網頁資訊安全現況分析探討-以運技中心為例

劉清松[1] 林雅雯[2] 蔡世璿[3] 李麗雯[4] 林珂如[5]

[1]交通部運輸研究所運輸技術研究中心副研究員
[2]交通部運輸研究所運輸技術研究中心科長
[3]交通部運輸研究所運輸技術研究中心副研究員
[4]交通部運輸研究所運輸技術研究中心資安工程師
[5]交通部運輸研究所運輸技術研究中心系統工程師

摘要

在當前數位化環境中，網頁應用程式因其普及性與開放性，成為駭客攻擊的主要目標。本研究以交通部運輸研究所運輸技術研究中心(以下簡稱運技中心)為例，探討其網頁資訊安全現況，並依據 OWASP TOP 10 標準進行弱點掃描，分析常見弱點如權限控制失效、危險或過舊元件及注入攻擊等，共有風險弱點種類 50 項，並透過第 2 次複掃檢測消除網頁弱點風險。本研究建議提出建立更新機制、實施最小權限原則、提升開發人員技能、執行複測確認弱點修補效果，並強調資安防護需隨技術進化持續改進。研究對提升系統安全性與降低風險提供具體參考。

一、研究緣起與目的

1.1 背景與現況

在當前數位化與網路化的環境中，網頁應用程式已成為企業、政府機構與社會大眾間的重要橋梁，其安全性直接影響業務運營的穩定性與資訊的保密性。自 108 年資通安全管理法[1]實施以來，公務機關依據資通安全責任等級劃分為 5 級(A 至 E)，各單位也需履行應辦事項，其涵蓋管理面、技術面及認知與訓練面三大面向[2]，確保機關資通安全作為落實。此外，為強化國家資安防護，蔡英文總統於 105 年提出「資安即國安」戰略，並於 111 年 8 月 27 日成立數位發展部，整合資安相關單位，推動機關配合執行資通安全法相關規定。為進一步提升國家資通安全科技能力，於 112 年 1 月 1 日成立國家資通安全研究院[3]，專責推動資通安全科技的研發及應用。

1.2 網頁安全挑戰與問題

隨著網頁應用程式的普及與開放性，其已成為駭客攻擊的首要目標。根據國家資通安全研究院(NICS)113 年第 3 季資通安全技術報告[4]，非法入侵與網頁攻擊已成為國內最常見的資安事件之一，其根源多來自於設計不當的系統與應用程式弱點。且參考美國通用弱點揭露(Common Vulnerabilities and Exposures,CVE)近 10 年弱點統計，網頁弱點會隨著時間演進與更迭變換，如

圖 1 所示[5]，運技中心目前主要對外服務系統，通常透過現場佈設的儀器設備蒐集資訊，再利用資訊傳輸技術將資料傳送至中心資料庫，經品管後提供系統存取與展示應用。港區環境資訊與資料庫服務系統的安全性，在資通安全法規範要求下面臨極大挑戰，因此，如何防止資訊系統被駭客攻擊，已為當前迫切需解決的問題。

Year	Overflow	Memory Corruption	Sql Injection	XSS	Directory Traversal	File Inclusion	CSRF	XXE	SSRF	Open Redirect	Input Validation
2014	824	627	304	1099	207	3	266	67	10	48	532
2015	1040	1104	221	776	152	6	249	50	8	46	379
2016	1181	1173	97	497	99	12	87	41	16	33	520
2017	2480	1545	505	1500	282	155	334	109	57	97	940
2018	2086	1739	503	2042	571	112	479	188	118	85	1256
2019	1206	2032	546	2388	490	126	560	137	103	121	910
2020	1219	1888	465	2202	440	110	416	119	132	100	822
2021	1666	2543	743	2724	551	91	520	126	195	133	683
2022	1875	3388	1789	3406	731	97	769	126	231	146	798
2023	1714	2587	2154	5164	792	131	1396	136	245	183	694
2024	1829	2425	2516	7220	928	260	1352	109	360	122	209
Total	17120	21051	9843	29018	5243	1103	6428	1208	1475	1114	7743

圖 1 近 10 年主要弱點類型發生次數統計表

1.3 研究目的與策略

面對資通安全挑戰，如何提出有效的防禦策略，已為提升系統防護能力主要關鍵。本研究以運技中心為例，探討網頁資訊安全現況並盤點現行對服務系統防禦方式與弱點掃描結果，識別系統可能存在的安全弱點。最終，透過研究結果提出具體且有效的建議，協助提升系統資安防護能力，降低駭客攻擊風險，確保系統穩定性與資料安全性。

二、文獻回顧

本研究首先釐清駭客的定義，知曉其分類方式，並瞭解其攻擊思維方式。其次，盤點重要資訊安全資源組織，明析資訊安全弱點的定義、分級標準、類型分類，以及現行弱點檢測規範(特別參考國家資通安全研究院相關指引)與安全測試方式與步驟。

