淺談軟體安全

作者 | 叡揚資訊 資訊安全事業處 產品顧問

根據資訊安全相關組織 x-force、WASC、OWASP、CWE 所提出的年度公開報告，應用程式與網頁應用程式所產生的資訊安全漏洞處於居高不下的狀態。應用程式的安全威脅主要是來自於未經驗證輸入(Input Validation)的弱點，造成 SQL Injection、XSS 及 Command Injection 等攻擊。這些利用程式弱點所產生的攻擊，其主因在於程式開發者在軟體開發生命週期中，未能考慮軟體安全的因素，像是對程式中的弱點無所認知、資安的意識不足及可能濫用第三方套件及應用程式版本過舊(例如 Interner Explorer 版本)等所造成的漏洞問題。

依 x-force 整理出的年度漏洞通報成長表，如圖 1，顯示應用程式的安全漏洞已是逐年呈等比級數之增長，IT 人員每年付出更多時間，幫軟體做漏洞的修正更新。要如何降低每年的修補所花的時間、金錢與工作量，提升軟體安全的要求便因應而生，而確保軟體符合安全標準，提升軟體品質，便是一個重要的議題。

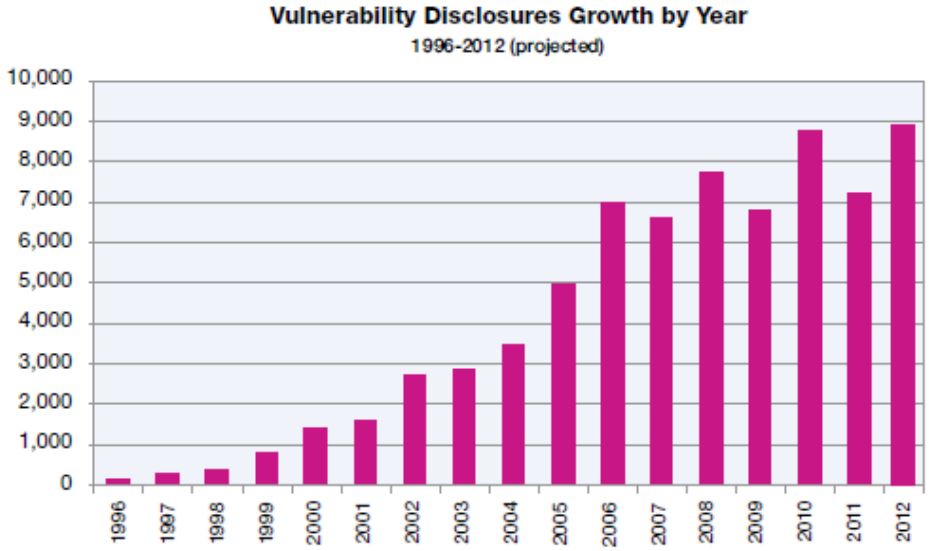

圖 1.年度漏洞通報成長表

眾所周知，資安是相對的，而非絕對的，由於科技不斷的演變，駭客的攻擊手法不斷的推陳出新，以至於應用系統安全的防護需不斷的更新，來保護應用系統的有效運作，所以需要相關機制及軟硬體工具來做為輔助基準，

GSS 叡揚資訊 Galaxy Software Services
台北總公司：10461 台北市中山區德惠街 9 號 5 樓 TEL：(02)2586-7890 FAX：(02)2586-8787
高雄辦公室：80453 高雄市明華路 315 號 13 樓之 3 TEL：(07)586-6195
海外據點：上海、北京 營業範圍：兩岸三地及日本 www.gss.com.tw

但在這之前要先確保使用的應用軟硬體工具及機制是符合可用性、可靠性以及完整性，以符合軟體安全保證指標的有效檢測，降低軟體風險。

在軟體安全理論中，其中以 McGraw 所提出的 Touchpoints 最為著名，軟體安全是由三大支柱所構成的，分別是風險管理(Risk Management)、知識(Knowledge)及軟體安全的控制措施 (Touchpoints)，並將軟體安全所有實務行為滙整成的 7 個控制措施，包含：濫用案例(Abuse Cases)、安全需求制定(Security Requirements)、風險分析(Risk Analysis)、基於風險分析的安全測試(Risk-Based Security Tests)、程式碼檢測(Code Review)、滲透測試(Penetration Testing)和安全操作(Security Operations)；並將 7 個控制措施於適當時機點介入軟體發展生命週期，從需求與使用案例(Requirements And Use Cases)、設計與架構(Architecture And Design)、測試計畫(Test Plans)、程式碼(Code)、測試及測試結果(Test And Test Results)、到上線後系統使用的回饋(Feedback From The Field)，讓每一個發展階段都與軟體安全有著密切的關係，如圖 2。

