【XCTF 攻防世界】CRYPTO 密码学 新手练习区 easychallenge

原创

Kal1 于 2020-08-09 11:26:57 发布 532 收藏

分类专栏： CTF刷题 密码学 文章标签： python base64 反编译 安全

本文链接：https://blog.csdn.net/weixin_45844670/article/details/107891073

题目链接：https://adworld.xctf.org.cn/task/answer?type=crypto&number=5&grade=0&id=5119

下载附件，得到一个pyc文件

有关pyc文件的介绍：https://www.jianshu.com/p/7a3a547952c0

那么我们反编译一下看看它的源码是什么

在线反编译：在线pyc反编译

得到以下代码：

```python
#! /usr/bin/env python 2.7 (62211)
#coding=utf-8
# Compiled at: 2018-08-08 22:29:44
#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 encode1(ans):
    s = ''
    for i in ans:
        x = ord(i) ^ 36
        x = x + 25
        s += chr(x)

    return s


def encode2(ans):
    s = ''
    for i in ans:
        x = ord(i) + 36
        x = x ^ 36
        s += chr(x)

    return s


def encode3(ans):
    return base64.b32encode(ans)


flag = ' '
print 'Please Input your flag:'
flag = raw_input()
final = 'UC7KOWVXWVNKNIC2XCXKHKK2W5NLBKNOUOSK3LNNVWW3E==='
if encode3(encode2(encode1(flag))) == final:
    print 'correct'
else:
    print 'wrong'
```

自己写一个解密脚本：

```python
import base64
def decode1(ans):
    s=''
    for i in ans:
        x=ord(i)-25
        x=chr(x^36)
        s+=x
    return s

def decode2(ans):
    s=''
    for i in ans:
        x=i  //在这里不用再使用ord()了，因为base32decode输出的是int
        x=x ^ 36
        x=chr(x-36)
        s+=x
    return s

def decode3(ans):
    return base64.b32decode(ans)

final='UC7KOWVXWVNKNIC2XCXKHKK2W5NLBKNOUOSK3LNNVWW3E==='
flag=decode1(decode2(decode3(final)))
print(flag)
```

需要注意的是

1，base32decode输出的是int

2，^按位异或，一个字符串两次按位异或即为原字符串

得到flag