**PHP重點複習**

**PHP Mail**

* Mail server可以自己架設，也可以使用中華電信等isp的server，範例檔案就是以中華電信為SMTP server。
* 因為smtp規定郵件的内容必须全部是7-bit的us-ascii碼，且76字符需加一個換行符號。

所以必須將郵件內容序列化(base64)轉換成ascii碼，並用chunk\_split ()函數做分行動作。

* 透過程式在headr部分可自訂寄件者信箱，所以寄件者可以伪造。
* 有附檔時content-type為….，且每個文件開頭都要有一個獨有的ID
* 目前有pear，phpmailer等第三方Source

**MYSQL**

* Mysql有以關聯陣列傳回資料函數(mysql\_fetch\_assoc)，和數字陣列函數(mysql\_fetch\_row )。
* 關聯陣列是以字串做索引值(“name”,”tel”,….)，數字陣列是以數字做索引值(0,1,2,..)。
* 數字陣列可直接透過index存取，但若我們不知道關聯陣列的欄位名稱，可透過foreach依然可以做依序存取的動作。

**PDO**

Pdo讓各種不同的資料庫系統都使用同一套函式庫處理資料庫，只要在dsn設定為何種資料庫系統。

**Session**

* 從開啟網頁到關閉網頁為一個Session連線。
* 不同瀏覽器有不同的session連線。
* 每個人的session也是獨立不同的，有自己的session id。

**XML**

* xml命名空間：當一份xml文件有來自其他應用程式或xml詞彙的標記，此時可能發生名稱相同的衝突，這時可為xml標記建立命名空間。讓xml解析器能分辨兩個是不同的標記。
* asXML()函數：無帶參數則將xml存回原xml檔案；如果帶參數如asXML (“xxx”)則將XML寫入xxx檔案。
* XPath是一個簡單的語言，類似檔案系統的路徑命名方式。可以選出 XML檔案中，路徑符合某個模式的所有節點出來。
* 有三種處理XML的方法 , DOM , SAX , SimpleXML。

Spry (補Demo)

* 充分了解命名空間 , DTD屬性之應用。

網站安全性(待補Demo)

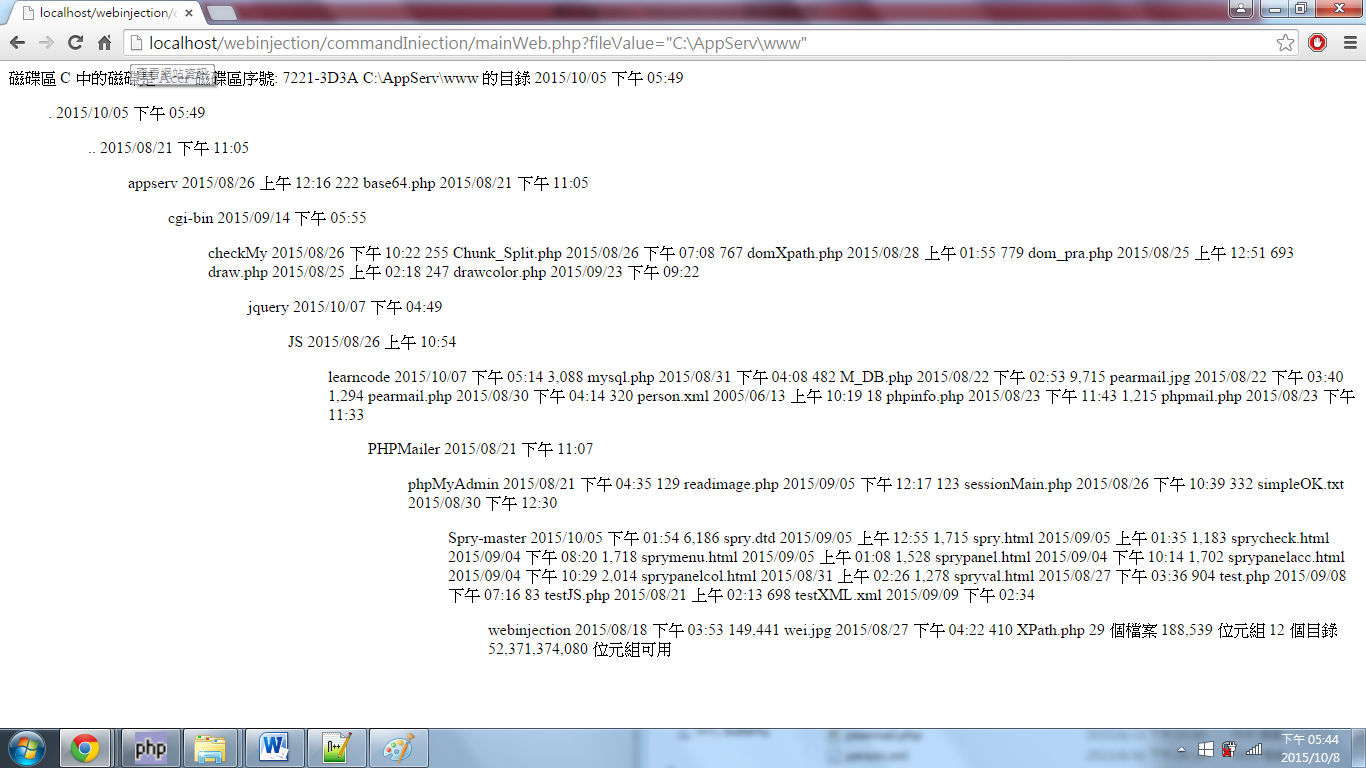
* Register Globals (可更改Session值 ,php.ini)
* Magic Quotes，自動加入跳脫字元
* **command injection** (透過處理字元或某些函數可解決)

