[BUUCTF]一路到底

原创

wangjin7356 已于 2022-03-14 17:07:08 修改 548 收藏

分类专栏： python CTF 文章标签： 安全

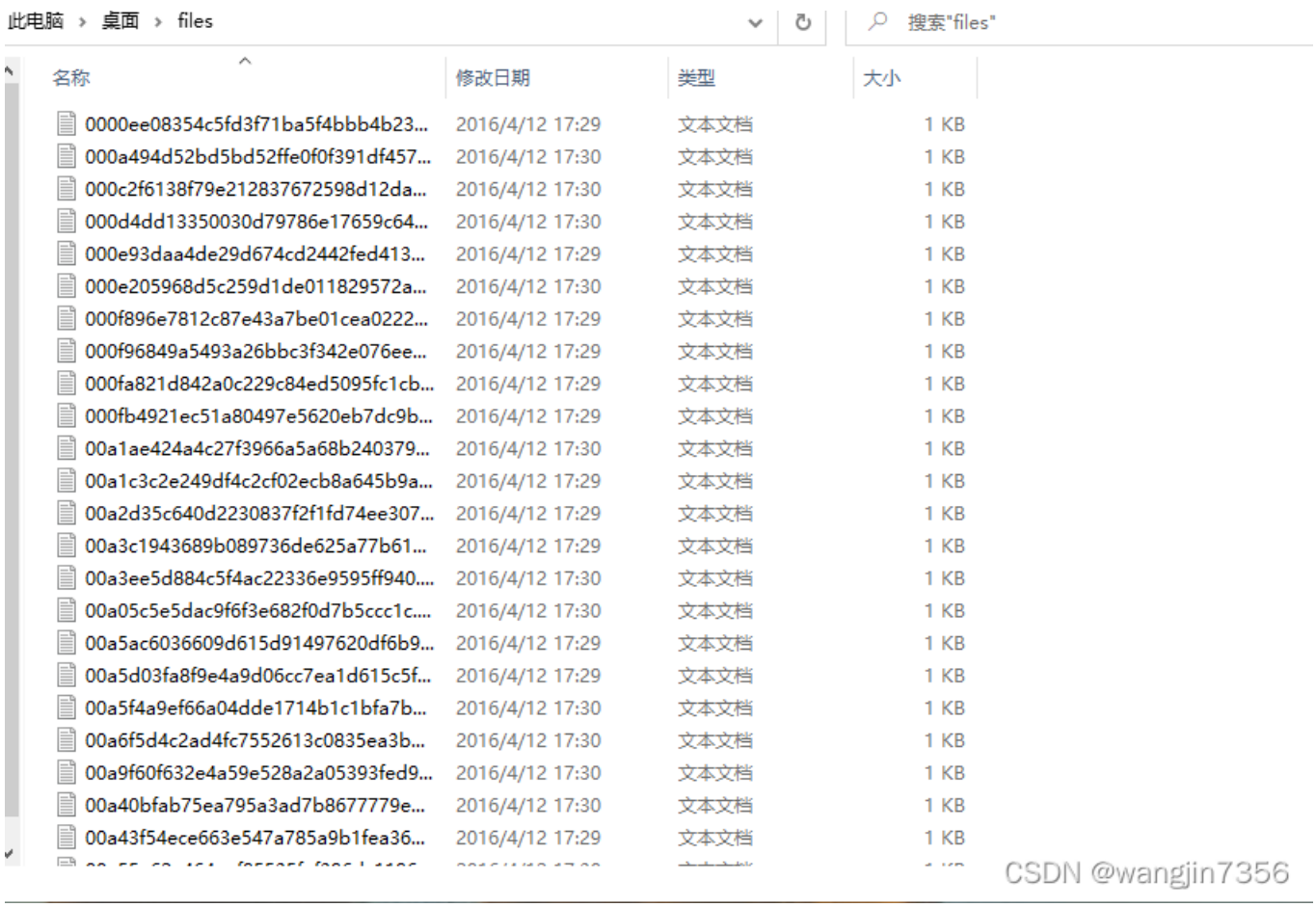
于 2022-03-13 01:32:34 首次发布

题目链接

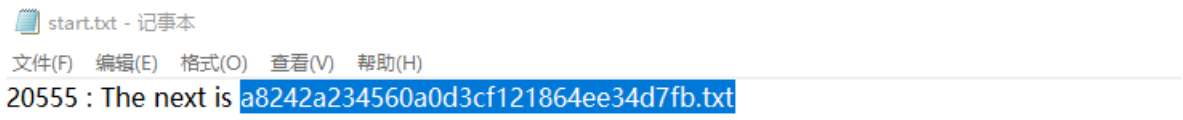
```
https://buuoj.cn/challenges#%E4%B8%80%E8%B7%AF%E5%88%B0%E5%BA%95
```

解题过程

打开题目，有1万多个txt文件，好家伙，真让人头疼。



在里面找到个start.txt文件,应该是第一个，先打开看看内容吧：



下一个文件是：`a8242a234560a0d3cf121864ee34d7fb.txt`,打开看看：

套路好深呀！冒号前面的数字20555、772代表什么呢，转换下看看吧：

熟悉吧，原来是zip的文件头。原来每个文件里包含了zip文件的数据（冒号前面的数字）。这么多文件只好用脚本提取数据了。

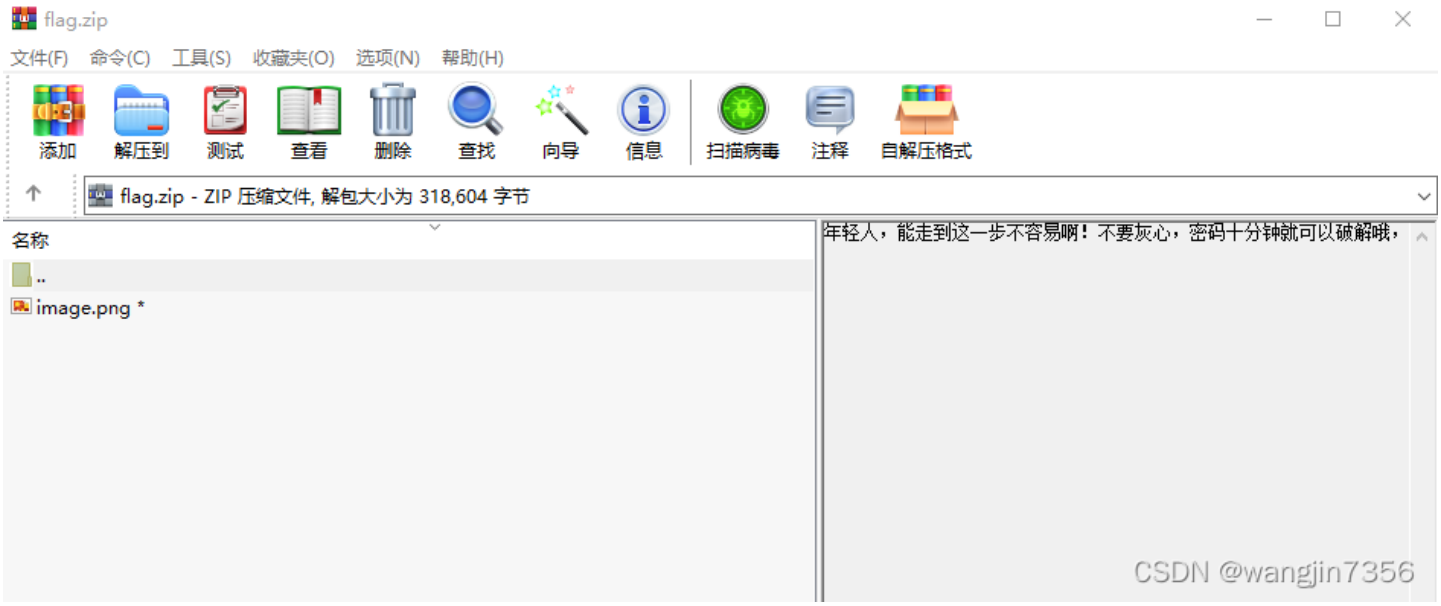
```python
# python3.10
import binascii

path = "files/"
hex_data = ''
next_file = 'start.txt'

while True:
    filename = ''.join([path, next_file])
    try:
        with open(filename, 'r') as f:
            line = f.read()
            idx = line.index(':')
            dec_data = int(line[:idx - 1])
            hex_data += f'{dec_data:04x}'
            next_file = line[-36:]
    except:
        break

zipfile = path + 'flag.zip'
with open(zipfile, 'wb') as ff:
    ff.write(binascii.unhexlify(hex_data))
```

