導入源碼檢測機制 建立安全程式開發觀念

歐付寶藉 Checkmarx 打造安全第三方支付平台

撰文 | 叡揚資訊 行銷部

一分鐘看問題

導入單位

歐付寶電子支付股份有限公司

導入產品

Checkmarx 源碼安全檢測工具

面臨挑戰

- 平台交易牽涉金流與個資，公司所有系統不容許有任何風險或漏洞。
- 開發語言多，開發環境複雜，包括：ASP.NET、PHP、Node.js、iOS 和 Android 等，需要透過系統化的源碼檢測，杜絕所有風險與弱點。

導入效益

- 補強人工 Code review 的限制，與黑箱弱掃搭配應用
- Checkmarx 搭配資安、開發團隊專業分工，徹底發揮源碼檢測工具效益。
- 容易且快速的發現軟體的風險程度，進而評估系統修補的緊急性，也降低修補難度。
- 培養內部開發人員安全程式開發觀念。

2011 年成立的歐付寶屬金融科技業，業務範圍與金流息息相關，對資安的需求比照金融業網路銀行，因此特別重視軟體資安，除了防範各種可能發生的資安風險，同時也建立民眾與客戶對歐付寶的信任。歐付寶受電子支付機構管理條例規範，目前已導入 ISO27001 認證，每年需進行 PCI-DSS 安全認證稽核。除上述規範外，也希望建立內部安全程式開發機制以及培養開發人員安全程式開發的概念。

為強化源碼檢測機制 不採人工 Code Review

歐付寶資訊處副總經理梁維誠說：「我從事軟體開發多年，曾在某大型會議上，資深工程師分享 Source Code，其中竟有明顯的 SQL Injection 。這事讓我明白，開發人員功力高低關係到系統安全，但即便是資深人員都可能犯錯，所以全面檢視程式碼是有必要的。雖然開發人員都在公司自建的 Framework 下開發，雖能對源碼開發安全有基本框架規範，但還是有

歐付寶資訊處副總經理梁維誠

風險，人工 Code Review 不夠全面，希望由系統化源碼檢測機制，防止各種風險。」

叡揚資安團隊建議 Checkmarx 工具特性成採用關鍵

歐付寶目前正處快速成長期，開發人員人數眾多，且開發環境也相對複雜，包含 ASP.NET、PHP、Node.js、iOS 和 Android 等。梁副總回想當初評估源碼檢測工具時，比較 Checkmarx、Open Source 和國外工具。後來叡揚資安團隊提出 **Checkmarx 三大優點：不需重建開發環境即可檢測，提升使用的方便性；語言支援度高，可檢測範圍大；檢測報告易讀，清楚直指弱點所在**，並於 POC 時驗證，獲得歐付寶青睞。

源碼檢測報告非照單全收 資安專家評估才是重點

歐付寶建立完善團隊分工，將源碼檢測工作獨立於 MIS 和 AP 團隊之外，由專責資安工程師負責源碼檢測報表，再說明需修改的弱點，同時提供最新漏洞資訊做內部教育訓練。梁副總分享：「資安風險應全盤考量，源碼檢測這類資安工具，雖可協助快速判斷軟體是否隱含資安威脅，但掃描報告不建議照單全收，應檢視實際風險再評估如何利用修改原始碼或搭配其他資安措施解決。」全盤考量資安風險而非片面追求軟體弱點檢測報告零風險的思維，是許多國際大型企業導入源碼檢測的實務做法。

關注資安議題 必須杜絕所有漏洞

歐付寶所有系統不容許任何弱點和風險，但因系統包含多種平台與程式語言，甚至還有許多的舊系統，而開發新功能時程較為緊急，往往無法兼顧修補原始碼掃描報告的全部弱點，在資安政策考量下，採漸進式導入。

先針對付款和會員兩系統進行源碼檢測，再導入所有系統，**並擬定4項導入目標：1.優先修補確定的高風險弱點2.修補中風險以上弱點 3.定期掃描並修補 4.上版前皆須經掃描且修補後方能上版**，未來也會結合 Jenkins 機制。

持續強化資安架構

歐付寶的資訊安全管理機制因導入Checkmarx而有效發現軟體專案風險。未來，也將逐步完善內部資安架構，也希望叡揚資安團隊能持續協助提供源碼檢測教育訓練及顧問建議，強化開發人員的資安能力。