流浪者 攻防世界

北风~ 于 2020-04-01 10:26:17 发布 1067 收藏 1

分类专栏： 逆向与保护 文章标签： python 安全

逆向与保护 专栏收录该内容

65 篇文章 4 订阅

订阅专栏

流浪者题目链接

这个题进行了两次加密

第一次：根据if条件判断对每个字符操作

```
12  v1 = (CWnd *)((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 )          // if条件判断
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 }
```

第二次：将第一次加密的值作为数组下标，取另一数组里的值再组成"原料数组"

```
1 BOOL __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;
0   while ( *(_DWORD *)(a1 + 4 * v4) < '>' && *(_DWORD *)(a1 + 4 * v4) >= 0 )
1   {
2     Str1[v4] = aAbcdefghiabcde[*(_DWORD *)(a1 + 4 * v4)];// a1+4*v4是在遍历a1数组
3     ++v4;
4   }
5   Str1[v4] = 0;
6   if ( !strcmp(Str1, "KanXueCTF2019JustForhappy") )// 关键比较
7     result = sub_401770();
8   else
9     result = sub_4017B0();
0   return result;
1 }
```

脚本

```python
table = "abcdefghiABCDEFGHIJKLMNjklmn0123456789opqrstuvwxyzOPQRSTUVWXYZ"
s = "KanXueCTF2019JustForhappy"
ff = []
for i in s:
    ff.append(table.index(i))

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

print (flag)
```

flag{j0rXl4bTeustBilGHeCF70DDM}