提取后保存到flag.zip,打开压缩包：

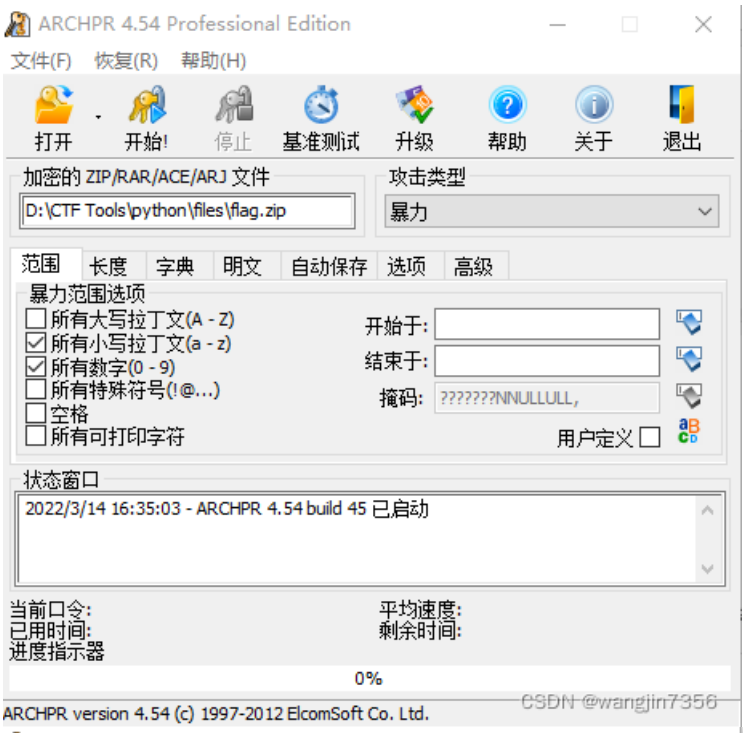


到这一步确实不容易。还要密码，也不给个提示什么的，怎么破解呀。夜深了，暂时先到这儿吧。

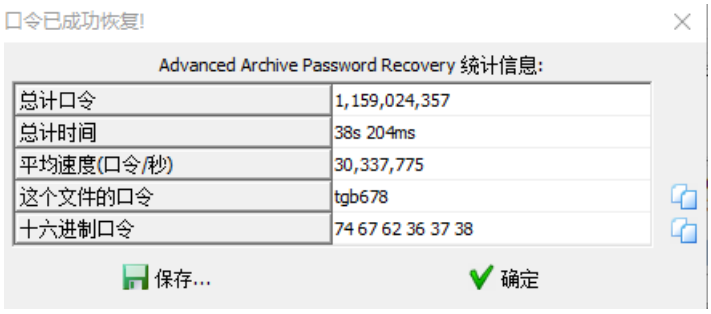
2022年3月13日凌晨

3月14日继续

密码没有头绪，瞎分析吧。统计分析txt文件名：使用了小写字母和数字，大写的只出现一次。使用ARCHPR 4.54破解，范围选“所有小写拉丁文（a-z）”和“所有数字（0-9）”，长度根据以往做题经验，没有提示长度的话一般选6。
试试看吧。