本研究同時探討 MITRE 攻擊性策略、技術和常識 ATT&CK 框架與網路殺傷鏈(Cyber Kill Chain)模型，知悉駭客攻防策略，從偵察階段到目標實現。藉此，我們希望提出有效的網頁應用程式安全性措施，進一步減少網站資安事件的發生。

本研究不僅於駭客攻防行為與網頁弱點相關分析，還對網頁弱點的防禦策略進行具體建議，期望這些成果能為運技中心及其他相關單位提供參考與實務應用，從而提升整體網頁應用程式的安全性與可靠性。

2.1 駭客(白帽、灰帽、黑帽)

在駭客領域透過 Shital[6]文獻回顧，根據其意圖和行為，可將駭客分為白帽、灰帽與黑帽 3 種類別，以下說明其差異：

1. 白帽駭客：又稱為「道德駭客」，以合法和負責任的方式使用其技術技能。其主要目的為識別並修補系統或資料庫中的弱點，以防止黑帽駭客的惡意攻擊。白帽駭客通常在取得明確授權或簽訂合約後，執行安全測試工作。優先確保自己的行為符合道德與法律規範，並注重保持匿名性。

2. 黑帽駭客：由惡意意圖驅動，專注於非法入侵系統、竊取敏感資料或破壞系統穩定性。其不考慮合法性或道德性，通常以謀取個人利益、施行報復或滿足自我挑戰為目標，對網路安全構成嚴重威脅。

3. 灰帽駭客：具有黑帽與白帽駭客的雙重特徵，可能會在未經授權的情況下進行系統滲透，但目的並非純粹惡意，而是為了發現並報告弱點。有時會提供安全服務，幫助系統防禦，但並不試圖操控系統或謀取私利。「灰色」一詞反映了其行為的模糊性，介於合法與非法之間，且通常依情況而有所不同。

駭客攻擊思維 4 個步驟：

1. 資訊蒐集：為攻擊的第一步，測試者專注於蒐集目標的各種資訊，為後續測試提供依據。這包括利用搜索引擎、掃描工具及 HTTP 請求等方式，蒐集系統配置、結構及互動數據，即使看似無關的資訊，也可能於後續階段發揮作用。

2. 弱點掃描：在蒐集足夠資訊後，測試者開始對目標應用進行弱點掃描，測試範圍涵蓋配置管理、認證機制、數據驗證、業務邏輯及 Web 服務等領域。透過全面分析，識別如輸入驗證缺陷、會話管理問題等可能被惡意利用的弱點。

3. 弱點利用：完成弱點分析後，測試者聚焦於易受攻擊的區域，利用已識別的弱點進行模擬攻擊，驗證其可行性及潛在威脅。此階段使用專業工具與技術，測試弱點可能對系統造成的實際影響。

4. 測試分析階段：駭客彙整測試結果，向委託者提供詳細報告，說明攻擊過程發現的弱點與對每個弱點的描述、其潛在影響以及任何支持證據。

2.2 資訊安全重要組織

1. 通用弱點列舉(Common Weakness Enumeration, CWE) [7]：CWE 組織是專注於軟體和硬體弱點標準化描述和分類的工作，其目標是幫助開發者、測試人員以及安全專家了解、識別和提高軟體開發安全性。

2. 開放式 Web 應用程式安全專案(Open Web Application Security Project, OWASP) [8]：專注於網頁應用程式安全，提供免費的資源和工具。係一個開放性社群與非營利組織，專注於研議解決網路安全問題的標準、開發工具及撰寫技術文件。該組織長期致力於協助政府與企業了解並提升應用程式的安全性，成為網路安全領域的重要推動者。其中，最具代表性的計畫是「OWASP TOP 10」[9]，該計畫透過資安公司與組織的調查，結合業界問卷結果，並參考國際 Bug Bounty 平臺的資料，歸納出十大最常見或最值得關注的弱點。「OWASP TOP 10」詳細描述了這些弱點的特性與風險，並提供實用的防護建議，幫助企業有效應對弱點與風險，強化自身的防禦能力。

3. 安全性檢測(MITRE ATT&CK) [10] ：隨時掌握最新威脅和攻擊技術，透過定期更新應對新興威脅。此外，該架構可協助企業改善整體安全狀況，識別並優先處理相關威脅，制定有效對策。可藉此將資源集中於關鍵領域，有效降低風險，提升防禦能力。

4. 網路殺傷鏈(Cyber Kill Chain) [11]：由洛克希德·馬丁(Lockheed Martin) 於 2011 年提出，為其網路安全團隊基於軍事「殺傷鏈」概念設計的框架。原始軍事殺傷鏈用於描述敵方目標之識別與打擊流程，而 Cyber Kill Chain 將這一概念應用到網路安全領域，俾以更易理解和防禦網路威脅。

