「專案管理」及「獨立驗證與認證」**工作。
- 以協助主計畫，達成專案管理品質之提升、品質之監控查核、審查作業效率提高，及確保系統建置、產品服務推廣得以符合需求且具永續性



5

本計畫與主計畫之關係



6

計畫工作內容

1.專案管理服務

- 追蹤管控數位轉型推動計畫執行過程之相關問題與議題。
- 協助辦理「商業模式設計與數位轉型推動實務(1/2)」計畫之採購、期中、期末審查、經費支用查核等作業。
- 協助督導辦理與彙整「小客車租賃業數位轉型發展計畫(1/1)」期末報告。
- 簽約日起30日內，提出「商業模式設計與數位轉型推動實務(1/2)」之風險控管計畫，逐月滾動檢討R2與R3之風險擬定與對應方法。
- 針對「商業模式設計與數位轉型推動實務(1/2)」計畫執行團隊規劃之數位轉型輔導、營運模式及相關策略等，協助審驗並研提建議與評估業者及使用者接受度。

2.專業知識諮詢

- 協助督導**小客車租賃業數位轉型**工作，提供明確工作範疇、里程碑與交付標的、系統分析設計與測試、系統上線與驗收等各階段確認問題與驗證之專業技術諮詢服務。

3.獨立監督審驗

- 針對推動數位轉型之平台，提出系統相關功能測試及API測試計畫，據此執行並詳實記錄測試過程及結果，彙整缺失紀錄、產出測試報告並提出相關建議，以確認系統符合需求，且正常運作。
- 透過協助審查數位轉型推動計畫於執行過程中，依據契約相關文件規範，所交付之各項文件與系統，研提相關審查意見。

7

02. 文獻回顧與分析

智慧租車及營運現況探討

- **小客車租賃業**為**可同時提供車輛租用及駕駛人代駕服務，但是不能執行計程車客運業之相關服務內容**。該業務之計費以時租或日租為主，其租用服務最少時間為一小時。
- 目前國內除了和運租車(iRent)規模較大且完整外，其他業者普遍規模小，且**資訊化程度不足(以紙本作業為大宗)**。
- 據交通部106年小客貨車租賃業營運狀況調查資料顯示，國內**小客貨車租賃業者**計有**1,755家**(157,228輛車)。
  - 短租車**例假日**平均出租率僅**37.5%**
  - **平常日**更**低於30%**
  - 可見車輛的**閒置與空車率過高**，造成營運困境

9

國內外小客車租賃業之營運模式比較

	格上租車	和運租車	gogoout	Expedia	Renatlcars
總部	台灣	台灣	台灣	美國	英國
營運範圍	台灣	台灣	台灣、美國	美國	180個國家
服務模式	租車/包車	租車/包車	租車	租車	租車
付款方式	至租車地繳款/線上付款	線上付款	線上付款	線上付款	線上付款
站點數	約50個	約50個	約9,000個	-	約46,000個
平台特性	獨立運作	獨立運作	租車代理平台	租車代理平台	租車代理平台
合作平台	N/A	N/A	N/A	Trivago、Hotels.com	Booking、agoda

10

智慧租車及營運現況探討

- **結合MaaS讓租賃業者於平台上架車輛**(即提供線上租賃服務)，**讓使用者可以透過平台適時適地選擇適合的業者與車輛**進而達到小客車出租率的提升。
- 智慧型手機普及率幾乎是人手一機的情況下，**資訊系統平台與手機APP在「智慧租車平台系統與應用開發」扮演著重要的角色**。
- 一千多家小客車租賃業者在數位化轉型的過程中，會衍生許多問題與需求，在專案執行上會面臨資源配置的問題、**風險評估與控管**。

11

專案管理及監督審驗

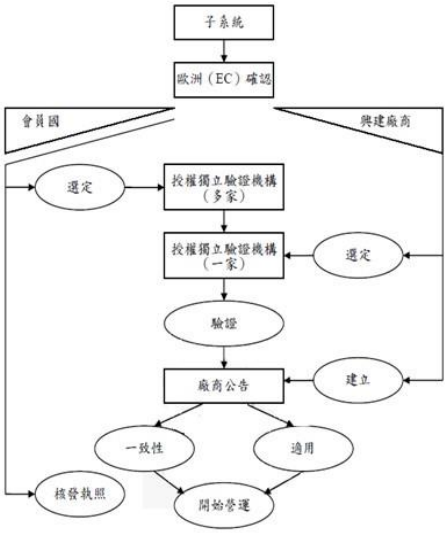
- **獨立驗證與認證**(Independent Verification and Validation, **IV&V**)之基本概念是藉由一個公正獨立的第三方單位或組織，針對一個系統發展的各個階段採用一系列方法與技術進行驗證並對成果進行認證，用以確認系統的品質、安全與功能。
- **IV&V觀念於1970年代首次被提出**，因**美國陸軍發展愛國者反飛彈系統時，為能有效降低軍事開發的高度失敗風險之特性**，於是透過建立計畫、方法、工具、技術發展及驗收準則等，有效提高研發成功率與產品可靠度。
- 發展至今，其觀念與機制已廣泛運用於軟體開發、航太科技與軍事工業上。近年大型基礎公共建設，亦開始導入IV&V機制，確保其可靠性與安全性。
- 一般而言，IV&V執行單位需具備三要件，分別為：技術獨立、管理獨立及財政獨立。

12

獨立驗證與認證案例(1/2)

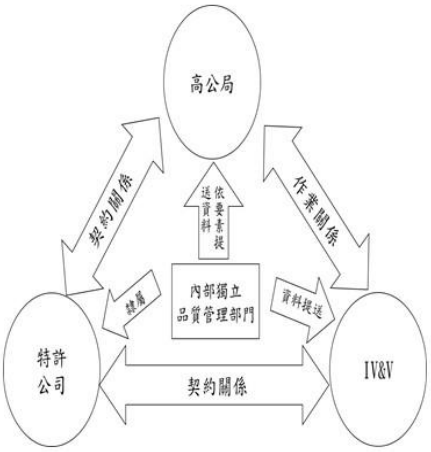
●歐盟15國

驗證高速鐵路系統符合交互運轉技術規範(TSIS)之要求。



●高速公路局

特許公司審查以確保符合契約要求，查核結果再送高公局審查。

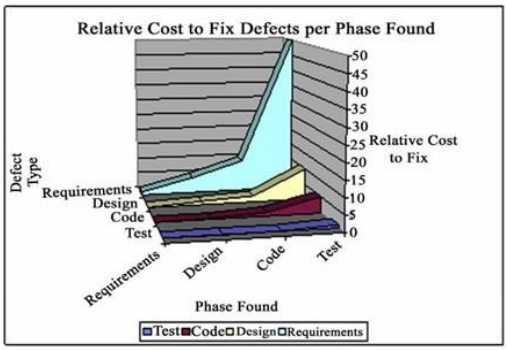


13

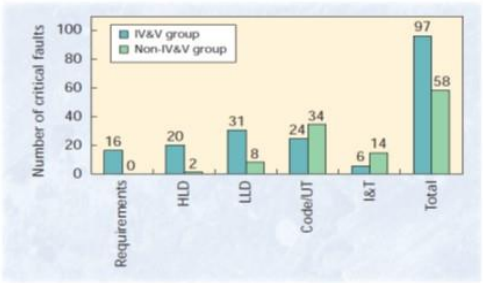
獨立驗證與認證案例(2/2)

