

# CTF Writeup

R10922043 黃政瑋

## 比賽資訊:

Data: 2021/11/20~2021/11/21 online

CTF account: cwhuang1937

Team: labaCCS

Member: 黃政瑋、李柏漢、吳添毅、洪邵澤(交大)

Rank: 38

## Square CTF 2021

星期六, 20 十一月 2021, 09:00 CST — 星期日, 21 十一月 2021, 09:00 CST 📅

### On-line

A [Square CTF](#) event.

Format: Jeopardy 🎲

Official URL: <https://squarectf.com/>



### Participated in CTF events

2021

Overall rating place: 5189 with 5,540 pts in 2021

Country place: 47

Place	Event	CTF points	Rating points
38	<a href="#">Square CTF 2021</a>	300.0000	5.540

### Team members

Current

[cwhuang1937](#)

[ntu-ye](#)

[phlee1117](#)

[ccs100203](#)

		2:44:58 PM EST	
38	labaCCS	300	Nov 20, 2021 @ 3:01:47 PM EST

## 前言:

這次是第一次比 CTF 比賽，最後解出了三題(柏漢 2 題、添毅 1 題)拿到了 38 名的成績。那時比賽時，才剛學完 web，基本上 reverse 跟 pwn 我都還不大會，只有解過 hw0 時很淺很淺的知識。剛好這次幾題比較簡單的都放在 reverse，那時我還沒看 reverse 第一周的課程...因此很多 reverse 基本的知識都沒有，很可惜一題都沒有解出來。

這篇挑幾題我想了很久跟後來賽後讓我感觸最深的題目。

### 1. Huge Primes(Web, 50, solved)

這題為 web，基本上是簽到的水題，給你一個很大的質數，要讓你求出是哪兩個大數相乘，直接用 sage 的 factor()跑一段時間即可拿到 flag。這題由於添毅是用桌機，因此他第一個跑出來並拿到 flag。

### 2. its just an xor(reversing, 150 solved)

這題的分類非常奇怪，雖然是 reverse，但卻需要連上 remote 才能拿 flag。題目看起來非常簡單，用 IDA 看會發現單純把輸入跟 key 做 xor 後要等於“yoteyeet”即可拿到 flag，我們在本地端也成功拿到 flag 了，但 remote 怎樣都拿不到。

```

8
9 v8 = __readfsqword(0x28u);
10 puts("password pls, no brute forcing:");
11 fgets((char *)s, 64, stdin);
12 s1 = s[0] ^ xor_key;
13 sleep(2u);
14 if ( !strcmp((const char *)&s1, "yoteyeet") )
15 {
16     stream = fopen("flag.txt", "r");
17     fgets(v7, 64, stream);
18     fclose(stream);
19     printf("nice work, here's the flag! %s", v7);

```

後來 deadline 前柏漢有在 init 那邊發現，這程式會用 `sys_ptrace` 判斷有沒

有掛上 `gdb`，有掛上的話則會將 `key` 改掉，發現了之後即可成功解決

`remote` 會錯的問題，並拿到 flag。

```

8 result = (_QWORD *)sys_ptrace(0LL, 0LL, 0LL, v0);
9 if ( (_DWORD)result != -1 )
10 {
11     for ( i = 0; i <= 255; i += 8 )
12     {
13         v3 = (_QWORD *)(i + ((unsigned __int64)_do_global
14         if ( *(_QWORD *)(i + ((unsigned __int64)_do_glot
15             break;
16     }
17     result = v3;
18     *v3 ^= 0x119011901190119uLL;
19 }
20 return result;
21}

```

後來上完 reverse 後，覺得這題真的是超級超級簡單!就只是最基本的在 init

或 fini 中藏東西而已，真的深深明白，沒看過的東西，真的想再久都很難想

出來，也希望之後期末能好好利用所學把該解的解出來。

### 3. Korean Space Program(web, 150 unsolved)

這題是看了官方的解答才會的，這題非常的...簡單?!

簡單來說這題當時看了半天都沒有發現任何漏洞，原來是他的空白不是真的

空白，而是 `U+3164`(為 Hangul Filler，一個韓文的填充字)，在 browser

上並看不出來，但放在 vscode 就可以發現怪怪的，如下圖所示。

```
25 app.get('/login', async (req, res) => {
26   const {
27     username,
28     password,
29   } = req.query;
30
31   // Note: Auth check here, only bypassable in staging or dev envs
32   if ((stringsEqual(USERNAME, username) && stringsEqual(PASSWORD, password)) ||
33       (+ENV_STAGE_EAST == +ENVIRONMENT || +ENV_STAGE_WEST == +ENVIRONMENT) ||
34       (+ENV_DEV_EAST == +ENVIRONMENT || +ENV_DEV_WEST == +ENVIRONMENT)) {
35     res.status(200);
36     res.send(FLAG);
37   } else {
38     res.status(401);
39     res.send('UNAUTHORIZED');
40   }
41 });
```

知道藏有那個奇怪的填充字後，這題的判斷式就很好 bypass。最後很可惜的就錯失了 200 分的題目。

## 賽後心得:

這次是我的第一次比賽，很可惜一題都沒有解出來，但現在學完 pwn 跟 reverse 了，作業也都算很順利的寫出來，希望 final CTF 能好好在這兩個題型有所貢獻(雪當時比賽一題都沒解出來的恥)。

比賽會有時間的壓力，我覺得可以讓我更專注，更可以絞盡腦汁想各種方法，我覺得非常有趣，也希望結束這學期的課程後，偶爾也能參與線上的 CTF，然後從中學到一些新知識，並讓自己動動腦。