5. 通用弱點評分系統(CVSS)：是評估軟體安全弱點嚴重性的標準化框架，根據可攻擊性、保密性、完整性、可用性和所需許可權的影響等因素進行評分，以「低(low)0.1 至 3.9 分、中(medium)4.0 至 6.9 分、高(high)7.0 至 8.9 分和嚴重(Critical)9.0 至 10 分」等級標示。

6. 臺灣漏洞揭露平臺 [12]：自 107 年起，臺灣漏洞揭露平臺加入美國 MITRE 的通用弱點揭露(CVE®) 計畫，並成為 CVE 編號管理者 (CNA)。該平臺旨在協助國內外廠商處理產品弱點，透過快速完成弱點的緩解與修補，降低弱點被利用的風險，避免駭客攻擊對使用者造成影響，同時建置臺灣弱點紀錄(Taiwan Vulnerability Note, TVN) 平臺，以提升資安防護能力。

2.3 攻擊模型與防禦策略

MITRE ATT&CK 與網路殺傷鏈(Cyber Kill Chain) 是 2 種主流的攻擊行為模型，如表 1 所示。

1. MITRE ATT&CK：強調攻擊行為的細化與技術分析，適用於威脅偵測與模擬攻擊場景。
2. 網路殺傷鏈(Cyber Kill Chain)：關注攻擊生命周期、宏觀策略設計與防禦措施的規劃。

表 1 攻擊行為模型比較

特徵	MITRE ATT&CK	網路殺傷鏈(Cyber Kill Chain)
核心目標	描述細緻的攻擊技術與行為模式	描述攻擊生命周期的高層次結構
層次	戰術、技術與子技術的多層結構	七個固定的階段
應用靈活性	非線性，適用於各種攻擊場景	線性，適用於典型攻擊過程
細節深度	技術細節豐富，具體化	抽象化，細節較少
應用場景	威脅檢測、行為分析、模擬攻擊	防禦策略設計、事件分析
使用者群體	側重技術分析人員(SOC、藍隊、紅隊)	側重戰略決策者與防禦工程師

2.4 網頁弱點檢測依循標準

弱點掃描服務主要協助機關發現網頁安全弱點或個資揭露風險，提供掃描結果與修補建議，並於完成修補後進行複測，以確認弱點已修正。Web 網頁弱點掃描分為初次檢測與複測，掃描項目應符合 OWASP TOP 10 最新標準(如表 2 說明)。根據 數位發展部國家資通安全研究所之「弱點掃描服務」委外規範與 113 年共同供應契約規範，檢測應以 OWASP TOP 10 為遵循標準，如檢視包括權限控制失效、注入攻擊、不安全設計等弱點。此外，國內也有臺灣電腦網路危機處理暨協調中心(TW-NCERT)，提供國內所開發軟硬體系統漏洞揭露平臺。故本計畫執行相關網頁漏洞檢測將遵循 OWASP TOP 10 標準與專業工程師協助，確保網頁弱點檢測與修補作業之準確性與完整性，OWASP 2021 所公佈最新十大漏洞，如表 2 所示。

表 2　OWASP TOP 10

網路攻擊類型	說明
A01：權限控制失效	當應用程式未能正確實施訪問控制時，可能允許攻擊者訪問未授權的功能或數據。如：上傳下載路徑沒寫好、預設權限沒設好、可修改 URL、用自訂工具繞過檢查等。
A02：加密機制失效	涉及加密演算法、金鑰管理和密碼學實踐的不當使用，可能導致敏感數據洩露或系統被攻破。避免明碼傳輸、淘汰老舊加密演算法及強度不足的金鑰、驗證憑證有效性... 等。
A03：注入式攻擊	當應用程式將不受信任的數據作為命令或查詢的一部分傳遞給解析器時，可能會發生注入漏洞。包括 SQL 注入、NoSQL 注入、OS 注入等。
A04：不安全設計	強調與設計缺陷相關的風險，指出安全控制的缺失可能導致安全攻擊。預訂餐廳未經任何驗證(Email/電話)、演唱會搶票網站沒有防機器人驗證機制。
A05：安全設定缺陷	應用程式或基礎架構的不安全配置可能導致安全漏洞。例如不必要的 Port、帳號或權限、未改掉預設帳號密碼、未移除具安全缺陷的預設範例程式... 等等。
A06：危險或過舊的元件	使用已知存在安全漏洞的元件或過時的函式庫，可能使應用程式容易受到攻擊。如測試和評估風險的元件太舊。
A07：認證及驗證機制失效	包括失效的身份認證，還包括與識別錯誤相關問題。因防禦不足被取得帳密名單的自動化攻擊、暴力破解、允許強度不足的密碼、使用脆弱的密碼或重設密碼機制、密碼以明碼/加密或強度不足的雜湊儲存、缺乏多因子認證... 等等。
A08：軟體及資料完整性失效	攻擊者可能破壞應用程式的完整性，進行惡意活動。夾帶惡意程式庫、透過自動更新散佈惡意程式... 等等。
A09：資安記錄及監控失效	缺失的日誌記錄和監控，可能導致安全事件未被及時發現或回應。常見狀況：未記錄登入成功/失敗/重要交易之稽核事件、告警或錯誤未留下日誌或保存訊息不足、未監控程式或 API 日誌之可疑活動、日誌只保存在本地端、滲透測試工具未發揮效果、未能偵測及通告進行中的攻擊，導致重大損失。
A10：伺服端請求偽造	攻擊者可以通過伺服器端，請求來訪問或操作內部系統。攻擊者操縱請求內容，成功克服防火牆、VPN 或存取控管，控制網站發送捏造的請求給非預期對象。