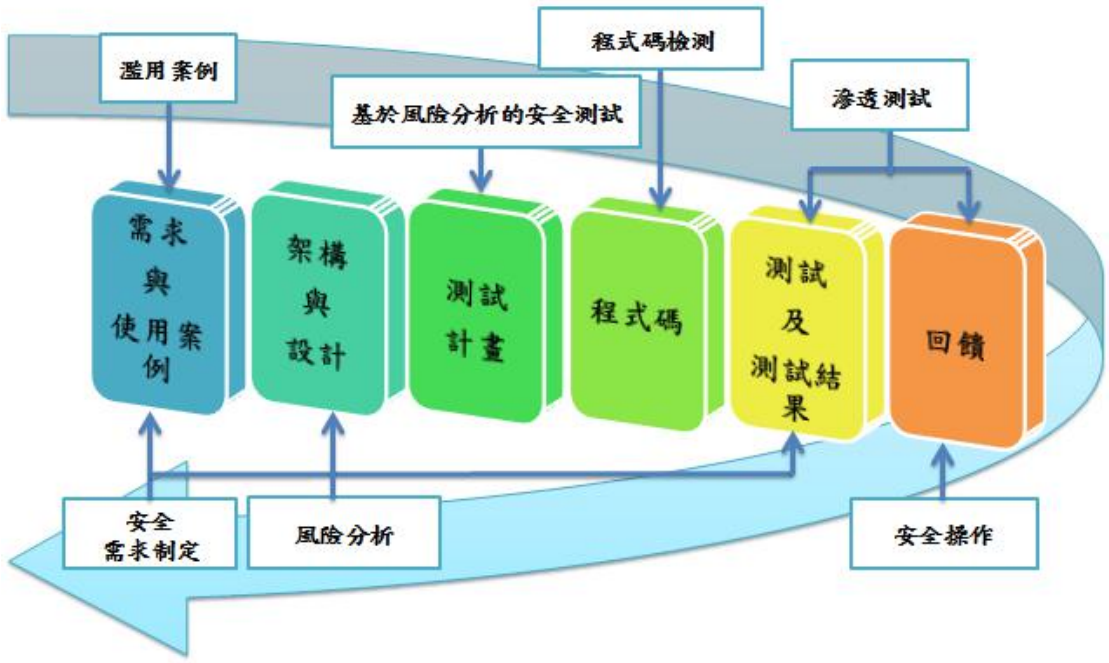

圖 2.McGraw Touchpoint

一個新的軟體專案開發流程，通常會依以往的專案經驗，於制定安全需求的同時排除不好的過往案例，專案的流程設計架構是否會造成安全問題，需進行風險分析的安全測試，對於專案程式的部份進行品質面及安全面的風險分析，盡可能的修正風險問題，並模擬上線後的測試以及使用者可能的不安全操作，所造成的問題給予回報。

GSS 叡揚資訊 Galaxy Software Services
台北總公司：10461 台北市中山區德惠街 9 號 5 樓 TEL：(02)2586-7890 FAX：(02)2586-8787
高雄辦公室：80453 高雄市明華路 315 號 13 樓之 3 TEL：(07)586-6195
海外據點：上海、北京 營業範圍：兩岸三地及日本 www.gss.com.tw

在軟體開發流程中的程式碼檢測及滲透測試這 2 個控制措施，我們可藉由白箱的源碼檢測工具 HP Fortify SCA 及黑箱滲透測試工具 WebInspect，做為軟體安全的輔助稽核工具，主要是希望在整個專案從程式開發到完成階段，將專案程式碼可能造成資安風險的漏洞因素考慮進去，則可以事先達到避免因安全漏洞而產生的問題。

白箱 Fortify SCA 主要是從系統內部協助軟體應用程式識別安全漏洞，除了使用白箱測試以外，還需要透過黑箱測試 WebInspect 從外部進行檢測，找出應用程式可能發生的弱點，以補足白箱測試的一些不足之處。不安全程式漏洞會導致系統的不運作或是大量情資的被竊取及外洩，造成業主及客戶的不便，再加上政府於 2012/10/1 實施個人資料保護法，對於資料的蒐集、處理及利用都需符合個資法規定，若經由第三方不法取得個人資料，導致業主洩漏個資，影響客戶權益，業主則需面臨罰緩及刑責，最高可被求償 2 億及 5 年刑期。

由於近年網路的興盛，基於網路應用的軟體服務越來越多，資安威脅已不像早期都著重於網路層，而是都轉向到了應用層的軟體應用程式，若惡意使用者對軟體應用程式加以揣測攻擊，並經由其漏洞，對該網路應用程式進行不當行為，例如竊取大量資料或影響網站營運，所以需即時修改應用程式弱點，以維護應用程式的正常營運，建議對專案應用程式定期進行黑白箱檢測並修正弱點，以確保資訊安全防護是持續且有效地進行運作。

GSS 叡揚資訊 Galaxy Software Services
台北總公司：10461 台北市中山區德惠街 9 號 5 樓　TEL：(02)2586-7890　FAX：(02)2586-8787
高雄辦公室：80453 高雄市明華路 315 號 13 樓之 3　TEL：(07)586-6195
海外據點：上海、北京　營業範圍：兩岸三地及日本　www.gss.com.tw