**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)

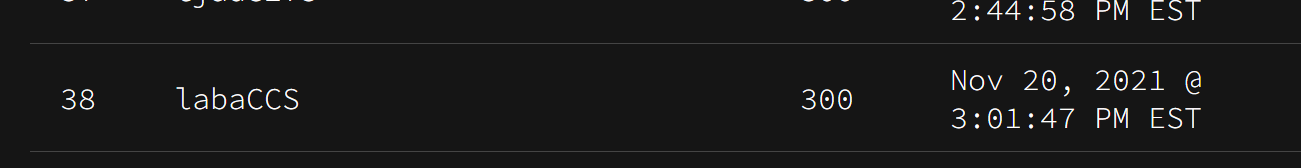
Rank: 38

一張含有 文字 的圖片

自動產生的描述

一張含有 文字 的圖片

自動產生的描述



**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。

1. **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。

一張含有 文字 的圖片

自動產生的描述

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。

一張含有 文字 的圖片

自動產生的描述

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。

1. **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。

一張含有 文字, 監視器, 螢幕擷取畫面, 螢幕 的圖片

自動產生的描述

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。