2.5 風險計算方法

1. CVE(Common Vulnerabilities and Exposures，公共弱點與暴露)：本身是一個弱點命名和跟蹤系統，並不直接提供風險計算，如要進行風險計算，通常利用 CVSS(Common Vulnerability Scoring System，通用弱點評分系統)[13]，來量化每個 CVE 的嚴重性和影響。

2. CVSS 風險計算方法和關鍵組成：CVSS v4.0 由 4 個指標組成(如圖 2 所示)：基礎、威脅、環境和補充。基本分數根據弱點的內在特徵反映了弱點的嚴重性，這些特徵隨著時間的推移保持不變，並假設不同部署環境中合理的最壞情況影響。威脅指標根據概念驗證程式碼的可用性或主動利用等因素，調整弱點的嚴重性。環境指標進一步細化了特定計算環境的嚴重性評分。考慮諸如該環境中是否存在緩解措施，以及易受攻擊系統的關鍵屬性等因素。最後，補充指標描述並測量弱點的其他外部屬性。

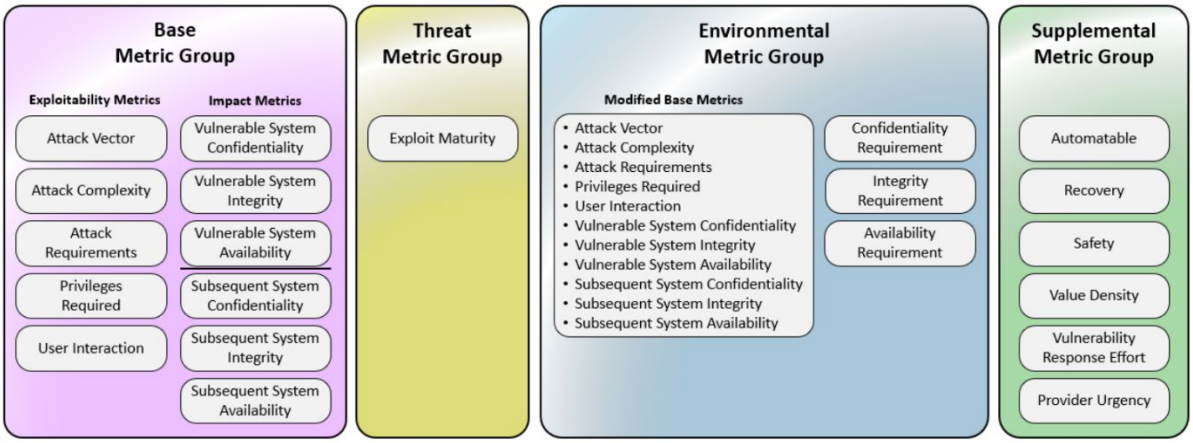

圖 2 CVSS 風險計算方法和關鍵組成

風險等級主要用於評估安全弱點的嚴重性，幫助識別弱點對系統穩定性與安全性的潛在威脅。通過區分低、中、高及危急等級，便於優先處理高風險與危急問題，降低系統受攻擊的可能性。風險等級由低至高分為 4 類，說明如下：

