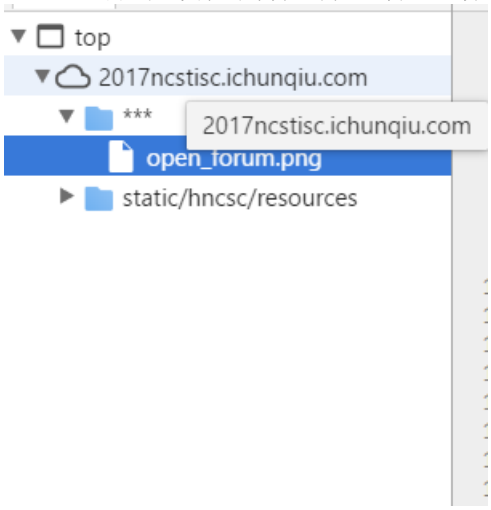
小Writeup

转载

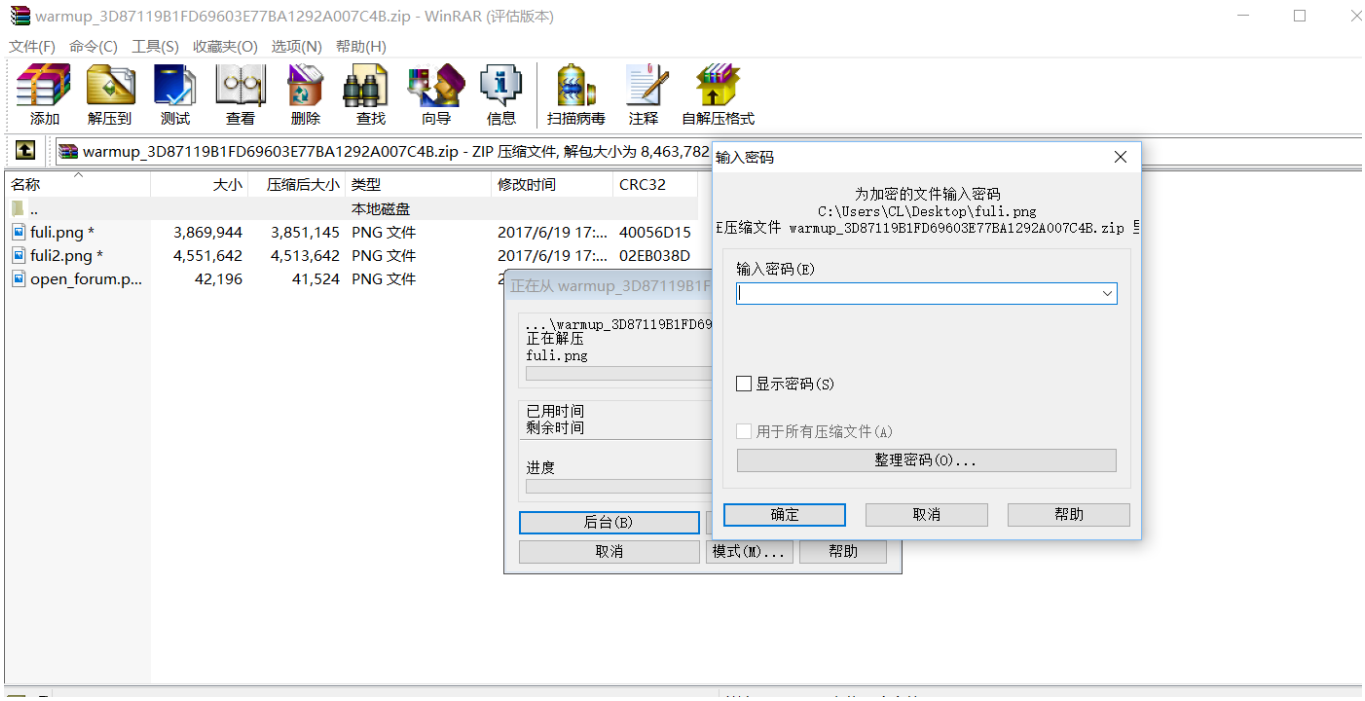
weixin_30332241 于 2017-07-09 22:05:00 发布 130 收藏
原文链接：http://www.cnblogs.com/ycll/p/7143370.html

Misc 100

- 下载文件之后是一个zip压缩包。因为一开始没有给任何提示信息，题目也什么都没说，爆破了一会无果。同时不是伪加密，所以应该是明文攻击。之后官方给出提示，是一个网址。
- F12进入调试，发现结构很奇怪，明显是特意这么弄的



