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

撰稿：叡揚資訊　資訊安全事業處

前言

隨著資安觀念的普及以及駭客手法日新月異的翻新，來自資訊系統以及網路等設備被發掘的安全弱點數量，近年已呈現持平或下降的趨勢。根據 HP 2010 年網路安全風險研究報告指出，Web 應用程式的安全弱點即佔了所有漏洞總數的一半，同時美國國家標準與技術研究所(NIST)研究並統計出現有駭客的攻擊，大約 92%是來自於應用系統，而不是傳統的網路層，同時運用網頁惡意工具套件進行複雜有效攻擊行為也大幅度地提升。

自 1990 年代初期 Web 技術的提出，如今 Web 應用程式已成為個人於生活（如收發郵件）、企業於營運中（如電子商務網站）及政府於施政中（如政令宣導），不可或缺的一環，至今 Web 2.0 技術不斷推陳出新，各種社交、社群與論壇網站如雨後春筍般地進駐到我們的日常生活中，Web 應用系統幾乎已經成為上網族，每天必須接觸的系統。此趨勢更進一步將傳統個人電腦、大型企業或政府部門內部的傳統應用軟體轉換為 Web 應用系統，以便與外部用戶進行更廣泛的連結與資訊交換工作。由於 Web 應用程式，通常會與後台的資料庫伺服器進行連接與溝通，一旦被駭客入侵成功，不僅資料庫所存放的資料被竊取，甚至假使資料庫管理系統權限設定不當，甚至會讓駭客取得控制權，進而進行更多的破壞行為。常見的 Web 開發語言包括 ASP、PHP、JSP 及具備完整配套開發框架的 J2EE 與.NET 等架構。因此，Web 應用程式安全已成為當前重要的資安課題。

常見的 Web 應用系統安全弱點

OWASP（Open Web Application Security Project）是一個全球性開放社群，也是一個非營利組織，長期致力於改善 Web 應用程式的安全性，主要目標在於建立 Web 應用程式安全的標準、工具與技術文件，並提供給政府和業界參考，以降低 Web 應用程式在設計、開發及部署過程可能產生的安全弱點，防止駭客利用這些安全弱點來進行破壞。

OWASP 從 2004 年起就開始評鑑 Web 應用程式的安全弱點並予以排名，並每隔三年，會依據駭客最新的攻擊手法歸納出前十大安全性弱點，該組織在 2010 年依「攻擊與威脅來源廣度」、「攻擊手法難易度」、「弱點流行程度」、「弱點偵測難易度」、「技術面衝擊程度」及「營運面衝擊程度」等六大因素，評鑑出 Web 應用程式十大弱點（OWASP Top 10），其內容簡述請參考 https://www.owasp.org/index.php/OWASP_Top_10，其內有詳細的說明。

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

2010 OWASP Top 10 除了新增「A6.不當的安全組態」與「A10.未驗證的轉址與轉送」兩項，其他八項都與前幾年相同。這說明了已被公布的 Web 應用程式安全弱點，仍未能獲得妥適的處理，可能原因有：(1)找不到原來 Web 應用程式的開發廠商或是缺乏足夠的人力進行安全弱點修補；(2)使用未經安全驗證的第三方外掛程式，例如：Joomla、Drupal 等；(3)Web 應用程式的原始程式碼或架構太過複雜，擔心修補造成不穩；(4)自行開發或委外開發 Web 應用程式時，未將資訊安全視為功能性需求，結合安全考量於傳統的軟體開發生命週期的各階段，導致產生可被駭客利用的各種安全弱點；(5)RD 開發人員本身對安全程式碼開發的資安意識不足，撰寫習慣仍然未有改變，因此這些弱點仍然層出不窮。

本文將針對網站應用系統(Web Application)的重大防護方向，提出一些最佳實踐。冀未來 Web 應用系統開發人員能夠有足夠的技術，針對現有的弱點以及網站應用系統安全性開發方向能有所瞭解。

Web 應用系統安全防護的十大最佳實踐

從 OWASP（Open Web Application Security Project） 所公布的前十大 Web 應用程式的安全弱點，我們歸納了幾點方向，從網站應用系統的架構設計、程式開發到網站部署，提供了幾點防護方向，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。

(1) 輸出入資料的驗證(Input and Output Data Validation)