$fileValue=$\_GET["fileValue"];

system("dir ".$fileValue);

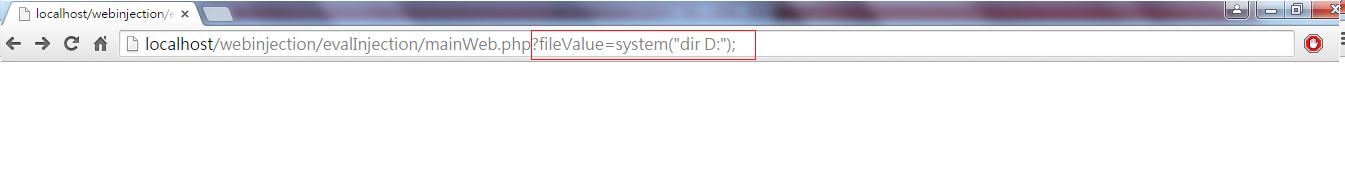


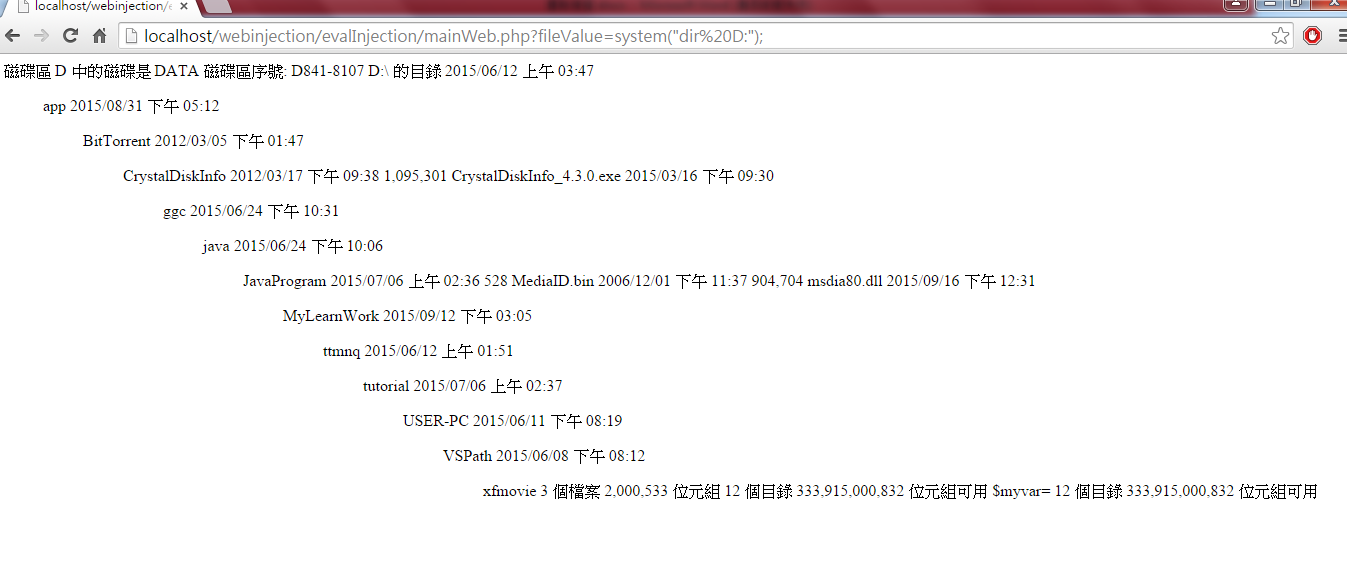
攻擊結果:



