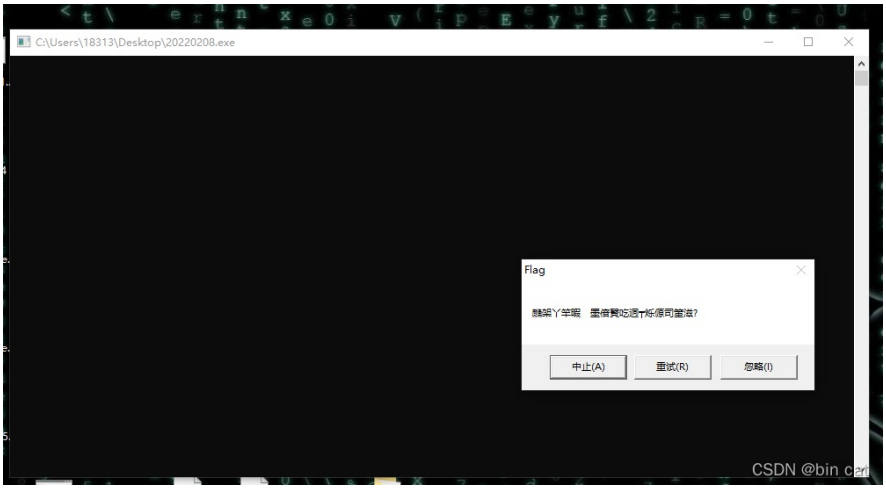
攻防世界csaw2013reversing2Writeup

原创

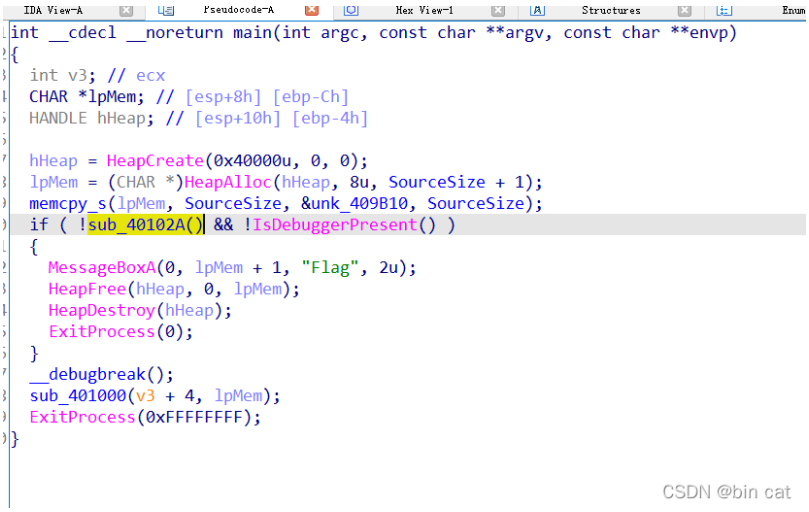
bin cat 于 2022-01-08 14:20:56 发布 231 收藏
文章标签： 安全

