ISCC2018线下赛河南赛区的一道Reverse题writeup

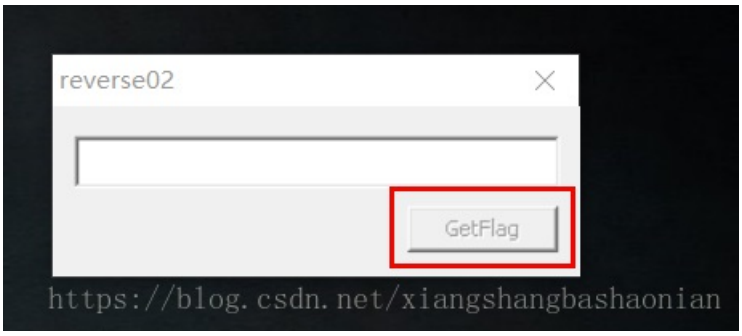
原创

iqiqiya 于 2018-08-20 15:44:01 发布 941 收藏 1
分类专栏： 我的CTF之路 我的CTF进阶之路 文章标签： ISCC2018线下赛河南赛区 Reverse writeup

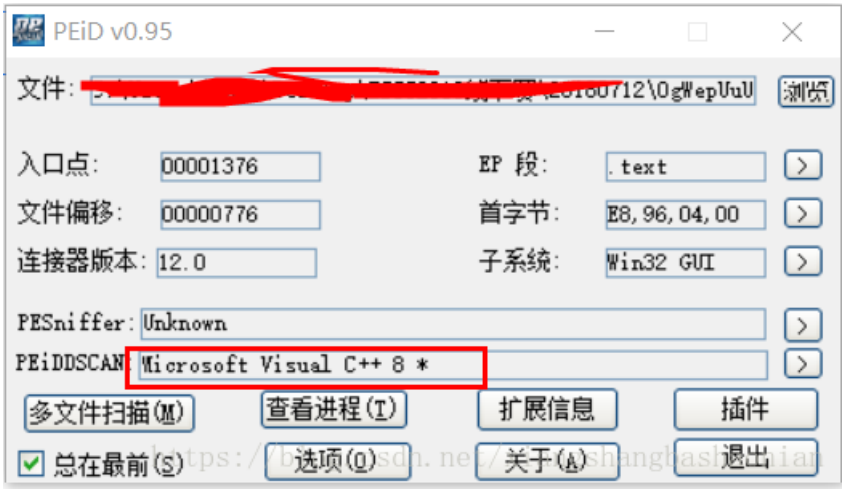
本文链接：https://blog.csdn.net/xiangshangbashaonian/article/details/81872296

0x01:先运行一下 发现GetFlag按钮是灰色的 输入无反应

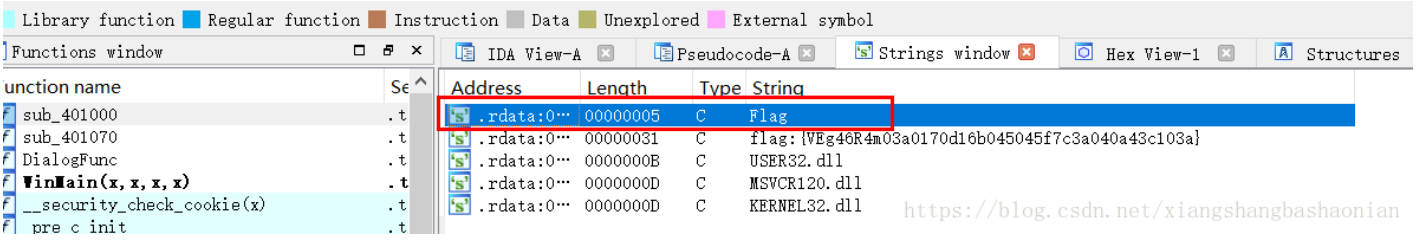
直接用灰色按钮克星激活（spy++也行） 点击后出现假的flag（当时还傻傻提交好多次。。。）



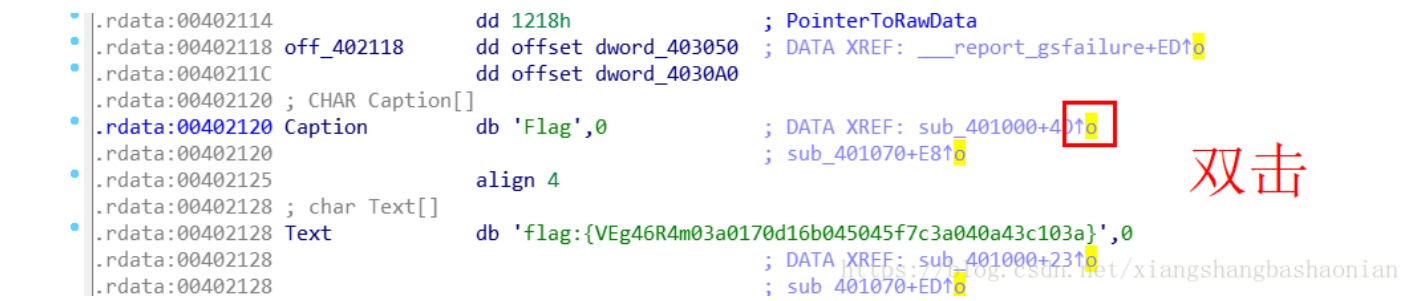
0x02:PEiD查壳 发现无壳 VC编译的程序



0x03:既然没有加壳 直接IDA载入分析 shift+F12看看有没有可疑字符串



双击Flag进入



双击向上的箭头（是一个引用）

接着F5大法

分析之后 发现就是一个异或

IDA View-A | Pseudocode-B | Pseudocode-A | Strings window | Hex View-1 | Structures | Enums

```
1  int sub_401000()
2  {
3    char *v0; // eax
4    char Dst; // [esp+0h] [ebp-38h]
5    char v3; // [esp+1h] [ebp-37h]
6    char v4; // [esp+Fh] [ebp-29h]
7
8    Dst = 0;
9    memset(&v3, 0, 0x30u);
10   strncpy_s(&Dst, 0x31u, "flag:{VEg46R4m03a0170d16b045045f7c3a040a43c103a}", 0x30u);
11   v0 = &v4;                                     // v4就是Dst[15:]   *v4 = 3a0170d16b045045f7c3a040a43c103a
12   if ( v4 != '}' )
13   {
14     do
15     {
16       *v0 ^= 7u;                                // 将3a0170d16b045045f7c3a040a43c103a每位都与7异或
17       ++v0;
18     }
19     while ( *v0 != '}' );                       // 直至遇到“}”停止
20   }
21   return MessageBoxA(0, &Dst, "Flag", 0);
22 }
```


Py大法好：

File Edit Format Run Options Window Help

```
a = "3a0170d16b045045f7c3a040a43c103a"
out = ""
for i in a:
 out += chr(ord(i)^7)
print out

flag = "flag:{VEg46R4m0" + out +"}"
print flag
```

```
================== RESTART: [redacted]/Desktop[redacted].py ==================
4f7607c61e732732a0d4f737f34d674f
flag:{VEg46R4m04f7607c61e732732a0d4f737f34d674f}
>>>
```


最后得到flag:{VEg46R4m04f7607c61e732732a0d4f737f34d674f}

题目+idb分析文件+py脚本已全部打包

百度网盘下载链接: https://pan.baidu.com/s/1V-inJEXtPwopyKHtTqP02A 密码: qiu3

本人首发：合天智汇