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
   i. sys.database_name
   ii. user
   iii. table_name from all_table
   iv. 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)
9. 找到 Very secret column
   FLAG{hey___or@cle_d4tab4s3__inj3cti0n_i5____to0OoO0ooO0OO_e4sy!!!!!??}