32位无壳

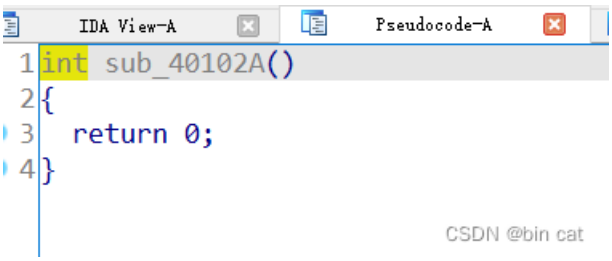
先试着运行exe文件，得到如下结果符合题目 描述输出的玩意是乱码



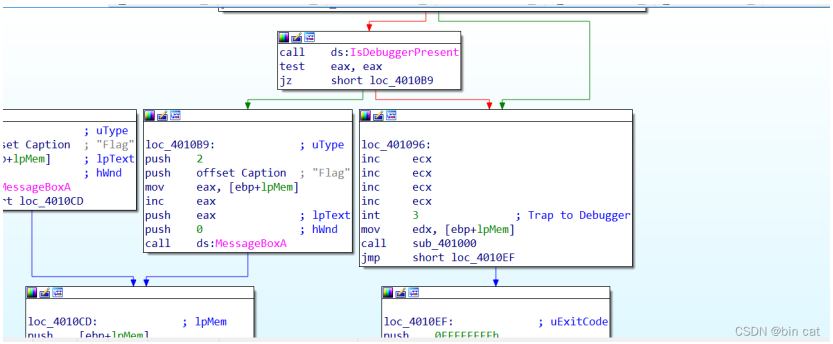
用ida解析



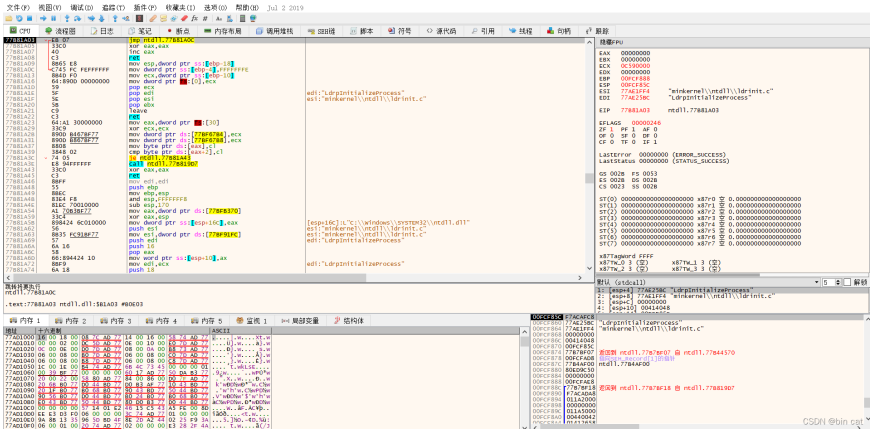
主函数逻辑，跟进sub_40102A()函数中



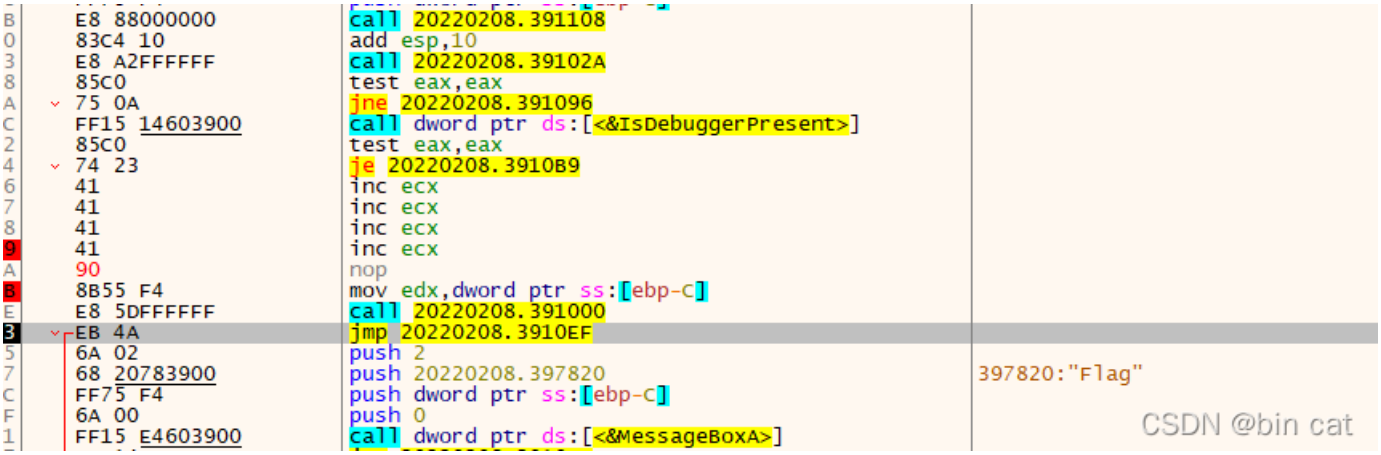
发现函数的返回值默认为0，但是!0就意味着if所包含的语句会一直被默认执行 ，联想到我们一开始看到程序运行起来的乱码，我们就确定if所包含的语句就是导致乱码发生的原因



