研　習　紀　錄

隨著企業數位轉型與雲端服務的普及，網頁應用程式（Web Applications）已成為駭客入侵組織內部網路的主要破口。在眾多資安標準中，OWASP（Open Worldwide Application Security Project）所發布的 OWASP Top 10 被視為檢視網頁安全性的黃金標準，它揭露了當前最嚴峻的關鍵安全風險。

在目前的網頁攻擊手法中，失效的存取控制（Broken Access Control）躍升為首要威脅。這類漏洞發生在系統未能正確執行權限驗證，導致攻擊者可以存取未經授權的功能或數據。例如，攻擊者透過修改 URL 或 API 參數，進行垂直越權（Privilege Escalation）取得管理員權限，或是水平越權（IDOR, Insecure Direct Object References）竊取其他使用者的個資。

其次為加密機制失效（Cryptographic Failures），即過去所稱的敏感資料外洩（Sensitive Data Exposure），也是重災區。這通常源於使用弱加密演算法、預設密碼，或是在傳輸過程中未強制使用 HTTPS/TLS 協定，導致機敏資料以明文（Plaintext）傳輸而被中間人攻擊（MitM）攔截。

經典的注入攻擊雖然排名稍有變動，但威脅不減。最著名的 SQL 注入（SQL Injection, SQLi）允許駭客在輸入欄位中惡意植入資料庫指令，進而竊取或破壞整個資料庫。此外，現代網頁前端常遇到的 跨站腳本攻擊（Cross-Site Scripting, XSS）雖在 2021 年版被歸類於注入類別，但仍是客戶端攻擊的主流，攻擊者透過惡意腳本劫持使用者的 Session ID 或進行釣魚。

另一個值得關注的是危險或過舊的元件（Vulnerable and Outdated Components）。現代開發大量依賴開源函式庫與 Frameworks，若未及時修補如 Log4j 這類已知漏洞（CVE），駭客便能輕易利用現成的攻擊腳本（Exploit）進行自動化攻擊。

面對這些威脅，單靠防火牆已不足夠。企業必須在軟體開發生命週期（SDLC）中導入安全檢測，實踐 DevSecOps。透過靜態應用程式安全測試（SAST）、動態測試（DAST）以及定期的滲透測試（Penetration Testing），才能有效修補安全設定錯誤（Security Misconfiguration），構建具備韌性的網頁應用環境。

備註：一、研習紀錄內容請用電腦繕打。
二、研習紀錄請先上傳（校園入口網　其他類 E 話系統　研討會心得上傳），連同補助教師舉辦校內研習申請表及研習相關資料影本，並經單位主管簽章後，送人事室核銷。

記錄者簽章	單位主管簽章	人事室主任簽章
年　月　日	年　月　日	年　月　日