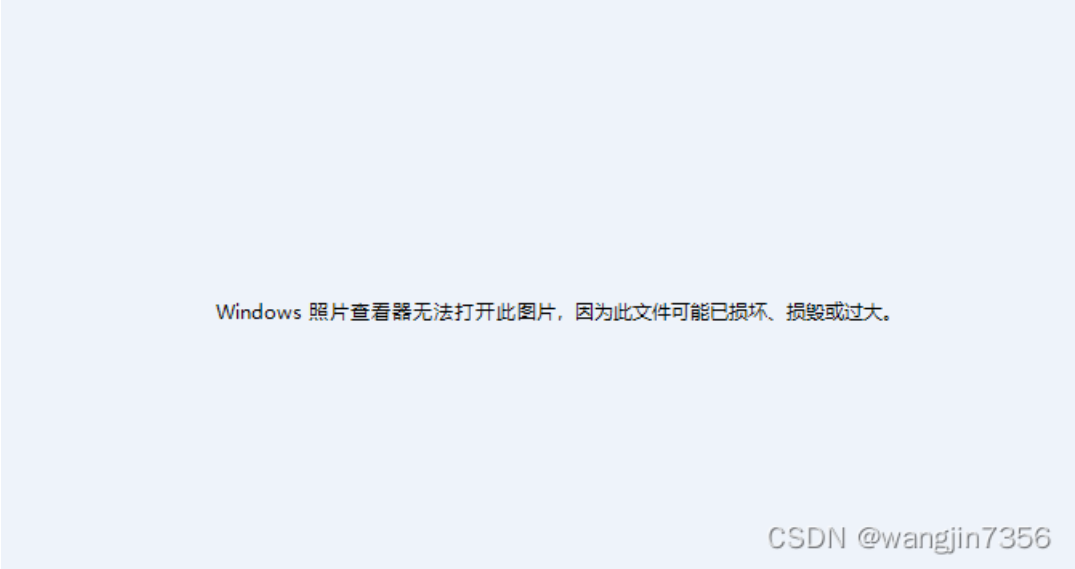


密码居然找到了：

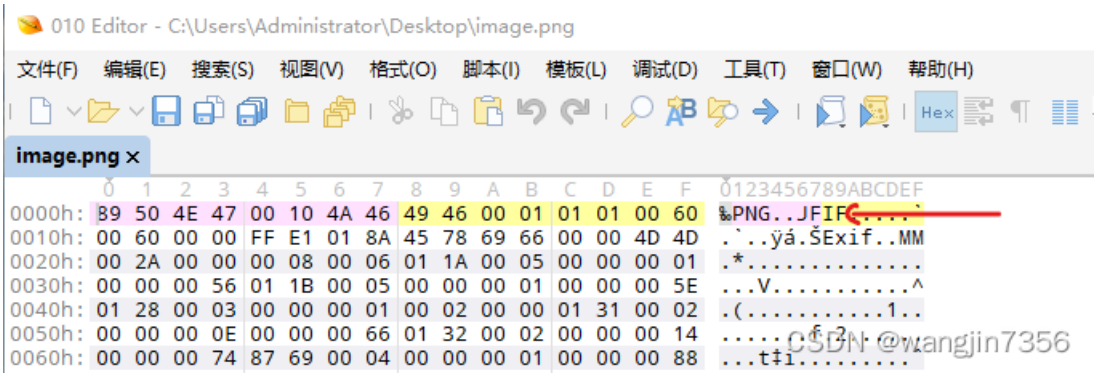


解压压缩包，得到一张png图片：

但是打不开



用010Editor分析：



应该是文件头错误，本身是个jpg图片格式。用FF D8 FF E0替换89 50 4E 47，然后另存为jpg文件，看到了flag。


```
flag{0c6b489ca956e2fd94dce12be4bf0729}
```