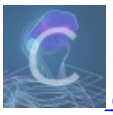
re学习笔记（60）2020 DCICHF 虎符网络安全赛道 Re-game

原创

Forgo7ten 于 2020-04-20 11:05:19 发布 990 收藏

分类专栏： ctf小白成长ing # reverse 文章标签： python z3 信息安全 CTF Reverse

本文链接：https://blog.csdn.net/Palmer9/article/details/105628568



新手一枚，如有错误（不足）请指正，谢谢！！

下载下来就一个文本文档，逆python2的字节码，，，，
没啥好办法，一点点查一点点还原呗

python不是太好，还原的代码也不能运行咳咳，，只能意会，，，

```
arr0 = [249,91,149,113,16,91,53,41]
arr1 = [43,1,6,69,20,62,6,44,24,113,6,35,0,3,6,44,20,22,127,60]
arr2 = [90,100,87,109,86,108,86,105,90,104,88,102]

def check0:
    all = (ord(x) for x in range(32,128)
    iter(s)
    #判断字符范围 32到128
def check1(s): # 爆破得len = 39
    if len(s)<100:
        if len(s)**2 % 777 ^ 233  == 513:

            return True
        else:
            False
    else:
        False

def check2:
    if ((((ord(s[0])*128 + ord(s[1]))*128+ord(s[2]))*128+ord(s[3]))*128+ord(s[4]))*128+ord(s[5]) == 353388946987
7:
    # 前6个元素的约束
        if ord(s[-1]) == 125:
            return True
        else:
            False
    else:
        False
```

```
def check3:
    arr = map(ord,s)# 先转换为ord列表
    a = arr[6:30:3] # 再取元素
    while True:
        try:
            i = next(iter(range(len(a))))# 循环判断列表里的八个元素
            if (a[i] * 17684 + 372511)%257 != arr0[i]:
                return False
            except StopIteration:
            break
    b = arr[-2:33:-1]*5
    c = map(lambda x[0]:x[0]^x[1],zip(b,arr[7:27]))
    if c == arr1:
        p = 0
        for i in range(28,34):
            if (arr[i]+107)/16+77 == arr2[p]:
                if (arr[i]+117)%16+99==arr2[p+1]: #; 两个主要约束
                    p += 2
    else:
        False

lambda x[0]:x[0]^x[1]

flag = input()

if check0(flag):
 if check1(flag):
  if check2(flag):
   if check3(flag):
    print('ok')
            else:
                print('No')
```

大概就这样吧，然后逆是没法逆的，要不python爆破，要不z3。我是写的z3脚本。。

```
from z3 import *
arr0 = [249,91,149,113,16,91,53,41]
arr1 = [43,1,6,69,20,62,6,44,24,113,6,35,0,3,6,44,20,22,127,60]
arr2 = [90,100,87,109,86,108,86,105,90,104,88,102]
k = Solver()
s = [BitVec('s[%d]'%i,64)for i in range(39)]
for i in range(39):
    k.add(32<=s[i])
    k.add(s[i]<128)
k.add(((((s[0]*128+s[1])*128+s[2])*128+s[3])*128+s[4])*128+s[5] == 3533889469877)
k.add(s[-1]== ord('}'))
arr =  list(s)
a = arr[6:30:3]
for i in range(len(a)):
    k.add((a[i]*17684+372511)%257==arr0[i])

b = arr[-2:33:-1]*5
c = list(map(lambda x:x[0]^x[1] ,zip(b,arr[7:27])))
for i in range(len(c)):
    k.add(c[i]==arr1[i])

p = 0
for i in range(28,34):
    k.add(arr2[p] == (arr[i]+107)/16+77)
    k.add((arr[i]+117)%16+99==arr2[p+1])
    p+=2
print(k.check())
print(k.model())
```

然后取z3的输出转换为字符

```
s = [0]*39
s[5]=53
s[4]=123
s[34]=117
s[7]=90
s[6]=76
s[30]=52
s[18]=86
s[35]=51
s[33]=78
s[24]=80
s[12]=120
s[11]=101
s[20]=69
s[15]=105
s[3]=103
s[25]=76
s[23]=101
s[2]=97
s[16]=55
s[29]=53
s[17]=53
s[22]=89
s[36]=70
s[21]=53
s[8]=71
s[13]=53
s[28]=108
s[26]=73
s[14]=89
s[0]=102
s[37]=113
s[31]=49
s[10]=48
s[1]=108
s[9]=53
s[27]=75
s[32]=112
s[19]=113
s[38]=125
for i in range(39):
   print(chr(s[i]),end="")
```

得到最终flag