1. 低(0.1–3.9)：風險對系統影響小。

2. 中(4.0–6.9)：可能影響系統穩定性或安全性。

3. 高(7.0–8.9)：對系統構成重大威脅。

4. 危急(9.0–10.0)：極高風險，需立即修復。

2.6 網頁安全檢測方法 5 階段

Sathvik Babu[14]提到網頁安全檢測可分為偵察、掃描、評估、發現與分析和報告與修補 5 個階段，每一階段之主要工作重點，說明如下：

1. 偵查(Reconnaissance)：

   (1) 蒐集目標網站或系統相關資訊，包括 IP 地址、子域名、技術堆棧、公開的電子郵件地址等。

   (2) 使用技術(如 Google Dorking) 或工具(如 Harvester 或 Wappalyzer)瞭解目標之潛在攻擊面，為後續測試建立基礎。

2. 掃描(Scanning)：

   (1) 利用掃描工具(如 Nmap 或 Angry IP Scanner)進行網絡掃描，找出開放的端口和相關服務。

   (2) 確認應用程序的端點(endpoints)，並初步定位可能的弱點，包括未經身份驗證的端點或可疑的服務。

3. 評估(Evaluation)：

   (1) 對發現的潛在弱點進行分類與優先排序，根據弱點的嚴重性(如 Critical, High, Medium, Low)來分配修復資源。

   (2) 評估測試階段的準備度，包括驗證用戶訪問控制(UAC)和掃描的有效性。

4. 發現與分析(Discovery and Analysis)：

   (1) 深入分析掃描階段中確認的弱點，確定弱點的技術細節及可能的利用方式。

   (2) 使用工具或手動方式對弱點進行詳細測試，並記錄其潛在影響。

5. 報告與修補(Reporting and Patching)：

   (1) 生成詳細的測試報告，內容包括弱點清單、影響分析、修復建議等。

   (2) 如果獲得權限，實施修補操作以修復弱點，並確保應用程序無法被進一步利用。

三、研究方法

本研究採 4 步驟進行，分別為現況系統盤點，網頁弱點掃描，網頁弱點初掃結果分析，網頁弱點複掃結果分析，說明如下：

3.1 現況系統盤點

主要對運技中心對外服務網頁辦理數量與檢測所需資訊，但在資訊安全考量下，會省略敏感資訊，用代表性資訊來說明，檢測所需資訊盤點項目，如表 3 所示。

表 3 資訊盤點項目

項目	說明
網站基本資訊	1. 網站域名(Domain Name)：主要掃描目標的完整域名(如 www.example.com)。 2. 子域名清單(Subdomains)：需一併掃描的所有子域名。 3. IP 地址(IP Address)：網站伺服器的公開 IP 或內部測試環境的 IP 範圍。 4. 網站使用的協議(Protocol)：HTTP 或 HTTPS。
系統架構	1. 伺服器資訊： (1) 網頁伺服器類型(如 Apache、Nginx、IIS)。 (2) 作業系統類型與版本(如 Linux、Windows Server)。 2. 應用程式框架： (1) 使用的程式語言(如 PHP、Python、Java)。 (2) 使用的 Web 框架(如 Laravel、Spring、Django)。 3. 後端技術： (1) 資料庫類型(如 MySQL、PostgreSQL、MongoDB)。 (2) API 技術(如 REST、GraphQL)。
權限相關資訊	1. 測試帳號與權限：提供至少一組測試用的帳號，包含一般使用者與管理員帳號，便於檢測權限相關弱點。 2. 驗證機制： (1) 驗證方式(如表單驗證、單一登入 SSO、多因素驗證 MFA)。 (2) 提供測試用的驗證憑證(如測試密碼或 API 金鑰)。
網站功能與範圍	1. 網站功能清單：包括登錄頁面、資料提交表單、購物車、檔案上傳功能等。 2. 測試範圍與限制： (1) 明確界定哪些子系統或模組可以掃描，哪些不可以。 (2) 特別聲明對生產環境的影響(如性能負載)。
現有安全性機制	1. 防火牆配置(WAF)：是否有部署網頁應用防火牆，是否需暫時調整規則。 2. DDOS 保護機制：提供掃描白名單，避免被誤判為惡意攻擊。 3. 安全策略與風險偏好：了解現行的安全策略和合規要求(如 PCI DSS、GDPR)。

掃描需求與時間安排	1.掃描目標與範圍：確定是進行全面掃描還是針對特定模組。 2.掃描排程：選擇影響最小的時間進行測試，如非高峰時段。 3.掃描報告需求：明確需要生成的報告格式(如 PDF、CSV)及內容深度。
聯絡人與緊急處理	1.技術聯絡人：包括測試期間的技術支援聯絡資訊。 2.緊急處理流程：發現重大弱點時的回報與應對程序。

3.2 網頁弱點掃描

本研究以 OWASP TOP 10 弱點做為檢測範圍，使用 HCL AppScan Standard 工具進行 Web 應用程式安全掃描。該工具採用動態應用程式安全測試(DAST) 技術，為一種黑盒測試方法，專注於識別執行中應用程式的安全脆弱性。其操作方式包含掃描潛在輸入點、注入異常或惡意數據(如 SQL 注入、XSS 和長輸入字串)，並根據應用程式的回應行為判斷弱點的存在。本次掃描結果顯示，整體目標的網頁弱點種類共計 50 項，如圖 3 所示。

