

第二题-wp

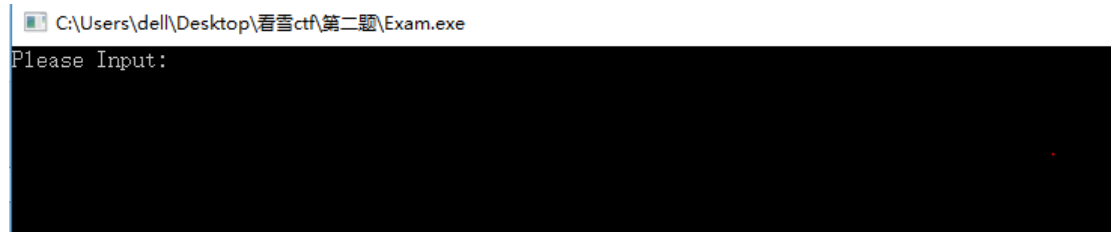
0x00

其实做了几道题才发现，逆向工程确实，跟它名字描述的一样，是一个逆向求解的过程，程序的执行是从上到下的过程，最后输出。而逆向工程是根据输出，找算法。

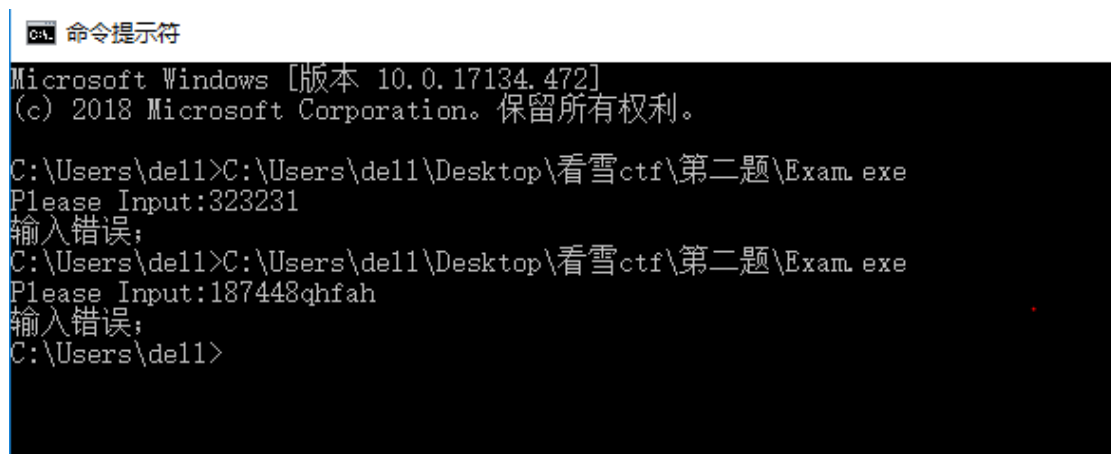
此篇题解根据看雪论坛诸位大佬的 writeup 所写，自己没做出来。

0x01

首先运行程序，任意输入，发现闪退，emmmm，



百度得到解决方法，使用 cmd，或者 powershell 运行



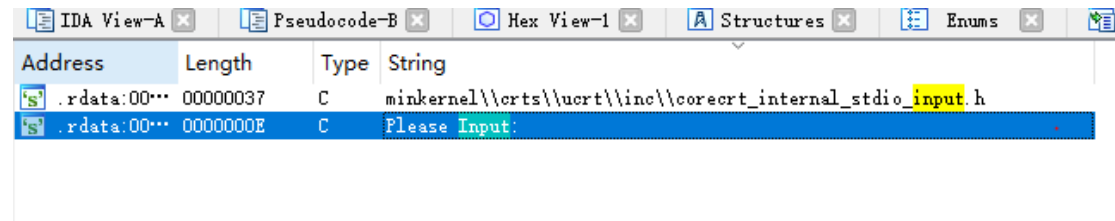
0x02

拖入 IDA，F5 失效，啥也出不来，找不到入口函数。

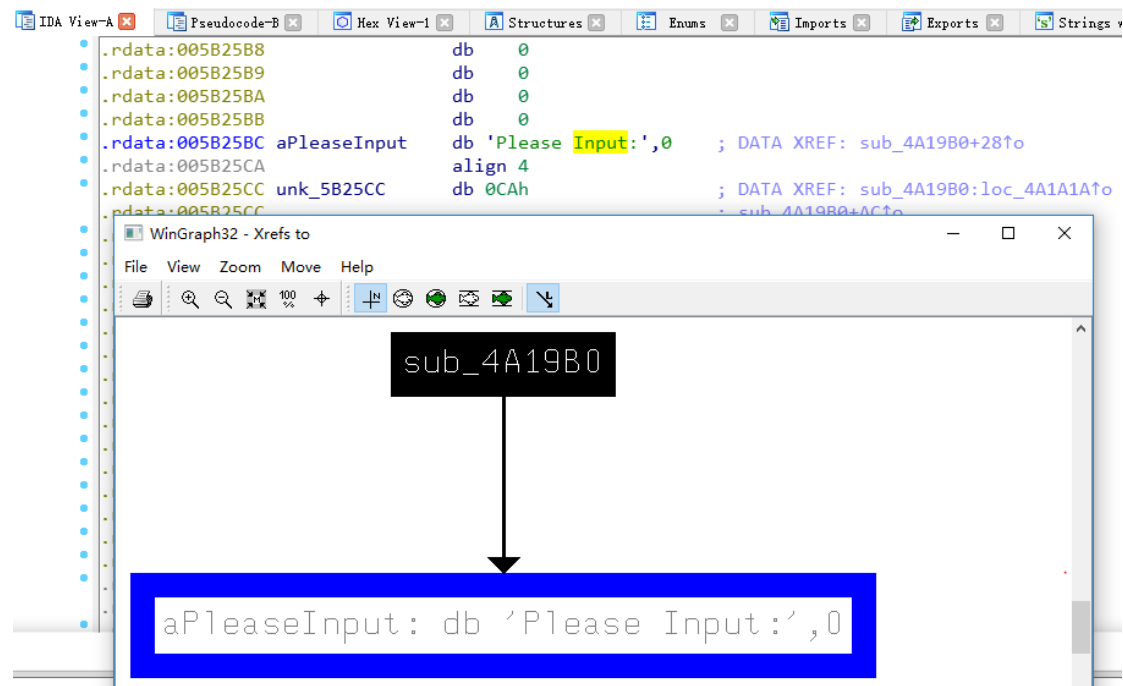
根据大佬 writeup，可以通过输出的 “Please input” 字符串查找入口函数。

它的原理根据我的理解就是，输出函数 printf 之类的这种函数执行之前，肯定会有函数对他进行调用。

于是通过 shift+12 查找字符串，“Please input”



点进去，查看哪个函数调用了它，使用右键——然后 xref



是 sub_4A19B0 函数，然后查看这个函数内容，双击函数，然后 F5

```

IDA Vie... Pseudocod... Pseudocod... Hex Vie... Structu... Enums Impo... Expo...
1 int __usercall sub_4A19B0@<eax>(int a1@<xmm0>)
2 {
3     int v1; // edx
4     int v2; // ecx
5     int v4; // [esp+D0h] [ebp-8h]
6
7     sub_48D7B4((int)&unk_5F6007);
8     printf((int)&unk_5F31E0, (int)"Please Input:");
9     scanf("%s", &input, 30);
10    v4 = len((int)&input);
11    if ( v4 > 30 || v4 < 10 ) // 判断输入长度是不是>30,或者<10,如果是,直接退出
12    {
13        sub_48A6DB(a1, (int)&unk_5B25CC);
14        exit(0);
15    }
16    sub_48E5BF(input1, 30, &input); // 这是把输入,拷贝到dword中
17    if ( *(_BYTE *)(&input1 + 7) != 'A' ) // 第8个字符==ascii (A)
18    {
19        sub_48A6DB(a1, (int)&unk_5B25CC); // 输入不正确
20        exit(0);
21    }
22    sub_48D3A4(a1, input1); // 又一次检验,下面看一下检验过程
23    return sub_48D935(v2, v1, 1, 0, a1);
24 }

