

# 攻防世界 Reverse高手进阶区 2分题 流浪者

原创

思源湖的鱼 于 2020-12-22 13:28:31 发布 137 收藏

分类专栏: [ctf](#) 文章标签: [ctf](#) [攻防世界](#) [reverse](#)

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/weixin\\_44604541/article/details/111537726](https://blog.csdn.net/weixin_44604541/article/details/111537726)

版权

## CTF

[ctf 专栏收录该内容](#)

200 篇文章 23 订阅

订阅专栏

### 前言

继续ctf的旅程

攻防世界Reverse高手进阶区的2分题

本篇是流浪者的writeup

发现攻防世界的题目分数是动态的

就仅以做题时的分数为准了

### 解题过程

PE查壳



扔进IDA

```

1 int __thiscall sub_401890(CWnd *this)
2 {
3     struct CString *v1; // ST08_4
4     CWnd *v2; // eax
5     int v3; // eax
6     int v5[26]; // [esp+4Ch] [ebp-74h]
7     int i; // [esp+B4h] [ebp-Ch]
8     char *Str; // [esp+B8h] [ebp-8h]
9     CWnd *v8; // [esp+BCh] [ebp-4h]
10
11     v8 = this;
12     v1 = (CString*)((char *)this + 100);
13     v2 = CWnd::GetDlgItem(this, 1002);
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) )
18         return CWnd::MessageBoxA(v8, &byte_4035DC, 0, 0);
19     for ( i = 0; Str[i]; ++i )
20     {
21         if ( Str[i] > 57 || Str[i] < 48 )
22         {
23             if ( Str[i] > 122 || Str[i] < 97 )
24             {
25                 if ( Str[i] > 90 || Str[i] < 65 )
26                     sub_4017B0();
27                 else
28                     v5[i] = Str[i] - 29;
29             }
30             else
31             {
32                 v5[i] = Str[i] - 87;
33             }
34         }
35         else
36         {
37             v5[i] = Str[i] - 48;
38         }
39     }
40     return sub_4017F0((int)v5);
41 }

```

[https://blog.csdn.net/weixin\\_44604541](https://blog.csdn.net/weixin_44604541)

```

1 int __cdecl sub_4017F0(int a1)
2 {
3     int 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 )
11    {
12        Str1[v4] = aAbcdefghiabcde[*(_DWORD *)(a1 + 4 * v4)];
13        ++v4;
14    }
15    Str1[v4] = 0;
16    if ( !strcmp(Str1, "KanXueCTF2019JustForhappy") )
17        result = sub_401770();
18    else
19        result = sub_4017B0();
20    return result;
21 }

```

[https://blog.csdn.net/weixin\\_44604541](https://blog.csdn.net/weixin_44604541)

```

.rdata:00403580 aAbcdefghiabcde db 'abcdeFGHIJKLMNOPQRSTUVWXYZ',0
.rdata:00403580                                     ; DATA XREF: sub_4017F0+21fo
.rdata:004035BF                                     align 10h
.rdata:004035C0 aKanxuectf2019j db 'KanXueCTF2019JustForhappy',0
.rdata:004035C0                                     ; DATA XREF: sub_4017F0+1Afo
.rdata:004035DA                                     align 4

```

根据逻辑编写脚本

```
s1 = 'abcdefghiABCDEFGHIJKLMNjklmn0123456789opqrstuvwxyzOPQRSTUVWXYZ'
n = 0
map = {}
for i in s1:
    map[i] = n
    n += 1

s2 = 'KanXueCTF2019JustForhappy'
l = []
for i in s2:
    l.append(map[i])

res = ''
for i in l:
    if(i < 10):
        res += chr(i+48)
    elif(i < 36):
        res += chr(i+87)
    else:
        res += chr(i+29)

print(res)
```

点击运行

Python 在线工具

清空

```
2 n = 0
3 map = {}
4 for i in s1:
5     map[i] = n
6     n += 1
7
8 s2 = 'KanXueCTF2019JustForhappy'
9 l = []
10 for i in s2:
11     l.append(map[i])
12
13 res = ''
14 for i in l:
15     if(i < 10):
16         res += chr(i+48)
17     elif(i < 36):
18         res += chr(i+87)
19     else:
20         res += chr(i+29)
21
22 print(res)
```

j0rXl4bTeustBilGHeCF70DDM

[https://blog.csdn.net/weixin\\_44604541](https://blog.csdn.net/weixin_44604541)

得到flag

## 结语

简单题



[创作打卡挑战赛](#)

[赢取流量/现金/CSDN周边激励大奖](#)