CTF论剑场 misc 二维码

原创

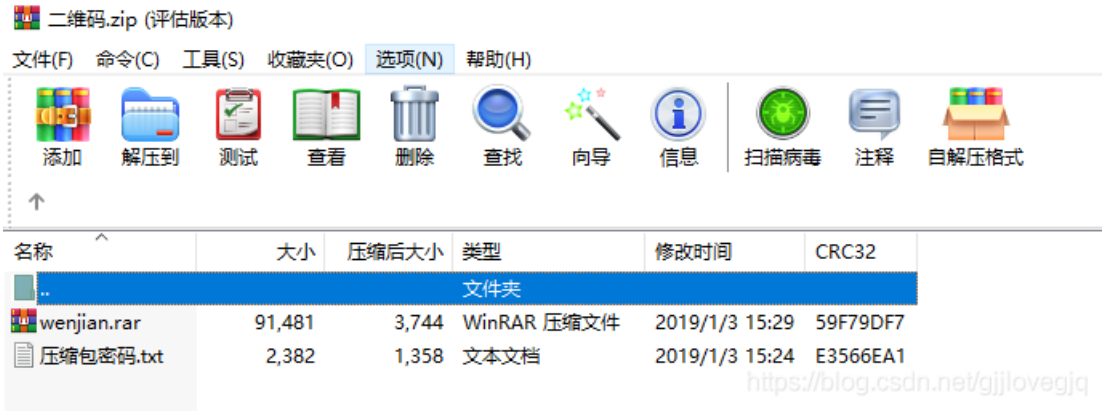
憨厚老实 于 2019-10-31 08:50:37 发布 2094 收藏 5

文章标签： CTF 论剑场 misc

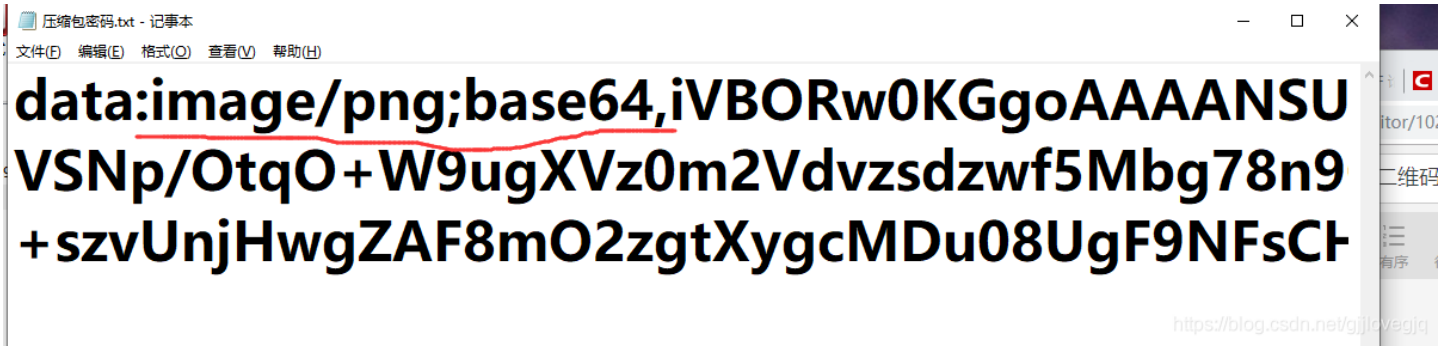
本文链接：https://blog.csdn.net/gjjlovegjq/article/details/102830922

