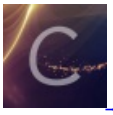
【WhaleCTF逆向题】Warmup题目writeup

原创

iqiqiya 于 2018-09-27 18:11:45 发布 1255 收藏
分类专栏： 我的逆向之路 我的CTF之路 ------WhaleCTF 我的CTF进阶之路 文章标签： 【WhaleCTF逆向题】Warmup题目writeup 【WhaleCTF逆向题】Warmup题目

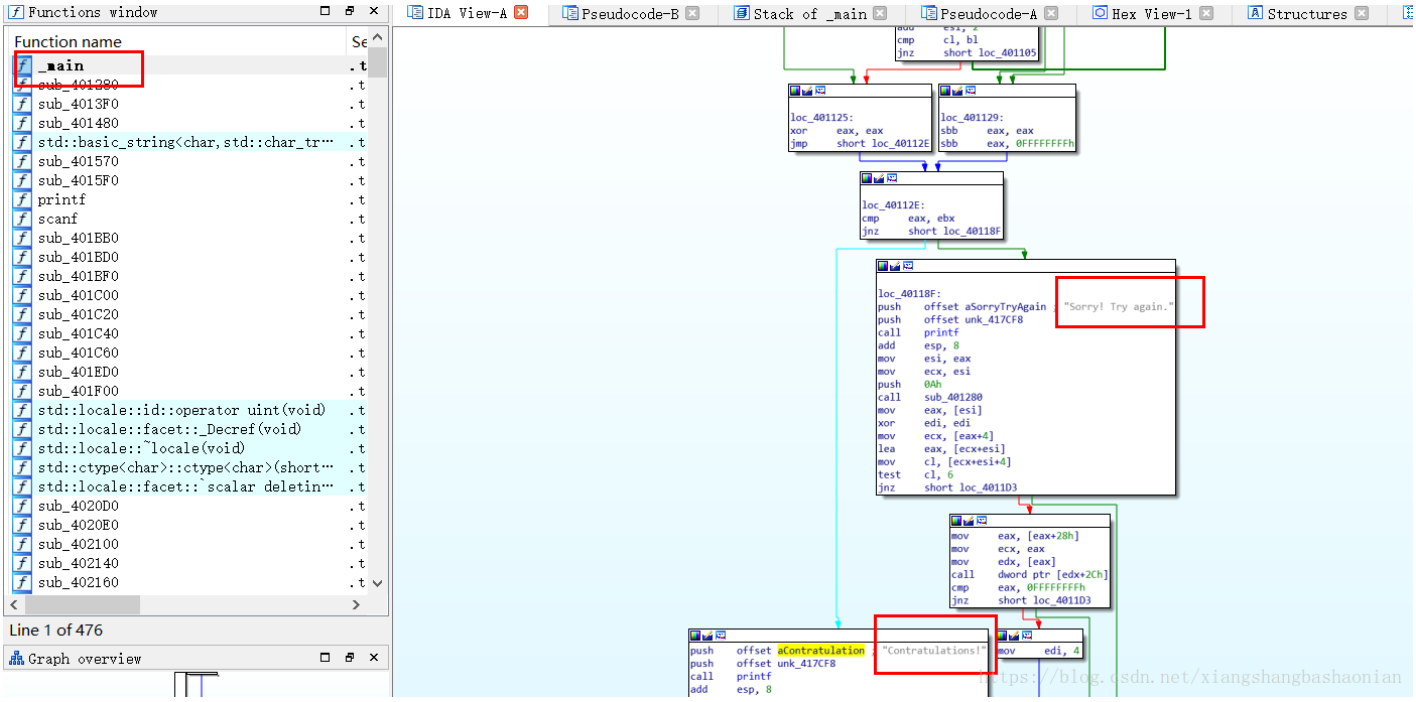

我的逆向之路 同时被 3 个专栏收录
108 篇文章 10 订阅
订阅专栏


我的CTF之路
92 篇文章 5 订阅
订阅专栏


------WhaleCTF
8 篇文章 0 订阅
订阅专栏

题目信息：

IDA直接载入　双击_main　图形视图直接向下拉一点就可以看到关键



直接F5看伪代码就可以

```
45  v26 = 0;
46  scanf(&dword_417D88, &flag);                  // 获取输入
47  i = 0;
48  v7 = strlen(&flag) + 1;                       // v7 = len(flag) + 1
49  if ( (v7 - 1) > 0 )                           // 如果输入flag长度不为0
50  {
51    do
52    {
53      *(&flag + i) ^= 0xEu;
54      ++i;
55    }
56    while ( i < (v7 - 1) );
57  }
58  if ( !strcmp(&flag, s_36_) )
59  {
60    v8 = printf(&unk_417CF8, aContratulation);  // 成功
61    sub_401280(v8, 0xAu);
62    v9 = 0;
63    v10 = &v8[*(*v8 + 4)];
64    if ( !(*(v10 + 4) & 6) && (*(**(v10 + 40) + 44))(*(v10 + 40)) == -1 )
65      v9 = 4;
66    if ( v9 )
67      sub_4013F0(v9 | *&v8[*(*v8 + 4) + 4], 0);
68  }
69  else
70  {
71    v11 = printf(&unk_417CF8, aSorryTryAgain);  // 失败
72    sub_401280(v11, 0xAu);
73    v12 = 0;
74    v13 = &v11[*(*v11 + 4)];
75    if ( !(*(v13 + 4) & 6) && (*(**(v13 + 40) + 44))(*(v13 + 40)) == -1 )
76      v12 = 4;
```


更关键的地方就是从46行开始　我是直接将一些不好看的标识符给改了

整个程序其实就是一个while循环将输入的每个字符与0xE进行异或

再与s_36_进行比对　看是否一致　若一致则成功

```
.data:004140CA                 align 4
.data:004140CC aContratulation db 'Contratulations!',0 ; DATA XREF: _main+132↑o
.data:004140DD                 align 10h
.data:004140E0 s_36_           db 'LDYVLQMZHuY:|cQ[^Qyo|cQ{~QYO\CQ[^/s'
.data:004140E0                                         ; DATA XREF: _main:loc_40
.data:00414103                 db    0
.data:00414104 unk_414104      db  50h ; P             ; DATA XREF:  main+1E↑o
```


那么我们python来求解一下：

（下面的s数组就是将s_36_转成十六进制）

```
s = [0x4C, 0x44, 0x59, 0x56, 0x4C, 0x51, 0x4D, 0x5A, 0x48, 0x75,
  0x59, 0x3A, 0x7C, 0x63, 0x51, 0x5B, 0x5E, 0x51, 0x79, 0x6F,
  0x7C, 0x63, 0x51, 0x7B, 0x7E, 0x51, 0x59, 0x4F, 0x5C, 0x43,
  0x51, 0x5B, 0x5E, 0x2F, 0x73]
flag = ''
for i in range(0,len(s)):
    flag += chr(s[i] ^ 0xE)
    print(flag)#比较喜欢这样让flag慢慢输出 嘻嘻
```

运行得到flag