出國報告（出國類別：國際會議）

出席 2014 年網路應用程式安全組織（OWASP）官方亞洲年會出國報告

服務機關：財政部財政資訊中心

姓名職稱：莊景全設計師

派赴國家：日本

出國期間：103 年 3 月 19 日至 103 年 3 月 20 日

報告日期：103 年 5 月 22 日

摘　要

今年網路應用程式安全組織，簡稱 OWASP（Open Web Application Security Project）亞洲年會自 2014 年 3 月 19 日至 3 月 20 日，於日本東京 Sola City 國際會議中心舉行，OWASP 係一開放社群、非營利性組織，目前全球有 82 個分會近萬名會員，其主要目標是研議協助解決 Web 應用程式相關安全標準、工具與技術文件，長期致力於協助政府或企業瞭解並改善網頁應用程式與網頁服務的安全性。

由於智慧型行動裝置持有率越來越普及，個人隱私資訊外洩或病毒入侵手機等隱憂亦如影隨形，尤其機關在開發行動 App 應用程式時，應留意程式是否存在安全弱點與漏洞，避免民眾安裝 App 應用程式後遭病毒、駭客入侵，造成隱私資訊外洩，因此如何撰寫出安全的程式碼係 App 安全的第一道防線，而透過 OWASP 所提出的 OWASP Top 10 Mobile Risks 十大行動安全風險，了解應用程式開發時之注意事項，協助機關開發出安全的應用程式，降低病毒及駭客入侵之威脅。

目　次

壹、目的

資訊科技與網際網路蓬勃發展，使資通訊科技應用儼然已成為每人日常生活中的一部份，令人擔憂的是資訊科技帶來的資訊安全問題，尤其我國政經情勢特殊，面對全球複雜多變的資訊環境，以及日益嚴重的資訊安全威脅，機關應持續掌握新知趨勢與精進資訊安全防護工作。

當機關透過 Web 開放網頁服務時，就必須讓來自全球的網頁請求進入機關網頁伺服器，此時駭客可能藉由隱藏在合法的網頁請求中，通過防火牆或其他防禦系統的偵測，進入機關內部或藉由機關網站充當跳板與中繼站，向其他受害者發動攻擊。因此網頁程式碼亦須成為機關的安全防護之一，當機關網頁服務的規模與複雜性增加時，暴露於外之風險亦逐漸增加。

然而面對網路、雲端、行動通訊持續發展與普及，機關運用資訊科技創新業務，提升行政效率與便民服務，不斷開發網路應用程式與行動裝置 App 服務供民眾使用，該應用程式能正確提供服務外，更不能讓機敏資料或個人隱私資料外洩。如何開發安全之應用程式及掌握資訊安全趨勢，為機關重要之資訊安全議題。

貳、過程

網路應用程式安全組織，簡稱 OWASP（Open Web Application Security Project）OWASP 係一開放社群、非營利性組織，目前全球有 82 個分會近萬名會員，其主要目標是研議協助解決 Web 應用程式相關安全標準、工具及技術文件，長期致力於協助政府或企業瞭解並改善網頁應用程式與網頁服務的安全性。

美國聯邦貿易委員會(FTC)強烈建議所有企業需遵循 OWASP 所發布的十大 Web 弱點防護守則，美國國防部亦將其列為最佳實務，國際信用卡資料安全技術 PCI 標準更將其列為必要元件。目前 OWASP 有 30 多個進行中的計畫，包括最知名的 OWASP Top 10(十大 Web 弱點)、WebGoat(代罪羔羊)練習平台、安全 PHP/Java/ASP.Net 等計畫，針對不同的軟體安全問題在進行討論與研究。