●軟體系統開發作用說明

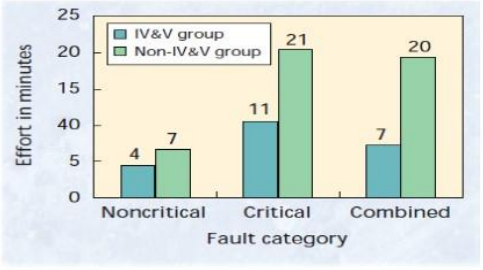
軟體系統平台開發首重於系統的完整性、可靠性及操作環境的友善性，其中導入IV&V之團隊相比未導入之各項差異說明如各圖。



不同開發週期下，軟體系統平台缺陷修正所需的相對成本



軟體系統平台各階段缺陷數量比較



軟體系統平台缺陷改善時間比較

14

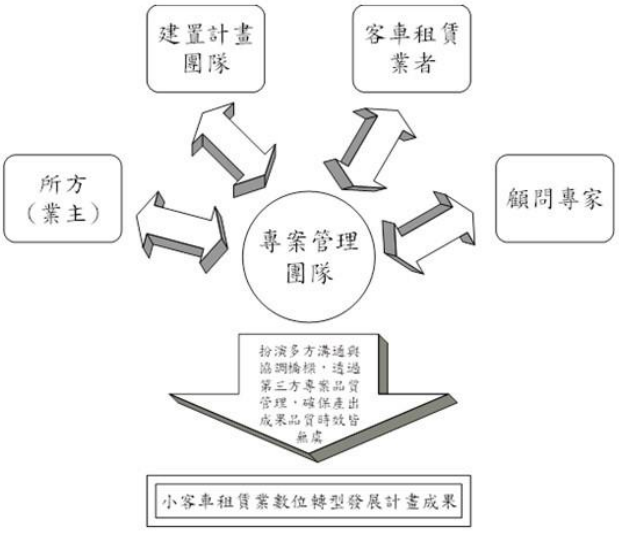
文獻評析(1/2)

- **小客車租賃業以目前國內市場**來說，已呈現**大者恆大**且只有**單一廠商獨佔市場**之局勢，無法顯出良好的商業競爭關係，如何突破窘境，使規模較小之小客車業者也能嶄露頭角，提升整體小客車租賃之使用率，創造更大效益。
- **輔導小客車租賃業數位轉型**，主要以「智慧租車平台服務」讓小規模之小客車租賃業者能夠於平台即時顯示尚可接受承租之車輛，讓使用者透過該平台選擇適合的業者與車輛。
- **IV&V觀念與機制已逐漸被推廣應用於公共建設計畫的管理監督查核**。目前國內政府相關單位逐漸導入IV&V機制，如高公局所管之國道電子收費或交通部運輸研究所推動之MaaS專案，皆為確保專案達如期、如質、如實之優良品質於公共工程之案例。

15

文獻評析(2/2)

- 本團隊做為溝通橋梁，填補多方溝通與協調縫隙，並提高專案溝通之順暢度，再透過第三方專案品質管理，確保產出成果品質、時效符合所方需求之成果。

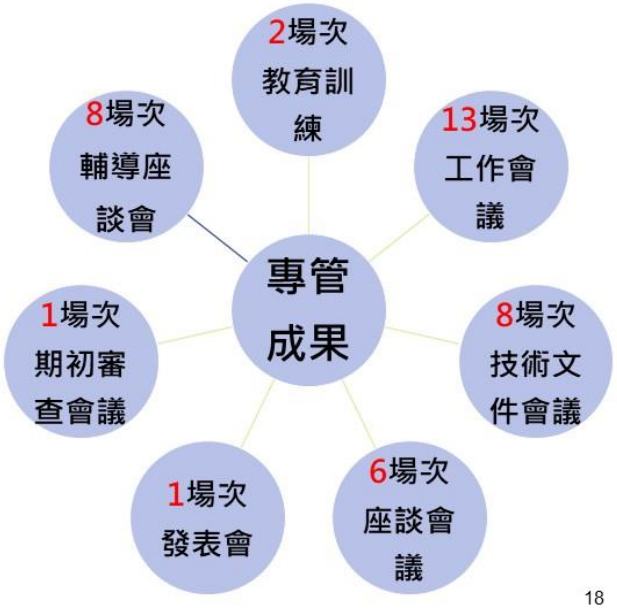


16

3. 專案管理服務

專案進度控管

- **截至12/20，計15項工作任務**
  - 多項工作配合建置商之進度，於期末報告繳交時，持續進行系統測試及驗證，截至12/20已完成所有工作內容。工作進度如期，無延遲。



專案管理平台

- 採用符合專案管理知識體指南（PMBOK® Guide）之 ezteamwork 專案管理平台
- 確保漢名科技各工作項目可如期、如質完成
  - 以下範例：經與所方確認討論後，才延後期初發表會辦理時程

任務名稱	預定開始日期	預定完成日期	實際開始日期	實際完成日期
1 先期作業（簽約日30天內）				
1.1 RFP(二)-1 期初發表會				
1.1.1 會議內容規劃（時間、地點、人員、流程、設備）	2021-04-26	2021-04-29	2021-04-26	2021-08-31
1.1.2 繳交規劃書與IOT確認內容與邀請名單等	2021-05-03	2021-05-10	2021-05-03	2021-08-31
1.1.3 修正期初發表會規劃內容	2021-05-11	2021-05-19	2021-05-11	2021-08-31
1.1.4 重新提交予IOT	2021-05-21	2021-05-24	2021-05-21	2021-08-31
1.1.5 IOT內部簽呈報部及會議討論	2021-05-25	2021-06-04	2021-05-25	2021-08-31
1.1.6 計畫說明簡報製做	2021-08-02	2021-08-20	2021-08-02	2021-08-31
1.1.7 IOT內部流程（含中間意見修改）	2021-08-09	2021-08-31	2021-08-09	2021-08-31
1.1.8 發表會資料準備	2021-08-23	2021-09-20	2021-08-23	2021-09-20
1.1.9 發邀請函、出席貴賓邀請	2021-08-31	2021-09-03	2021-08-31	2021-09-03
1.1.10 會議場地、設備、餐盒、防疫措施確認	2021-08-02	2021-08-20	2021-08-02	2021-08-20
1.1.11 場地佈置與召開期初發表會	2021-09-13	2021-09-17	2021-09-13	2021-09-23

19

知識諮詢成果

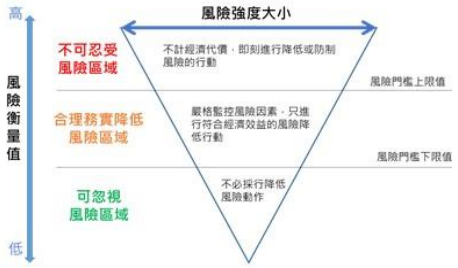
- 針對漢名科技提交之相關文件，研提意見與建議，並追蹤漢名科技辦理狀況與進度

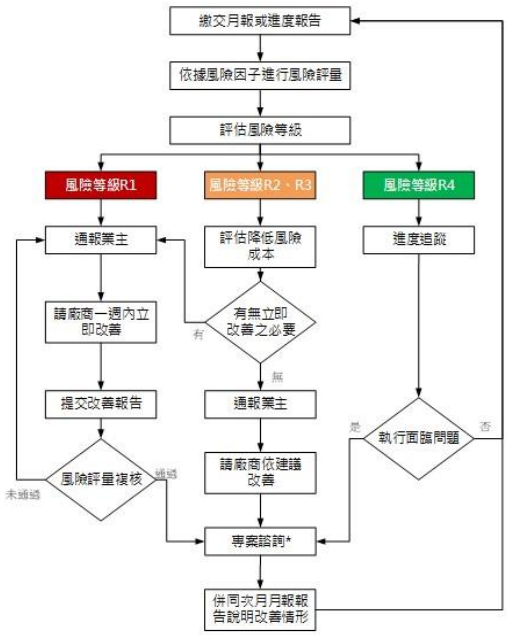
文件	意見數量
服務建議書	10
期初發表會簡報與企劃書	3
小客車租賃業者招募相關文件	28
深度訪談計畫	9
系統建置、測試等相關文件	20

