

2019KCTF 晋级赛Q1 | 第一题点评及解题思路

小雪 看雪学院 3月26日

历时14天的看雪CTF晋级赛Q1已经结束，名次也于昨日公布：英雄榜 | 2019 看雪CTF 晋级赛Q1 排行榜出炉！

相信很多小伙伴对比赛中出现的题目想有一个更深入的了解与探讨，那么接下来的几天，我们将对这些题目进行一些点评与破解思路的讨论，也希望有更多的人在公众号下方，或者论坛进行一些互动与交流。

第一题 流浪者

已结束




出题战队: Vagaeth

围观人数: 5499

开始时间: 2019-03-10 12:00:00

首先是第一题“流浪者”，出题战队是**Vagaeth**，这道题目围观人数达到了**5499**人，这个只有一人组成的战队所出的题目，让大家产生了浓厚的兴趣。

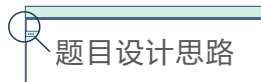
Vagaeth		
战队信息	战队成员(1)	成员动态
成员名称	职位	积分
 Vagaeth	队长	0

看雪ID: Vagaeth

<https://bbs.pediy.com/user-722186.htm>



《流浪者》此题总体来说比较简单，程序逻辑不复杂，也没有加壳保护。可以通过使用IDA的查看所有字符串的功能快速定位关键字符串，再依此找到关键程序逻辑，此题就能迎刃而解。



根据密文KanXueCTF2019JustForhappy 每个字符在其字典
abcdefghijklmnopqrstuvwxyzOPQRSTUVWXYZ里的下标 和
明文 W4p2Cq4TCj0rXI4bH5ustz 在其字典
0123456789abcdefghijklmnopqrstuvwxyzABCDEFGHIJKLMNOPQRSTUVWXYZ里面的下标
相同来进行算法验证破解先求出密文在其字典里的下标 然后根据下标在明文的字典里取字符
即可得到答案：

=>j0rXI4bTeustBilGHeCF70DDM

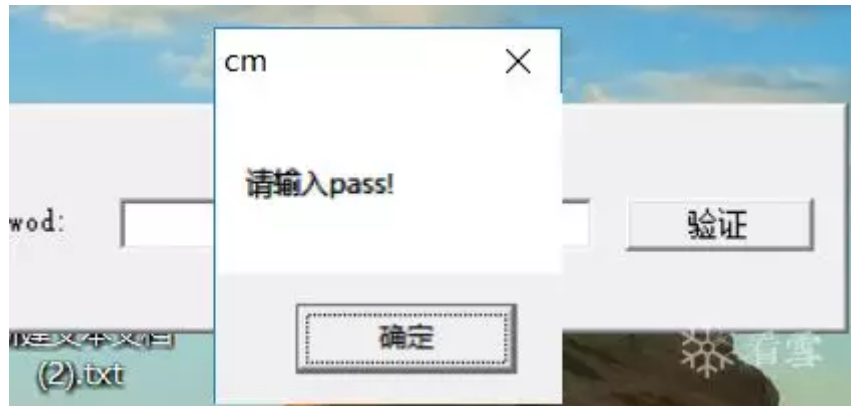
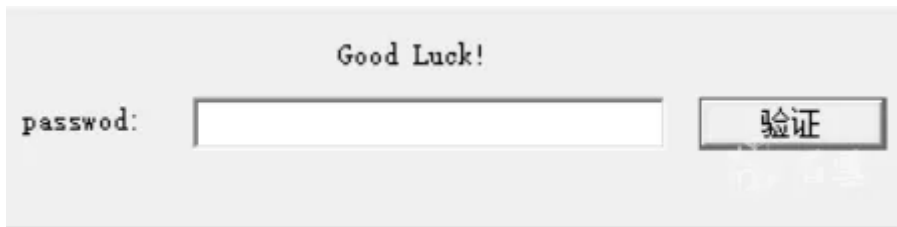