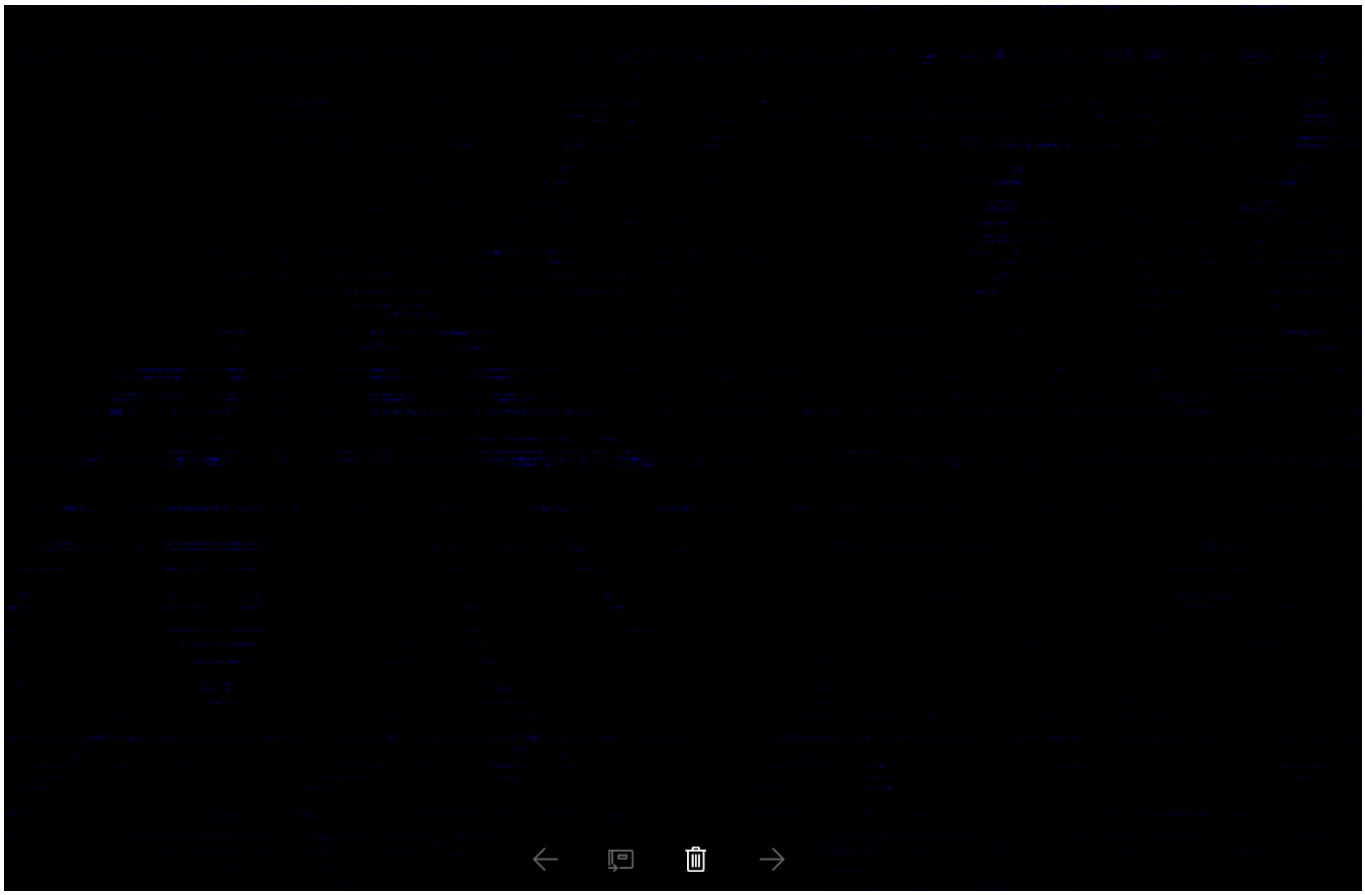
- 之后以为是把这个html给更改为png，然后进行压缩。但是压缩信息与原压缩包中不符，所以不对。