20

各階段風險與管控措施

		頻率/機率(執行進度)				
		>=0%	0%~-5%	-5%~-10%	-10%~-15%	>-15%
重要程度	非常重要	R4	R2	R1	R1	R1
	重要	R4	R3	R2	R1	R1
	普通	R4	R3	R2	R2	R1
	不重要	R4	R3	R3	R2	R2
	非常不重要	R4	R4	R3	R3	R2





21

各階段風險與管控措施

風險類別	風險因子
遴選與競標風險	1. 備標規範缺漏 2. 廠商遴選時程延宕 3. 簽約及議約期程延宕
專案執行風險	1. 未如期交付開發成果 2. 未如實登載計畫執行
系統開發與整合風險	1. 技術轉移失敗及不完全 2. 轉型推廣量能不足 3. 數據資料無法介接 4. 與現存其他機關系統無法整合
財務風險	1. 開發財務不足 2. 擴充或維護財務不足 3. 促銷推廣所需財源無法支應
營運風險	1. 平台數據接收遺失 2. 法源規範不足 3. 業者加入、退出衍生事務及成本
資安風險	1. 硬體或平台受損 2. 資料遭竊取或遭他人使用
其他不可控制風險	1. 其他不可抗力風險

22

各階段風險與管控措施(1)

類別	風險因子	重要程度	發生機率	風險等級
遴選與競標風險	備標規範缺漏	重要	-5%~-10%	R2
	廠商遴選時程延宕	普通	0%~-5%	R3
	簽約及議約期程延宕	普通	0%~-5%	R3
專案執行風險	未如期交付開發成果	普通	-5%~-10%	R2
	未如實登載計畫執行	重要	0%~-5%	R3
系統開發與整合風險	技術轉移失敗及不完全	非常重要	0%~-5%	R2
	轉型推廣量能不足	普通	-5%~-10%	R2
	數據資料無法介接	普通	-5%~-10%	R2
	與現存其他機關系統無法整合	普通	-5%~-10%	R2
	系統儲存、備份或運作量能不足	重要	-5%~-10%	R2
財務風險	開發財務不足	重要	0%~-5%	R3
	促銷推廣所需財源無法支應	普通	0%~-5%	R3

23

各階段風險與管控措施(2)

類別	風險因子	重要程度	發生機率	風險等級
營運風險	平台數據接收遺失	重要	-5%~-10%	R2
	法源規範不足	普通	-10%~-15%	R2
資安風險	硬體或平台受損	重要	-5%~-10%	R2
	資料遭竊取或遭他人使用	重要	-5%~-10%	R2
其他不可抗力風險	其他不可抗力風險	不重要	0%~-5%	R3

24

風險控管—風險控制(1)

- 遴選與競標風險

風險因子	重要程度	發生機率	風險等級	風險控制方法
備標規範缺漏	重要/嚴重 ⬇ 普通	-5%~-10% ⬇ 0%~-5%	R2 ⬇ R3	招標單位依據採購法巨額採購相關辦法，進行廠商特定條件以及規範書審訂，降低重要/嚴重程度及發生機率。
廠商遴選時程延宕	普通	0%~-5% ⬇ >=0%	R3 ⬇ R4	備標過程文件及規範說明，尤以廠商資格條件擬定說明，並於廠商提出疑義時儘快精準回復，降低發生機率。
簽約及議約期程延宕	普通	0%~-5% ⬇ >=0%	R3 ⬇ R4	依採購法相關規定，制定底價或議約條件，且逐項先行擬定說明，降低發生機率。

25

風險控管—風險控制(1)

- 專案執行風險

風險因子	重要程度	發生機率	風險等級	風險控制方法
未如期交付開發成果	普通 ⬇ 不重要	-5%~-10%	R2 ⬇ R3	透過進度報告(月報)確認執行進度，並制定預期罰責，並透過本計畫訂定之風險控制流程(R2)進行追蹤，降低重要/嚴重程度。
未如實登載計畫執行	重要 ⬇ 不重要	0%~-5%	R3 ⬇ R3	透過定期工作會議確認執行內容，並於計畫執行期間審視與追蹤，降低重要/嚴重程度。

26

風險控管—風險控制(3)

- 系統開發與整合風險

風險因子	重要程度	發生機率	風險等級	風險控制方法
技術轉移失敗及不完全	非常重要 ↓ 普通	0%~-5% ↓ 0%~-5%	R2 ↓ R3	• 於簽約後繳交工作執行計畫書並安排審議會議。 • 執行廠商需列出關鍵技術及移轉做法，供審議委員進行檢視。 • 要求每次需求訪談需製作紀錄，並且將會議結論及作法陳報備查。
轉型推廣量能不足	普通	-5%~-10% ↓ 0%~-5%	R2 ↓ R3	• 於簽約後繳交工作執行計畫書並安排審議會議。 • 依據合約規畫推廣家數，分批(比例)進行檢核，並依據檢核點條件，完成後才能逕付款項。
數據資料無法介接	普通 ↓ 不重要	-5%~-10%	R2 ↓ R3	• 進行兩階段測試，第一階段對於試運轉資料進行測試，第二階段進行所有數據資料接受測試，資料完整度須達標準。

27

風險控管—風險控制(4)

- 財務風險

風險因子	重要程度	發生機率	風險等級	風險控制方法
開發財務不足	重要 ↓ 不重要	0%~-5% ↓ >=0%	R3 ↓ R4	• 於定期工作會議時，留意開發進度，若進度落後，可就財務面進行檢視。
促銷推廣所需財源無法支應	普通 ↓ 不重要	0%~-5%	R3 ↓ R3	• 於簽約後繳交工作執行計畫書並安排審議會議。 • 請**廠商擬定促銷推廣所需經費項目及預算，檢視各項經費項目是否妥適**，可透過工作會議方式，於執行前進行討論修正。

28

風險控管—風險控制(5)

- 營運風險

風險因子	重要程度	發生機率	風險等級	風險控制方法
平台數據接收遺失	重要 ↓ 不重要	-5%~-10% ↓ >=0%	R2 ↓ R4	• 請得標廠商提出資料備份機制，以確保數據儲存遺失。 • 亦請廠商於營運期間，每日追蹤資料筆數及內容，若當日出現數據資料落差，應於指定期間完成修復。
法源規範不足	普通 ↓ 不重要	-10%~-15%	R2 ↓ R3	• 請得標廠商就法律或規範面，於期中期間提出研究成果，並列出建議解決辦法。 • 對於受到較低法律位階之規定限制者，可優先討論修改或調整辦法，減少營運過程受到法令或規範限制之項目。

29

風險控管—風險控制(6)