本研究以 A、B、C、D、E 表示對外服務系統網站標的，以符合本單位資安管理制度，確保網站不淪為駭客攻擊目標，降低服務中斷及資料外洩的風險。

項次	目標	弱點種類				弱點數量			
		危急	高	中	低	危急	高	中	低
1	A系統	0	0	4	5	0	0	6	7
2	B系統	0	1	4	5	0	9	50	22
3	C系統	1	1	6	5	10	11	14	12
4	D系統	0	1	4	2	0	1	13	15
5	E系統	0	1	4	6	0	1	44	7
	總計	1	4	22	23	10	21	127	63

圖 3 整體弱點種類統計

從上圖中可以看到各目標之網頁弱點種類分布：

1. 危急風險弱點：共 1 項。
2. 高風險弱點：共 4 項。
3. 中風險弱點：共 22 項。
4. 低風險弱點：共 23 項。

弱點種類計 50 項，其高風險和危急弱點的數量雖然較少，但依循本所資訊安全管理制度規定，應優先處理以減少系統的重大安全威脅。

對各目標進行初次弱點掃描結果，其弱點種類與數量分布，如表 4 所示。

表 4 弱點種類與數量分布

目標	說明
A 系統	弱點種類：中風險 4 項，低風險 5 項。 弱點數量：共 13 項。
B 系統	弱點種類：高風險 1 項，中風險 4 項，低風險 5 項。 弱點數量：共 81 項，集中於中低風險。
C 系統	弱點種類：危急弱點 1 項，高風險 1 項，中風險 6 項，低風險 5 項。 弱點數量：共 47 項。
D 系統	弱點種類：高風險 1 項，中風險 4 項，低風險 2 項。 弱點數量：共 29 項。
E 系統	弱點分類：高風險 1 項，中風險 4 項，低風險 6 項。 弱點數量：共 52 項。

3.3 網頁弱點初掃結果分析

本項工作主要是彙整網頁弱點初掃結果，並針對弱點嚴重性依序分析，給出建議改進措施。弱點初掃結果，如圖 4 所示。

項次	目標	弱點種類			
		危急	高	中	低
1	A01:權限控制失效	0	2	8	
2	A02:加密機制失效	0	0	0	
3	A03:注入式攻擊	0	1	1	
4	A04:不安全設計	0	0	4	
5	A05:安全設定缺陷	0	0	2	
6	A06:危險或過舊的元件	1	1	3	
7	A07:認證及驗證機制失效	0	0	1	
8	A08:軟體及資料完整性失效	0	0	3	
9	A09:資安記錄及監控失效	0	0	0	
10	A10:伺服端請求偽造	0	0	0	
總計		1	4	22	

圖 4 網頁弱點種類初掃結果

3.3.1 弱點初掃掃總結

OWASP TOP 10 分類下的弱點評估結果，主要問題如下，這表示系統主要弱點來自於使用過時元件以及權限控制機制的問題。

1. 危急弱點：1 項，位於 A06 危險或過舊的元件。

2. 高風險弱點：4 項，分布於 A01 權限控制失效 和 A06 危險或過舊的元件。

3. 中風險弱點：22 項，集中於多個分類，尤其是 A01 權限控制失效 和 A04 不安全設計。

3.3.2 主要問題分析

中心對外服務網頁，經弱點初掃後，顯示之主要弱點種類及建議，如表 5 所示。

表 5 網頁主要弱點種類描述及建議

弱點種類	說明及建議
A06：危險或過舊的元件	1.弱點數量：危急弱點 1 項，高風險 1 項，中風險 3 項。 2.問題描述： 使用過時或有弱點的第三方元件會讓系統容易被攻擊者利用。 3.建議改進措施： (1) 建立元件管理機制，確保所有元件定期更新到最新版本。 (2) 使用自動化工具來檢測過時元件。 (3) 移除未使用的第三方程式庫或模組。
A01：權限控制失效	1.弱點數量：高風險 2 項，中風險 8 項。 2.問題描述：權限控制失效會導致攻擊者未經授權即可存取敏感資料或進行未授權的操作。 3.建議改進措施： (1) 實施基於角色的權限控制。 (2) 確保每次操作都進行充分的權限驗證。 (3) 避免直接暴露內部資料連結，並定期進行權限檢查。
A03：注入攻擊	1.弱點數量：高風險 1 項，中風險 1 項。 2.問題描述：SQL 注入、命令注入等問題會讓攻擊者能夠直接控制後端資料庫或系統。 3.建議改進措施： (1) 所有使用者輸入應進行參數化處理，避免直接嵌入到查詢語句中。 (2) 對所有輸入進行嚴格的白名單驗證。

A04：不安全設計	1.弱點數量：中風險 4 項。 2.問題描述：系統架構或設計未充分考慮安全性，導致潛在的攻擊面。 3.建議改進措施：在設計完成階段要委託第三方進行原碼檢測。

