**郭又嘉**

**AosoraKuo**

**B06705020**

**Casino++**

這題就是用上次的漏洞去改GOT

首先把PUTS的GOT改成CASINO

這麼一來程式可以一直進行迴圈

然後要leak出base的值

所以選用libc\_start\_main來把它用改GOT的方式塞進seed裡面

再把srand改成printf

如此一來我們就有了printf(libc\_start\_main的library address)

接下來用助教上課交的方法把他減掉offset的值

就可以得到base

再來把system的offset加上去

然後把name改成 ‘/bin/sh\0’ 放到seed裡面去

最後把printf再次改成system

就可以system(‘/bin/sh\0’)取得shell

再來就是去/home/casino++/cat flag拿flag