

[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

版权声明: 本文为博主原创文章, 遵循 [CC 4.0 BY-SA](#) 版权协议, 转载请附上原文出处链接和本声明。

本文链接: <https://blog.csdn.net/wangjin7356/article/details/123453477>

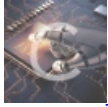
版权



python 同时被 2 个专栏收录

8 篇文章 0 订阅

订阅专栏



CTF

49 篇文章 0 订阅

订阅专栏

题目链接

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

解题过程

题目 [解题快手榜](#) ×

一路到底

1

跟着指引者的指示能发现宝藏哦! 注意: 得到的 flag 请包上 flag{} 提交

[38ff11ef-e3...](#)

Flag

CSDN @wangjin7356

打开题目, 有1万多个txt文件, 好家伙, 真让人头疼。

名称	修改日期	类型	大小
0000ee08354c5fd3f71ba5f4bbb4b23...	2016/4/12 17:29	文本文档	1 KB
000a494d52bd5bd52ffe0f0f391df457...	2016/4/12 17:30	文本文档	1 KB
000c2f6138f79e212837672598d12da...	2016/4/12 17:30	文本文档	1 KB
000d4dd13350030d79786e17659c64...	2016/4/12 17:30	文本文档	1 KB
000e93daa4de29d674cd2442fed413...	2016/4/12 17:29	文本文档	1 KB
000e205968d5c259d1de011829572a...	2016/4/12 17:30	文本文档	1 KB
000f896e7812c87e43a7be01cea0222...	2016/4/12 17:29	文本文档	1 KB
000f96849a5493a26bbc3f342e076ee...	2016/4/12 17:29	文本文档	1 KB
000fa821d842a0c229c84ed5095fc1cb...	2016/4/12 17:29	文本文档	1 KB
000fb4921ec51a80497e5620eb7dc9b...	2016/4/12 17:29	文本文档	1 KB
00a1ae424a4c27f3966a5a68b240379...	2016/4/12 17:30	文本文档	1 KB
00a1c3c2e249df4c2cf02ecb8a645b9a...	2016/4/12 17:29	文本文档	1 KB
00a2d35c640d2230837f2f1fd74ee307...	2016/4/12 17:29	文本文档	1 KB
00a3c1943689b089736de625a77b61...	2016/4/12 17:29	文本文档	1 KB
00a3ee5d884c5f4ac22336e9595ff940...	2016/4/12 17:30	文本文档	1 KB
00a05c5e5dac9f6f3e682f0d7b5ccc1c...	2016/4/12 17:30	文本文档	1 KB
00a5ac6036609d615d91497620df6b9...	2016/4/12 17:29	文本文档	1 KB
00a5d03fa8f9e4a9d06cc7ea1d615c5f...	2016/4/12 17:29	文本文档	1 KB
00a5f4a9ef66a04dde1714b1c1bfa7b...	2016/4/12 17:30	文本文档	1 KB
00a6f5d4c2ad4fc7552613c0835ea3b...	2016/4/12 17:30	文本文档	1 KB
00a9f60f632e4a59e528a2a05393fed9...	2016/4/12 17:30	文本文档	1 KB
00a40bfab75ea795a3ad7b8677779e...	2016/4/12 17:30	文本文档	1 KB
00a43f54ece663e547a785a9b1fea36...	2016/4/12 17:29	文本文档	1 KB

在里面找到个start.txt文件,应该是第一个,先打开看看内容吧:

start.txt - 记事本

文件(F) 编辑(E) 格式(O) 查看(V) 帮助(H)

20555 : The next is a8242a234560a0d3cf121864ee34d7fb.txt

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

a8242a234560a0d3cf121864ee34d7fb.txt - 记事本

文件(F) 编辑(E) 格式(O) 查看(V) 帮助(H)

