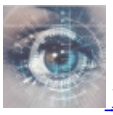
XCTF python-trade

原创

YenKoc 于 2020-01-15 10:19:49 发布 465 收藏

分类专栏： XCTF

本文链接：https://blog.csdn.net/YenKoc/article/details/103984271



一.查看文件类型

后缀名为pyc，说明是python字节码文件，python和java在编译方式上很像，都是编译兼并解释型，先编译成字节码，在虚拟机上解释成机器代码。

二.反编译

```
#! /usr/bin/env python 2.7 (62211)
#coding=utf-8
# Compiled at: 2017-06-02 21:20:43
#Powered by BugScaner
#http://tools.bugscaner.com/
#如果觉得不错,请分享给你朋友使用吧!
import base64

def encode(message):
    s = ''
    for i in message:
        x = ord(i) ^ 32
        x = x + 16
        s += chr(x)

    return base64.b64encode(s)


correct = 'XlNkVmtUI1MgXWBZXCFeKY+AaXNt'
flag = ''
print 'Input flag:'
flag = raw_input()
if encode(flag) == correct:
    print 'correct'
else:
    print 'wrong'
```


三.写个exp

分析每个字符的acsill值都先异或32，再加，之后base64编码

那么逆向回来的话，先base解码，再减少，再异或，转成字符串。

```
import base64
correct ='XlNkVmtUI1MgXWBZXCFeKY+AaXNt'
first=base64.b64decode(correct)
s=''
for i in first:
    s+=chr((i-16)^32)
print(s)
```

注意：这里base64.b64decode这里解码后，for循环中的i已经变成了ascii值了。不需要用ord了。