CTF 微心得

ddaa

Who am I

- dada = ddaa = 0xddaa = 達達 != 大大
- Start to play CTF since last year
- One of the members in HITCON CTF team.

故事的開始是這樣的

大四跨校選課，選修程式安全

http://wargame.cs.nctu.edu.tw

幹，好難

~~(助教可以給更多 hint 嗎 T_T)~~

結果研究所不小心進了 SQLab……

學長：”你們也有報名 HITCON ？

那當天就一起來打 wargame 吧。“

我：“……OAO ”

一題都沒解出來 T___T

可是拿到冠軍了，學長們太強了 XD

一題[illegible]_T

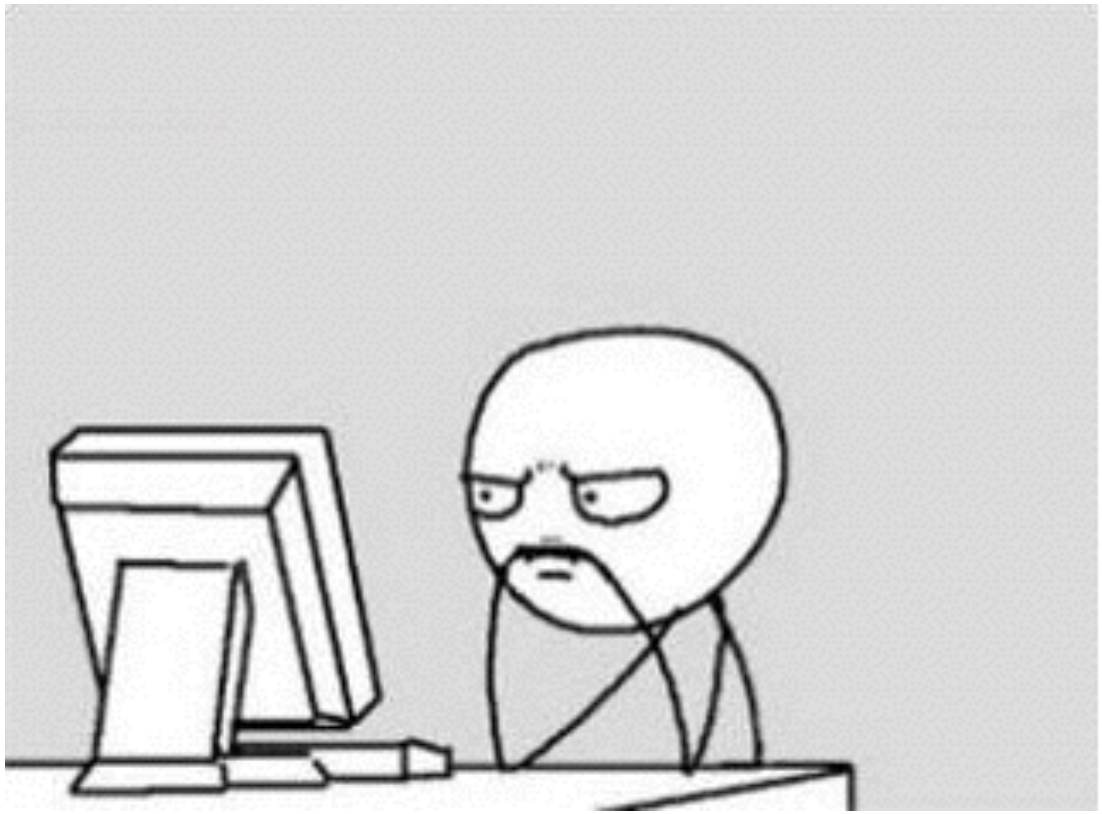
可是拿到冠[illegible]太強了 XD

因為 CTF 很好玩

後來就一直玩一直玩一直玩 (?)

（不過一開始都解不出來....）

Before solving the problem…



After solving the problem…

第一個解出的 CTF 題目

- 30C3CTF 2013 NUMBERS 100 guess
- 猜數字
- 破解偽隨機數生成器
- Mersenne Twister
- http://ddaa.logdown.com/posts/171272-30c3ctf-numbers-100-guess

~~（到現在還是覺得這題不該只值 100 分啊 Q＿＿Q）~~

第一個解出的 CTF 題目

- 30C3CTF 2013 NUMBERS 100 guess

```
You have 1/10 right guesses, whats your next guess? Yes! That was correct, awesome...
You have 2/10 right guesses, whats your next guess? Yes! That was correct, awesome...
You have 3/10 right guesses, whats your next guess? Yes! That was correct, awesome...
You have 4/10 right guesses, whats your next guess? Yes! That was correct, awesome...
You have 5/10 right guesses, whats your next guess? Yes! That was correct, awesome...
You have 6/10 right guesses, whats your next guess? Yes! That was correct, awesome...
You have 7/10 right guesses, whats your next guess? Yes! That was correct, awesome...
You have 8/10 right guesses, whats your next guess? Yes! That was correct, awesome...
You have 9/10 right guesses, whats your next guess? You did it! The flag is: 30C3_b9b1579866cccd28b1918302382c9107
```

  - numbers 100 guess

~~（到現在還是覺得這題不該只值 100 分啊 Q＿＿Q）~~

哇哦，CTF 好有趣，該如何入門呢？

http://overthewire.org/wargames/

http://bright-shadows.net/

http://wargame.cs.nctu.edu.tw/

1. 選一題你認為比較有趣
或是比較有可能解的題目

如果完全沒有頭緒，得先 google 一些題目相關的背景知識

2. 努力看懂題目，接著試著想出這題的解法

如果一時想不出來，也可以跟別人討論看看

但別直接去找解答來看 >__<

3. 如果想法正確，恭喜成功拿到 flag :D

將過程寫成 write up，並且與其他人交流做法~

4. 如果想法錯誤，別氣餒，想想其他的解法

可能會花上數小時、甚至數天

但是在摸索的同時也會慢慢進步！！

5. 如果到最後還是想不出來
就看看其他人的 write up 吧 :P

照著做一遍，真正弄懂這題的解法
下次遇到類似的題目就會做了！

其實打 CTF 只需要...

興趣 + 耐心 + 求知慾

程式能力, 逆向工程, 密碼學, 演算法, 資訊隱藏, 鑑識分析, 滲透測試, ... , etc

這些都可以慢慢學 XD

The most important……

Never give up!!!

也可以參考台大或交大的課程網頁

https://csie.ctf.tw/

http://secprog.cs.nctu.edu.tw/

~~王商時間 (誤)~~