- 資安風險

風險因子	重要程度	發生機率	風險等級	風險控制方法
硬體或平台受損	重要 ↓ 不重要	-5%~-10%	R2 ↓ R3	• 請得標廠商提出資料備份機制，以確保數據儲存遺失。 • 硬體或平台需定期進行檢視或是掃毒作業，並留意作業平台重大安全更新，並進行系統或韌體升級，避免硬體受損或是中毒情形出現，。
資料遭竊取或遭他人使用	重要 ↓ 不重要	-5%~-10%	R2 ↓ R3	• 儲存空間伺服器置放地點應進行人員管制，並定期進行掃毒及漏洞掃瞄作業，確保資料能妥善保存。此外，資料控管應具名，或做帳號管理，以確保資料不被他人使用。

30

風險控管—風險控制(7)

- 其他不可抗力風險

風險因子	重要程度	發生機率	風險等級	風險控制方法
其他不可抗力風險	不重要 ↓ 非常不重要	0%~-5%	R3 ↓ R4	• 於合約期間，訂定因不可抗力因素之條款，例如：因天災因素能夠合理展延，或非歸咎雙方疏失需調整合約之可能。 • 施工或是合約期間之不可抗力之情事，可透過保險方式避險，。

- 風險控管成效
  - 目前漢名科技各項風險因子尚在本計畫掌控之中
  - 為避免漢名科技招募業者數量不足，致轉型推廣量能不足之風險產生，本案於相關工作會議中研提以下招募進度：

檢核日期	9/30	10/15	10/30	11/15	12中旬
契約要求家數	100	-	-	-	628
逢甲建議家數	150	300	450	600	-
漢名實際家數	238	395	-	-	-

31

風險管理實際作為—落實於契約

專責單位、承諾負責

成立專責推動與後續營運團隊

＋

平台經營計畫書

時程與數量控管

辦理產業數位轉型座談會

＋

累計輔導業者數位轉型

＋

產業數位轉型暨平台推廣應用之座談會、說明會、論壇、工作坊

＋

租賃車業者小客車之人車路數據資料

工作月報

契約

降低各風險發生可能

32

實際風險與管控措施

- 邀請「中華民國小客車租賃商業同業公會全國聯合會」列席工作會議，聽取產業端對於該系統的期許及看法，適時納入公會的意見，以使該系統未來能更順利的推廣及使用。
- 但全聯會認為該系統應以前期資策會所建置的平台進行推廣營運即可，無需再額外開發旅遊生態系之平台，應將此經費運用於小客車租賃業者端的推廣上。而開發旅遊生態系平台為契約工作項目，造成全國聯合會對於此計畫不支持，甚至提出「建置商有分化公會之疑慮」
- 致使原計畫KPI須納入600家業者加入此平台，並需有10,000筆人車路數據資料，且提升出租率3%，進度無法順利推廣。

33

實際風險與管控措施

① 請建置商前往拜訪全聯會，進一步磋商取得共識。

② 積極辦理平台推廣說明會，並逐一聯繫業者邀請加入平台。

③ 選擇較積極配合的地區公會、業者，進一步洽談推廣細節。以此將10,000筆人車路數據資料，且提升出租率3%，能夠有效提升。目前選擇臺中公會進行積極推廣。

- 依照上述相關風險管控措施，由**建置商先行與臺中公會洽談相關招募與合作事宜，截至11月26日已有628家小客車租賃業者參與「小客車租賃業數位轉型發展計畫」，並積極請業者協助完成10,000筆人車路數據資料。**
- 另外亦請**建置商多次拜訪全聯會，於商談達成共識後，全聯會表示願意協助與支持建置商完成相關工作項目**，如招募業者加入平台、辦理業者座談會與產業說明會等，並**願意由全聯會輔導業者籌組營運團隊，以及接手後續平台營運業務**。

34

4. 獨立監督審驗

系統測試與驗證

- **漢名科技於7/16提交90天內建置的智慧租車共通平台**
  - 智慧租車共通平台系統相關文件-系統彙整報告附件
  - 團隊進行
    - 實際操作，給予三項修正建議
    - 文件檢視，給予八項修正建議，讓後續文件更臻完善
- **漢名科技於9/14、17提供金流文件與測試用資料**
  - 金流設計規格書、使用手冊
  - 團隊進行
    - 實際操作，給予二項修正建議
    - 文件檢視，給予五項修正建議

編號	逢甲大學意見	漢名科技辦理情形
1	建議使用手冊應考量營運商端、車商端在金流驗證上所需之相關流程，較為完善。 因目前平台並無紀錄單一車商金流總收費，未來可能是由車商自行統計應收金額，若此金額與綠界撥款金額不一致，可能導致收費爭議。 建議應制定相對應的帳務稽核程序，並有文件清楚描述相關的金流統計、撥款統計範圍(例如前月的26~該月的25日)、撥款日以及相關手續費等說明，可放在使用手冊或是營運規章中，以便未來帳務稽核時使用。	1. 後續整體的完整金流會放於旅遊生態系服務平台上，智慧租車共通平台僅提供派車等其他租還車及派遣等業務功能。 2. 後續將補充於整體平台業者加入使用條款中，以利加入之小客車租賃業者遵循。

- 漢名科技於11/15、11/22、12/2提供文件
  - 文件檢視，給予十項修正建議
- 12/1開始正式進行系統測試
  - 功能性測試
    - 測試評估缺失等級說明

等級	標準	測試標準說明	備註
A	重大缺失	功能項目無法運作 嚴重安全性漏洞	測試失敗 系統上線前建議完成修正
B	缺失	功能項與預期不符 安全性漏洞	需立即修正 建議安排適當時機修正
C	錯誤	文字描述易產生誤導，流程操作有高困難度	需改善操作，可安排適當時機修正
D	補強	錯別字、版面異常	可安排適當時機修正

37

平台與車商作業端

項目	成功	失敗	其他	備註
車商管理（平台端）	✓			
營運統計表（平台端）	✓			
站點管理	✓			定位功能誤差大，**評比為 C**。 Icon 使用跟操作內容建議調整，**評比為 D**。
車輛管理	✓			新增車輛的資訊無任何格式檢查，**評比為 C**。 系統操作的回饋資訊建議改善，**評比為 D**。
駕駛管理	✓			站點資料選擇的功能在特定操作下會異常，**評比為 C**。
員工管理	✓			在密碼輸入欄位並非強制欄位，**評比為 B**。
車商價格管理	✓			在編輯功能可以編輯目前表單內沒有的車型，建議釐清後安排修正，**評比為 D**。
站點價格管理			✓	此功能所呈現的資訊跟車商價格管理一樣，看不出其差異。
內附項目管理			✓	進行新增操作會顯示異常，**評比為 B**。
加購項目管理			✓	進行新增操作會顯示異常，**評比為 B**。
上架管理			✓	車輛上架過程中在特定操作下會遇到錯誤，而且操作過程中的系統處理時間很長(數十秒以上)，因此容易讓使用者誤以為系統異常，**評比為 C**。 上架資料不會馬上顯示於 CarU 平台，而且也沒有相關系統回饋資訊可以檢視，如進度查詢、預期上架時間等，建議至少提供一些可檢視進度方式的資料，**評比為 C**。 經團隊反覆測試後，某些情況下，車商上架的車種在 CarU 平台經消費者帳號搜尋比對後，數量會不一致，**評比為 A。(此問題後續反應給漢名後，有得到修正)**。
訂單管理			✓	訂單判斷與顯示邏輯疑似異常，訂單在取消的狀態，同時也列入租用車輛數的計數，**評比為 A**。 訂單的各種操作狀態沒有前後關係的檢查，因此可能會發生奇怪的操作組合導致無法有效的檢視訂單正確性，**評比為 B**。