* **eval injection**

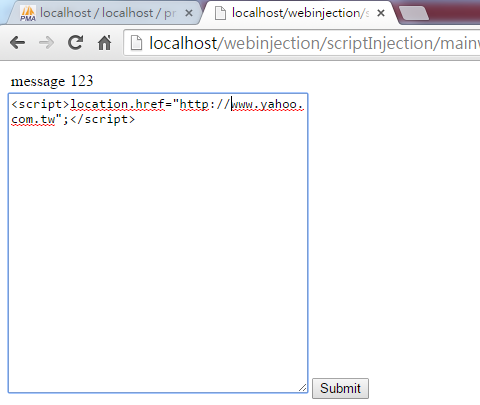
args = system(“dir c:”);

攻擊結果



* **ScriptInjection**

範例中為駭客植入攻擊執行碼在留言版上，使用者瀏覽時會從資料庫讀出駭客留言的攻擊碼而受到攻擊。

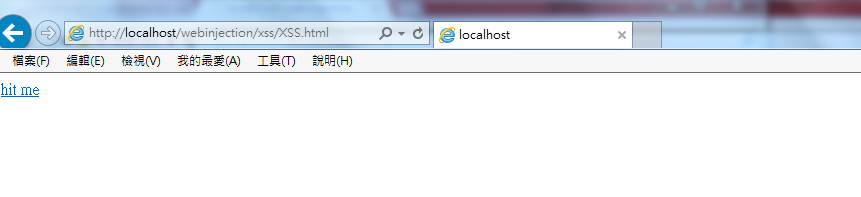


攻擊結果:



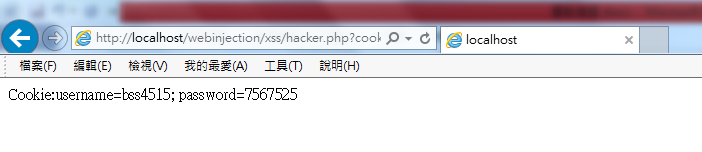
* **Cross Site Script**

範例中藉由Xss.html的惡意連結到有Xss漏洞的site.php，利用document.cookies傳回site.php與受害人之間的cookies給駭客。

