支援行動裝置 APP 及建置好用上手

政府單位善用 Checkmarx 多找出上千個弱點
補強既有阿碼源碼檢測機制

撰文 | 叡揚資訊　行銷部

對於公部門精簡的 IT 單位來說，系統開發以委外為主，工作權責以管理為重，故須建立一套審核機制建立內控制度，以符合 ISMS、ISO27001 標準。尤其，本次受訪機關為駭客攻擊主要目標，如何從基本的源碼檢測鞏固防禦更是不可輕忽之本。

從阿碼科技到 Checkmarx 持續強化源碼安全檢測

隨著資安概念成熟，以 WAF（網站應用程式防火牆）防禦之作法已經趨近國外以監控為主，治本的源碼檢測成為最佳 Solution。過去，該機關遵循資安指標落實系統弱點掃描結果，但隨著源碼掃描工具日新月異，原工具不但維護不易，檢測效果也落後由叡揚資訊代理的全球重量級源碼掃描工具—Checkmarx，故今年導入 Checkmarx。導入後，不但多找出各系統上百至上千個弱點，同時解決疑似駭客入侵的網站弱點（原源碼檢測工具無法找出），大幅增加該機關防護能力。

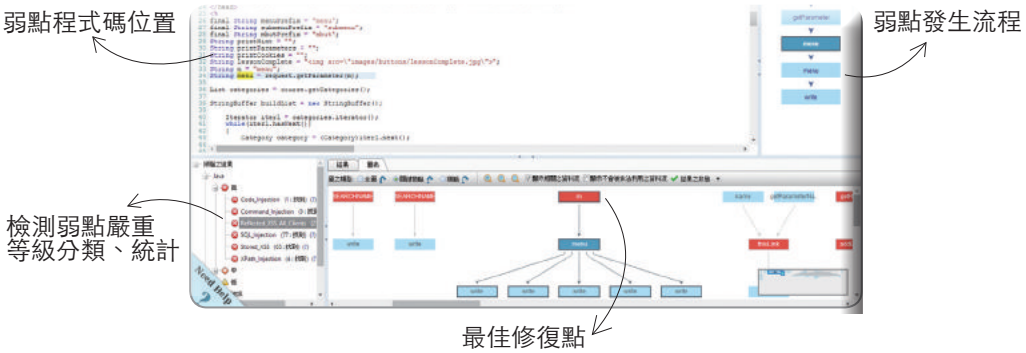
Checkmarx 多掃出上百上千弱點

承辦人坦言，源碼掃描的確是甜蜜的負擔，「但長遠來看，沒有要求委外廠商將原始程式碼的安全性考慮進去，或無法落實把關，日後發現問題時，全盤整修恐怕會花上更多成本。」承辦人更直言，「引進 Checkmarx 之後，發現上百上千弱點時，負責此專案的承辦人會面對更多準時上線壓力，不過感謝叡揚資訊的專業服務，會及時協助判斷灰色地帶及建議，舒緩修復壓力。」

Checkmarx 領先支援行動裝置 APP

「轉換成 Checkmarx 的考量主因包括：1. 既有工具（阿碼科技 Armorize）被併購後發展方向轉變。2. 涵蓋率及準確率較高。3. 支援行動裝置 APP，且不受開發環境版本限制的特性，領

一目了然 簡單好操作 AP、稽核愛用的源碼掃描介面

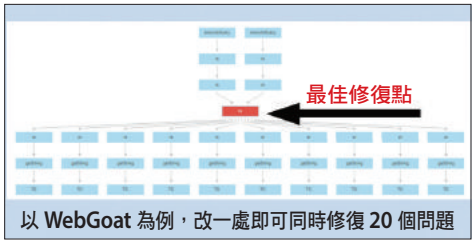


先所有源碼掃描產品。4. 簡易上手、不用高複雜度的建置環境，使用單位學習快速。5. 國際大廠使用，如：美國陸軍、Salesforce、Samsung、CocaCola 等。承辦人強調，再加上叡揚資訊在源碼檢測經驗豐富，產業別廣且深，專業服務形象大大加分！

隨著公部門服務民眾管道多元化趨勢，APP 平台的互動及資訊交流也愈趨頻繁，「不論是 Android、iOS 或未來 Windows，都可以用 Checkmarx 檢查源碼安全性，不然原有工具無法達成。」承辦人表示，人工檢核難度高且執行效率不彰，需藉由源碼掃描工具來執行，故檢測效能、支援多種系統平臺、程式語言和開發框架之功能相當重要，真正落實源碼掃描之效益。

簡易好上手
委外廠商也好用

「我們比較常用的語言為 JAVA、JSP、VB。」面對 10 多個委外廠商，數十套系統在運作，Checkmarx 的簡易上手不僅我們讚賞，委外廠商解讀結果報表也不吃力。「源碼健檢完後，我們會跟廠商討論修改時間，



以 WebGoat 為例，改一處即可同時修復 20 個問題

通常是全部都要改完，如果不行就是要更換元件。」承辦人表示，好用的源碼檢測工具可以讓甲乙雙方合作愉快，也不會造成額外的壓力給內部同仁，讓專案可以更順利進行。

精準找出漏洞所在的收斂功能
舒緩修改壓力

另外，Checkmarx 具備精準找出漏洞所在的收斂功能，並指出共同原因點，可同步自動修復相關弱點，大大提升開發人員修改效能。

「實際上，太複雜的源碼工具可能會導致內部反彈及低使用率，Checkmarx 目前也是市面上少數可以容易檢測 APP 安全之產品，加上簡易好操作上手的確很符合我們組織需求。」承辦人笑笑地說，有鑑於公部門容易遭受駭客攻擊，儘管已有建置 WAF、執行滲透測試等，源碼檢測的確是必要之務，讓防護盡可能完善。

更多客戶案例、資安資源 http://www.gss.com.tw/index.php/focus/security