3.4 網頁弱點複掃結果分析

依據表 5 之建議，進行網頁改善及檢測，並接續執行弱點複掃，複掃結果如圖 5 所示。

項次	目標	弱點種類			
		危急	高	中	低
1	A01:權限控制失效	0	0	3	
2	A02:加密機制失效	0	0	0	
3	A03:注入式攻擊	0	0	0	
4	A04:不安全設計	0	0	0	
5	A05:安全設定缺陷	0	0	1	
6	A06:危險或過舊的元件	0	0	0	
7	A07:認證及驗證機制失效	0	0	0	
8	A08:軟體及資料完整性失效	0	0	1	
9	A09:資安記錄及監控失效	0	0	0	
10	A10:伺服端請求偽造	0	0	0	
總計		0	0	5	

圖 5 網頁弱點種類複掃結果統計

3.4.1 弱點複掃總結

OWASP TOP 10 分類下的弱點評估結果，主要問題包含，本次網頁弱點複測掃描中風險弱點有 5 項，集中於 3 個分類，依序為 A01 權限控制失效(共 3 項)、A05 不安全設計(共 1 項) 與 A08 軟體及資料完整性失效(共 1 項)，這表示系統主要弱點來自於權限控制機制、安全設定缺陷以及使用過時或漏洞的軟體組件問題。

3.4.2 總體改進建議

1. 優先處理 A01 權限控制失效問題：

   (1)此問題的數量最多，且影響範圍廣，應列為首要處理項目。

   (2)檢查敏感資源存取規則，並測試所有角色與權限設定的有效性。

2. 全面優化安全配置：根據 A05 的建議，檢查伺服器與應用層安全配置，避免使用不安全的預設配置。

3. 定期更新與驗證元件：解決 A08 的問題，定期檢查與更新軟體元件，並針對資料完整性設置更嚴密的保護機制。

四、結論與建議

隨著數位科技的普及，網頁應用程式已成為企業與組織日常運作的關鍵工具，但同時也面臨日益嚴峻的網路安全威脅。駭客攻擊技術不斷演進，常見的攻擊手法如 SQL 注入、跨站腳本攻擊（XSS）及不安全的身份驗證機制，皆可能導致資料外洩與系統入侵，進而造成企業營運風險。為了提升網頁應用程式的安全性，本研究探討提升網頁資安防禦強度，包括建立更新機制、強化權限管理、提升開發人員安全技能、完善弱點掃描與複測機制等，藉此減少網頁應用程式的安全弱點，提升整體防禦能力，降低資安風險。

除了技術層面的強化，本研究亦關注資安管理機制的建立與改進。透過設立資安預警資訊群組，持續追蹤與通報最新資安威脅，確保修復工作的時效性與完整性。此外，檢測報告的準確性對於弱點修補至關重要，因此，強調報告審核機制與專業審查標準，確保資安人員具備 OWASP TOP 10 的專業知識與相關證照，提升弱點識別與修復建議的正確性。面對不斷演變的網路攻擊手法，資安防護必須持續改進與更新，本研究期望透過多層次的防禦措施，為組織建立更安全的網頁應用環境，以下是本研究之建議。

1. 建立更新機制：確保網頁應用程式、作業系統與相關應用軟體的套件定期更新，避免因使用危險或過時元件而導致的安全弱點，降低被攻擊風險。

2. 限制最小權限：在不影響應用程式正常運作的前提下，實施最小使用權限原則，防範因權限控管失效而引發的安全問題，提升系統的整體防禦能力。

3. 提升開發人員技能：強化對外服務應用程式的開發能力，鼓勵工程師具備 OWASP TOP 10 防禦經驗或取得相關證照，從源頭減少安全弱點，提升程式碼質量與安全性。

4. 掃描與複測機制：在進行網頁弱點初次掃描後，需執行複測以確認弱點修補的成效，確保已識別的問題獲得妥善解決。然而，即使完成複掃，仍可能存在未被完全修復的弱點，故需配合相關輔助機制。本研究特別設立資安預警資訊群組(如圖 6)，負責持續追蹤弱點修復進度，並即時通報可能的資安威脅。

5. 報告審核與專業要求：自動生成的檢測報告需經人工審核排除誤判。審核人員需熟悉前後端開發技術(如 HTML、CSS、JavaScript)與 OWASP TOP 10 等安全標準，具備實際弱點驗證經驗，並取得相關證照，才能精準識別弱點並提供修復建議。

6. 持續改進：整體資訊安全防禦架構圖如下圖所示，本研究網頁弱點掃描範圍位於圖中黃色區域，更能明瞭資安領域的廣闊，隨著技術與駭客手法的進化，資安防護需要不斷更新與改進。如何有效應對新威脅並強化防禦策略，將是永無止境的挑戰。

