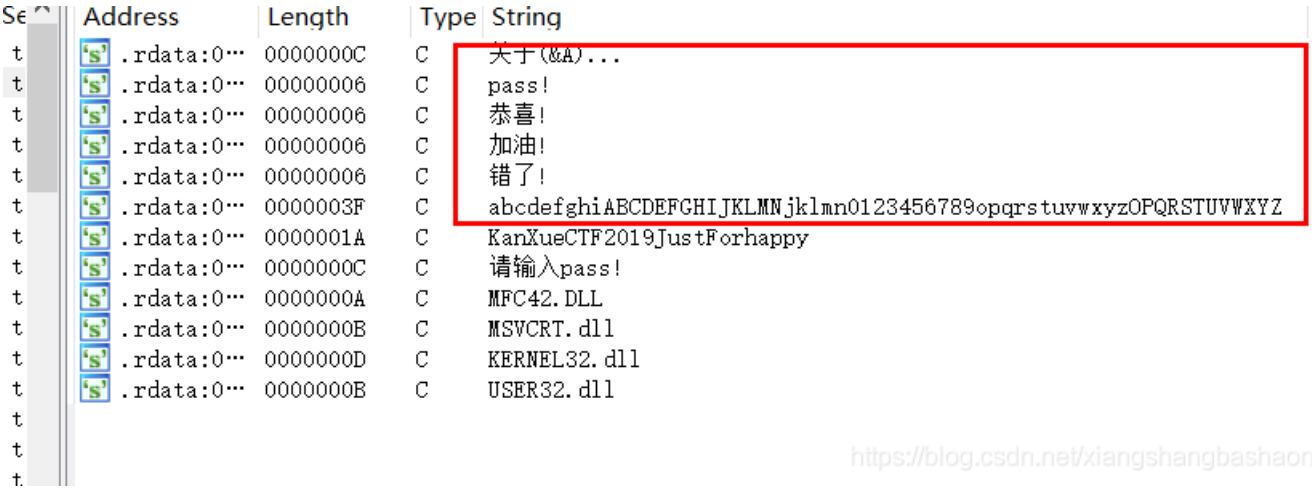
Kanxue看雪KCTF2019-Q1第一题【流浪者】Writeup

原创

iqiqiya 于 2019-03-25 20:38:47 发布 713 收藏 2
分类专栏： 我的CTF之路 ------看雪KCTF2019-Q1 文章标签： 看雪CTF KanXueCTF2019-Q1 write up

> 第一题：流浪者

IDA载入查看字符串 可以看到很多有用的信息



双击pass 接着F5查看伪代码

```
CWnd::GetWindowTextA(v2, v1);
v3 = sub_401A30((char *)v8 + 100);
Str = CString::GetBuffer((CWnd *)((char *)v8 + 100), v3);
if ( !strlen(Str) )                             // 如果输入为空 就弹窗“请输入pass”
  return CWnd::MessageBoxA(v8, "请输入pass!", 0, 0);
for ( i = 0; Str[i]; ++i )
{
  if ( Str[i] > '9' || Str[i] < '0' )           // 我们的输入范围应满足下面三个if语句
  {
    if ( Str[i] > 'z' || Str[i] < 'a' )         // 0-9,a-z,A-Z组成的字符
    {
      if ( Str[i] > 'Z' || Str[i] < 'A' )
        sub_4017B0();
      else
        v5[i] = Str[i] - 0x1D;                  // 若满足A-Z  就减去0x1d
    }
    else
    {
      v5[i] = Str[i] - 0x57;                    // 若满足a-z 就减去0x57
    }
  }
  else
  {
    v5[i] = Str[i] - 0x30;                      // 若满足0-9 就减去0x30
  }
}
return sub_4017F0((int)v5);                     // 接着去sub_4017f0()
}
```



```
BOOL __cdecl sub_4017F0(int a1)
{
  BOOL result; // eax
  char Str1[28]; // [esp+D8h] [ebp-24h]
  int v3; // [esp+F4h] [ebp-8h]
  int i; // [esp+F8h] [ebp-4h]

  i = 0;
  v3 = 0;
  while ( *(_DWORD *)(a1 + 4 * i) < 0x3E && *(_DWORD *)(a1 + 4 * i) >= 0 )
  {
    Str1[i] = aAbcdefghiabcde[*(_DWORD *)(a1 + 4 * i)];// abcdefghiABCDEFGHIJKLMNjklmn0123456789opqrstuvwxyzOPQRSTUVWXYZ
    ++i;
  }
  Str1[i] = 0;
  if ( !strcmp(Str1, "KanXueCTF2019JustForhappy") )// 最后的串与"KanXueCTF2019JustForhappy"一致
    result = sub_401770();                      // 恭喜
  else
    result = sub_4017B0();                      // 错了
  return result;
}
```