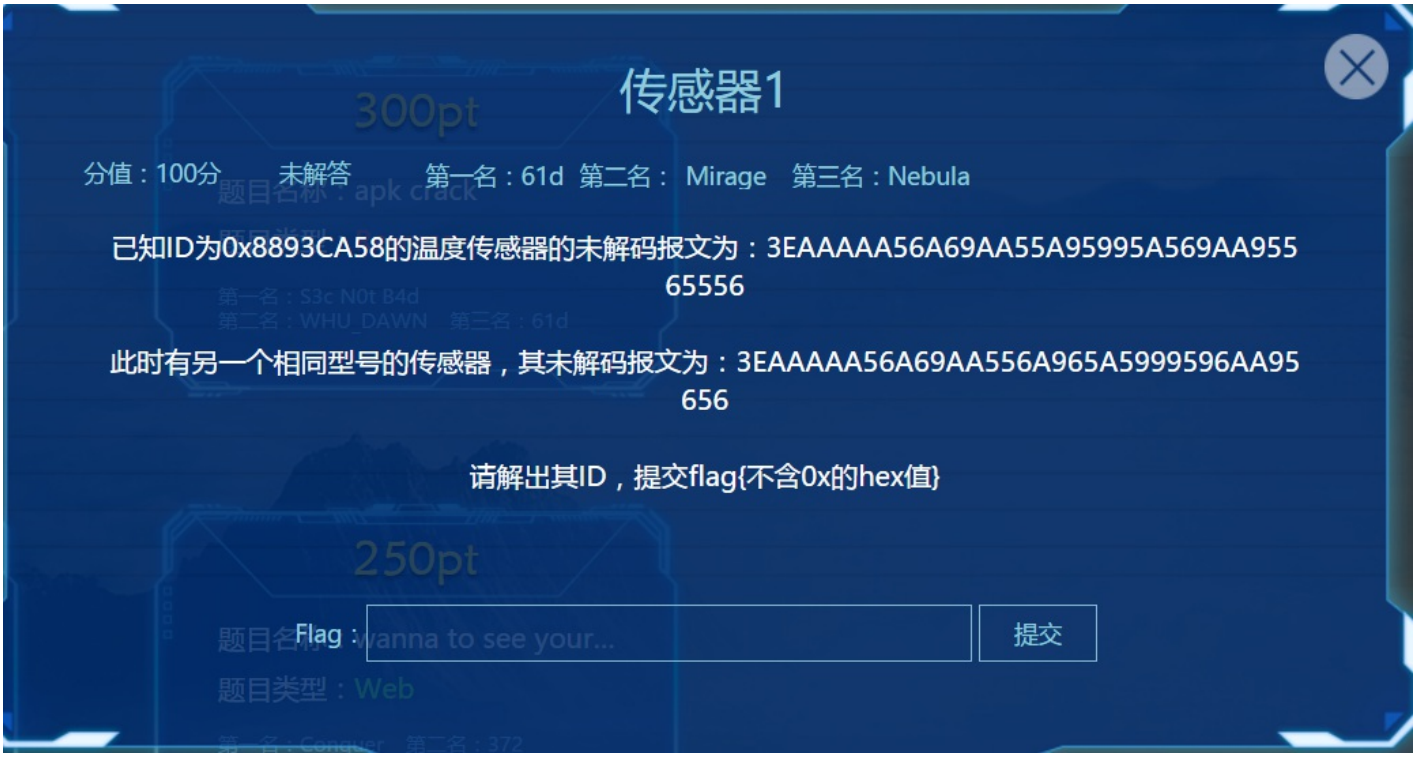
- 后来又经过很长时间的寻找，突然想到界面的图片是不是可以利用，果然发现了一个和压缩包中相同命名的图片

```
        </div>
        <a href="https://2017ncstisc.ichunqiu.com/kaiwusignup"><img src="https://2017ncstisc.ichunqiu.com/static/hncsc/resources/images/index/open_forum.png" alt="开
    </div>
    <div class="peaks">
        <ul>
```

- 把图片下载后再压缩，信息与压缩包中一致。使用archpr明文攻击，果然跑出来了。
- 又得到两张相同图片，因为图片大小不一致，想到以前做的题，有没有可能是异或后改二维码。就又对图片做对比。
- 但是区别太大，没法继续进行下去