这道题目破解思路由看雪ID：**深天深天** 提供



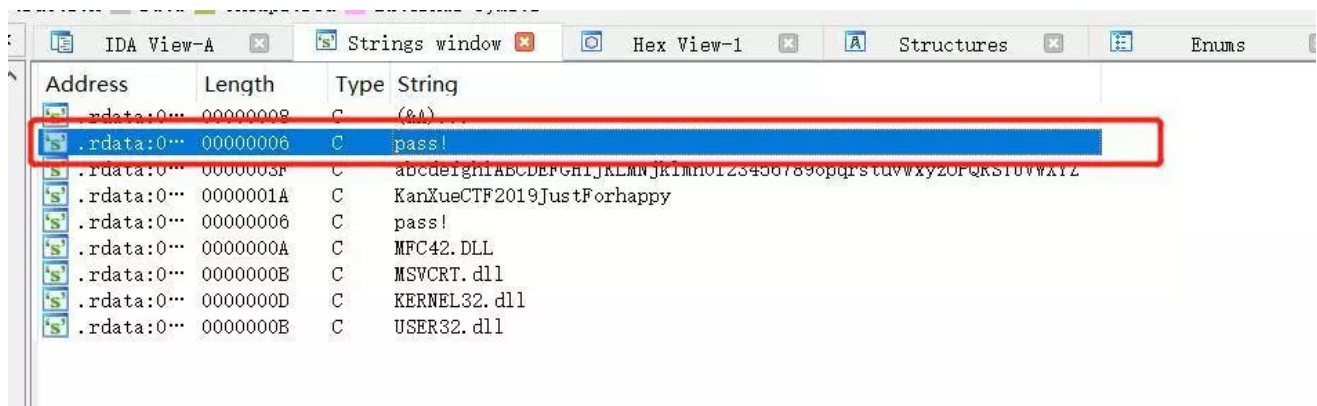
1. 首先先双击运行程序看看~

可以获得相关字符串



2. 然后丢入ida里 (32位)

通过查找字符串可以看到pass，双击进去，一步一步可以找到源码，



```

.rdata:00403560 ; CHAR Text[]
.rdata:00403560 Text      db 'pass!',0          ; DATA XREF: sub_401770+10fo
.rdata:00403566          align 4
.rdata:00403568 ; const CHAR Caption
.rdata:00403568 Caption  db 0B9h          ; DATA XREF: sub_401770+Bfo
.rdata:00403569          db 0A7h
.rdata:0040356A          db 0CFh
.rdata:0040356B          db 0B2h
.rdata:0040356C          db 21h : !

```

```

.text:00401771      mov     ebp, esp
.text:00401773      sub     esp, 44h
.text:00401776      push    ebx
.text:00401777      push    esi
.text:00401778      push    edi
.text:00401779      push    0             ; uType
.text:0040177B      push    offset Caption ; lpCaption
.text:00401780      push    offset Text    ; "pass!"
.text:00401785      push    0             ; hWnd
.text:00401787      call    ds:MessageBoxA
.text:0040178D      call    ds:GetCurrentProcess
.text:00401793      mov     [ebp+hProcess], eax
.text:00401796      push    0             ; uExitCode
.text:00401798      mov     eax, [ebp+hProcess]
.text:0040179B      push    eax            ; hProcess
.text:0040179C      call    ds:TerminateProcess
.text:004017A2      pop     edi
.text:004017A3      pop     esi
.text:004017A4      pop     ebx
.text:004017A5      mov     esp, ebp
.text:004017A7      pop     ebp
.text:004017A8      retn
.text:004017A8      sub_401770      endp

```

3. 用F5大法

可以看到MessageBox，这里是输入内容成功返回的地方，按x返回上一步看看是谁调用了它

~

```

1 BOOL sub_401770()
2 {
3     HANDLE hProcess; // ST5C_4
4
5     MessageBox(0, "pass!", &Caption, 0);
5     hProcess = GetCurrentProcess();
7     return TerminateProcess(hProcess, 0);
3 }

