

竹 苗 區 網 服 務 報 告

交通大學資訊技術服務中心 技術發展組

報告人：楊詠仁

連絡電話：03-5712121#31724

網路電話：92931724

Mail：houston0219@mail.nctu.edu.tw

區網服務項目

➤ 不當網頁阻擋服務：

- 提供學童乾淨的校園網路學習環境。

➤ PROXY服務：

➤ 教育部網站應用程式弱點監測平台服務：

- URL：<http://ewavs.hcrc.edu.tw/>
- 針對SQL-Injection及XSS進行檢測。

 依據資通安全基本防護系統政策限制您進入該網頁

原因: 類別: 賭博 被阻擋。

URL: http://www.casino8net.com/skills.htm

如您覺得本網頁有教學必要, 或其它問題需要反應,
請與下列負責窗口連繫:
貴校網路管理員或交大竹苗區網中心 楊詠仁先生
電話: 03-5712121#31724
E-mail: houston0219@mail.nctu.edu.tw

選項: 按一下[詳細資訊](#), 以瞭解更多存取政策的相關資訊。

按一下「[繼續](#)」, 以立即檢視與工作相關的網站。 [繼續](#)

按一下「[返回](#)」或利用瀏覽器的「上一頁」按鈕, 回到上一頁。 [返回](#)



區網服務項目

➤ 不當網頁阻擋服務：

- 提供學童乾淨的校園網路學習環境。

➤ PROXY服務：

➤ 教育部網站應用程式弱點監測平台服務：

- URL：<http://ewavs.hcrc.edu.tw/>
- 針對SQL-Injection及XSS進行檢測。

修護建議

範例介紹：	透過網頁上的 TextBox 控制項輸入資料或直接從IE的URL網址列輸入攻擊字串
防護方法：	嚴格限制回傳參數與過濾輸入之特殊字元, 要防止XSS跨站式腳本攻擊主要是要在查詢字元串(QueryString)，表單數據 (PostData) 以及Cookie甚至HTTP報頭 (Header) 中防止掉一些javascript關鍵字和一些敏感的字元 (單引號, 分號) 以及SQL語言的關鍵字, 以及防止他們使用encode編碼。
修護方式：	聲明：以下動作可能會導致網站功能出現錯誤，修改弱點程式檔前請先備份檔案。 Step1: 到網站伺服器預設根目錄C:/Program Files/Apache Group/Apache2/htdocs或使用者自行設定的目錄，找出弱點程式，並進行備份。 Step2: 檔案備份完成後，用文字編輯器開啓弱點檔案ex: filename.php，搜尋(Ctrl+F)出弱點參數ex: \$_POST['argument']，在該檔案的位置。 Step3: 找到弱點參數後，在弱點參數前面加入下列任一函式，ex: addslashes(\$_POST['argument']) <pre> } } else { //如果magic_quotes_gpc=On，那麼就不處理 } //返回\$content return \$content; }??> </pre> 將需要引用在資料庫查詢等等中的字元前面加上反斜線，傳回加上反斜線的字串，這些字元有單引號(')、雙引號(")、斜線(\)及NULL(null byte)。 fgetss --- 取得檔案指標所指的行及去除HTML標籤 語法: string fgetss (int fp, int length [, string allowable_tags]) 說明: 與fgets()相同，不同處在於此函式會試著去除所讀取檔案中，任何的HTML及PHP的標籤。你可以使用參數allowable_tags來決定那個標籤不被去除。 strip_tags --- 去除字串中的HTML和PHP標籤 語法: string strip_tags (string str [, string allowable_tags]) 說明: 此函式試著從給予的字串中去除所有HTML和PHP標籤，如果是不完整或是假的標籤時則會有錯誤，它和fgetss()使用相同的方法去除標籤。你可以使用第三個參數來指定不去除那些標籤。 利用格式檢查方式避免對數字型別進行的SQL Injection攻擊
造成影響：	此為惡作劇程式、顯示討厭的訊息、廣告視窗等程式或物件。 而攻擊者可利用XSS弱點可造成以下更重大的影響與危害： -- 盜取各類用戶帳號，如機器登錄帳號、用戶網銀帳號、各類管理員帳號 -- 控制瀏覽器，進而竊取、篡改、添加、刪除企業敏感性資料 -- 盜竊企業重要的具有商業價值的資料 -- 非法轉帳 -- 強制發送電子郵件 -- 網站掛馬 -- 控制受害者機器向其它網站發起攻擊

活動訊息：

➤教育部網站應用程式弱點監測平台

- 說明會：6/18(五):13:30~16:30
- 教育訓練：7/29(四)~7/30(五):9:00~16:30
- 地點：交通大學-資訊技術服務中心-PC4教室
- 報名網址：<http://www.twisc.ncku.edu.tw/seminar/>