跨站腳本攻擊(Cross-Site Scripting, XSS)概述

文章來源: WhiteHat Security 翻譯整理: 叡揚資訊 資訊安全事業處

Cross-Site Scripting(XSS)跨站腳本攻擊概述

XSS 弱點在 80%的網站中都曾經發現過。但其實了解 XSS 弱點的原理後，對於軟體開發人員來說是非常容易去解決的。XSS 攻擊是當網站讀取時，執行攻擊者提供的程式碼。XSS 通常是透過 HTML/JavaScript 這類不在伺服器端執行、而在使用者端的瀏覽器執行。可用來竊取用戶的 cookie，甚至於冒用使用者的身份。像是網路銀行、電子郵件、部落格或其他需要有帳號才能進入的網站。近年來的研究中可以發現 XSS 攻擊可以完整的控制瀏覽器，就像木馬程式一樣。

XSS 攻擊可以分為兩種：

一、使用者點擊特製的連結稱為 **Reflected Attack**

二、另一種是單純的瀏覽網頁，且該網頁中已植入惡意的語法稱為 **Persistent Attack** 除了要注意攻擊的手法外，電腦保持更新至最新版也是很重要的。瀏覽器廠商、軟體開發人員與安全專業人員的工作便是防止這些攻擊的關鍵。

Reflected Attack

若駭客想透過某個網站(在此稱為：http://victim/)利用 XSS 攻擊使用者。第一步會先找出 http://victim/網站中 XSS 的漏洞，再製造一個惡意的 URL 連結。這個連結是網站中的某個功能，該功能會接收使用者端提供的資料，並回應到使用者端的畫面，如資料檢索功能。

圖 1 是常見的網站，XSS 漏洞常見於資料檢索功能。在搜尋欄位輸入「test search」，結果在不同頁面中顯示剛才輸入的 「test search」，如圖 2。該 URL 帶有查詢字串。此 URL 的值可以被修改，甚至包含 HTML 或 Javascript 內容。

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

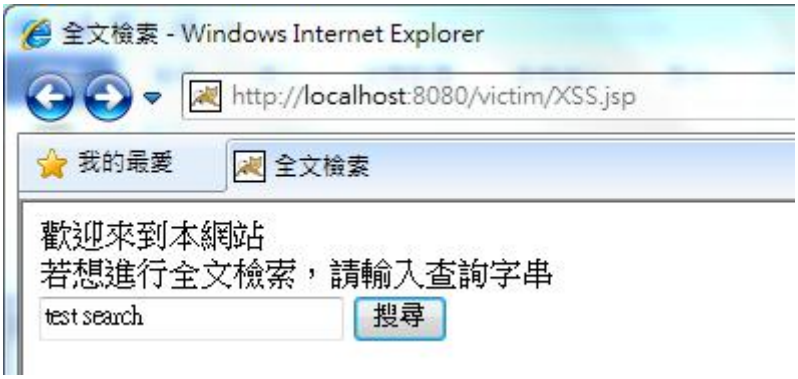

圖 1 檢索功能頁面

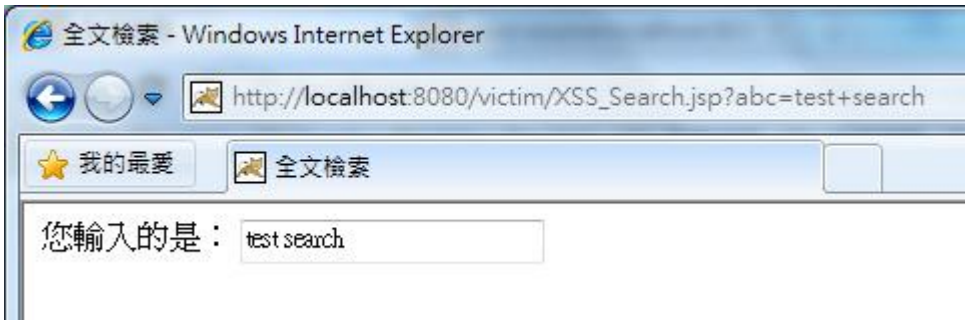

圖 2 檢索結果頁面

若搜尋時使用 HTML 或 JavaScript 取代原本的值，會產生什麼結果：

範例一：輸入「"><script>alert('XSS%20Testing')</script>」

搜尋結果頁面顯示了一個警告的對話框，且顯示部份先前輸入的內容與執行 JavaScript 如圖 3。觀察此頁的原始檔可以發現原本的內容被加上了 HTML 或 Javascript，如圖 4。此時若駭客繼續修改 URL，便可攻擊使用者，如偷取使用者的 cookies 等。

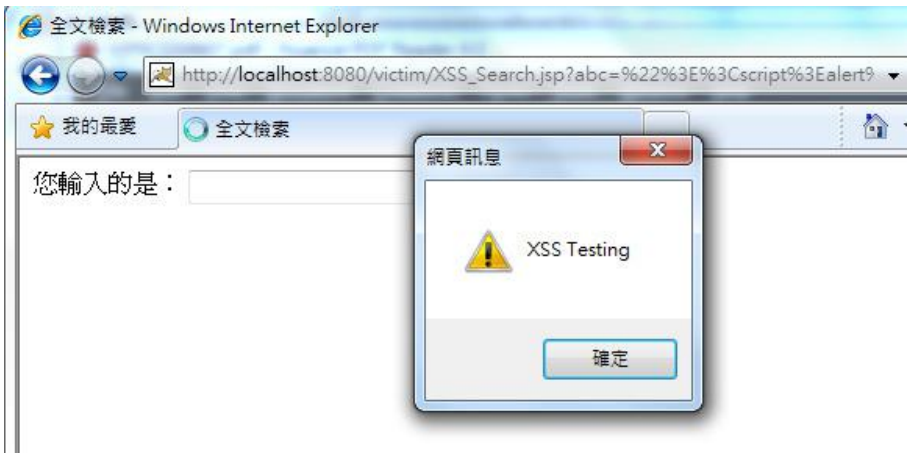

圖 3 將 Html/JavaScript 取代原查詢字串

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

圖 4 檢測原始碼，原始碼中出現新的 HTML/JavaScript

Persistent Attack

Persistent XSS 攻擊常發生於社群網站或電子郵件等，不需執行特定的連結即可發生。駭客事先將攻擊的語法送至可能被其他使用者造訪的網站。有可能為部落格回應、留言板貼文、聊天室、HTML 電子郵件以及其他。當使用者造訪被感染的網頁，會自動執行攻擊。因此 Persistent 比 Reflected 更加危險，使用者完全無法保護自己。

無論是 Reflected 還是 Persistent，駭客會持續攻擊都是為了造成網路或財務上的損失。

*若想深入了解 XSS 弱點，可以搜尋「XSS cheat sheet」取得進一步的資訊。

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