```

然后得到以下关键，可以知道代码段，对输入内容做变形处理后，如果字符串等于KanXueCTF2019JustForhappy，就可成功pass

```

1: __cdecl sub_4017F0(int a1)
2{
3:  __bool result; // eax
4:  char Str1[28]; // [esp+D8h] [ebp-24h]
5:  int v3; // [esp+F4h] [ebp-8h]
6:  int v4; // [esp+F8h] [ebp-4h]
7
8:  v4 = 0;
9:  v3 = 0;
10: while ( *((_DWORD *) (a1 + 4 * v4)) < 62 && *((_DWORD *) (a1 + 4 * v4)) >= 0 ) // 变形2
11 {
12     Str1[v4] = abcdefghiabcde[*((_DWORD *) (a1 + 4 * v4))]; // abcdefghiABCDEFGHIJKLMNjklmn0123456789opqrstuvwxyzOPQRSTUVWXYZ
13     ++v4;
14 }
15 Str1[v4] = 0;
16 if ( !strcmp(Str1, "KanXueCTF2019JustForhappy") )
17     result = sub_401770(); // pass
18 else
19     result = sub_4017B0(); // 加油! (错误提示)
20 return result;
21 }

```

```

v8 = this;
v1 = (CWnd *) ((char *) this + 100);
v2 = CWnd::GetDlgItem(this, 1002);
CWnd::GetWindowTextA(v2, v1);
v3 = sub_401A30((char *) v8 + 100);
Str = CString::GetBuffer((CWnd *) ((char *) v8 + 100), v3);
if ( !strlen(Str) ) // 如果未输入内容
    return CWnd::MessageBoxA(v8, &re_input, 0, 0);
for ( i = 0; Str[i]; ++i ) // 变形1
{
    if ( Str[i] > '9' || Str[i] < '0' )
    {
        if ( Str[i] > 'z' || Str[i] < 'a' )
        {
            if ( Str[i] > 'Z' || Str[i] < 'A' )
                sub_4017B0(); // 加油! (错误提示)
            else
                v5[i] = Str[i] - 29; // 不是数字, 也不是小写字母, 更不是大写字母, -29 36-61
        }
        else
        {
            v5[i] = Str[i] - 87; // 不是数字, 但是是小写字母, -87 10-35
        }
    }
    else
    {
        v5[i] = Str[i] - 48; // 如果是数字, -48 0-9
    }
}
return sub_4017F0((int) v5); // 关键
}

```

4. 简单来说, 变形就是一个替换算法:

abcdefghiABCDEFGHIJKLMNjklmn0123456789opqrstuvwxyzOPQRSTUVWXYZ
 0123456789abcdefghijklmnopqrstuvwxyzABCDEFGHIJKLMNopqrstuvwxyz
 上下一一对应, 这样只要根据"KanXueCTF2019JustForhappy"反推输入即可。

5. 脚本如下

```

#!/usr/bin/python
str1='abcdefghijklmnopqrstuvwxyzOPQRSTUVWXYZ'
str2='0123456789abcdefghijklmnopqrstuvwxyzABCDEFGHIJKLMNopqrstuvwxyz'
enc='KanXueCTF2019JustForhappy'

```

```
flag=""
```

```
list1=list(str1)
```

```
list2=list(str2)
```

```
list3=list(enc)
```

```
i = 0
```

```
while i < len(list3):
```

```
flag+=list2[list1.index(list3[i])]
```

```
i+=1
```

```
print(flag)
```


```
#j0rXI4bTeustBiIGHeCF70DDM
```

明天我们将对题目“**变形金刚**”进行分析
与讨论，感兴趣的小伙伴记得不要错过，
准时守住我们的公众号更新哦~



- End -

推荐图书

戳  ，立即购买~

往期文章一览



- 1、[FastHook——远超YAHFA的优异稳定性](#)
- 2、[【走进企业看安全】第18站 娜迦信息，圆满落幕！](#)
- 3、[微软Chromium版Edge安装程序泄露](#)



新鲜·有料·实用的技术干货和资讯

长按 关注，和业内精英一起学习

公众号ID: ikanxue

官方微博: 看雪安全

商务合作: wsc@kanxue.com



点击阅读原文，打开新页面

阅读原文