[BUUCTF]REVERSE——[ACTF新生赛2020]easyre

原创

Angel~Yan 于 2020-11-18 19:30:22 发布 462 收藏 4

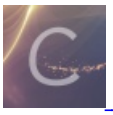
分类专栏： REVERSE BUUCTF刷题记录

本文链接：https://blog.csdn.net/mcmuyanga/article/details/109782044

REVERSE 同时被 2 个专栏收录

75 篇文章 1 订阅

订阅专栏



BUUCTF刷题记录

198 篇文章 14 订阅

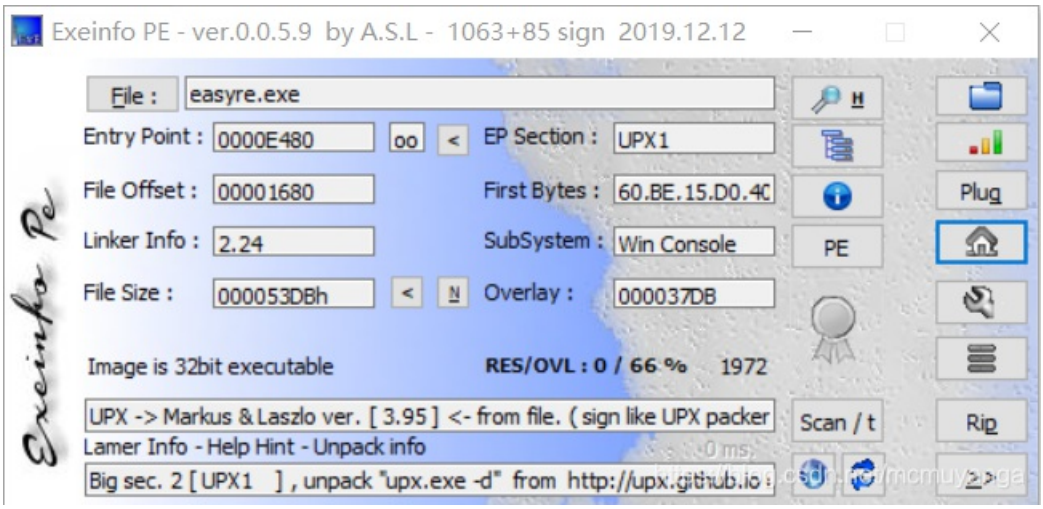
订阅专栏

[ACTF新生赛2020]easyre

附件

步骤

查壳，32位程序，upx壳儿



脱完壳儿，扔进ida

```
27
28  sub_401A10();
29  v4 = 42;
30  v5 = 70;
31  v6 = 39;
32  v7 = 34;
33  v8 = 78;
34  v9 = 44;
35  v10 = 34;
36  v11 = 40;
37  v12 = 73;
38  v13 = 63;
39  v14 = 43;
40  v15 = 64;
41  printf("Please input:");
42  scanf("%s", &v19);
43  if ( (_BYTE)v19 != 'A' || HIBYTE(v19) != 'C' || v20 != 'T' || v21 != 'F' || v22 != '{' || v26 != '}' )
44    return 0;
45  v16 = v23;
46  v17 = v24;
47  v18 = v25;
48  for ( i = 0; i <= 11; ++i )
49  {
50    if ( *(&v4 + i) != byte_402000[*((char *)&v16 + i) - 1] )
51      return 0;
52  }
53  printf("You are correct!");
54  return 0;
55}
```


分析

一开始给我们定义了一个数组，

v4=[42,70,39,34,78,44,34,40,73, 63, 43, 64]

之后让我们输入一个字符串，根据43行的if判断可以知道我们输入的字符串的开头是ACT{}，就是flag

根据48行的if判断可知。ACT{}括号里的值长度为12，v4=byte_402000[输入的数组的每一位值-1]

在ida里可以看到byte_402000数组的值

```
.data:00402000                 ;org 402000h
.data:00402000 ; char byte_402000[]
.data:00402000 byte_402000     db 7Eh                  ; DATA XREF: _main+EC↑r
.data:00402001 aZyxwvutsrqponm db '}|{zyxwvutsrqponmlkjihgfedcba`_^]\[ZYXWVUTSRQPONMLKJIHGFEDCBA@?>='
.data:00402001                 db '<;:9876543210/.-,+*)(',27h,'&%$# !"',0
.data:00402060                 align 40h
```

根据这个算法逆向一下就能得到我们输入的字符串，也就是flag

```python
v4 = [42,70,39,34,78,44,34,40,73,63,43,64]
string = chr(0x7E)+"}|{zyxwvutsrqponmlkjihgfedcba`_^]\[ZYXWVUTSRQPONMLKJIHGFEDCBA@?>=<;:9876543210/.-,+*)(" + ch
r(0x27) + '&%$# !"'
flag=""

for i in v4:
    for j in range(1,len(string)):
        if i == ord(string[j]):
            flag+=chr(j+1)

print ("flag{"+flag+"}")
```

```
flag{U9X_1S_W6@T?}
>>>
```