【Writeup】i春秋网络安全领域专项技能赛_Reverse_flat

原创

BAKUMANSEC 于 2019-08-17 17:44:38 发布 274 收藏

分类专栏： ichunqiu - Writeups 文章标签： Writeup Reverse

本文链接：https://blog.csdn.net/m0_38100569/article/details/99695948

0x01 解题思路

尝试运行一下

```
wby@wby-virtual-machine:~/Desktop/BUUCTF/Re$ ./flat
please input string:
aljfdslkf
what a shame !!!
```

拖入ida64，F5

```
v22 = 0;
printf("please input string:\n", argv, envp);
gets(s);
v18 = strlen(s);
v19 = 5;
v16 = -1046111848;
while ( 1 )
{
  while ( 1 )
  {
    while ( 1 )
    {
      while ( v16 == -2012804730 )
      {
        memcpy(&dest, "J", 0x90uLL);
        v4 = fun_check1(s);
        v5 = -1855144052;
        if ( v4 & 1 )
          v5 = 1890735184;
        v16 = v5;
      }
      if ( v16 != -1855144052 )
        break;
      v16 = -1153978545;
      LODWORD(v15) = printf("what a shame !!!\n", v15);
    }
    if ( v16 != -1612797716 )
      break;
    v10 = fun_check4(s);
    v11 = -1855144052;
    if ( v10 & 1 )
      v11 = -842747696;
    v16 = v11;
  }
  if ( v16 == -1153978545 )
    break;
  switch ( v16 )
  {
    case -1046111848:
```



```
    case -194644933:
      v16 = -1153978545;
      HIDWORD(v15) = printf("you got it !\n", v15);
      break;
```

```
fun_check1(char *)                    .t
fun_check2(char *)                    .t
fun_check3(char *)                    .t
fun_check4(char *)                    .t
fun_check5(char *,int *)              .t
```

- 分析代码逻辑

代码看起来复杂，但是其实很容易分析出来，只要用户输入的字符串通过了5个check函数就会输出"you got it !"，从而获取flag，否则输出“what a shame !!!”。

对5个fun_check进行分析，发现前四个只是规定了flag的格式为UUID格式，即 `flag{xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx}`

最后一个进行了字符校验，如果用户输入的字符是0-9的数字，那么加上17比对；如果等于-，直接比对；如果是小写字母，就减去48进行比对；其余范围的字符直接比对。

0x02 EXP

```
mystr = "J2261C63-3I2I-EGE4-IBCC-IE41A5I5F4HB"
flag = "flag{"
for i in mystr:
 if (ord(i)-17)>=48 and (ord(i)-17)<=57:
  flag += chr(ord(i)-17)
 elif (ord(i)+48)>=97 and (ord(i)+48)<=122:
  flag += chr(ord(i)+48)
 else:
  flag += i
flag += '}'

print flag
```

获取flag：

```
flag{9bbfa2fc-c8b8-464d-8122-84da0e8e5d71}
[Finished in 0.2s]
```