攻防世界 Reverse高手进阶区 2分题 hackme

原创

思源湖的鱼 于 2020-12-15 13:04:05 发布 159 收藏 1

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/111194731

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hackme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

```
__int64 sub_400F8E()
{
  char v1[136]; // [rsp+10h] [rbp-B0h]
  int v2; // [rsp+98h] [rbp-28h]
  char v3; // [rsp+9Fh] [rbp-21h]
  int v4; // [rsp+A0h] [rbp-20h]
  unsigned __int8 v5; // [rsp+A6h] [rbp-1Ah]
  char v6; // [rsp+A7h] [rbp-19h]
  int v7; // [rsp+A8h] [rbp-18h]
  int v8; // [rsp+ACh] [rbp-14h]
  int v9; // [rsp+B0h] [rbp-10h]
  int v10; // [rsp+B4h] [rbp-Ch]
  _BOOL4 v11; // [rsp+B8h] [rbp-8h]
  int i; // [rsp+BCh] [rbp-4h]

  sub_407470((unsigned __int64)"Give me the password: ");
  sub_4075A0((unsigned __int64)"%s");
  for ( i = 0; v1[i]; ++i )
    ;
  v11 = i == 22;
  v10 = 10;
  do
  {
    v7 = (signed int)sub_406D90() % 22;
    v9 = 0;
    v6 = byte_6B4270[v7];
    v5 = v1[v7];
    v4 = v7 + 1;
    v8 = 0;
    while ( v8 < v4 )
    {
      ++v8;
      v9 = 1828812941 * v9 + 12345;
    }
    v3 = v9 ^ v5;
    if ( v6 != ((unsigned __int8)v9 ^ v5) )
      v11 = 0;
    --v10;
  }
  while ( v10 );
  if ( v11 )
    v2 = sub_407470((unsigned __int64)"Congras\n");
  else
    v2 = sub_407470((unsigned __int64)"Oh no!\n");
  return 0LL;
}
```



```
.data:00000000006B4270 byte_6B4270     db 5Fh                  ; DATA XREF: sub_400F8E+AF↑r
.data:00000000006B4271                 db 0F2h
.data:00000000006B4272                 db  5Eh ; ^
.data:00000000006B4273                 db  8Bh
.data:00000000006B4274                 db  4Eh ; N
.data:00000000006B4275                 db  0Eh
.data:00000000006B4276                 db 0A3h
.data:00000000006B4277                 db 0AAh
.data:00000000006B4278                 db 0C7h
.data:00000000006B4279                 db  93h
.data:00000000006B427A                 db  81h
.data:00000000006B427B                 db  3Dh ; =
.data:00000000006B427C                 db  5Fh ; _
.data:00000000006B427D                 db  74h ; t
.data:00000000006B427E                 db 0A3h
.data:00000000006B427F                 db    9
.data:00000000006B4280                 db  91h
.data:00000000006B4281                 db  2Bh ; +
.data:00000000006B4282                 db  49h ; I
.data:00000000006B4283                 db  28h ; (
.data:00000000006B4284                 db  93h
.data:00000000006B4285                 db  67h ; g
.data:00000000006B4286                 db    0
.data:00000000006B4287                 db    0
```


于是有

- v7是0~21的整数
- byte_6B4270数组实际长度应该就是22
- 取10位输入的字符，异或后，与byte_6B4270比较是否相同

得到脚本

```
byte_6B4270 = [0x5F,0xF2,0x5E,0x8B,0x4E,0x0E,0xA3,0xAA,0xC7,0x93,0x81,0x3D,0x5F,0x74,0xA3,0x09, 0x91,0x2B,0x49,0x28,0x93,0x67]

flag = ''

for i in range(22):
    v6 = i + 1
    v10 = 0
    v11 = 0
    while v10 < v6:
        v10 = v10 + 1
        v11 = 1828812941 * v11 + 12345
    flag += chr((byte_6B4270[i]^v11)&0xff)
print (flag)
```

得到flag：`flag{d826e6926098ef46}`

结语

理清逻辑