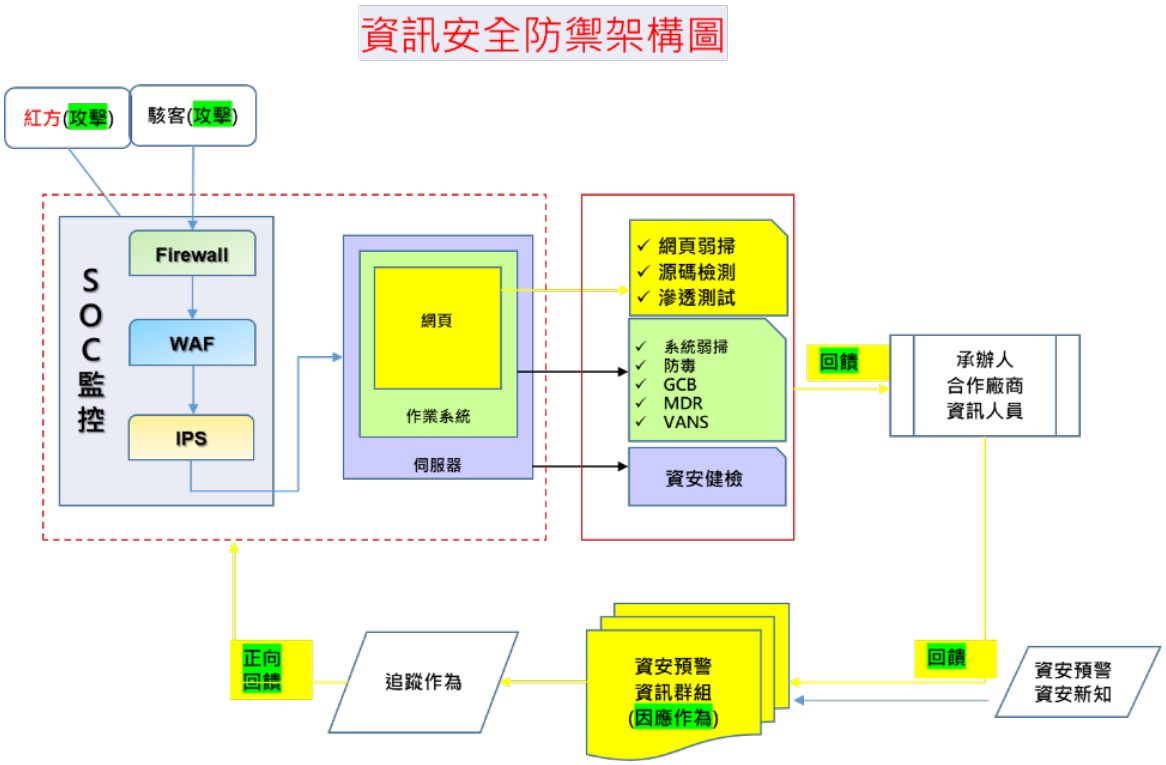

圖 6 資訊安全防禦架構圖(本計畫產出)

參考文獻

1. 法務部，全國法規資料庫，資通安全管理法，https://law.moj.gov.tw/LawClass/LawAll.aspx?pcode=A0030297。
2. 法務部，全國法規資料庫，資通安全責任等級分級辦法 https://law.moj.gov.tw/LawClass/LawAll.aspx?pcode=A0030304。
3. 國家資通安全研究院，https://www.nics.nat.gov.tw/。
4. 國家資通安全研究院，113 年第 3 季資通安全技術報告，https://www.nics.nat.gov.tw/cybersecurity_resources/publications/Technical_Reports/。
5. Vulnerabilities By Types/Categories，https://www.cvedetails.com/vulnerabilities-by-types.php。
6. Shital Dilip Jadhav.(2024).Exploring Ethical Hacking: Tools, Techniques, and Defensive Strategies.
7. CWE (Common Weakness Enumeration)，https://cwe.mitre.org/data/index.html。
8. OWASP TOP 10 2021，https://owasp.org/Top10/zh_TW/A00_2021_Introduction/。
9. iThome，https://www.ithome.com.tw/pr/150400。
10. MITRE ATT&CK，https://attack.mitre.org。

11. Cyber Kill Chain，https://www.lockheedmartin.com/en-us/capabilities/cyber/cyber-kill-chain.html。
12. 臺灣電腦網路危機處理暨協調中心，臺灣漏洞揭露平臺 (TVN)，https://www.twcert.org.tw/tw/np-131-1.html。
13. CVSS，https://www.first.org/cvss/v4.0/specification-document。
14. Sathvik Babu Mundru.(2023).Web Application Security through Comprehensive Vulnerability Assessment.