楊力行 b06705001 b06705001

先用 ida 查看程式， NX 跟 ASLR 都是關著的

首先發現 name 可以 overflow 並且改變 seed 的值，以此可以固定 lottery 的值，再利用動態分析就可以輕鬆地讓程式輸出 you win，接著發現 name 這裡無法動到其他的地方以及暫存器，因此需要找其他的洞，接著發現藉由給予 guess[idx] 中的 idx 負的值可以修改到 GOT 表的內容，而每次可以修改 4 個 BYTES 可修改 2 次共 8 個 BYTES，可以完成 GOT HIJACKING，而在 casino 中 put 函式只有在輸出 you win 時才被呼叫，也就是不會在修改一半時就被呼叫到，因此選擇對它進行劫持，又因為 NX 是關著的，所以直接利用 NAME，在 AGE 的後面寫下 execve(/bin/sh)的 shellcode，再將 put@got.plt 的指向位址改成 shellcode 的開頭 0x602108 就完成了。

具體執行時，先用 NAME 的 GET overflow 將 SEED 修改，並把 shellcode 放到 age 後，接著隨便輸入>20 的數字到 AGE 再來先輸入錯誤的 guess，接者選擇要修改，先輸入-43(0x6020d0 到 0x602020 的差除上 int 的 4 個 BYTES 為-44，又輸入後會自動減一)，再輸入 6299912(0x602108 的十進位)再來輸入正確的 guess 再輸入-42，改 0x602024-0x602027 的值為 0，就成功 get shell 了，之後在 home/casino/flag 找到了 FLAG。