CTF hw7

> b05902127 劉俊緯

Cei8a

> FLAG{Easy_blacbox_postgresql_injection:)}

- Login去github打cei8a就會看到kaibro創了repo裡面放了帳號密碼。
- 進去之後，存好cookie，對所有網頁都掃一遍sqlmap，就可以找到教師頁面的td是injectable。之後就一個一個搜尋，找到flag放在public後，dump出來即可。

```
python2 sqlmap.py -u "http://csie.ctf.tw:10137/teacher.php?op=s2&td=admin" --cookie
"my_cookie" -dbms mysql -level 3  --tamper=space2comment --dump -D public
```

XSS_kitichen

> FLAG{y0u_R_XsS_M4st3r!}

- baseline: 先以" , --> , ' 等各種字串結尾後接 `<script>alert()</script>`
  - `"--><script>alert()</script>`
- 之後拿官方html每一個element的結尾都trytrysee，寫個script去暴搜，就可以解完囉~
- 爆搜完後一個一個接上去，去可以拿到10項料理惹：`</xmp></script></title></style>"--><script>alert()</script>`
- (雖然kaibro之後用CSRF擋掉爬蟲惹，不過我們還是可以一個一個試試看(meta)。)