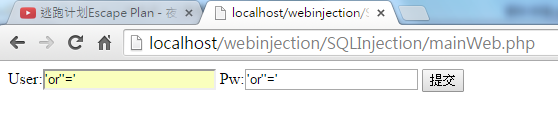


攻擊結果

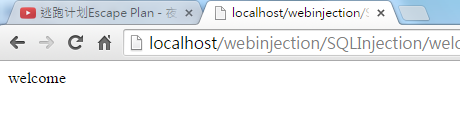
過程中連結過site.php並傳送其cooike到hacker.php



* **SQL植入攻擊**

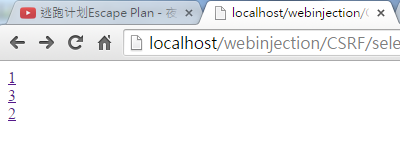


攻擊結果

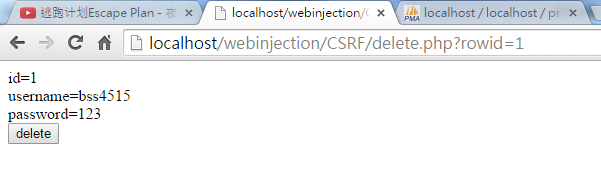


* **Cross Site Request Forgeries(CSRF)**

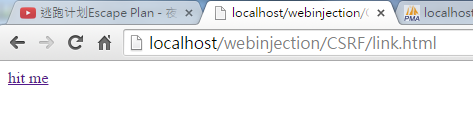
Select.php顯示有3筆資料



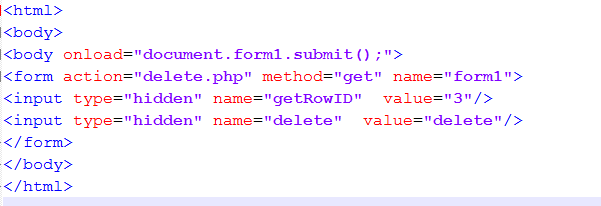
點選id連結進入delete.php(刪除功能頁面)顯示該筆資料



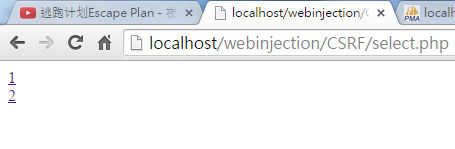
駭客攻擊頁面link.html(hit me連結至CSRF.html攻擊頁面)



CSRF.html(藉由使用者自己發出http請求將id=3的資料刪除)

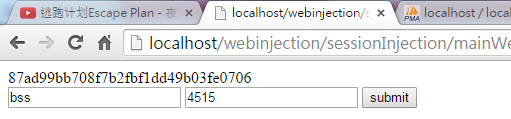


攻擊結果

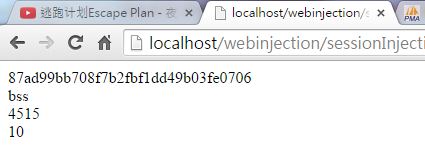


* **Session挾持攻擊**

mainWeb.php設定帳密與item參數=10，87ad…0706為sessionid

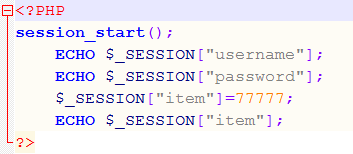


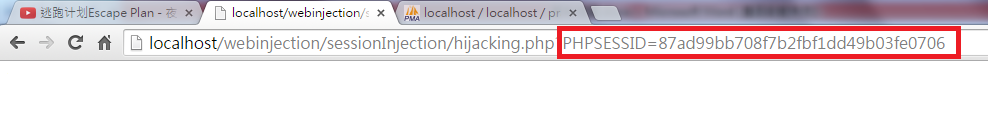
Welcome.php(顯示session資料)

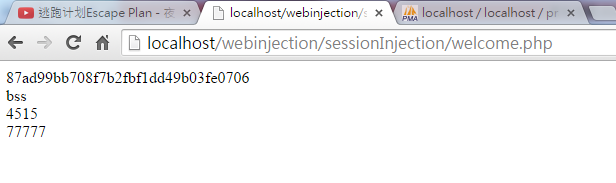


**攻擊結果**

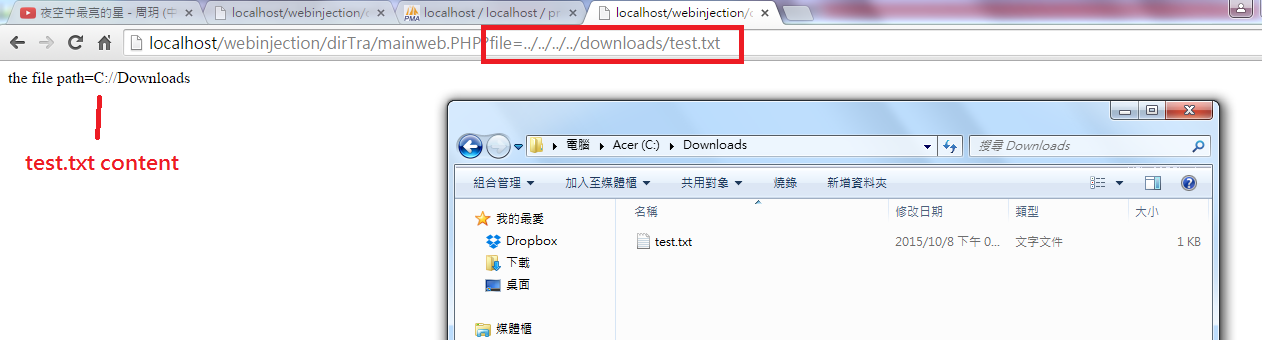
hijacking.php(藉由sessionid去更改參數item)



Welcome.php



* **目錄遊走攻擊**



AJAX