38

行動門市端

項目	成功	失敗	其他	備註
核銷作業			✓	核銷作業進行時，沒有檢查消費者端的訂單是否是屬於該門市，因為目前的系統架構是每一個門市都一組帳號，導致車商在多個門市之間要如果忘記做帳號切換，或是登入錯誤門市的帳號，就會發生資料流程的議題。**評比為 A。**
交車作業			✓	流程可順利操作完成，不過輸入的「實際交車車號」，並沒有跟管理平台端的派車進行功能整合上的綁定，**評比為 B。**
結案作業	✓			流程可順利操作完成，不過訂單上的結案時間有誤，**評比為 C。**

附駕司機

項目	成功	失敗	其他	備註
開始任務			✓	問題同行動門市端的核銷描述，可以透過司機的帳號進行核銷作業，且核銷對象沒有檢查其合法性與正確性，後續運行時恐衍生諸多問題，**評比為 A。**
結束任務	✓			

39

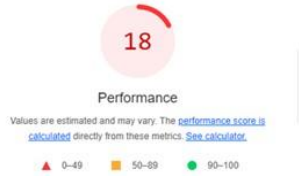
消費者端

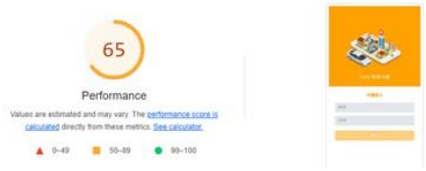
項目	成功	失敗	其他	備註
登入	✓			
車輛搜尋	✓			熱門租車資料較多時，建議限縮或以其他方式提供，以免造成資訊版面的誤用，**評比為 D。**
購物車與購買		✓		購物車資訊於金流交易取消後會不見，呈現購物車為空的狀態，**評比為 B。** 當下如果有使用優惠券，優惠券也會消失，顯示為已使用，**評比為 A。**
金流交易			✓	購物車所帶的金額跟金流所顯示的金額不同，**評比為 A。** 金流頁面取消操作，平台端顯示訂單成立，**評比為 A。** **這兩點於測試當下即回報執行團隊，已完成問題修訂。**
檢視訂單			✓	下訂後結果檢視訂單為付款失敗，但是有收到交易成功資相關訊息，**評比為 A。**這點於測試當下即回報執行團隊，已完成問題修訂。 在使用者端有顯示圖片，不過在管理頁面端是空白的，**評比為 A。** 管理端如果取消訂單，使用者端狀態不會更新，**評比為 B。**
顯示 QRcode	✓			訂單完成後需等待 5 分鐘後才會顯示 QRcode，建議在交易狀態顯示進行調整；或是於訂單流程中進行提醒跟告知，以免造成消費者的誤會，**評比為 C。**

40

系統測試與驗證-PWA檢視

- 實施上沒問題

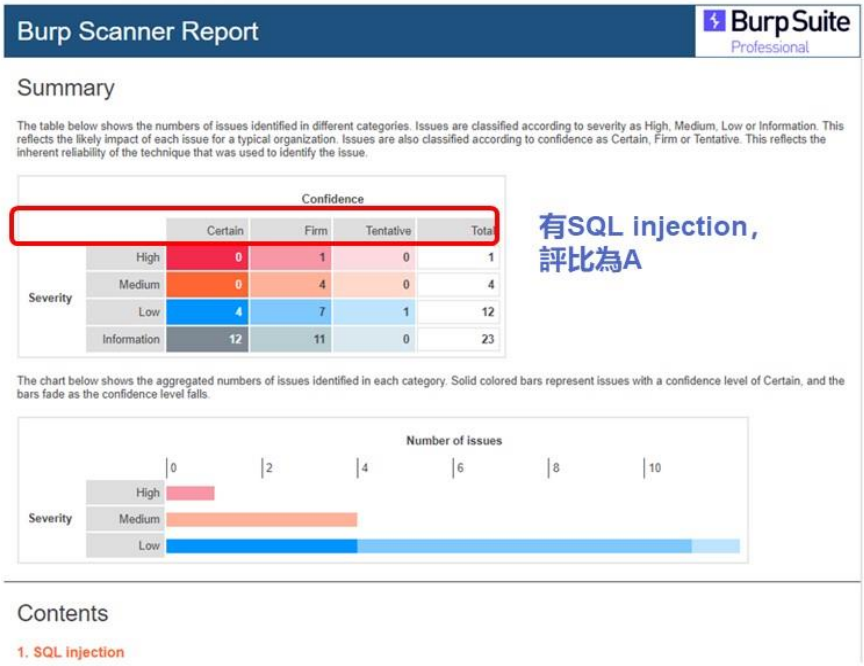




41

系統測試與驗證-資安相關

- 網站弱點掃描



有SQL injection，評比為A

42

系統測試與驗證-資安相關 (續)

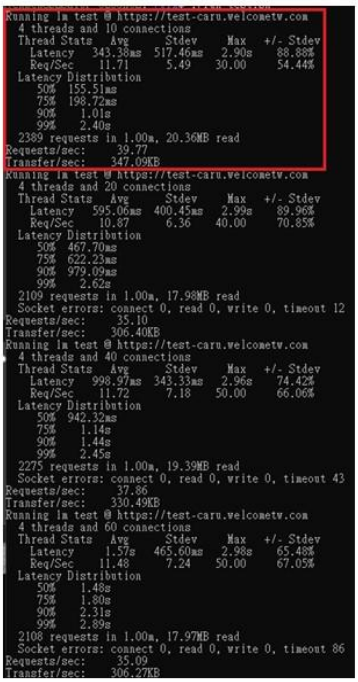
- **SSL憑證**
  - 無明顯問題

- **內部API**
  - API Token未確實進行驗證，隨意輸入即可進行，**評比為A**
  - 新智慧租車平台的相關操作可透過URL更改ID後進行資料檢視跟編輯，**評比為A**

43

系統測試與驗證-壓力測試 (wrk)

- **測試標的**
  - CarU平台、新智慧租車平台、行動門市與附駕司機
- **測試結果**
  - CarU平台服務水準為**每秒同時有20位使用服務的時候，其90%的使用者可在1秒以內可以收到伺服器的回應。**建議未來實際上線運行的時候可以適當增加硬體效能。
  - 其他平台無明顯問題。



44

系統測試與驗證-易用性測試

- **測試時間：**12/1-2、12/6-8
- **受測者：**
- 6位消費者，平均年齡約30歲(最小約24歲，最大約50歲)
- 4位車商，平均年齡約42歲(最小約28歲，最大約60歲)
- **四項測試情境**
  - 情境一：消費者租車(自駕)
  - 情境二：消費者取車(自駕)、門市人員核銷
  - 情境三：消費者租車(附駕)、司機接單執行代駕
  - 情境四：平台管理人員查看訂單狀態、車商主管派車並上架車輛
  - **※消費者主要測試內容為情境一至三，車商為情境四**

45

系統測試與驗證-易用性測試

- **使用性問題嚴重程度分級表**
  - 本表之分級是透過**是否成功/失敗、操作順暢度**來判定，由於考量到同一異常事件對不同使用者的阻擋程度不同，故此為受測者提出他認定的判定結果，並綜合測試人員之觀察所得出最終的數據。

  - 分級標準

等級	程度描述
1級-嚴重程度低	使用者能完成任務
2級-嚴重程度中	完成任務會有困難，有效性、效率皆被影響
3級-嚴重程度高	會導致任務失敗，沒有其他方法能完成任務