本次 OWASP 亞洲年會(OWASP AppSec APAC 2014)議程自 2014 年 3 月 19 日至 3 月 20 日，為期 2 日，於日本東京 Sola City 國際會議中心舉行，其中包含 OWASP 參考指引說明、網站存取控制、XSS 攻擊及 OWASP TOP10 討論等議題，OWASP Top10 目前被業界視為網站安全參考指標，亦為本次會議重點。另行動通訊發展及智慧型行動裝置之持有率日益普及，智慧行動裝置延伸出之資安市場需求從 2010 年 4 億美元，預估將成長至 2015 年 19 億美元。(詳如圖 1)

圖 1、2010-2015 年全球智慧手機資安市場規模

伴隨著智慧型行動裝置的普及、雲端技術的發展，使用者與應用程式開發者之資訊操作模式已逐漸從主機平台移至可攜式行動裝置或智慧型手機，而本機關致力於創新開發各項行動 App 便民服務，如：財政園地 App、發票精靈 App 等，一般程式開發常將專注力集中於功能需求，而忽略了安全需求，最終程式碼存在許多弱點與風險，成為駭客攻擊之目標，因此除追求滿足功能需求外，開發過程中亦應考量安全需求，如何撰寫出安全的程式碼係 App 安全的第一道防線。故本次研討會心得將以 OWASP 所提出移動式裝置的十大弱點風險做介紹，以期透過參考 OWASP Top 10 Mobile Risks 了解目前 App 開發可能遭遇之弱點與風險，於應用程式 App 開發過程中降低資安風險發生之機率。

OWASP 於 2011 年 9 月 23 日在美國發表關於移動式裝置的十大弱點風險，採用可攜式裝置威脅模型(Mobile Threat Model)的研究方法，該方法將可攜式裝置遭受威脅分成 6 大分類，分別為：詐欺(Spoofing)、拒絕(Repudiation)、阻斷服務(Denial of Service)、竄改(Tampering)、資訊洩漏(Information Disclosure)、提升權限(Elevation of Privilege)，OWASP 再將上述分類依風險所造成嚴重性衝擊(例如：機密性、完整性、可用性)加以定出十大弱點，分別說明如下：

1.Insecure Data Storage

指敏感性資料未受到適當保護，一般常見如敏感性資料未加密，或是一些不常用到之暫存資料可能含有敏感訊息(例如：登入帳號與密碼)，可能造成機密性資料損失、憑證外洩、侵犯隱私權等衝擊。

【建議防護措施】只儲存必要資訊，不將敏感資料存放於開放式儲存媒體(例如：SD 卡)，採用安全之檔案加密應用程式介面，設定檔案讀取與寫入權限等。

2.Weak Server Side Controls

Mobile 之弱點並非只存在於 Mobile 端，所開發之 App 應用程式或雲端系統的程式亦可能存在弱點。

【建議防護措施】於伺服器端開發應用程式時，應避免產生 OWASP Web Top 10 或 OWASP Cloud Top 10 相關弱點。

3.Insufficient Transport Layer Protection

可攜式行動裝置於傳輸機敏性資料時，常發生未加密情況，例如：瀏覽器本身不支援 HTTPS 功能，或使用的 App 應用程式未採用加密方式進行資料傳輸(如：登入系統、交易資料等)，因此可能造成駭客使用中間人攻擊(Man-in-the-middle attacks)，從中竄改或竊取封包資料，進而造成機敏資料洩漏。

【建議防護措施】程式開發者應確保所有敏感性資料採用加密方式進行傳輸，傳輸媒介可包含網路連線、Wifi 連線，甚至是近場通訊(Near Field Communication, NFC)連線等，若只採用明文方式傳遞，攻擊者可輕易透過網路監聽方式(Sniffer)竊取機敏性資料。

4.Client Side Injection

Injection 攻擊一直是相當好用的攻擊手法，即使移到了可攜式行動裝置之網頁應用程式，若網頁應用程式存有 Injection 弱點，攻擊者仍可利用 SQL Injection 或 XSS 攻擊手法來提升可攜式行動裝置的權限，或利用網路盜打市話(Toll Fraud)的情況發生。

