Web Application 安全防護的最佳實踐(Best Practice)(下)

撰稿：叡揚資訊　資訊安全事業處

上期我們介紹了 Web Application 的 4 項安全防護的最佳實踐 Web Application 安全防護的最佳實踐(Best Practice)(上) (http://www.gss.com.tw/index.php/epaper/security/932-gss0064)，本期將持續**從 OWASP（Open Web Application Security Project）公布的前十大 Web 應用程式的安全弱點**，從網站應用系統的架構設計、程式開發到網站部署，提供幾點防護方向，以降低 Web 應用程式的安全弱點，防止駭客利用這些安全弱點來進行破壞，而造成個人、公司甚至國家的重大危害事件。

(5) 機密資料

近年來，由於 Web 應用系統逐漸普遍，因此許多政府機關、大型企業或者中小型企業，都開始採用 Web 應用程式來取代傳統的軟體。隨著 Web 應用程式使用率大幅度上升，各式各樣的機密資料，都有可能被放到 Web 應用程式所能存取得資料庫伺服器中，駭客攻擊的目標也由單純的應用程式伺服器，到竊取應用程式中的機密性資料，甚至將所竊取的機密性資料販賣給競爭對手或敵國，造成政府或公司重大的損害。

因此，在應用系統中的機密性資料，應該給予加密等防護措施。許多應用系統的程式開發者，都透過自行開發的演算法，對應用系統中的資料進行加密，不僅演算法的強度未經驗證，同時也存在開發者隨時可以還原原始資料的風險。因此，建議採取幾項措施來對機密性資料進行加密，如：(1)應使用公認的加密演算法；(2)良好的金鑰管理機制：金鑰應該分開保管，資料擁有者擁有金鑰，而管理者只能進行備份等其他權限而無法觀看資料內容；(3)避免使用薄弱的演算法(如自訂的演算法、加密強度低的演算法或已經遭破解的演算法)；(4)避免過度使用遭破解的 SHA1 或 MD5(駭客可以改變其檢查碼)。

(6) 工作階段

應用系統經常使用 Session 來進行工作階段的管理，使用者在應用系統間的活動，當使用者通過身份驗證後，應用系統會給予使用者一個工作階段識別碼，作為識別使用者的機制。一方便避免使用者需要經常重新進行驗證，一方面也可以保留使用者的工作階段資料，當使用者重複使用時，可以減少不必要的存取動作。但這樣的機制，現在已經變成駭客攻擊的重點，當駭客取得使用者的工作階段識別碼，或者擷取工作階段內容，就可以對應用程式進行資料竊取或入侵攻擊等行為。

通常會有幾項攻擊方式，如工作階段攔截(Session Hijacking)、工作階段重現(Session Replay)以及中間人攻擊(Man in the middle)。建議採取的防護措施，通常有下列幾項: (1)使用 SSL 建立加密的管道，驗證的 Cookie

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、東京　www.gss.com.tw

只允許在 HTTPS 上使用；(2)在應用系統中，應該建立登出的機制，如果有其他使用者想要使用相同的工作階段時，允許使用者終止該工作階段；(3)所有的 Session 都應該建立過期時間，雖然無法直接預防 Session 被攔截，但是卻能有效減少駭客能操作的時間；(4)當要存取重要資料或資源時，應該重新驗證使用者身份，防止 Session 被竊取而操作；(5)提供一個不要記住密碼等選項，讓使用者每次登入都必須重新驗證等較為嚴謹作法；(6)將要傳輸的資料進行加密，使用者將無法介入並竄改其資料。

(7) 密碼編譯

密碼編譯有助於防止資料被檢視或修改，也可以在一般情況下並不安全的通道上提供安全的通訊方式。早期登入資訊經常使用密碼，作為識別使用者的方式，因此密碼保護的重要性，就十分重要。現今駭客入侵系統，大多為了系統背後的資料而來，而針對資料的保護亦越來越重要了。其中常見的保護方式為資料可使用密碼編譯演算法加密，在加密的狀態下傳送，稍後並由所希望的一方解密。即使第三者攔截到這些加密資料也很難破解。

通常使用密碼編譯的情況為：假設 A 與 B 兩個通訊方在不安全的通道上通訊。這兩者希望確保他們的通訊不會被任何正在接聽的人所瞭解。甚至，由於位置距離遙遠，A 必須確定他從 B 收到的資訊，在傳輸時未經任何修改。同時，A 還必須要確定這些資訊的確是來自 B，而不是駭客模擬 B 所傳送來的。

通常可以使用密碼編譯達到以下目的：

- 機密性：利於避免使用者的身分或資料被讀取
- 資料完整性：利於避免資料被變更
- 驗證：確保資料是來自特定的一方

在加密時應該考量採用 AES 256、3DES 等強度比較強的公認演算法，而且金鑰的管理最好採用權責分離的方式來進行管理，盡量避免採用自製的演算法或過度使用遭破解的 SHA1 或 MD5(駭客可以改變其檢查碼)等 HASH 檢查碼方式。

