**Computer Security HW0x5**

R08946007 資科所 蔡昀達

Nickname : r08946007

**Casino**

1. 首先觀察source code可以發現使用的變數存在global，因此先把這些變數位置找出來

0x00000000006020b0 lottery

0x00000000006020d0 guess

0x00000000006020f0 name

0x0000000000602100 seed

0x0000000000602104 age

1. 觀察source code發現可以任意寫記憶體的地方

line51 : guess[idx] = read\_int();

1. 觀察source code發現read(0,name,0x100)會overflow，可以輸入0x100個byte
2. 通靈許久後終於發現可以got hijack，因此先用objdump找到got table存放各涵式的位置
3. 綜合以上擬訂策略:
   1. 將shellcode放在name變數
   2. 因為name會overflow覆蓋到age的位置，因此輸入age必須要保持shellcode的完整性
   3. 因為puts涵式剛好會先呼叫到一次，因此將got table的puts位置蓋成name的位置，也就是guess[-44]的位置，在第二次回圈時覆蓋成功後進入guess=lottery可以呼叫第二次puts
   4. 在guess[idx] = read\_int(); 複寫記憶體時 因為只能寫4byte因此必須複寫兩次才能覆蓋完整