【建議防護措施】網頁應用程式傳遞參數給雲端資料庫的內容，需過濾不受信任或不應該接受的內容，例如：SQL 執行語法、特殊字元等，同樣可採用 prepared statement 功能進行過濾。

5.Poor Authorization and Authentication

部分可攜式行動裝置的網頁應用程式僅採用永不變的數值來執行身分驗證與授權階段，例如：國際移動設備識別碼(International Mobile Equipment Identify Number, IMEI)、國際移動用戶識別碼(International Mobile Subscriber Identify, IMSI)或通用唯一識別碼(Universally Unique Identifier, UUID)。

【建議防護措施】使用嚴謹之身分驗證與授權(例如：雙因子認證)，避免使用可攜式行動裝置硬體 ID 標籤或永不變的 ID 識別碼做為身分驗證的因素。

6.Improper Session Handling

可攜式行動裝置的應用程式 session 過期時間，一般會設定比較長，原因是對使用者方便存取或使用，通常這些 session 經由 HTTP Cookies、Oauth Token、Single Sign-on 等方式來進行維護，建議避免使用裝置的硬體識別碼

來當作 session 值，很容易讓攻擊者猜到 session 內的機密性內容(例如：帳號或密碼)，進而造成提升攻擊者於可攜式行動裝置的權限，進行非授權的存取。

【建議防護措施】若需要提高安全性，相對其軟硬體設計(演算法或操作方式)的複雜度亦會增高，只要 session 值的過期時間應設定在一個可接受範圍內，就無需擔心讓使用者太頻繁的重新驗證，另外可攜式行動裝置遭遺失或竊取時，應有能夠快速撤銷 Token 之機制，使裝置無法更近一步遭受到濫用情況。

7.Security Decisions Via Untrusted Inputs

在各種可攜式行動裝置的平台均會發生(例如：iOS、Andriod)，應用程式可能經由惡意攻擊者精心設計，或是應用程式遭攻擊者透過 Client Side Injection 攻擊方式來消耗可攜式行動裝置之硬體資源或提升權限情形。舉例來說，假設 Skype 應用程式具有 HTML 或 Script Injection 弱點，攻擊者只要事先把具有惡意連結的 iframe 寫入某個特定網頁：

```
<iframe src="skype:17031234567?call"></iframe>
```

一但可攜式行動裝置的瀏覽器讀取到此 iframe 程式碼時，Skype 應用程式將無需使用者授權，自動開始播號給指定的電話號碼。

【建議防護措施】每個應用程式在設計時均應注意身分認證與授權問題，以確保可攜式行動裝置需經過使用者的身分驗證後才允許執行特殊的行為或功能。

8.Side Channel Data Leakage

Side Channel 像是可攜式行動裝置中的第三方應用程式，這些應用程式可能會自動幫使用者儲存一些敏感性資訊，例如：網頁暫存(Web Cache)、按鍵側錄(Keystorke Logging)、擷取畫面(Screenshots)、日誌檔(Logs)或暫存目錄(Temp Directories)等，一但攻擊者成功取得可攜式行動裝置權限時，將會侵犯使用者隱私，甚至導致資料洩漏情形。

【建議防護措施】較敏感性之資料應避免自動儲存於可攜式行動裝置內(例如：憑證資訊、帳號、密碼等)，檢查部分應用程式是否會儲存敏感性資訊，建議加以手動移除，或是選擇不自動儲存功能。

9.Broken Cryptography

加密失效分為兩種情況，一種是使用強健的加密演算法卻遭到破解，另一種為使用過於簡單的加密演算法遭到破解。前者要實現的困難度較高，後者則是相當容易。OWASP 提出幾個對於加密方法的謬誤，例如：編碼(Encoding)、混淆(Obfuscation)、序列化(Serialization)，上述嚴格說起來，並非為嚴謹加密方式，攻擊者能輕易破解簡單的加密演算法後，取得可攜式行動裝置的完整資訊，同樣也可做到提升權限或機敏資料遭洩漏等情況。