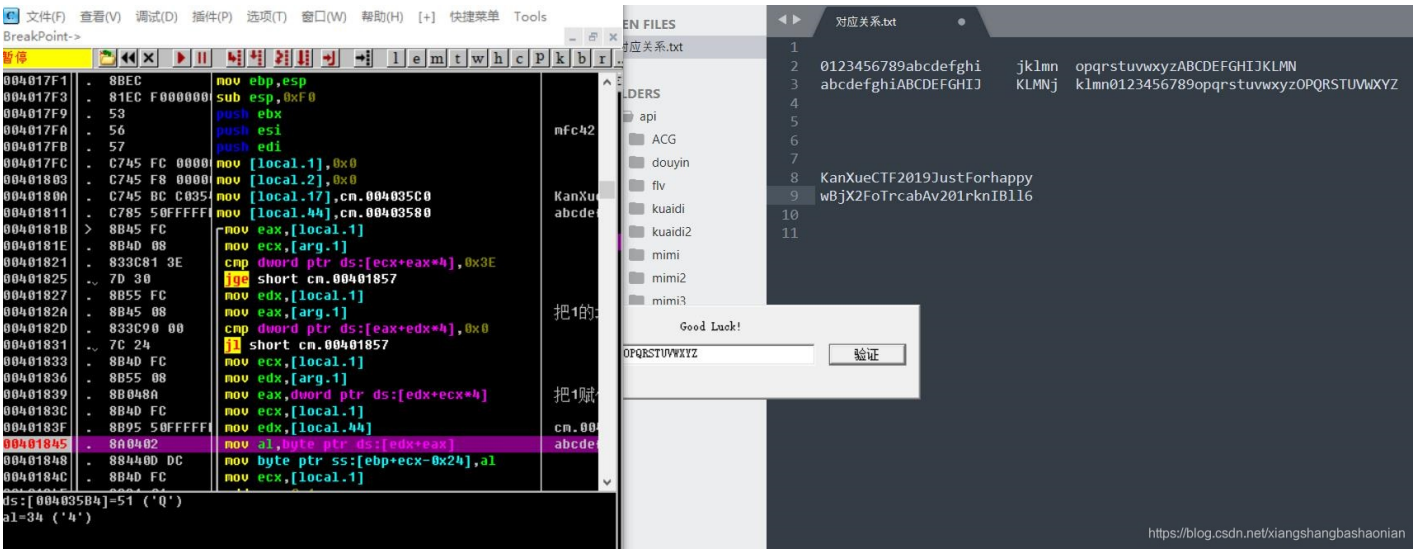

sub_4017f0() v5这个数组里边的元素作为下标映射出来

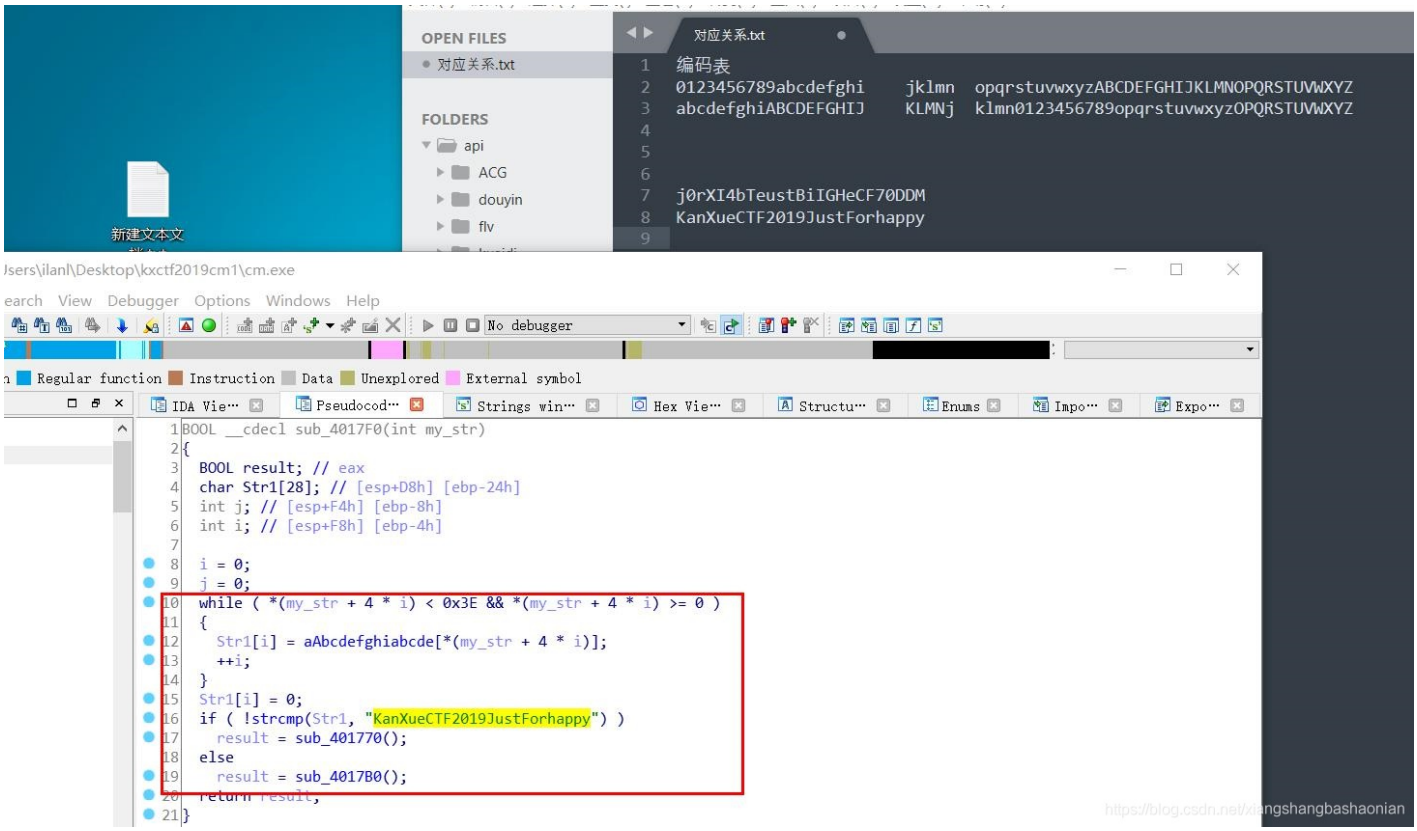
脚本如下：

```
table = "abcdefghiABCDEFGHIJKLMNjklmn0123456789opqrstuvwxyzOPQRSTUVWXYZ"
aa = "KanXueCTF2019JustForhappy"
bb = []
for i in aa:
    bb.append(table.index(i))

flag = ""
for i in bb:
    if 0 <= i <= 9:
        flag += chr(i + 48)
    elif 9 < i <= 35:
        flag += chr(i + 87)
    elif 36<= i <= 61:
        flag += chr(i + 29)

print flag
#j0rXI4bTeustBiIGHeCF70DDM
```

或者更简单的方法直接用OD进行动态调试 找出对应关系

就像下边这样




新建文本文
OPEN FILES
对应关系.txt
FOLDERS
api
ACG
douyin
flv
对应关系.txt
1 编码表
2 0123456789abcdefghi jklmn opqrstuvwxyzABCDEFGHIJKLMNOPQRSTUVWXYZ
3 abcdefghiABCDEFGHIJ KLMNj klmn0123456789opqrstuvwxyzOPQRSTUVWXYZ
7 j0rXI4bTeustBiIGHeCF70DDM
8 KanXueCTF2019JustForhappy
/sers\ilanl\Desktop\kxctf2019cm1\cm.exe
earch View Debugger Options Windows Help
No debugger
Regular function Instruction Data Unexplored External symbol
IDA Vie··· Pseudocod··· Strings win··· Hex Vie··· Structu··· Enums Impo··· Expo···
1 BOOL __cdecl sub_4017F0(int my_str)
2 {
3 BOOL result; // eax
4 char Str1[28]; // [esp+D8h] [ebp-24h]
5 int j; // [esp+F4h] [ebp-8h]
6 int i; // [esp+F8h] [ebp-4h]
7
8 i = 0;
9 j = 0;
10 while (*(my_str + 4 * i) < 0x3E && *(my_str + 4 * i) >= 0)
11 {
12 Str1[i] = aAbcdefghiabcde[*(my_str + 4 * i)];
13 ++i;
14 }
15 Str1[i] = 0;
16 if (!strcmp(Str1, "KanXueCTF2019JustForhappy"))
17 result = sub_401770();
18 else
19 result = sub_4017B0();
20 return result;
21 }
https://blog.csdn.net/xiangshangbashaonian