(8) 參數操作

駭客通常會透過竄改 Web 應用程式的 Client 端與 Server 端的所傳遞參數，來對應用程式進行攻擊。這些所傳遞的參數通常包含了 QueryString、表單資料(Form field values)、cookies 以及 HTTP 的檔頭資料(Headers)。建議防護的作法有下列幾項:

● QueryString(查詢參數)操作

不要在 QueryString 中，放入重要的敏感性資料，以避免被駭客擷取，重要且敏感性資料應該採用 Session 來進行識別與溝通，並將這些機敏性資料放在伺服器上。建議採用 POST method 而不是 QueryString，如果要使用，建議請加密其重要內容。

● 表單資料(Form field values)操作

一般來說，表單資料通常會存在 HTML Form 區域，容易遭受駭客監看其數值或資料，建議應該採用 Session 來進行識別與溝通，並將這些機敏性資料放在伺服器上。

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、東京 www.gss.com.tw

- **Cookies 操作**

一般來說，Cookie 資料通常會透過兩種方式存放，一種方式是儲存在實體機器上，另外一種則以記憶體暫存方式與使用者端瀏覽器等同時存在。現今駭客攻擊技術進步，有非常多的工具可以用來竄改記憶體中的 cookie 資料。而 Cookie 的操作通常則利用竄改資料，取得非法的授權或使用者身份而進行破壞性操作。雖然 SSL 可以保護 Cookie 在網路上的傳輸，但卻無法防止使用者端的 Cookie 被破解或竄改，建議應針對 Cookie 內容進行加密，以防止遭受竄改或復原。

- **HTTP Headers 操作**

許多應用程式是透過 Client 所傳送過來的 HTTP headers，來進行下一步動作的判斷或決定如何進行操作，駭客可以透過修改 HTTP Headers 來欺騙許多應用程式，很多例如 HTTP Referer 可能遭受竄改，而讓應用程式無法得知 Client 真實的來源位址。

(9) 例外管理

在傳統軟體開發生命週期中，最常容易被忽略的資安領域為例外管理。好的例外管理必須要能掌控所有非預期的行為，且對例外的回應內容加以管制，對程式或系統開發者可以輔以除錯，以確保系統正常運行的依據。對真正應用程式的操作人員(如一般使用者)則不該提供太豐富的訊息。一個良好且安全的應用程式，在例外發生的當下，也要做到安全失誤(Fail Secure / Fail Safe)，換句話說，就是發生故障的當下，也不會對整個系統安全造成危害；例如，當一個重要的安全鎖壞掉時，該開啟還是關閉?

如何進行安全性的設計考量，就端看安全鎖背後所保護的事物而決定，如果是金庫，或許該選擇關閉(Fail Secure)；是人，或許該開啟(Fail Safe)。在例外管理中，要注意當系統出現例外時，應用程式將不會把重要的系統資訊傳遞到使用者端，以避免做為駭客攻擊的依據。現今駭客經常使用的 DoS(Denial of Service)攻擊，是一種藉由系統產生例外錯誤時，而使系統造成癱瘓或無法繼續服務的攻擊。一個安全的應用程式，也必須將這些狀況考量進去。最好的處理方式，就是針對所有輸入的資料進行驗證，以確保系統的安全。

(10) 稽核與記錄

稽核與記錄(Auditing and logging)通常可以在某些攻擊或破壞事件前，偵測到使用者不正常的操作活動或者密碼暴力破解嘗試並給予一定的防護措施。這種方法也可以協助瞭解或記錄使用者被系統拒絕服務的相關動作，以便於瞭解使用者在系統中可疑的動作。一個良好的稽核與記錄機制，應該隨時可以去記錄下列幾項動作: (1)使用者嘗試使用服務被拒絕事件、(2)使用者登入或登出活動、(3)系統中重要的功能被使用等記錄、(4)不定期要備份所有的記錄。以確保事後可以針對不正常的活動或交易，進行稽核，甚至未來可以作為資安事件的重要證據。

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、東京 www.gss.com.tw

結論與討論

越來越多的使用者開始使用 Web 應用程式來取代傳統的應用程式或系統，無形之間，也增加讓駭客透過網路來對系統攻擊的頻率。如何做好 Web 應用程式的防範措施，首先要先瞭解威脅和風險來自於哪裡，才有辦法針對其行為做出防護的動作與措施。本文中提出了一些常見的防護處理措施，然而駭客技術日新月異，未來仍然需要不斷地瞭解其攻擊的手法，以及系統新的威脅，才能有效地防護 Web 應用程式的安全。

References：

1. 軟體工程 - 維基百科，自由的百科全書:
   http://zh.wikipedia.org/wiki/%E8%BB%9F%E9%AB%94%E5%B7%A5%E7%A8%8B
2. 軟體發展的生命週期
   http://www.cc.ntu.edu.tw/chinese/epaper/0002/20070920_2011.htm
3. Official (ISC)2 CSSLP Education Seminar
4. Improving Web Application Security: Threats and Countermeasures:
   http://msdn.microsoft.com/en-us/library/ff649874.aspx

GSS Galaxy Software Services 叡揚資訊
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、東京 www.gss.com.tw