Misc 100



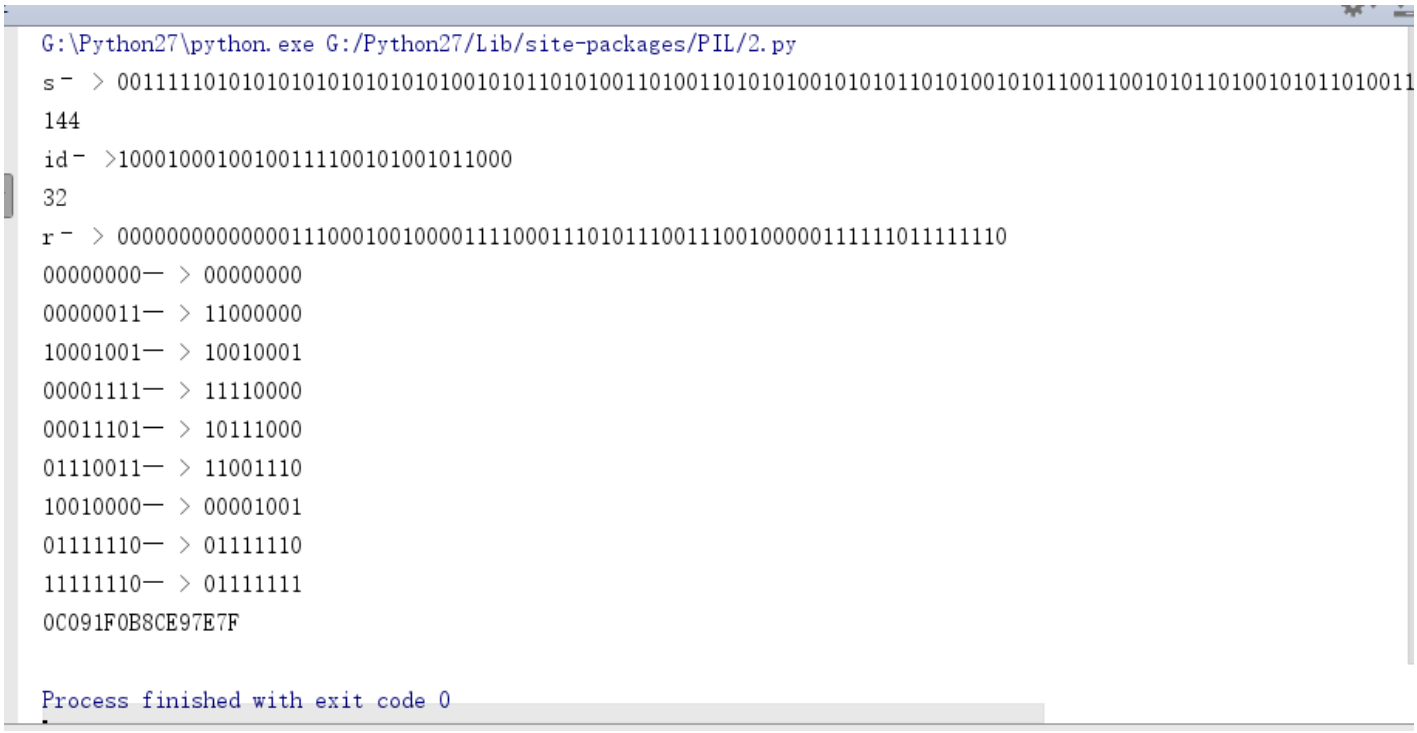
- 一开始是以为和以前的简单解密题一样，通过异或操作得到结果，但是很多次都不对，后来经过很多方法，考虑到是不是编码。找到以前的一些题的writeup

```
# -*- coding: utf-8 -*-
# coding:utf8

hexstr = "3EAAAAA56A69AA55A95995A569AA95565556"
id = "8893CA58"
# 30
# hexstr = “3EAAAAA56A69AA55A95995A569AA95565556”
# 转二进制字符串
s = ''
t=''
for i in xrange(len(hexstr) / 2):
    ch = hexstr[i * 2: i * 2 + 2]
    b = bin(int(ch, 16))[2:]
    b = '0' *(8 - len(b)) + b
    s += b
    r = ''
print 's- > ' + s
print s.__len__()

for i in xrange(len(id) / 2):
    ch = id[i * 2: i * 2 + 2]
    a = bin(int(ch, 16))[2:]
    a = '0' *(8 - len(a)) + a
    t += a
    r = ''
print 'id- >' + t
print t.__len__()

# 曼彻斯特解码， 01对应数据1， 10对应0
for i in xrange(len(s) / 2):
    c = s[i * 2: i * 2 + 2]
    if c == '01':
       r += '1'
    else:
      r += '0'
print 'r- > ' + r
ret = ''
for i in xrange(len(r) / 8):
    c = r[i * 8: i *8 + 8][::-1]  # 调整字节序
    print str(r[i * 8: i * 8+ 8]) + '— > ' + c
    ret += hex(int(c, 2))[2:].upper()
print ret
def main():
    pass
if __name__ == '__main__':main();
```



和题目所给ID不太一样，不管是长度还是其他什么。又试了好几种编码的排列，都没能得到那个ID值

我觉得大方向应该是没错的，通过题目给的ID和报文信息，找出对应的编码方案，然后用这个方案直接跑出另外那个报文的ID值。同理，Misc 250也是一样的，但是那题的编码方案应该是要在这基础上更进一步的。

转载于:https://www.cnblogs.com/ycll/p/7143370.html