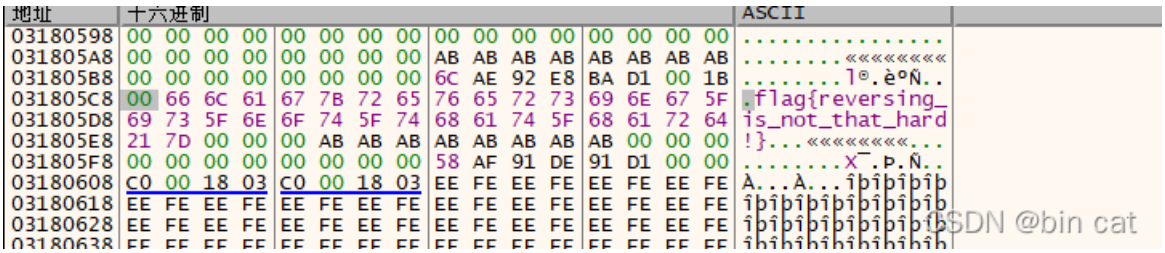
结合汇编发现if语句的默认正是跳过了sub_401000所以我们猜测这个被跳过的藏有flag



开始动态调试



执行完成后面就是退出不需要再执行此时edx地址中就存在flag



出flag

flag{reversing_is_not_that_hard!}

```
00391099    41              inc ecx
0039109A    90              nop
0039109B    8B55 F4         mov edx,dword ptr ss:[ebp-C]
0039109E    E8 5DFFFFFF     call 20220208.391000
003910A3    90              nop
003910A4    4A              dec edx
003910A5    6A 02           push 2
003910A7    68 20783900     push 20220208.397820                    3978
003910AC    FF75 F4         push dword ptr ss:[ebp-C]
003910AF    6A 00           push 0
003910B1    FF15 E4603900   call dword ptr ds:[<&MessageBoxA>]
003910B7  v EB 14           jmp 20220208.3910CD
003910B9    6A 02           push 2
003910BB    68 20783900     push 20220208.397820                    3978
003910C0    8B45 F4         mov eax,dword ptr ss:[ebp-C]
003910C3    40              inc eax
003910C4    50              push eax
003910C5    6A 00           push 0
003910C7    FF15 E4603900   call dword ptr ds:[<&MessageBoxA>]
003910CD    FF75 F4         push dword ptr ss:[ebp-C]
003910D0    6A 00           push 0
003910D2    FF75 FC         push dword ptr ss:[ebp-4]
003910D5    FF15 08603900   call dword ptr ds:[<&HeapFree>]
003910DB    8945 F8         mov dword ptr ss:[ebp-8],eax
003910DE    FF75 FC         push dword ptr ss:[ebp-4]
003910E1    FF15 0C603900   call dword ptr ds:[<&HeapDestroy>]
003910E7    6A 00           push 0
003910E9    FF15 00603900   call dword ptr ds:[<&ExitProcess>]
003910EF    6A FF           push FFFFFFFF
003910F1    FF15 00603900   call dword ptr ds:[<&ExitProcess>]
003910F7    C9              leave
003910F8    C3              ret
003910F9    3B0D 04903900   cmp ecx,dword ptr ds:[399004]
003910FF  v 75 02           jne 20220208.391103
00391101    F3:C3           ret
00391103  v E9 09020000     jmp 20220208.391311
00391108    8BFF            mov edi,edi
```


也可以将1处跳转nop掉单步走到003910C7去触发messageboxA

这样也能得flag