

hgame2020-week2-后排围观

凉了啊凉了啊

Reverse

babyPy

下载文件是个字节码，手动翻译一下，大概是这个样子

[参考网址](#)

```
tmp1=flag[::-1]
tmp2=list(tmp1)
for i in range(1,len(tmp2)):
    tmp3=tmp2[i-1]^tmp2[i]
    tmp2[i]=tmp3

res=bytes(tmp2).hex
print(res)
```

根据异或公式，可得 $m[i] = cipher[i] \oplus cipher[i-1]$

于是有如下

```
cipher=bytes().fromhex('7d037d045717722d62114e6a5b044f2c184c3f44214c2d4a22')
_cipher=list(cipher)
m=b''
_m=list(m)
for i in range(1,len(_cipher)):
    tmp=_cipher[i]^_cipher[i-1]
    _m[i]=tmp
flag=bytes(_m[::-1])
print(flag)
```

Crypto

Verification_code

由源码得 $sha256(yyyy + \text{已知字符串}) = \text{已知密文}$ ，爆破求yyyy，输入后再输入I like playing Hgame

```
#!/usr/bin/env python3
# -*- coding: utf-8 -*-
import socketserver
import os, sys, signal
import string, random
from hashlib import sha256
import itertools

myStr='L0zzlogdBwx1h1XC'
dstDigest='236abe814ce3691e1d5959bd36b79ca31e3d31b6daf941fa60d2fb7f9a01b61d'
```

```
for i in itertools.permutations(string.ascii_letters+string.digits,4):
    proof=''.join(i)+myStr
    digest=sha256(proof.encode()).hexdigest()
    if(digest==dstDigest):
        print(i)
```

Misc

Cosmos的午餐

(感谢出题人的耐心解答)

一开始以为在流量包里找png或者jpeg之类的，但是相关的提取出来感觉不太对劲... (根据题目图片应该是二次元妹子...)

先把log导入解密，在http中找，发现一个比较不一样的包

4901	snowplow.wetransfer.com	application/json	1041 bytes	tp2
4907	snowplow.wetransfer.com	text/plain	2 bytes	tp2
6103	wetransfer-us-prod-outgoing.s3.amazonaws.com	<u>application/x-www-form-urlencoded</u>	1220 kB	e418689cfbcc62
6131	e-10220.adzerk.net	application/json	1066 bytes	v2
6216	snowplow.wetransfer.com	application/json	1006 bytes	tp2

点进去看看发现含有zip文件格式，导出来看下里边有张图片，提示用outguess，并且备注里给了key，然后解密下就好，解完了是个网址，下载下来一个压缩包，里边的图片二维码扫一下就行

所见即为假

发现7z可以直接解压，注释中的F5 key提示了F5隐写，于是利用F5-steganography

```
java Extract ./11.jpg -e res -p N11D7CQon6dBsFLr
```

得到hex文本，复制进winhex可得flag

地球上最后的夜晚

解压得no password.pdf，想到pdf隐写，用wbStego4.3open解码得到一个txt文件，里边写着zip的解压密码，解压得一个doc文件，试试转成xml，用7z对doc解压后进入word文件夹，发现secret.xml，打开就是flag

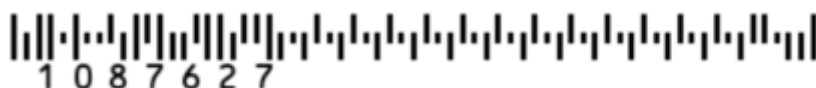
玩玩条码

下载得一个zip，里边注释:Decode JPNPostCode to get MSUStegoVideo password

俩文件对应注释里边内容，先看postcode，这是个日本的邮政编码，我是在生成条码网站上手动对比，一个个试的，不过也不复杂，有规律

[日本邮政条形码生成器](#)

条形码宽高:451 x 52 px



第二个，根据提示下了virtualdub2，再安MSU StegoVideo 插件，这个只能运行32位的，打开后根据网上教程，输入上一步骤所得的码进行解码，[使用 MSU StegoVideo](#)

打开txt文件可得zip密码，7z解压后得条形码，在线扫一下就好
[Free Online Barcode Reader](#)