



專題實驗組


資四A 98156113 林義泓

資四A 98156118 陳昱廷

初階網頁安全防護



目錄

- 環境架構介紹
 - 初階網頁安全防護
 - 參考資料
- 

環境架構介紹

- JSP 動態網頁
- DREAMWEAVER介紹
- CSS介紹
- 環境架構影片

初階網頁安全防護

- 前言
- 網頁入侵之SQL injection
- 網頁破解-範本一(影片)
- 網頁破解-範本二(影片)
- 附件-本次injection使用之語法介紹

前言

- 一般撰寫網頁時，程式設計師習慣將SQL語言傳遞給資料庫執行，藉此來建立或刪除資料，這是因為關聯式資料庫所有的動作都是遵循SQL命令，可以很方便的完全各種資料維護，但正是因為如此，只要有漏洞，同樣藉由SQL命令，將造成很大的危害，而我們的研究項目即是，以兩個版本的網頁，比較有無防護的差別，藉由SQL injection讓大家知道，有哪些需要注意的地方。

網頁入侵之SQL injection

- SQL injection被稱為駭客的填空遊戲，是一種故意製造錯誤，來利用錯誤訊息得知資料庫架構方式，藉以入侵網頁來影響網頁執行，達到獲得資料、偽造資料、破壞資料的方式。

網頁破解-範本一(影片)

- 網頁破解-範本一(影片)

網頁破解-範本二(影片)

- 網頁破解-範本二(影片)

附件

- 本次injection使用之語法介紹

本次injection使用之語法介紹

- HAVING

---先隨意輸入HAVING指令，不包含GROUP BY, 藉此會從錯誤訊息得到資料表名稱及一個欄位名稱。

- GROUP BY

---補上GROUP BY指令及得到的名稱，因為輸入的是正確的名稱，而由於HAVING 1=1的指令沒有滿足欄位可供判斷，仍會繼續錯誤而給出後面欄位值，不停補上直到錯誤訊息不回傳名稱為止，則可以得到所有欄位名稱。

本次injection使用之語法介紹

- INSERT

---而此時若資料庫設計不良，屬性皆為字串，即可能立即INSERT新資料。

如`;
INSERT INTO EMPLOYEE
VALUES('hacker','hacker','hacker')--

- UNION搭配INSERT

---假若資料庫欄位屬性不同，透過`UNION
SELECT 'abc',1,1,1 FROM tblUser --，假如第一個屬性原為int，將回報錯誤，第一欄位為int，藉此可試出所有欄位屬性。

本次injection使用之語法介紹

- UNION來獲得帳號

---`UNION SELECT UserName,1,1,1 FROM tblUser WHERE UserName>'a'--，假設第一個欄位為int，故意使他對應錯誤，我們將得到一個正確的，符合條件UserName>'a'的正確UserName。

- UNION來獲得密碼

---`UNION SELECT Password,1,1,1 FROM tblUser WHERE UserName='admin'--，若SELECT第一個欄位為int，故意使他對應Password將錯誤，會回報出UserName為'admin'的密碼是什麼。

參考資料

- http://www.microsoft.com/Taiwan/sql/SQL_injection_G1.htm
- <http://neural.cs.nthu.edu.tw/jang/books/asp/sql01.asp?title=18-3%A8%CF%A5%CE%20SQL%20%A8%D3%Co%CB%B5%F8%B8%EA%AE%C6>
- http://www.cg.com.tw/dreamweaver/htm/Dreamweaver_001.asp
- <http://www.csie.nctu.edu.tw/~yctsao/t1/index.htm>

參考資料

- SQL SERVER 2008 資料庫設計與應用(陳祥輝著)
- JSP 2.2 動態網頁技術第四版(呂文達著)