【建議防護措施】開發應用程式建議使用強健的加密演算法，並不斷進行反覆測試，直到應用程式開發完成時，仍需執行嚴格的挑戰測試(Battle-Tested)。

10.Sensitive Information Disclosure

指把輸入或輸出的相關參數直接寫入在程式碼當中，因此只要攻擊者能夠取得應用程式的原始碼(例如：透過逆向工程手法)，若原始程式碼內容含有敏感資訊，像是 API 金鑰、帳號或密碼等，可能會造成企業內部的智慧財產暴露或個人憑證洩漏等情況。

【建議防護措施】程式開發者應避免將敏感資訊寫入於原始程式碼中。

以上為本次研討會探討行動裝置十大安全弱點之簡要說明與建議防護措施，亦為機關程式開發者於撰寫應用程式 App 時之重要參考依據。

參、心得及建議事項

今年OWASP亞洲年會於日本東京舉行，有來自各國OWASP的會員及專家共同研討網站應用系統開發安全標準、OWASP參考指引、網站存取控制等，對於新接觸OWASP之人員，可先從OWASP目前已完成之相關應用安全基礎知識指南著手，例如：Developers Guide、Testing Guide、Code Review Guide等。對機關而言，在面對應用系統委外開發趨勢下，各應用系統負責人之角色由原程式撰寫轉換為進度控管與系統需求測試為主，其中OWASP Testing Guide包含應用安全測試的程序說明，則極具參考價值，可作為綜合應用安全驗證的一部分；另一參考文件為OWASP Application Security Desk Reference(應用安全基礎參考指南)，涵蓋所有應用安全中重要準則、攻擊手段、應用弱點、安全對策、技術衝擊和商業衝擊之基本定義和描述，建議系統負責人於程式開發期間及最後測試階段，可參考上揭兩份文件指南，俾提升應用程式開發品質。

台灣即將邁入4G時代，伴隨智慧型行動裝置持有率日益普及，個人隱私資訊外洩或病毒入侵手機等隱憂如影隨形，尤其政府機關在開發行動App便民服務時，應更加留意App是否存在漏洞或弱點，避免民眾安裝App後遭病毒或駭客入侵，造成隱私資訊外洩，損害民眾利益及機關名譽。例如日前負責國道電子計程收費的遠通電收，於2014年1月發生App遭DDoS攻擊事件，最後由行政院介入調查後，發現係該App設計不良所致。因設計不良造成App在斷線後不斷重新連線，導致大量連線使系統無法負荷，停止正常服務，最終App提供者及使用者皆受害。建議機關未來於行動App開發上可採取下列作法：

一、事前：

(一)透過教育訓練讓程式開發人員了解上述OWASP所提出之行動裝置十大安全弱點風險(OWASP Top10 Mobile Risks)，並參考各項風險所對應之建議防護措施進行程式開發，以建立安全程式開發觀念，撰寫出安全之程式源碼。

(二)若應用程式委外開發時，建議於需求規格書中敘明應用程式開發之安全需求，例如：「應用系統程式開發須禁止使用已被資訊安全組織公布，易遭駭客攻擊之弱點的開發方式，如：OWASP Top10 Mobile Risks前十大安全問題種類，及未來發布之安全問題種類」，以規範得標廠商之程式開發過程，並做為測試驗收的依據。

二、事中：以稽核方式透過源碼檢測 code review 工具，檢查現有 App 是否存在已知弱點或風險，提早發掘潛在風險 並即時加以修正。

三、事後：於發現應用程式相關弱點漏洞或遭攻擊時，應立即通報將 App 下架並請開發人員修正程式碼，即時控制風險避免損害持續擴大，造成大規模之資安事故。