健保局應用程式建置流程強化

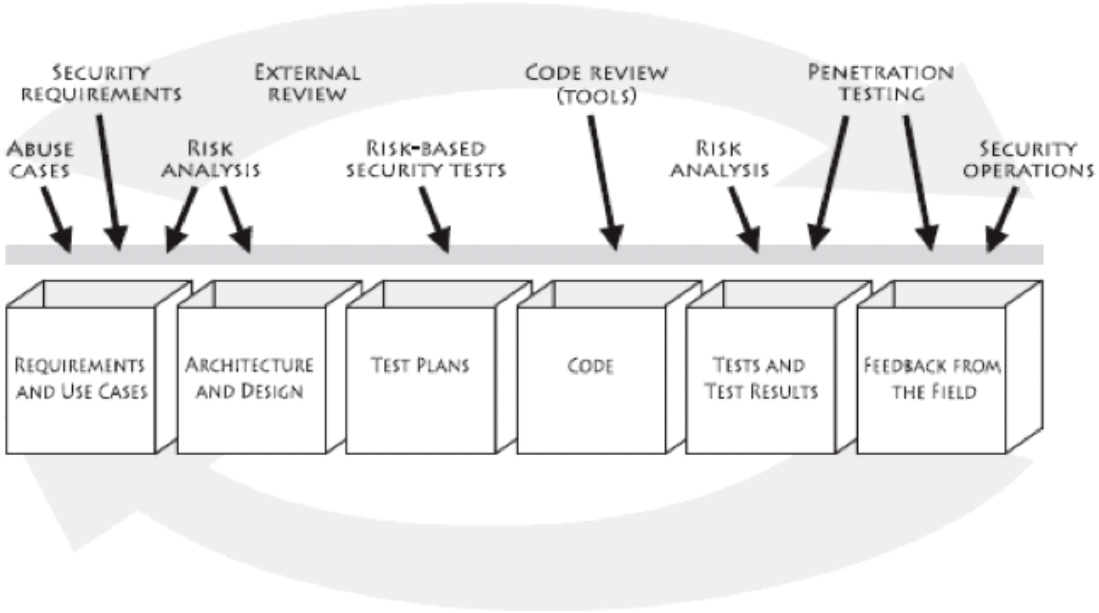
「安全」是軟體工程目前最流行的名詞

作軟體的人都知道，軟體的生命週期(SDLC)不外乎分成規劃、分析、設計、建置、維護五大領域。傳統軟體工程著重功能面的完整度，各系統功能是否能達到原始設計需求。安全並非當時關注的議題。直到.com 網路潮後，網站興起正好給駭客實驗攻擊的溫床，SQL Injection 與 Cross-Site Scripting 攻擊陸續出現，給了系統開發者當頭棒喝。

原來軟體開發並非功能完整就好

近幾年學者提倡 SSDLC(Secure Software Development Life Cycle)將傳統 SDLC 注入新的元素，藉由在傳統五大領域放入安全相關工作項目，就可以實踐應用系統安全。

下圖為安全開發流程非常具有專精的一位學者與科學家 Gary McGraw ，他提倡的安全軟體開發流程。



GSS Galaxy Software Services 叡揚資訊 地址：台北市 10461 中山區德惠街 9 號 5 樓 電話：+886-2-2586-7890 傳真：+886-2-2586-8787

SSDLC 儼然成為一門新興的知識領域，連 ISC^2 都推出了 CSSLP，推行 SSDLC 的技術人員可取得認證證明自己的技術能力。國內未曾聽聞有開發團隊導入整套 SSDLC 開發的方法論，一來開發時程拉長影響交付時間，二來資源不足成本提高。目前業界最常見的作法就是導入檢測工具。從之前的黑箱工具，漸漸轉移到目前熱門的白箱工具，現在開發人員都知道，白箱工具的確比黑箱工具涵蓋度高，精準度也高。

只導入檢測工具，就可以解決應用程式安全問題？當然不是。這好比從機車騎士晉升到有車階級，但是卻買了安全配備不足的車子。為了讓檢測工具能正確的運行，組織必須有配套方法，將檢測工具真正的使用在對的地方與時機。

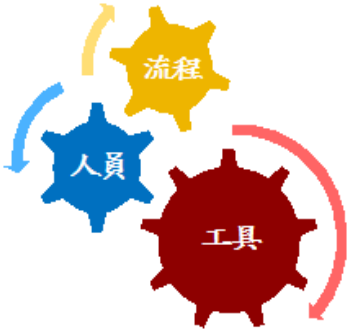
整體開發考量

開發應用程式涵蓋面向眾多，舉凡人員、流程、工具、準則、意識都必須加以考慮。針對應用程式安全性而言，開發人員的素質，安全意識、開發流程修正、開發工具與檢測工具的選用、應用程式能否上線的準則，都必須整體考量。

