**Computer Security HW0x7**

R08946007 資科所 蔡昀達

Nickname : r08946007

**Casino++**

1. 跟casino不同的地方是想要利用leak address的方式找到syscall位置
2. 先利用改寫puts@got來達到回圈執行casino涵式，可以多次寫記憶體
3. 因為seed變數可控，因此把srand@got 改寫成 printf@plt，把seed改寫成libc\_start\_main@got 來達到leak
4. Leak 出base address 之後算出syscall位置
5. 把atoi@got改寫成syscall位置
6. 再下一次read\_int涵式輸入/bin/sh 成功get shell
7. FLAG{Y0u\_pwned\_me\_ag4in!\_Pwn1ng\_n3v3r\_di4\_!}
8. 過程中syscall一直失敗，一直跳到vprintf，過很久才發現是link到本機的libc，吐血

* objdump –d casino++
  + printf@got, printf@plt
  + puts@got, puts@plt
  + atoi@got, atoi@plt
* objdump –R casino++
  + libc\_start\_main@got
* readelf –s ./libc.so | grep “libc\_start”
  + libc\_start\_main offset
* readelf –s ./libc.so | grep “system”
  + system offset