

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](#)

版权声明: 本文为博主原创文章, 遵循 [CC 4.0 BY-SA](#) 版权协议, 转载请附上原文出处链接和本声明。

本文链接: <https://blog.csdn.net/xiangshangbashaonian/article/details/88804295>

版权



[我的CTF之路](#) 同时被 2 个专栏收录

92 篇文章 5 订阅

订阅专栏



[-----看雪KCTF2019-Q1](#)

4 篇文章 0 订阅

订阅专栏

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

Se	Address	Length	Type	String
t	[s] .rdata:0...	0000000C	C	大于(&A)...
t	[s] .rdata:0...	00000006	C	pass!
t	[s] .rdata:0...	00000006	C	恭喜!
t	[s] .rdata:0...	00000006	C	加油!
t	[s] .rdata:0...	00000006	C	错了!
t	[s] .rdata:0...	0000003F	C	abcdefghijklmnopqrstuvwxyzOPQRSTUVWXYZ
t	[s] .rdata:0...	0000001A	C	KanXueCTF2019JustForhappy
t	[s] .rdata:0...	0000000C	C	请输入pass!
t	[s] .rdata:0...	0000000A	C	MFC42.DLL
t	[s] .rdata:0...	0000000B	C	MSVCRT.dll
t	[s] .rdata:0...	0000000D	C	KERNEL32.dll
t	[s] .rdata:0...	0000000B	C	USER32.dll
t				
t				
t				

<https://blog.csdn.net/xiangshangbashaonian>

双击pass 接着F5查看伪代码

```

14 CWnd::GetWindowTextA(v2, v1);
15 v3 = sub_401A30((char *)v8 + 100);
16 Str = CString::GetBuffer((CWnd *)((char *)v8 + 100), v3);
17 if ( !strlen(Str) ) // 如果输入为空 就弹窗“请输入pass”
18     return CWnd::MessageBoxA(v8, "请输入pass!", 0, 0);
19 for ( i = 0; Str[i]; ++i )
20 {
21     if ( Str[i] > '9' || Str[i] < '0' ) // 我们的输入范围应满足下面三个if语句
22     {
23         if ( Str[i] > 'z' || Str[i] < 'a' ) // 0-9,a-z,A-Z组成的字符
24         {
25             if ( Str[i] > 'Z' || Str[i] < 'A' )
26                 sub_4017B0();
27             else
28                 v5[i] = Str[i] - 0x1D; // 若满足A-Z 就减去0x1d
29         }
30         else
31         {
32             v5[i] = Str[i] - 0x57; // 若满足a-z 就减去0x57
33         }
34     }
35     else
36     {
37         v5[i] = Str[i] - 0x30; // 若满足0-9 就减去0x30
38     }
39 }
40 return sub_4017F0((int)v5); // 接着去sub_4017f0()
41 }

```

<https://blog.csdn.net/xiangshangbashaonian>

```

Se ^ 1|BOOL __cdecl sub_4017F0(int a1)
.t 2|{
.t 3|    BOOL result; // eax
.t 4|    char Str1[28]; // [esp+D8h] [ebp-24h]
.t 5|    int v3; // [esp+F4h] [ebp-8h]
.t 6|    int i; // [esp+F8h] [ebp-4h]
.t 7|
.t 8|    i = 0;
.t 9|    v3 = 0;
.t 10|    while ( *((_DWORD *) (a1 + 4 * i) < 0x3E && *((_DWORD *) (a1 + 4 * i) >= 0 )
.t 11|    {
.t 12|        Str1[i] = aAbcdefghiabcde[*( (_DWORD *) (a1 + 4 * i) ); // abcdefghiABCDEFGHIJKLMNjklmn0123456789opqrstuvwxyz0PQRSTUVWXYZ
.t 13|        ++i;
.t 14|    }
.t 15|    Str1[i] = 0;
.t 16|    if ( !strcmp(Str1, "KanXueCTF2019JustForhappy") ) // 最后的串与"KanXueCTF2019JustForhappy"一致
.t 17|        result = sub_401770(); // 恭喜
.t 18|    else
.t 19|        result = sub_4017B0(); // 错了
.t 20|    return result;
.t 21|}

```

<https://blog.csdn.net/xiangshangbashaonian>

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))

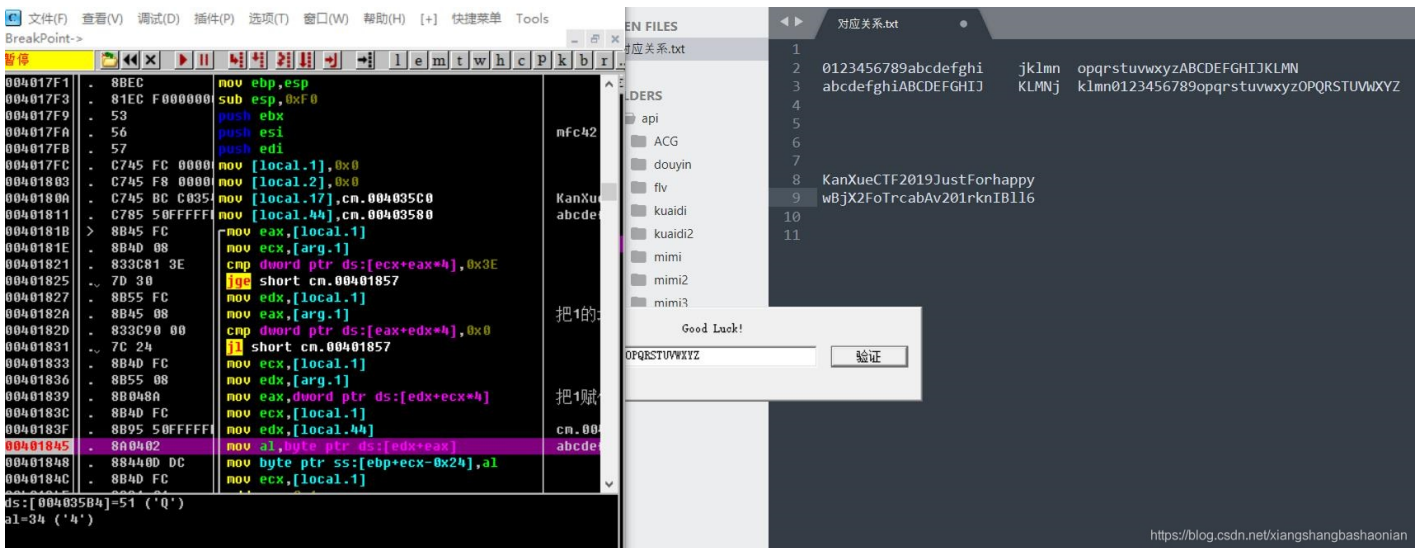
flag = ""
for i in bb:
    if 0 <= i <= 9:
        flag += chr(i + 48)
    elif 9 < i <= 35:
        flag += chr(i + 87)
    elif 36<= i <= 61:
        flag += chr(i + 29)

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



对应关系.txt

1	编码表		
2	0123456789abcdefghi	jkln	opqrstuvwxyzABCDEFGHIJKLMN
3	ABCDEFGHIJKLMN	OPQRSTUVWXYZ	0123456789opqrstuvwxyz
4			
5			
6			
7	j0rXI4bTeustBiIGHeCF70DDM		
8	KanXueCTF2019JustForhappy		
9			

```
Users\lan\Desktop\kxctf2019cm1\cm.exe
Search View Debugger Options Windows Help
No debugger
Regular function Instruction Data Unexplored External symbol
IDA View Pseudocod... Strings win... Hex Vie... Structu... Emms 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 }
```