Chang Max的部落格

歡迎光臨Chang Max在痞客邦的小天地

部落格全站分類：生活綜合

淺談OWASP Top 10 Mobile Risks

Feb 03 2012

前些年筆者有針對開放Web軟體安全計畫(Open Web Application Security Project，簡稱OWASP)

其中一項子計畫「網站應用程式十大弱點(OWASP Top 10)」進行研究，當時是2007年的版本，現在已

更新到2010版，弱點項目筆者是認為大同小異，倒是在弱點的發生率的高低將嚴重程度重新做一個排序。

而雲端技術快速的發展，不論是使用者或應用程式開發者，資訊的操作模式已逐漸地從主機平台移至可攜式

行動裝置或智慧型手機，即使平台不同，既然是由人所開發的應用程式，必定會產生一定程度的弱點風險。

OWASP於2011/9/23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

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再將上述分類依照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

別簡略說明如下：(由於OWASP並未公布中文名詞定義，筆者的翻譯僅供參考)

M1. 不安全的資料儲存(Insecure Data Storage)

意指敏感性資料未受到適當的保護，一般常見如敏感性資料未加密，或是一些不常用到的暫存資料可能含有

個人資訊

加入好友

加入訂閱

暱稱： Chang Max

分類： 生活綜合

好友： 共2位 (看全部)

敏感訊息(例如：登入帳號與密碼)，可能會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的儲存媒體(例如：SD卡)，採用安全

的檔案加密應用程式介面，設定檔案的讀取與寫入設定權限等。

M2. 弱伺服器端的控制(Weak Server Side Controls)

主要是說明Mobile的弱點並不只單存在於Mobile端，所開發的APP應用程式或雲端系統的程式亦有可能存

在弱點，例如：OWASP Cloud Top 10。

【建議防護措施】人員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，詳細內容可參考OWASP官方網站。

M3. 傳輸層保護不足(Insufficient Transport Layer Protection)

可攜式行動裝置於傳輸機敏性資料時，很常發生未加密情況，例如：瀏覽器本身不支援HTTPS功能，或是

使用的APP應用程式未採用加密方式進行資料的傳輸(如：登入系統、交易資料等)，因此可能會造成駭客使

用中間人攻擊(Man-in-the middle attacks)，從中竄改或竊取封包資料，進而造成機敏資料的洩漏。

【建議防護措施】程式開發者應確保所有敏感性資料有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。

M4. 客戶端注入(Client Side Injection)

Injection攻擊一直都是相當好用的攻擊手法，即使移到了可攜式行動裝置的網頁應用程式，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，或是利

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。

M5. 粗糙的授權與認證(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 Susscriber Identify, IMSI)或通用唯一識別碼(Universally Unique Identifier, UUID)。

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

M6. 不適當的會話處理(Improper Session Handling)

可攜式行動裝置的應用程式session過期時間，一般而言會設定的比較長，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遺遺失或竊取時，應有能夠快速撤銷Token的機制，使裝置無法更近一步遭受到濫用情況。

M7. 安全決策是經由不受信任的輸入(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的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。

(3204)RHCE證照取得
(1959)淺談OWASP Top 10 Mobile Risks
(837)Accessnow.org對於DoS攻擊防護的建議
(721)網頁置換手法案例介紹

文章分類

資通安全 (7)
其他雜類 (2)
國際證照 (4)
兩性 (1)
關西國防役 (12)
娛樂 (3)
笨點 (1)
心情 (14)

最新文章

踏上新的工作旅程
考取EC-Council原廠認證講師(CEI)
淺談OWASP Top 10 Mobile Risks
US-CERT對於Anonymous DDoS攻擊活動觀察
Accessnow.org對於DoS攻擊防護的建議

最新留言

01/17 zero：學長：您好 有關 CEH v8的...
11/10 ricky：請問CEH用Visual CertExam Su...
08/09 Chang Max：Hi, Marksong, 您想詢問...
07/26 版主回覆：您好： 有原廠認證的補習...
07/25 小宋：學長您好： 能否請您推...

【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的問題，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。

M8. 側通道資料洩漏(Side Channel Data Leakage)

這邊的Side Channel比較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】一些較敏感性的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。

M9. 加密失效(Broken Cryptography)

所謂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，後者則是相當常見。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)。

M10. 敏感資訊洩漏(Sensitive Informaiton Disclosure)

此弱點的洩漏方式，乃是指應用程式原始碼中，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各人憑證洩漏等情況。

【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。

其他更詳細的內容，有興趣的網友們可參考OWASP官方網站或這篇。

您可能會有興趣的文章

黃子佼愛3C~台灣歌手利得彙登陸APP

移動裝置的應用程式年底銷售額將達 30億美

移動裝置的應用程式年底銷售額將達 30億美

Chang Max 發表在 痞客邦 PIXNET 留言(0) 引用(0) 人氣(1960)

E-mail轉寄 轉寄至留言板

全站分類：進修深造
個人分類：資通安全
此分類上一篇： US-CERT對於Anonymous DDoS攻擊活動觀察
上一篇： US-CERT對於Anonymous DDoS攻擊活動觀察
下一篇： 考取EC-Council原廠認證講師(CEI)

▲top

⊟ 引用列表 (0)

http://squaremax.pixnet. 點我複製

⊟ 留言列表 (0)

Post comment

文章精選

所有文章列表

文章搜尋

搜尋

新聞交換(RSS)

PIXNET RSS
PIXNET ATOM
REPLY RSS

誰來我家


參觀人氣

本日人氣：2
累積人氣：15977

您尚未登入，將以**訪客**身份留言。亦可以上方服務帳號登入留言

您的暱稱 ...

留個言吧 ...

悄悄話

其他選項

送出留言