

buu re [ACTF新生赛2020]rome wp

原创

慢慢来882 于 2021-12-13 16:13:08 发布 107 收藏

文章标签: [python](#) [网络安全](#)

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_60553183/article/details/121907810

版权

拿到文件打开查strings

```
..... ~ .....  
[S] .rdata:0... 00000014 C _Jv_RegisterClasses  
[S] .rdata:0... 0000000E C Please input:  
[S] .rdata:0... 00000011 C You are correct!  
[S] .rdata:0... 00000018 C Mingw runtime failure:\n  
[S] .rdata:0... 00000031 C VirtualQuery failed for %d bytes at address %p
```

看到这个you are correct!不出意外flag的位置就在这里啦, 对他进行追踪

```
action Data Unexplored External symbol  
IDA View-A Pseudocode-A Stack of _func Hex View-1 Strings window Structures  
54 printf("Please input:");  
55 scanf("%s", &v5);  
56 result = v5;  
57 if ( v5 == 'A' )  
58 {  
59     result = v6;  
60     if ( v6 == 'C' )  
61     {  
62         result = v7;  
63         if ( v7 == 'T' )  
64         {  
65             result = v8;  
66             if ( v8 == 'F' )  
67             {  
68                 result = v9;  
69                 if ( v9 == '{' )  
70                 {  
71                     result = v14;  
72                     if ( v14 == '}' )  
73                     {  
74                         v1 = v10;  
75                         v2 = v11;  
76                         v3 = v12;  
77                         v4 = v13;  
78                         for ( i = 0; i <= 15; ++i )  
79                         {  
80                             if ( *((_BYTE *)&v1 + i) > 64 && *((_BYTE *)&v1 + i) <= 90 )  
81                                 *((_BYTE *)&v1 + i) = *((char *)&v1 + i) - 51 % 26 + 65;  
82                             if ( *((_BYTE *)&v1 + i) > 96 && *((_BYTE *)&v1 + i) <= 122 )  
83                                 *((_BYTE *)&v1 + i) = *((char *)&v1 + i) - 79 % 26 + 97;  
84                         }  
85                         for ( i = 0; i <= 15; ++i )  
86                         {  
87                             result = (unsigned __int8)*(&v15 + i);  
88                             if ( *((_BYTE *)&v1 + i) != (_BYTE)result )  
89                                 return result;
```

看到这里, 写脚本逆向, 直接暴力

逆向

```
Tools VCS Window Help py1 - E:\密码1\py1\venv\Lib\remo.py  
lucky.py × main.py × 1.py × 16 (1).py × jay.py × crypto rsa.py × remo.py × _pydev_execfile.py  
1 x=[81,115,119,51,115,106,95,108,122,52,95,85,106,119,64,108]  
2 flag=""  
3 for k in range(0,16):  
4     for i in range(0,127):  
5         z=i  
6         if (i>64 and i<=90):  
7             i=(i-51)%26+65  
8         if(i>96 and i<=122):  
9             i=(i-79)%26+97  
10        if(i==x[k]):  
11            flag+=chr(z)  
12    print(flag)
```

CSDN @慢慢来882

出flag{Cae3ar_th4_Gre@t}