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

本文链接：https://blog.csdn.net/weixin_44604541/article/details/111537726

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

```
int __thiscall sub_401890(CWnd *this)
{
  struct CString *v1; // ST08_4
  CWnd *v2; // eax
  int v3; // eax
  int v5[26]; // [esp+4Ch] [ebp-74h]
  int i; // [esp+B4h] [ebp-Ch]
  char *Str; // [esp+B8h] [ebp-8h]
  CWnd *v8; // [esp+BCh] [ebp-4h]

  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) )
    return CWnd::MessageBoxA(v8, &byte_4035DC, 0, 0);
  for ( i = 0; Str[i]; ++i )
  {
    if ( Str[i] > 57 || Str[i] < 48 )
    {
      if ( Str[i] > 122 || Str[i] < 97 )
      {
        if ( Str[i] > 90 || Str[i] < 65 )
          sub_4017B0();
        else
          v5[i] = Str[i] - 29;
      }
      else
      {
        v5[i] = Str[i] - 87;
      }
    }
    else
    {
      v5[i] = Str[i] - 48;
    }
  }
  return sub_4017F0((int)v5);
}
```



```
int __cdecl sub_4017F0(int a1)
{
  int result; // eax
  char Str1[28]; // [esp+D8h] [ebp-24h]
  int v3; // [esp+F4h] [ebp-8h]
  int v4; // [esp+F8h] [ebp-4h]

  v4 = 0;
  v3 = 0;
  while ( *(_DWORD *)(a1 + 4 * v4) < 62 && *(_DWORD *)(a1 + 4 * v4) >= 0 )
  {
    Str1[v4] = aAbcdefghiabcde[*(_DWORD *)(a1 + 4 * v4)];
    ++v4;
  }
  Str1[v4] = 0;
  if ( !strcmp(Str1, "KanXueCTF2019JustForhappy") )
    result = sub_401770();
  else
    result = sub_4017B0();
  return result;
}
```



```
.rdata:00403580 aAbcdefghiabcde db 'abcdefghiABCDEFGHIJKLMNjklmn0123456789opqrstuvwxyzOPQRSTUVWXYZ',0
.rdata:00403580                                         ; DATA XREF: sub_4017F0+21↑o
.rdata:004035BF                 align 10h
.rdata:004035C0 aKanxuectf2019j db 'KanXueCTF2019JustForhappy',0
.rdata:004035C0                                         ; DATA XREF: sub_4017F0+1A↑o
.rdata:004035DA                 align 4
```

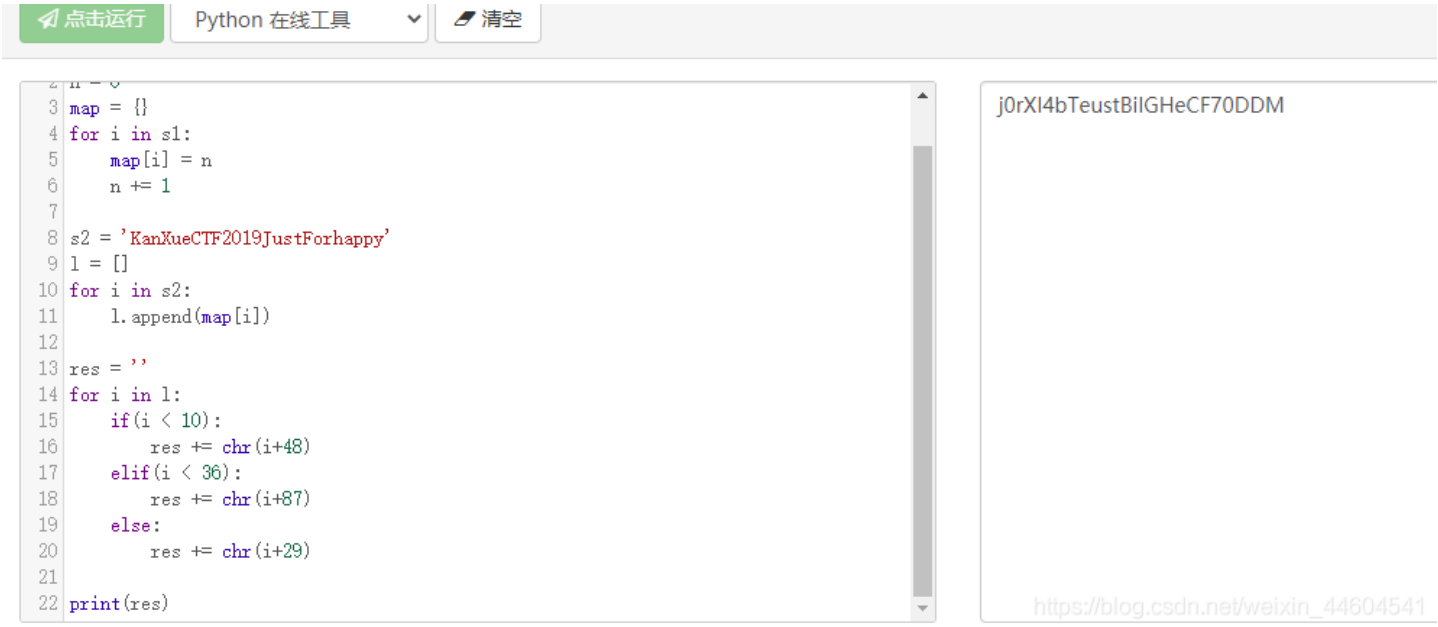
根据逻辑编写脚本

```python
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)
```



得到flag

结语

简单题