46

系統測試與驗證-易用性測試

- 使用性問題嚴重程度分級表
  - 情境一：消費者租車(自駕)

1.填寫時間方式不符合邏輯　2.註冊後下單時填寫內容被清除

受測者/測試任務	註冊帳號並登入	搜尋自駕租車商品	填寫時間、內容	訂購商品	付款
消費者 1	1	2	2	1	1
消費者 2	1	2	2	1	1
消費者 3	1	1	3	1	2
消費者 4	1	1	2	2	1
消費者 5	2	1	2	2	1
消費者 6	2	2	2	2	2
車商 1	1	1	2	1	3
車商 2	1	2	2	2	1
車商 3	2	1	2	2	2

47

系統測試與驗證-易用性測試

- 使用性問題嚴重程度分級表
  - 情境二：消費者取車(自駕)、門市人員核銷

1.找不到QRcode位置　2.相機無法使用、找不到核銷位置

受測者/測試任務	消費者出示QRcode	消費者取車拍照上傳	車商核銷
消費者 1	3	2	2
消費者 2	2	3	3
消費者 3	3	1	3
消費者 4	3	1	3
消費者 5	3	2	2
消費者 6	3	1	2
車商 1	2	1	2
車商 2	3	1	1
車商 3	3	3	1
車商 4	測試失敗		

48

系統測試與驗證-易用性測試

- 使用性問題嚴重程度分級表
  - 情境三：消費者租車(附駕)、司機接單執行代駕

1.附駕包車頁面標題仍寫自駕租車　2.未勾選「附駕駛」　3.功能未完成

受測者/測試任務	搜尋附駕包車商品	填寫時間、內容	訂購商品	司機核銷	司機開始任務	司機結束任務
消費者 1	2	1	1	1	1	3
消費者 2	2	2	1	1	1	3
消費者 3	1	2	3	1	1	3
消費者 4	1	1	1	3	3	3
消費者 5	3	1	1	1	3	3
消費者 6	3	1	3	1	1	3
車商 3	2	1	3	1	1	3

49

系統測試與驗證-易用性測試

- 使用性問題嚴重程度分級表
  - 情境四：平台管理人員查看訂單狀態、車商主管派車並上架車輛

1.找不到上架位置、不知是否上架成功　2.找不到過濾訂單時間功能

受測者/測試任務	查看訂單狀態(CarU後台)	查看庫存量	上架車輛	查看今日訂單(新智慧租車平台)	進行派車
消費者 1	2	1	3	2	2
消費者 5	1	1	2	2	1
消費者 6	1	1	2	2	1
車商 1	1	1	2	1	1
車商 2	1	1	2	1	1
車商 3	3	1	3	3	3
車商 4	測試失敗				

50

系統測試與驗證-易用性測試

- 易用性量表
  - 本表透過在受測者操作完所有流程後進行填寫，填寫後按照一固定公式進行換算並得出總分及評級。

  - 題目共十題：
    1) 我想我會經常使用這個產品。
    2) 我覺得這個產品過於複雜。
    3) 我認為這個產品是簡單好用的。
    4) 我想我需要有人協助才能使用這個產品。
    5) 我覺得這個產品的功能整合得很好。
    6) 我覺得這個產品有很多不一致的地方。
    7) 我認為其他人能快速學習使用這個產品。
    8) 我覺得使用這個產品很麻煩。
    9) 我很有自信地使用這個產品。
    10) 我需要學會很多資訊才能使用這個產品。

51

系統測試與驗證-易用性測試

- 易用性量表評量結果

受測者	第一題	第二題	第三題	第四題	第五題	第六題	第七題	第八題	第九題	第十題	SUS 總分	SUS 評級
消費者 1	2	5	2	3	2	3	2	5	2	1	32.5	E
消費者 2	3	1	4	1	3	4	4	2	5	1	75	C
消費者 3	1	5	1	5	1	5	1	5	4	5	7.5	E
消費者 4	4	2	4	2	3	4	3	2	4	2	65	D
消費者 5	2	2	3	2	1	4	2	2	3	3	45	E
消費者 6	1	4	2	5	2	5	1	4	2	5	12.5	E
車商 1	5	4	5	1	4	3	4	5	1	4	55	E
車商 2	5	4	4	4	4	3	4	2	4	2	65	E
車商 3	3	4	2	5	3	4	2	5	3	2	32.5	E
總體評分及評級											43.3	E

52

系統測試與驗證-改善建議

- 系統功能面
  - 相關操作流程**無前後關係或權限**的檢查，建議新增檢查點跟對應檢查機制，可以降低大量的錯誤操作
  - 上架管理的功能**非即時性且無相關狀態可檢視**，建議改即時或是可以有上架狀態的頁面可查詢
  - 資安問題經檢視有**SQL injection**的可能，還有使用者可以透過**修改URL檢視跟異動資料、API token檢查機制無確實動作**，都須於服務上線前前完成修訂
  - QRcode核銷**沒有綁定訂單屬性**(如門市與司機)，導致核銷方無論使用門市或是司機都可以執行，假設是功能特性，建議在操作上有個提醒，以免誤動作
  - 部分功能在**特定操作流程**有問題發生(如取消付款後，購物車的資料會消失)，建議服務上線前要修訂完成

53

系統測試與驗證-改善建議 (續)

- 易用性部分
  - 有些流程在無指示狀態下，使用者難以自行完成，或是得費時完成。對於初使用的使用者，**可加入簡易操作指示或步驟指南**，讓操作流程更無痛順暢。(CarU前台)
  - 重複性高的動作建議省略，例如：重複填寫時間、重複勾選附駕駛、重複填寫email等，**否則可能導致使用者忽略該步驟或感到繁複而放棄使用**。(CarU前台)
  - 有用詞與實際**操作邏輯不符情形**，例如：點選「立即訂購」不是直接跳付款頁面，建議再重新定義修正。(CarU前台)
  - 按鈕的功能**應避免重複及複雜化**，例如：多種儲存按鈕，常令使用者感到困惑。(新智慧租車平台)
  - **同樣顏色的文字**，有些是可點選的功能，有些不是，建議有所區分，否則使用者會因忽略其功能而無法完成任務。(新智慧租車平台)

(更詳盡之使用者回饋請見word文件)

54

監督審驗

●符合性認證說明 - 評估等級

評估等級	敘述	說明
A	嚴重不符	驗證結果與標準/規範需求有差異或有安全疑慮時，且此結果導致設計或程序需重新審視或進行變更，在此項目未解決前，認定此系統並不符合建置需求，此項目應即刻進行改善。
B	部分不符	驗證結果與標準/規範需求有差異或有安全疑慮時，但此結果並不會導致設計或程序需重新審視或進行變更，在此項目未解決前，認定此系統並不符合建置需求，此項目應即刻進行改善。
C	注意事項	驗證結果與標準/規範需求一致，但考量系統之功能性、正確性及安全性應可再進一步精進之項目，並不會導致設計或程序需重新審視或進行變更，此項目可不用立即改善，但可針對此項目擬定精進計畫。
+	已符合	此驗證/認證項目已被正確執行，可接受。
Q	問題	針對關注的問題需要進一步的釐清，在此項目未解決前，認定此系統暫時尚不符合建置需求，此項目應即刻進行改善。
F	格式	格式、錯字問題，不會導致設計、文件、程序的變動，且不一定要再進版更正。
N/A	不適用	此驗證/認證項目在本專案中不適用。

