攻防世界 Reverse高手进阶区 2分题 EasyRE

原创

思源湖的鱼 于 2020-12-19 16:56:59 发布 158 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/111404791

前言

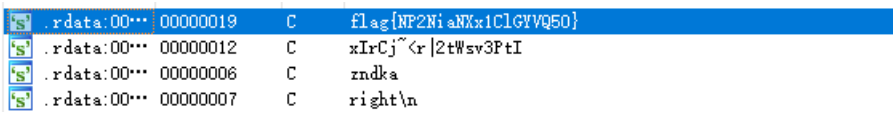
继续ctf的旅程
攻防世界Reverse高手进阶区的2分题
本篇是EasyRE的writeup

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
shift+F12发现第一行有flag



但这个不对

然后看到个right

跟踪

```
1  int sub_401080()
2  {
3    unsigned int v0; // kr00_4
4    signed int v1; // edx
5    char *v2; // esi
6    char v3; // al
7    unsigned int v4; // edx
8    int v5; // eax
9    __int128 v7; // [esp+2h] [ebp-24h]
10   __int64 v8; // [esp+12h] [ebp-14h]
11   int v9; // [esp+1Ah] [ebp-Ch]
12   __int16 v10; // [esp+1Eh] [ebp-8h]
13
14   sub_401020(&unk_402150, v7);
15   v9 = 0;
16   v10 = 0;
17   v7 = 0i64;
18   v8 = 0i64;
19   sub_401050((const char *)&unk_402158, (unsigned int)&v7);
20   v0 = strlen((const char *)&v7);
21   if ( v0 >= 0x10 && v0 == 24 )
22   {
23     v1 = 0;
24     v2 = (char *)&v8 + 7;
25     do
26     {
27       v3 = *v2--;
28       byte_40336C[v1++] = v3;
29     }
30     while ( v1 < 24 );
31     v4 = 0;
32     do
33     {
34       byte_40336C[v4] = (byte_40336C[v4] + 1) ^ 6;
35       ++v4;
36     }
37     while ( v4 < 0x18 );
38     v5 = strcmp(byte_40336C, (const char *)&unk_402124);
39     if ( v5 )
40       v5 = -(v5 < 0) | 1;
41     if ( !v5 )
42     {
43       sub_401020("right\n", v7);
44       system("pause");
45     }
46   }
47   return 0;
48 }
```


- 判断输入的字符长度为24
- 将字符串逆序
- 将每个字符+1后与6异或
- 与固定字符串比较相等则正确

```
.rdata:00402124 unk_402124      db  78h ; x             ; DATA XREF: sub_401080+A8↑o
.rdata:00402124                                         ; .rdata:0040215C↓o
.rdata:00402125                 db  49h ; I
.rdata:00402126                 db  72h ; r
.rdata:00402127                 db  43h ; C
.rdata:00402128                 db  6Ah ; j
.rdata:00402129                 db  7Eh ; ~
.rdata:0040212A                 db  3Ch ; <
.rdata:0040212B                 db  72h ; r
.rdata:0040212C                 db  7Ch ; |
.rdata:0040212D                 db  32h ; 2
.rdata:0040212E                 db  74h ; t
.rdata:0040212F                 db  57h ; W
.rdata:00402130                 db  73h ; s
.rdata:00402131                 db  76h ; v
.rdata:00402132                 db  33h ; 3
.rdata:00402133                 db  50h ; P
.rdata:00402134                 db  74h ; t
.rdata:00402135                 db  49h ; I
.rdata:00402136                 db  7Fh ;
.rdata:00402137                 db  7Ah ; z
.rdata:00402138                 db  6Eh ; n
.rdata:00402139                 db  64h ; d
.rdata:0040213A                 db  6Bh ; k
.rdata:0040213B                 db  61h ; a
```


于是可以得到脚本

```
data=[ 0x78, 0x49, 0x72, 0x43, 0x6A, 0x7E, 0x3C, 0x72, 0x7C, 0x32, 0x74, 0x57, 0x73, 0x76, 0x33, 0x50, 0x74, 0x4
9, 0x7F, 0x7A, 0x6E, 0x64, 0x6B, 0x61]
for i in range(24):
    data[i]=chr((data[i]^6)-1)
print(''.join(data)[::-1])
```

得到flag：`flag{xNqU4otPq3ys9wkDsN}`

结语

一开始没有shift+F12
就饶了好大圈儿