```

函数具体逻辑：v5 是输入字符串的长度，输入长度要在 10-30 之间然后将输入做拷贝至另一空间，我命名为 input1，然后使用 input1 进行计算检查，首先检查，第 8 位是不是 A，不是 A 也直接结束程序运行。随后的 sub_48D3A4 也是一个检验，跟进去。需要跟两次

```

IDA Vie... Pseudocod... Pseudocod... Hex Vie... Structu... Enums
1 int __usercall sub_49DBD0@<eax>(int xmm0_4_0@<xmm0>, int a1)
2 {
3     int v2; // edx
4     int v3; // ecx
5     unsigned int i; // [esp+D0h] [ebp-8h]
6
7     sub_48D7B4((int)&unk_5F6007);
8     *(_BYTE *)(&a1 + 7) = 35;
9     for ( i = 0; i < len(a1); ++i )
10        *(_BYTE *)(&i + a1) ^= 0x1Fu;
11    return sub_48D935(v3, v2, 1, a1, xmm0_4_0);
12 }

```

这个函数，跟 input 暂时无关，拉出来独立讨论，a1 是参数，把 a1 的第 8 个字符变成 ascii (35) = ‘#’，然后将 a1 的每一位都与 0x1F 异或。
至此，主函数部分追踪完毕。

0x03

根据大佬 wp，经验+直觉，对全局变量 input1，查找引用，

xrefs to input1			
Direction	Type	Address	Text
Up	w	sub_495810+3E	mov input1, eax
Up	r	sub_49DC80:loc_49DCEC	mov eax, input1
Up	r	sub_4A19B0+87	mov eax, input1
Up	r	sub_4A19B0+9D	mov edx, input1
Down	r	sub_4A19B0:loc_4A1A70	mov eax, input1

Line 2 of 5

OK Cancel Search Help

找到了下面的函数

```

1 int __userpurge sub_49DC80@<eax>(int a1@<xmm0>, int a2)
2 {
3     int v2; // edx
4     int v3; // ecx
5     unsigned int i; // [esp+E8h] [ebp-14h]
6
7     sub_48D7B4((int)&unk_5F6007);
8     if ( a2 )
9     {
10         for ( i = 0; i < len(a2); ++i )
11             *(_BYTE *)(i + a2) ^= 0x1Cu;
12         if ( !cmp(a2, input1) )
13         {
14             sub_48B4AA(&unk_5F31E0, 'o');
15             sub_48B4AA(&unk_5F31E0, 'k');
16         }
17     }
18     return sub_48D935(v3, v2, 1, 0, a1);
19 }

```

这又是一个校验函数，将 a2 的每一位，与 0x1C 异或，比较 a2 与 input 两者是否相等。这时，a2 是什么，就很关键了。查找对于该函数的上层引用。

```

int __userpurge sub_48DACA@<eax>(int a1@<xmm0>, int a2)
{
    return sub_49DC80(a1, a2);
}

```

没东西，再来一次

```

1 int __usercall sub_49CEB0@<eax>(int a1@<xmm0>)
2 {
3     int v1; // eax
4     int v2; // edx
5     int v4; // [esp+0h] [ebp-E8h]
6
7     sub_48D7B4((int)&unk_5F6007);
8     v1 = sub_48DACA(a1, (int)aInvalidArgumen_1);
9     return sub_48D935(v4, v2, 1, v1, a1);
10 }

```

可以看到，变量出现了，aInvalidArgumen_1，跟进去，查看值

```

.data:005F1000 aInvalidArgumen_1 db 'invalid argument',0
.data:005F1000 ; DATA XREF: sub_49CEB0+4C↑o

```

aInvalidArgumen_1==invalid argument

0x04

再理一遍逻辑

整个校验算法如下：

key[7]='A'

key[7]='#'

key = key^0x1F

flag = 'invalid argument'

flag = refkey ^0x1C

key==flag

可以写脚本了，运行如下

```

1 a = "invalid argument"
2 input = ''
3 for c in a:
4     input += chr(ord(c) ^ 0x1c ^ 0x1f)
5 input = input[:7] + 'A' + input[8:]
6 print input
7

```

D:\python\python.exe D:/python玩玩/123.py

jmubojgAbqdvnmw

命令提示符

```

Microsoft Windows [版本 10.0.17134.472]
(c) 2018 Microsoft Corporation。保留所有权利。

C:\Users\de11>C:\Users\de11\Desktop\看雪ctf\第二题\Exam.exe
Please Input: jmubojg#bqdvnmw
输入错误;
C:\Users\de11>C:\Users\de11\Desktop\看雪ctf\第二题\Exam.exe
Please Input: jmubojgAbqdvnmw
ok
C:\Users\de11>

```