55

監督審驗

●符合性認證說明 – 驗證結果說明

測試時間：110年12月1日 – 110年12月20日

測試地點：TÜV台中分公司

測試物件：共計6個測試物件

項次	測試物件	物件資訊
1	新智慧租車共通平台	https://dealer2.caru.com.tw/administrator
2	附駕司機PWA	https://driver.caru.com.tw/login
3	行動門市PWA	https://store.caru.com.tw/login
4	Taiwan CarU電商平台	https://test-caru.welcometw.com/admin
5	消費者WebSite	https://test-caru.welcometw.com
6	消費者App	未提供

測試結果：本次驗證測試共計90項，其結果如下表

+ (符合)	A (嚴重不符)	B (部分不符)	C (注意事項)	Q (問題)	F (格式)	N/A (不適用)
17	2	0	0	69	0	2

56

●符合性認證說明 – 驗證結果說明

項次	測試物件	發現說明
1	新智慧租車共通平台	總計20項測試，其中20項問題(Q) 多數功能雖可使用，惟平台操作手冊並無相關使用說明且針對各功能敘述過於簡略，故於實際維運使用時會有執行上的難處，建議應於相關手冊逐項說明各功能或機制，例如： • 權限設定總計有5種身分，但須先透過平台商於帳號管理建立車商，再於員工管理、駕駛管理建立相關身份 • 部分資訊需配合旅遊生態系平台，如平台價格管理中的車型無法自行新增。 • 部分變動非即時於消費者介面更新，例如內附項目管理的資訊需一段時間後才會更新。 • 平台資訊不易理解，例如訂單編號與消費者訂單編號不同、取還車的狀態有已還車與結案、已結案之車輛的車牌號碼於首頁仍顯示未派車。 • 使用上防呆機制較少，不熟稔的人員容易造成誤操作，例如變更核銷資訊的狀態、取還車狀態等 • 客戶資料為明碼顯示，容易有個資外露的疑慮 • 使用者上傳的車況照片無法於平台顯示 • M3功能於租車流程中並未進行確認，車號亦無機制防呆 • 營運報表無法以日報或月報方式呈現，使用不易

57

監督審驗

●符合性認證說明 – 驗證結果說明

項次	測試物件	發現說明
2	附駕司機PWA	總計6項測試，其中2項符合(+)、1項不符合(A)、3項問題(Q) 多數功能雖可使用，惟操作手冊並無相關使用說明且針對各功能敘述過於簡略，故於實際維運使用時會有執行上的難處，建議應於相關手冊逐項說明各功能或機制，例如： • 以人工核銷方式須先透過共通平台進行預先作業。 • 防呆機制較少，例如QR code若誤觸重新掃描功能則需要透過平台重新設定狀態。 • 人工核銷雖可進行結案作業，但過程中並無上傳合約等資訊。 • 操作手冊介面與目前使用不同，應進行更新 不符合(A)項目說明： 使用QR code掃描進行核銷作業，但於資訊確認後不會出現在”執行中”頁面，故無法透過PWA結案。

58

監督審驗

●符合性認證說明 – 驗證結果說明

項次	測試物件	發現說明
3	行動門市PWA	總計9項測試，其中4項符合(+)、5項問題(Q) 多數功能雖可使用，惟操作手冊並無相關使用說明且針對各功能敘述過於簡略，故於實際維運使用時會有執行上的難處，建議應於相關手冊逐項說明各功能或機制，例如： • 無法由PWA確認已完成項目，僅能由狀態確認是否已還車，另亦無訂單編號可與後台比對確認，造成比對不易。 • 防呆機制較少，例如QR code若誤觸重新掃描功能則需要透過平台重新設定狀態。 • 由PWA進行結案作業完成後，於平台仍顯示已還車並非結案 • 操作手冊介面與目前使用不同，應進行更新
4	Taiwan CarU電商平台	同消費者website項目確認 多數功能雖可使用，惟操作手冊並無相關與新智慧租車共通平台連動之說明，造成營運機制確認不易。

59

監督審驗

●符合性認證說明 – 驗證結果說明

項次	測試物件	發現說明
5	消費者WebSite	總計21項測試，其中11項符合(+)、1項不符合(A)、7項問題(Q)、2項不適用(N/A) 多數功能雖可使用，惟需相關營運規則及稽核制度方可順利營運，目前尚無明確手冊定義相關資訊，例如 • 目前線上仍有多數縣市無車輛可進行租賃。 • 防呆機制較為薄弱，例如會員年齡低於18歲，仍可進行租車作業；或可租車時間與營運時間無法連動，如車商營業為08:00~17:00，但系統仍可於此時段外進行租車作業。 • 線上無會員證件審核機制。 • 保險機制無法透過進階搜尋，且目前線上車商多數皆無此服務。 • 甲租乙還由文字方式呈現而非系統功能，需透過產品內容資訊於線下聯繫車商方式進行，無法由線上進行作業。 • 消費者訂單狀態不易理解，如完成付款尚未取車之車輛於狀態中顯示已完成，取車後亦顯示相同狀態。 • 無法透過線上進行延長訂單作業，亦須透過線下聯繫車商方式進行。 不符合(A)項目說明： Line連動註冊出現異常，無法透過Line進行註冊
6	消費者App	21項問題(Q)，目前無消費者App故無進行相關測試。

60

●符合性認證說明 – 驗證結果說明

項次	測試物件	發現說明
7	營運作業確認	總計13項測試，其中13項問題(Q) 部分招標計畫需求文件雖有部分說明但分散於各階段報告書中，建議應因確認招標計畫需求及營運需求訂定相關文件，例如： • 客服中心管理機制 • 資安維護計畫 • 營運規章 • 收費機制 • 維運標準 • 車輛整備與安全管理 另部分功能因尚未開始營運，故仍待後續導入後方能釐清如： • 金流清分及稽核作業 • 車輛合法性確認 • 各平台資訊安全檢測結果

61

5. 結論與建議

結論

1.專案管理服務

- 追蹤管控數位轉型推動計畫執行過程之相關問題與議題。
- 協助辦理漢名科技之採購、期初、經費支用查核等作業。
- 逐月管控漢名科技之風險控管。

2.專業知識諮詢

- 協助督導小客車租賃業數位轉型工作。
- 針對漢名科技提出之服務方案、研究方法、期初發表會簡報與企劃、招募計畫、深度計畫、系統相關文件等，協助審驗並研提建議。

3.獨立監督審驗

- 針對推動數位轉型之平台，進行技術文件檢視，及確認資安驗測與功能驗測成果。
- 設計整體租車驗測流程，確保漢名科技推動數位轉型之平台功能準備完善。

63

建議

1.專案管理服務

- 持續追蹤管控數位轉型推動計畫執行過程之相關問題與議題，並於12月中旬完成賸餘11項工作任務，確保計畫如期、如質完成。
- 協助辦理漢名科技之期中、期末經費支用查核等作業。
- 逐月管控漢名科技之風險控管。

2.專業知識諮詢

- 持續協助督導小客車租賃業數位轉型工作。
- 針對漢名科技提出之相關企劃與文件，協助審驗並研提意見與建議。

3.獨立監督審驗

- 針對「小客車租賃服務整合旅遊生態系平台」，進行相關技術文件檢視，及確認功能需求符合所方、小客車租賃業者之需求，預計12月中旬產出驗測報告。

64

附件-操作異常畫面

操作異常畫面

- CarU前台

67

操作異常畫面

- CarU前台

取消勾選後，選框仍留有打勾殘影，令使用者困惑有沒有取消成功(test on 12/1)