微軟的資安專家在 Writing Secure Code 這本書中提到這句話「All Input is Evil!」，意思是說所有的輸入都是邪惡的。以往我們設計網站應用系統時，在表單輸入欄位，經常只有檢查使用者輸入的格式是否正確，而沒有去確認使用者輸入的字串或字元，是否會被駭客藉以操作商業邏輯，而達到對系統進行惡意的攻擊或操作。在進行輸出入驗證時，可以採取下列三項措施:

- 資料的一致性

  在進行資料驗證時，應該檢查所輸出入的資料的一致性，以避免原始資料遭到駭客竄改，而造成系統的損害或重要資料損毀。

- 資料的正確性

  除了檢查資料是否被竄改外，還應該針對資料的正確性進行驗證，如資料的型別、長度以及是否包含惡意的攻擊語法或字元。此外，資料語法是否正確，是否已經包含安全性簽署，這些都是檢查的措施與方法。

- 資料的合理性

  除了驗證資料的正確與一致性外，應該要針對資料的合理性進行檢核，以避免駭客利用商業邏輯層的非法存取動作，進行對系統的破壞或偷走重要的資料，如個人資料。

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

(2) 身份識別(Authentication)

使用者身份識別主要是判斷使用者是否為合理的使用者，早期常使用最簡單的密碼作為身份識別與驗證的主要方式，駭客經常進行暴力攻擊的方式來破解使用者的密碼，一旦使用者所使用的密碼強度不夠，很容易遭受到破解而造成損害。建議應採用業界公認的強度較強不易被破解的加密方式，如 AES256、3DES 或更強的演算法等。在密碼為靜態的狀況下，將會產生某些問題，比如為了維護密碼安全性，必須嚴格規定密碼的長度、複雜性（例如：中英文數字夾雜，大小寫間隔，長度須超過 8 個字元以上）及定期更換的頻率。在驗證方式應使用較安全的驗證方式，如目前被認為較為安全的雙因素驗證方式等。

(3) 資源授權

授權是對應用程式的使用者，在經過身份驗證之後，會依據使用者的權限來決定是否接受這次的連線請求。當使用者登陸成功後，系統會接受使用者後續的要求，否則將拒絕使用者的任何要求。除了身份驗證通過後，針對使用者對於各項資源的請求使用授權，都必須做好嚴格的規範，以避免使用者利用系統漏洞或鬆散的權限管理機制，存取系統中機密性的資料，甚至竄改資料造成系統的損害。

一般來說，在進行應用系統設計時，應考量建立授權策略，建議採用角色式授權以及資源式授權等兩者方式。其中角色式的授權主要是依據使用者身份，以及使用者在應用系統中，所能進行的行為作為依據，規劃其所屬的權限；另外資源式的授權，則是以系統資源的使用角度來看，規劃使用者所能對資源進行各項存取動作。透過兩種方式結合，才能有效地對使用者進行授權。除此之外，應盡量避免將所有的權限授權給某一個特定角色。

(4) 設定管理

許多應用程式可能會儲存或使用對使用者而言是唯一的資訊。您可以使用這些儲存的資訊，讓使用者造訪網站時，能體驗到具有個人客製化風格的應用程式。一般來說，具有個人特色的 Web 應用程式，在進行個人風格客製化時，需要參考一些設定的資料。因此，程式開發者必須使用唯一的使用者識別項來儲存這些相關資訊，當使用者設定完成後，再度使用 Web 應用程式時，系統則可以識別其身份，並針對其身份進行反應。

因此，不當的設定檔，可能會造成 Web 應用程式重要的資訊外洩，甚至可以讓駭客間接找到攻擊網站的方法。下列有幾項建議的作法，可以減少駭客透過不良的設定方式而對系統進行攻擊。如：

(1) 避免將系統除錯資訊輸出到使用者端，如 ASP.net 系統的 Web.Config 檔案中有此選項，建議應用程式上線前，應檢查此一設定，並給予關閉。

(2) 許多應用程式會提供檔案上傳或寫入功能，請確定將其目錄的權限以及 NTFS 的權限，限制給應用程式角色寫入，請勿開放給所有人的角色存取。

(3) 在進行重要系統資源授權時，應考慮使用最小權限原則，讓使用者只能使用某一特定的資源，而不開放給其他使用者。

(4) 在應用伺服器端避免讓應用程式使用者可以有瀏覽網站目錄的權限。

< 待續 >

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