CTF论剑场 misc 二维码 writeup

下载附件，打开压缩包，发现有两个文件，一个压缩包，一个txt。

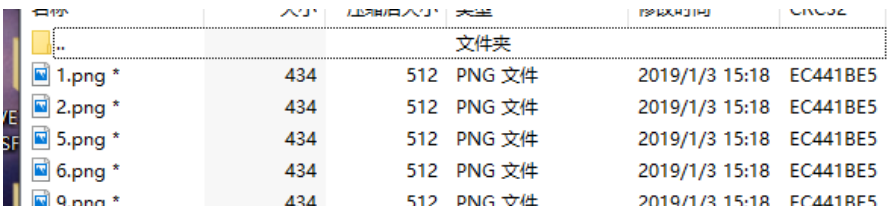


他说txt是压缩包密码，那我们就要相信他嘛，打开txt压缩包，发现是一堆base64,，根据提示，确定为base64图片编码



http://tool.chinaz.com/tools/imgtobase/ 解码网址附上

获得了压缩包密码，先放一边。接着打开另外一个压缩包，发现是一堆加密过后的文件。



10.png *	434	512	PNG 文件	2019/1/3 15:18 EC441BE5
12.png *	434	512	PNG 文件	2019/1/3 15:18 EC441BE5
13.png *	434	512	PNG 文件	2019/1/3 15:18 EC441BE5
17.png *	434	512	PNG 文件	2019/1/3 15:18 EC441BE5
18.png *	434	512	PNG 文件	2019/1/3 15:18 EC441BE5
23.png *	434	512	PNG 文件	2019/1/3 15:18 EC441BE5
25.png *	434	512	PNG 文件	2019/1/3 15:18 EC441BE5
26.png *	434	512	PNG 文件	2019/1/3 15:18 EC441BE5
29.png *	434	512	PNG 文件	2019/1/3 15:18 EC441BE5
30.png *	434	512	PNG 文件	2019/1/3 15:18 EC441BE5
31.png *	434	512	PNG 文件	2019/1/3 15:18 EC441BE5
33.png *	434	512	PNG 文件	2019/1/3 15:18 EC441BE5
34.png *	434	512	PNG 文件	2019/1/3 15:18 EC441BE5
35.png *	434	512	PNG 文件	2019/1/3 15:18 EC441BE5
36.png *	434	512	PNG 文件	2019/1/3 15:18 EC441BE5
38.png *	434	512	PNG 文件	2019/1/3 15:18 EC441BE5
39.png *	434	512	PNG 文件	2019/1/3 15:18 EC441BE5
41.png *	434	512	PNG 文件	2019/1/3 15:18 EC441BE5
43.png *	434	512	PNG 文件	2019/1/3 15:18 EC441BE5
47.png *	434	512	PNG 文件	2019/1/3 15:18 EC441BE5
49.png *	434	512	PNG 文件	2019/1/3 15:18 EC441BE5
51.png *	434	512	PNG 文件	2019/1/3 15:18 EC441BE5
54.png *	434	512	PNG 文件	2019/1/3 15:18 EC441BE5
57.png *	434	512	PNG 文件	2019/1/3 15:18 EC441BE5
58.png *	434	512	PNG 文件	2019/1/3 15:18 EC441BE5
62.png *	434	512	PNG 文件	2019/1/3 15:18 EC441BE5
63.png *	434	512	PNG 文件	2019/1/3 15:18 EC441BE5
65.png *	434	512	PNG 文件	2019/1/3 15:18 EC441BE5
66.png *	434	512	PNG 文件	2019/1/3 15:18 EC441BE5
68.png *	434	512	PNG 文件	2019/1/3 15:18 EC441BE5
69.png *	434	512	PNG 文件	2019/1/3 15:18 EC441BE5

总计 70,115 字节(160 个文件)

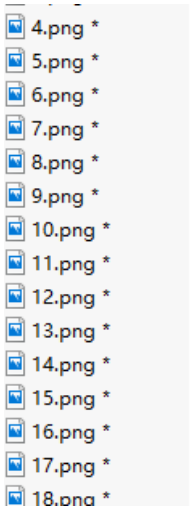
用之前解码出来的压缩包密码打开图片，扫了几个二维码后，发现都是1，就当我想来想去想不明白1能做什么的时候，翻到下

8	EC441BE5
8	EC441BE5
8	EC441BE5
8	EC441BE5
8	EC441BE5
8	EC441BE5
8	EC441BE5
8	EC441BE5
8	EC441BE5
8	EC441BE5
8	53D8CB...
8	53D8CB...
8	53D8CB...
8	53D8CB...
8	53D8CB...
8	53D8CB...
8	53D8CB...
8	53D8CB...
8	53D8CB...
8	53D8CB...

面，发现crc32值不一样的一堆二维码，扫一下为0。猜测为二进制解码。

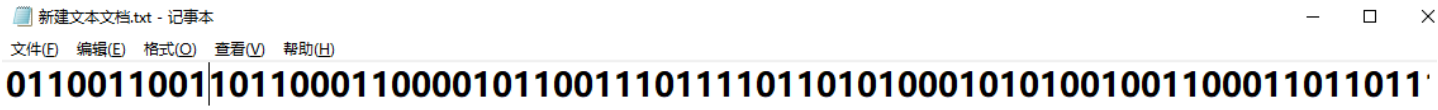
可是这么多二维码，顺序杂乱，一个一个扫，就很麻烦。楼主比较笨，提供一个我解题的方法。排序方式为大小，图片就会从0

0.png *
1.png *
2.png *
3.png *



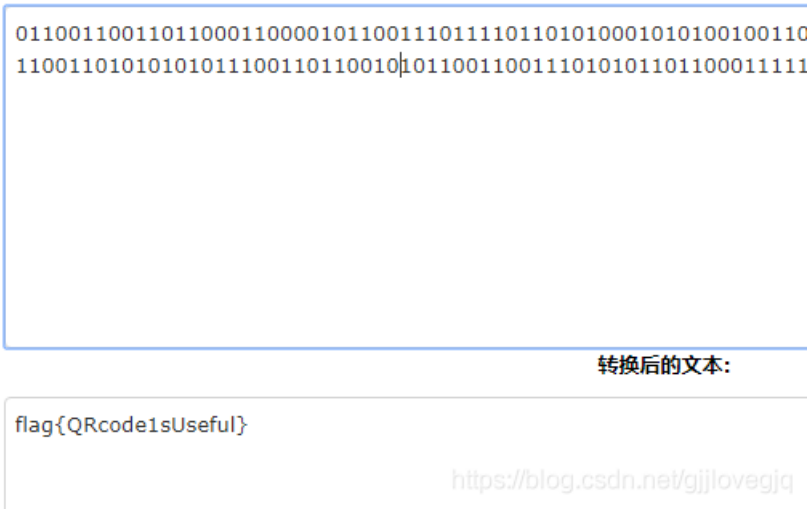
到最后一张。

接着根据crc32值为53D8CBB3的图片为0，EC441BE5的为1.



附上脚本

```
import os
for i in range(160):
a = os.path.getsize(str(i) + '.png')
if a == 443:
print(0,end='')
else:
print(1,end='')
```



得到flag。