使用者常按了立即訂購才發現要再按一次預訂，此流程不符合邏輯 (test on 12/5)

使用者會不斷點擊日期欄位，不知道要點選下方日曆的日期，造成時間的耗費，更提高困惑程度 (test on 12/1)

操作異常畫面

- CarU前台

照片正在上傳中，速度過慢且無上傳中相關提示，使用者以為上傳失敗 (test on 12/5)

「我的訂單」藏在「會員資訊」中，令使用者花費較多時間查找(test on 12/2)

訂單無任何QRcode查找之提示，導致使用者不知道有QRcode (test on 12/2)

操作異常畫面

- 行動門市及附駕司機app

「掃得很重」的意義不明，應為「重新掃描」(test on 12/2)

司機開始任務之後，畫面顯示無執行中任務，也找不到結束任務功能 (test on 12/6)

70

操作異常畫面

- CarU後台

消費者已付款，訂單狀態顯示「待付款」，付款狀態卻顯示「已付款」 (test on 12/2)

71

操作異常畫面

- 新智慧租車平台

數字的呈現與按鈕太過類似，導致許多使用者以為這是按鈕而不斷的點按 (test on 12/2)

系統顯示「已還車」，卻還可以做派車的動作(test on 12/6)

已建立之車輛資料於手機頁面均無法顯示 (test on 12/7)

使用者對於這三個按鈕感到困惑，不知道要按哪一個 (test on 12/6)

72

操作異常畫面

- 新智慧租車平台

訂單為「空租」，取還車狀態卻顯示「代駕開始」 (test on 12/6)

使用者幾乎都不知道可以點選「車型」去做每日上架(test on 12/5)

車輛總數為1，上架數和庫存數卻大於1(test on 12/5)

過濾時間的提示不明顯，且要按兩次才會完成過濾

一般來說最新訂單會在最上方，這裡的排序卻在最下方，令使用者找不到最新訂單 (test on 12/2)

73

操作異常嚴重分級表

測試情境一：消費者租車(自駕)					測試情境二：消費者取車(自駕)、車商核銷		
步驟 1 註冊帳號並登入	步驟 2 搜尋自駕租車產品	步驟 3 填寫時間、內容	步驟 4 訂購商品	步驟 5 付款	步驟 6 消費者出示QRcode	步驟 7 消費者取車拍照上傳	步驟 8 車商核銷(掃碼/人工)
2 - 不知道密碼不能少於8字元，註冊後選項被清除	2 - 找不到搜尋結果	3 - 多次重覆按填寫時間還是無效	2 - 註冊後填寫內容被清除	3 - 跑不出付款頁面	3 - 找不到QRcode位置	3 - 上傳速度過慢，以為沒有成功	3 - 相機無法使用
2 - 不知道密碼不能少於8字元	2 - 多次查無商品	2 - 重複按了填寫日期的地方	2 - 註冊後填寫內容被清除	2 - 未填寫信箱	3 - 找不到QRcode位置	3 - 上傳速度過慢，以為沒有成功	3 - 網頁版相機無法使用，用app開才可以
2 - 不知道密碼不能少於8字元，註冊後選項被清除	2 - 無法搜尋指定車商	2 - 重覆按「立即訂購」，沒有填寫取還車時間、重複點選日期欄位	1 - 有效	2 - 付款失敗還是有QRcode，不知道要不要重新付款	3 - 無法載入訂單內容	2 - 上傳速度慢	3 - 網頁版相機無法使用，用app開才可以
1 - 有效	2 - 多次查無商品	2 - 重複按了填寫日期的地方	2 - 註冊後填寫內容被清除	2 - 付款成功，卻顯示「已確認，待付款」，以為要重新付款	3 - 找不到QRcode位置	2 - 找不到現場拍攝之相機位置	2 - 找不到核銷位置
1 - 有效	1 - 有效	2 - 重覆按「立即訂購」和日期欄位	2 - 註冊後填寫內容被清除	1 - 有效	3 -訂單無顯示QRcode	1 - 有效	2 - 找不到核銷位置
1 - 有效	1 - 有效	2 - 重覆按「立即訂購」，沒有填寫取還車時間	2 - 註冊後填寫內容被清除	1 - 有效	3 - 訂單無顯示QRcode	1 - 有效	2 - 核銷後未顯示在畫面上
1 - 有效	1 - 有效	2 - 重複按了填寫日期的地方	1 - 有效	1 - 有效	3 - 找不到QRcode位置	1 - 有效	2 - 找不到核銷位置
1 - 有效	1 - 有效	2 - 重複按了填寫日期的地方	1 - 有效	1 - 有效	2 - 找了很久才找到QRcode	1 - 有效	1 - 有效
1 - 有效	1 - 有效	2 - 重複按了填寫日期的地方	1 - 有效	1 - 有效	2 - 找了很久才找到QRcode	1 - 有效	1 - 有效

74

操作異常嚴重分級表

測試情境三：消費者租車(附駕)、取車(附駕)、司機核銷						測試情境四：車商主管派車、上架車輛				
步驟 9 搜尋附駕租車產品	步驟 10 填寫時間、內容	步驟 11 訂購商品	步驟 12 司機核銷QRcode	步驟 13 司機開始任務	步驟 14 司機結束任務	步驟 15 從CarU後台查看付款狀態	步驟 16 查看庫存量	步驟 17 上架車輛	步驟 18 查看今日訂單並其狀態	步驟 19 進行派車
3 - 未找到附駕包車	2 - 忘記剛剛填寫過的時間	3 - 未勾選「附駕駛」	3 - 相機無法使用	3 - 無法使用	3 - 找不到結束任務功能	3 - 看不到內容(手機)	1 - 有效	3 - 看不到內容(手機)	3 - 看不到內容(手機)	3 - 看不到內容(手機)
3 - 未找到附駕包車	2 - 一直按「立即訂購」而不是「預訂」	3 - 未勾選「附駕駛」	1 - 有效	3 - 不知道要開啟定位	3 - 找不到結束任務功能	2 - 與前台顯示狀態不一致	1 - 有效	3 - 找不到從哪裏上架	2 - 找不到過濾訂單時間功能	2 - 以為儲存即會關閉頁面
2 - 多次點選附駕租車，頁面仍顯示自駕租車	1 - 有效	3 - 未勾選「附駕駛」	1 - 有效	1 - 有效	3 - 找不到結束任務功能	1 - 有效	1 - 有效	2 - 不知道是否上架成功，重複上架	2 - 找不到過濾訂單時間功能	1 - 有效
2 - 改變搜尋條件以為搜尋結果會跟著變，等了一下才發現沒有變	1 - 有效	1 - 有效	1 - 有效	1 - 有效	3 - 找不到結束任務功能	1 - 有效	1 - 有效	2 - 不知道怎麼上架	1 - 有效	1 - 有效
2 - 點選附駕租車，頁面仍顯示自駕租車，重複點選	1 - 有效	1 - 有效	1 - 有效	1 - 有效	3 - 找不到結束任務功能	1 - 有效	1 - 有效	2 - 不知道怎麼上架	1 - 有效	1 - 有效
1 - 有效	1 - 有效	1 - 有效	1 - 有效	1 - 有效	3 - 找不到結束任務功能	1 - 有效	1 - 有效	2 - 上架後看不到數量改變，重複上架	1 - 有效	1 - 有效
1 - 有效	1 - 有效	1 - 有效	1 - 有效	1 - 有效	3 - 找不到結束任務功能					

75