叡揚資訊重要的伙伴客戶--健保局，瞭解應用程式安全的重要，針對資訊開發的安全性，委託叡揚資訊設計一套搭配現有開發與版本更新建置流程的安全檢測機制，作為管控應用系統開發安全的依據。

PPT

叡揚資訊認為，人員(People)、流程(Process)與技術(Technology)為資訊安全之三大基石，我們在健保局專案針對各個領域的安全性，設計了不同的專案目標：



- 提升專案程式碼安全品質
- 專案程式碼安全弱點修正
- 改善目前不安全的程式撰寫方式
- 建立原始碼弱點檢測處理標準作業程序
- 訂定對外服務網站應用程式安全標準供局內同仁及委外開發廠商遵循
- 結合現行 Web 軟體開發程序，建立軟體開發流程檢測機制
- 建立應用程式上線作業準則
- 建立局內同仁與開發人員安全程式碼學習平台(Secure Coding Standards)
- 提升資訊安全意識，進行應用程式安全開發教育訓練
- 進行技術轉移，培訓種子教官，將程式碼安全開發觀念與工具使用技巧深植組織內部

GSS Galaxy Software Services 叡揚資訊 地址：台北市 10461 中山區德惠街 9 號 5 樓 電話：+886-2-2586-7890 傳真：+886-2-2586-8787

規劃設計

健保局選擇 Fortify SCA 作為應用程式檢測工具，著眼於 SCA 是目前白箱檢測工具功能最強大，檢測項目最廣泛也最深入。此外叡揚資訊提供配套之導入服務，依據客戶現有作業流程與作業環境，進行客戶需求訪談，為客戶設計目前最適合的安全機制。

外包應用程式開發目前是個趨勢，健保局也不例外。外包開發人力的管理並不容易，除了應用程式功能開發滿足需求，若再加入安全需求，所需資源與技術並非業主可獨立負擔。叡揚資訊提供客戶「導入服務」，由訪談結果衍生出設計概念，搭配叡揚特有的安全程式碼撰寫顧問服務，與流程改善計畫，將原本程式碼建置流程，改良為有 Fortify SCA 把關的安全建置流程，同時提升承辦人與外包開發人員的安全意識與安全程式碼撰寫能力。

健保局應用系統除了開放給對全省醫療院所、醫療單位與投保單位，還有提供民眾醫療與健保資訊的網站。經過專業顧問的評估，將健保局應用程式分為三個安全類別，不同的應用程式依據開放對象與屬性，給予不同的安全類別等級。不同安全類別等級之應用程式，有對應的上線或建置門檻標準，未達到安全標準皆無法上線或建置。

Fortify 檢測方式非常彈性，除了有圖形介面供使用者手動操作之外，叡揚特地為了不同需求使用者客製自動化批次執行檢測。有了自動化批次檢測，使用者可隨時依據需求設定掃描時間，每日進行一次或數次應用程式檢測。

對於人員的資安意識提升，和資安技術能力提升，是本專案最重要的人力訓練項目。現有健保局人員已經有基礎的資安意識，如何將檢測工具導入，搭配應用程式建置流程，讓承辦人，或是應用程式開發人員提升資安能量是我們的目標。針對健保局內使用的開發工具與應用程式，經過顧問專業建議與評估，針對找出來對應的弱點與風險，設計一系列安全程式碼開發課程，與基礎的資訊安全教育訓練課程，如此可對應下藥，加速弱點的消除。

除此之外，我們為健保局設計安全程式碼教學平台，包括.NET 與 Java 的 Secure Coding Standard，與 Secure Coding 的 e-Learning 平台，讓局內所有同仁可以隨時隨地，不限時間的上課，開發人員在進行應用程式開發時，有安全程式的開發準則可遵循，面對可能發生資安問題的程式碼不再手忙腳亂，到處尋找參考資料。而我們針對各應用程式承辦人，進行較密集的教育訓練與會議，為的就是讓他們成為健保局內資訊安全的先鋒與種子教官，我們稱之為「技術轉移」。不但將叡揚的資訊安全技術傳授給他們，對於工具的使用也相當熟稔，可作為健保局內種子教官，將本次專案的精髓傳遞給局內其他同仁。

GSS Galaxy Software Services 叡揚資訊 地址：台北市 10461 中山區德惠街 9 號 5 樓 電話：+886-2-2586-7890 傳真：+886-2-2586-8787

全新的體驗

藉由導入安全機制到開發與建置流程，搭配精心設計的作業程序與準則，對於健保局、叡揚資訊和台灣軟體安全開發來說，又往前邁開了一大步。

GSS 叡揚資訊 Galaxy Software Services 地址：台北市 10461 中山區德惠街 9 號 5 樓 電話：+886-2-2586-7890 傳真：+886-2-2586-8787