攻防世界_Crypto_easychallenge

原创

好想变强啊 于 2022-03-22 11:26:14 发布 1963 收藏

分类专栏： 攻防世界刷题记录 文章标签： python 网络安全

本文链接：https://blog.csdn.net/qq_38798840/article/details/123652957

攻防世界刷题Crypto篇

文章目录

前言

昨天去攻防世界网站做了Crypto类的新手练习区题目，今天来记录一下不会做的题。这道题叫easychallenge。

进入题目后下载附件，发现是一个.pyc文件。

用Python IDLE和vs code都打不开（我好无知……），就去搜别人写的wp了。得到如下新知识：

pyc是一种二进制文件，是由py文件经过编译后生成的文件，是一种byte code。py文件变成pyc文件后，运行加载的速度会有所提高；另一反面，把py文件编译为pyc文件，可以实现部分的源码隐藏，保证了Python做商业化软件时的安全性。

求解这道题，首先要想办法得到源码，可以用uncompyle6对题目给的pyc文件进行反编译。

本文关于uncompyle6的内容来自：
https://www.jianshu.com/p/aafdedcbab4f
感谢素不相识的大佬的文章，侵删

一、关于uncompyle6

uncompyle6是一个原生Python的跨版本反编译器和fragment反编译器，是decompyle、uncompyle、uncompyle2等的接替者，可将Python字节码转换回等效的Python源代码

github项目地址：https://github.com/rocky/python-uncompyle6

在Python3下安装uncompyle6：
pip3 install uncompyle6

这里很顺利地直接安装成功~

二、解题步骤

1.反编译pyc文件

这里我把题目给出的pyc文件重命名为test.pyc，反编译后的源代码放入test.py中，无需事先创建test.py，直接在pyc文件所在位置打开终端，输入下面这句命令即可：
（我用的是MacBook）
uncompyle6 -o test.py test.pyc

> 反编译得到的代码如下（得到的是Python2的代码）：

```
# uncompyle6 version 3.8.0
# Python bytecode 2.7 (62211)
# Decompiled from: Python 3.8.10 (v3.8.10:3d8993a744, May  3 2021, 08:55:58)
# [Clang 6.0 (clang-600.0.57)]
# Embedded file name: ans.py
# Compiled at: 2018-08-09 11:29:44
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'
```

2.编写Python脚本

按照反编译得到的加密脚本，把加密过程倒过来进行解密即可。
1）首先对于encode3，解密时，就是对base32解密，调用base64.b32decode()。
2）然后对于encode2，将在1）中得到的bytes，先分出单个数字，然后^36（异或的逆运算还是异或），再-36，最后转回字符，拼接成字符串。
备注：base64.b32decode('UC7KOWVXWVNKNIC2XCXKHKK2W5NLBKNOUOSK3LNNVWW3E===')的输出结果是：
b'\xa0\xbe\xa7Z\xb7\xb5Z\xa6\xa0Z\xb8\xae\xa3\xa9Z\xb7Z\xb0\xa9\xae\xa3\xa4\xad\xad\xad\xad\xad\xb2'
3）最后对于encode3，将在2）中得到的字符串，先分出单个字符，转ascii码十进制数，然后-25，再^36，最后转回字符，拼接成字符串。

这里用到的模块：base64
用到的函数：ord将单个字符转ascii码十进制数，chr将单个ascii码转字符

> 代码如下（自己写的Python3的代码）：

```
import base64

def decode3(ans):
    m3=base64.b32decode(ans)
    return m3

def decode2(ans):
    s=''
    for i in ans:
        i=(i^36)-36
        s+=chr(i)
    return s

def decode1(ans):
    s=''
    for i in ans:
        i=(ord(i)-25)^36
        s+=chr(i)
    return s
print(decode1(decode2(decode3('UC7KOWVXWVNKNIC2XCXKHKK2W5NLBKNOUOSK3LNNVWW3E===''))))
```

贴上自己的运行结果：

```
cyberpeace{interestinghhhhh}
```

总结

以上就是这道题的全部记录了，主要就是新学到了用uncompyle6进行反编译pyc文件得到Python源代码。