772 : The next is 5d2ecc80d506dc00c6457a2cb6430d54.txt

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:

```
Python 3.10.2 (tags/v3.10.2:a58ebcc, J
Type "help", "copyright", "credits" or
>>> hex(20555)
'0x504b'
>>> hex(772)
'0x304'
>>>
```

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。

```

# python3.10
import binascii

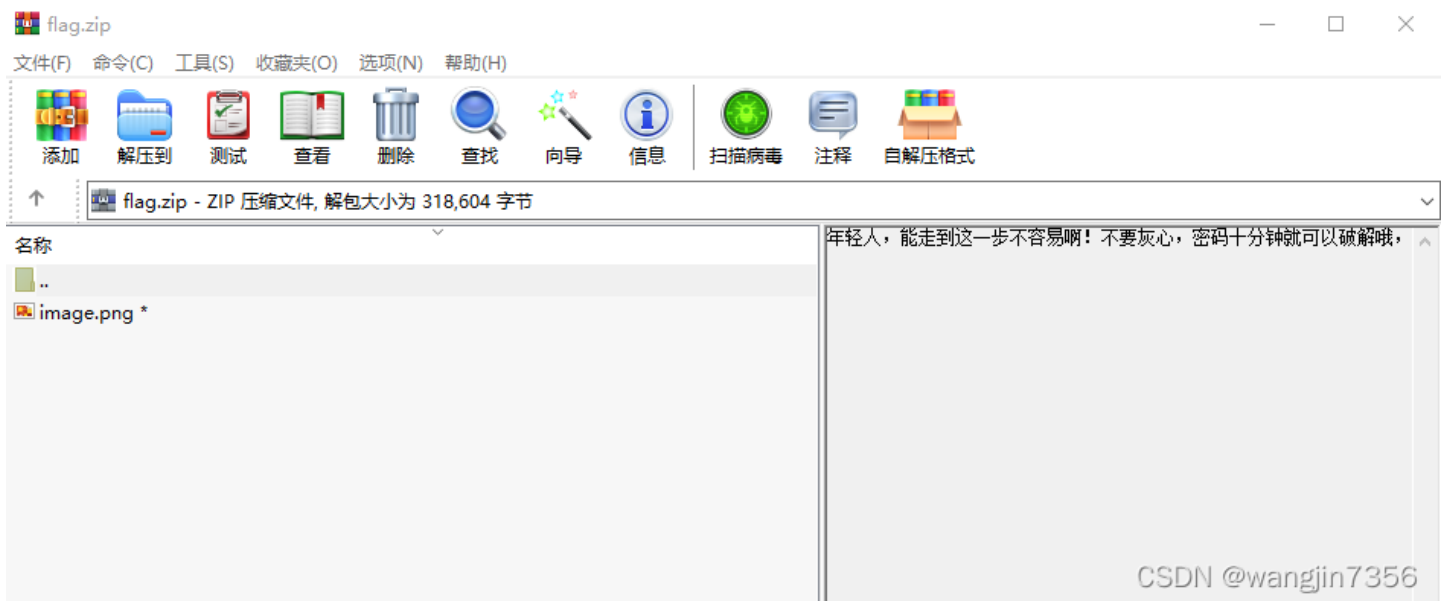
path = "files/"
hex_data = ''
next_file = 'start.txt'

