**Computer Security HW0x4**

R08946007 資科所 蔡昀達

Nickname : r08946007

**how2xss**

1. 嘗試輸入發現會過濾除付的字元
2. 使用html encode跟unicode encode成功alert
3. 查到一些可以bypass 長度限制的方法，湊domain塞import有點麻煩，後來採用eval(name)的方法
4. 先放一個網頁設定name讓admin訪問再導到dom-xss的網頁就可以成功執行
5. FLAG{babyxss\_easy\_peasy\_yo}

**Cathub**

1. 先用投影片上教的測試sql injection去試哪個地方有機會，發現vid?最可疑，會過濾空白字元還會跳出bad cat
2. 使用/\*\*/替換空白
3. 嘗試幾次發現是oracle db
4. 使用union based的方法，使用order by發現有3個欄位，又發現資料型態不同，第一欄為數字，二三欄為字串
5. 第二欄位會輸出結果在頁面，因此使用
   1. sys.database\_name
   2. user
   3. table\_name from all\_table
   4. column\_name from all\_columns
6. 先使用order by和offset觀察table\_name
7. 寫scipt爆出所有table name找到S3CRET
8. 接著要找出column\_name，但因為過慮引號，因此使用 in 來指定table\_name

select column\_name from all\_tab\_collumns where table\_name in (select table\_name from all\_tables order by table\_name offset 44)

1. 找到Very secret column

FLAG{hey\_\_\_or@cle\_d4tab4s3\_\_inj3cti0n\_i5\_\_\_\_to0OoO0ooO0OO\_e4sy!!!!!??}