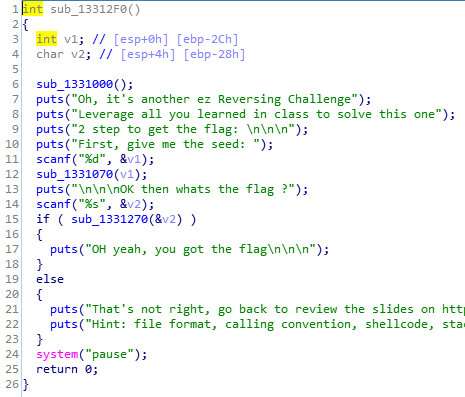
**Computer Security HW0x2**

R08946007 資科所 蔡昀達

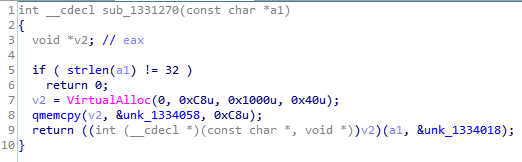
Nickname : r08946007

1. 使用ida pro & hex ray decompiler 先decompile IDAmudamudamuda.exe 可以得到原始碼大概理解這隻程式的功能



1. 找到seed跟flag兩個涵式

Flag:

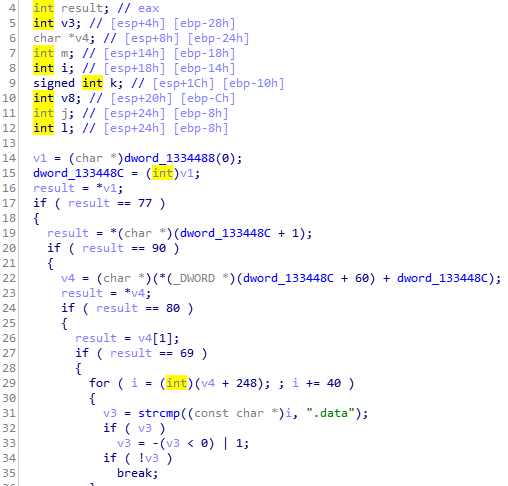


可以發現flag的涵式將 &4058 位置載入記憶體並做為涵式執行

&4058 記憶體位置內容為一段shellcode

輸入的flag和 &4018 位置的內容做為參數傳進涵式

Seed:



可以發現seed 涵式只有在最下面的地方使用到輸入的seed變數

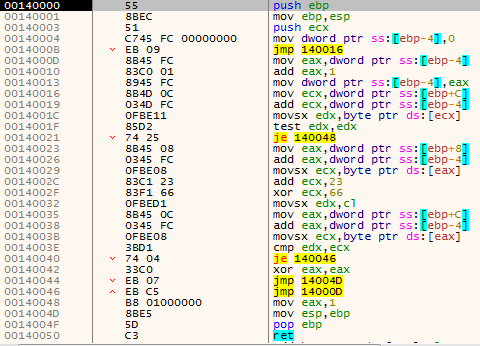
觀察可以發現他在更改某一段記憶體

正好是flag涵式中shellcode的位置

因此可以理解為seed改寫 &4058 的記憶體內容讓他成為一段shellcode

1. 根據x86 calling convention合理猜測shellcode開頭為push結尾為ret來反推seed，可以得到正確的seed為16
2. 取的seed之後就得到了shellcode然後反組譯之後

可以發現這段組語將 &4018的記憶體內容 add 23然後xor 66 就會是正確的flag



1. 最終得到flag : FLAG{y3s!!y3s!!y3s!!0h\_my\_g0d!!}