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

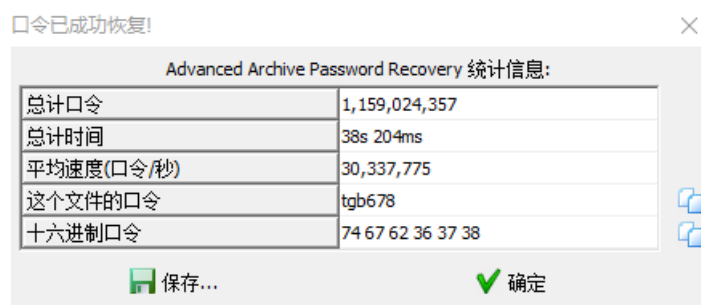
3月14日继续

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。

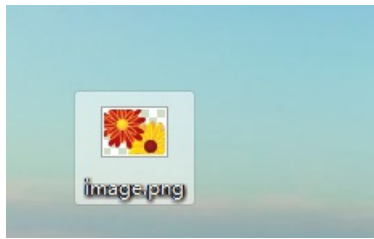
试试看吧。



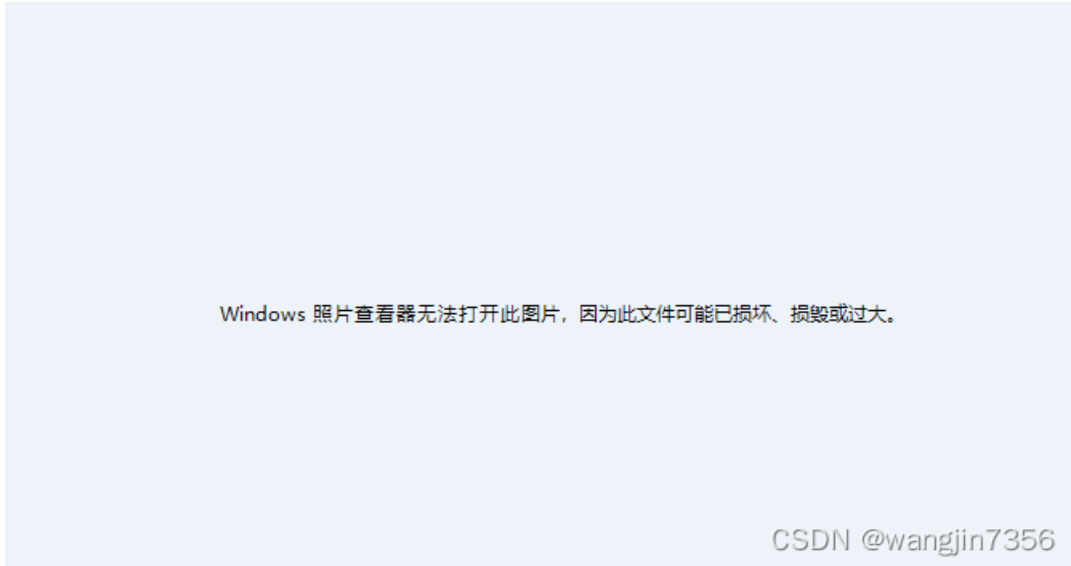
密码居然找到了：



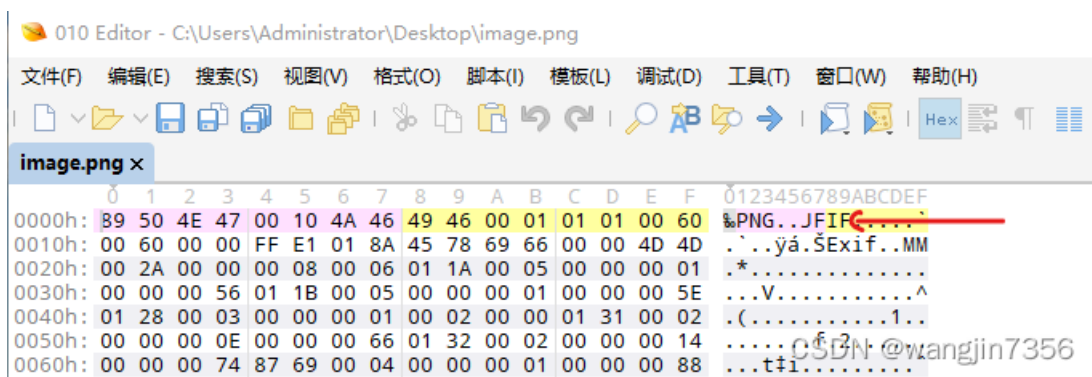
解压压缩包，得到一张png图片：



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}



CSDN @wangjin7356

flag{0c6b489ca956e2fd94dce12be4bf0729}