

BUUCTF: 一路到底

原创

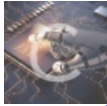
末初 于 2021-03-07 14:24:17 发布 638 收藏 3

分类专栏: [CTF_MISC_Writeup](#)

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/mochu777777/article/details/114482689>

版权



[CTF_MISC_Writeup](#) 专栏收录该内容

246 篇文章 45 订阅

订阅专栏

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

Challenge 47 Solves

一路到底

79

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 Submit

<https://blog.csdn.net/mochu777777>

38ff11ef-e3d3-4f8a-b163-3d300bc016ea.zip - Bandizip 6.27

文件(F) 编辑(E) 查找(I) 选项(O) 视图(V) 帮助(H)

| 名称 | 压缩后大小 | 原始大小 | 类型 | 循环冗余检验(CRC) | 修改日期 |
|--------------------------------------|-------|------|------|-------------|--------------------|
| .. | | | | | |
| 0000ee08354c5fd3f71ba5f4b4b4b23d.txt | 58 | 56 | 文本文档 | b7747688 | 2016/4/12 17:29:35 |
| 000a494d52bd5bd52ffe0f0f391df457.txt | 58 | 56 | 文本文档 | 1b401c41 | 2016/4/12 17:30:12 |
| 000c2f6138f79e212837672598d12da3.txt | 58 | 56 | 文本文档 | 99d334be | 2016/4/12 17:30:36 |
| 000d4d13350030d79786e17659c64ba.txt | 58 | 56 | 文本文档 | b8a0ae53 | 2016/4/12 17:30:27 |
| 000e93daa4de29d674cd2442fed41361.txt | 58 | 56 | 文本文档 | ee82014c | 2016/4/12 17:29:31 |
| 000e205968d5c259d1de011829572a21.txt | 58 | 56 | 文本文档 | 37b22e26 | 2016/4/12 17:30:23 |
| 000f896e7812c87e43a7be01cea02222.txt | 58 | 56 | 文本文档 | 511be993 | 2016/4/12 17:29:19 |
| 000f96849a5493a26bbc3f342e076ee6.txt | 58 | 56 | 文本文档 | fbfd4b59 | 2016/4/12 17:29:23 |
| 000fa821d842a0c229c84ed5095fc1cb.txt | 58 | 56 | 文本文档 | 75a6be87 | 2016/4/12 17:29:28 |
| 000fb4921ec51a80497e5620eb7dc9ba.txt | 58 | 56 | 文本文档 | abb26c57 | 2016/4/12 17:29:24 |
| 00a1ae424a4c27f3966a5a68b240379d.txt | 58 | 56 | 文本文档 | 40d96578 | 2016/4/12 17:30:43 |
| 00a1c3c2e249df4c2cf02ecb8a645b9a.txt | 58 | 56 | 文本文档 | 47ab0e9e | 2016/4/12 17:29:31 |
| 00a2d35c640d2230837f2f1fd74ee307.txt | 58 | 56 | 文本文档 | b0e7d212 | 2016/4/12 17:29:29 |
| 00a3c1943689b089736de625a77b61a7.txt | 58 | 56 | 文本文档 | 249f4661 | 2016/4/12 17:29:07 |
| 00a3ee5d884c5f4ac22336e9595ff940.txt | 58 | 56 | 文本文档 | 2732692c | 2016/4/12 17:30:16 |

| | | | | | |
|--------------------------------------|----|----|------|----------|--------------------|
| 00a05c5e5dac9f6f3e682f0d7b5ccc1c.txt | 58 | 56 | 文本文档 | 95c80227 | 2016/4/12 17:30:03 |
| 00a5ac6036609d615d91497620df6b98.txt | 58 | 56 | 文本文档 | c6500d61 | 2016/4/12 17:29:15 |
| 00a5d03fa8f9e4a9d06cc7ea1d615c5f.txt | 58 | 56 | 文本文档 | bd958cbd | 2016/4/12 17:29:29 |

文件: 155534, 文件夹: 1, 压缩包大小: 37.6 MB

此电脑 > 下载 > files

搜索 "files"

| 名称 | 修改日期 | 类型 | 大小 |
|--------------------------------------|-----------------|------|------|
| da2a20c071200c102e321107c3304.txt | 2016/4/12 17:28 | 文本文档 | 1 KB |
| daf9616796dccb642227f88b0b9a4fb3.txt | 2016/4/12 17:28 | 文本文档 | 1 KB |
| de2b7a2b2d6b6e27d159b203547c787a.txt | 2016/4/12 17:28 | 文本文档 | 1 KB |
| de6a9bb6d4c72e3374eeceed7740e1bd.txt | 2016/4/12 17:28 | 文本文档 | 1 KB |
| e8c0b821396fb4cdedec29ce350af2f3.txt | 2016/4/12 17:28 | 文本文档 | 1 KB |
| e36aca53458b77717f8344eba5903693.txt | 2016/4/12 17:28 | 文本文档 | 1 KB |
| e36c5263bd8c551d3fee6a27573a055e.txt | 2016/4/12 17:28 | 文本文档 | 1 KB |
| e68e39ae3a2cde089c62c9dcbb30802a.txt | 2016/4/12 17:28 | 文本文档 | 1 KB |
| e340c4cbdda4ed7fa2ac681315a2f044.txt | 2016/4/12 17:28 | 文本文档 | 1 KB |
| e0443c8c325c396c799e67aacd9cad81.txt | 2016/4/12 17:28 | 文本文档 | 1 KB |
| e1044806b245d1491d0aae61750811b0.txt | 2016/4/12 17:28 | 文本文档 | 1 KB |
| ea66633a9be76a463246e2aa90d22016.txt | 2016/4/12 17:28 | 文本文档 | 1 KB |
| eab93b09296df4aaf06759fc18a8f715.txt | 2016/4/12 17:28 | 文本文档 | 1 KB |
| efbaa964687c9eaabf19e9cf8093949c.txt | 2016/4/12 17:28 | 文本文档 | 1 KB |
| efbfa79bc62318388d9443f4bb854cd1.txt | 2016/4/12 17:28 | 文本文档 | 1 KB |
| f0b8f89d6f052356da2d20810f757d09.txt | 2016/4/12 17:28 | 文本文档 | 1 KB |
| f0fa10f43ab5a4b5688c87da4e239a41.txt | 2016/4/12 17:28 | 文本文档 | 1 KB |
| f4eded1b81d458d00c919a95f4929f7c.txt | 2016/4/12 17:28 | 文本文档 | 1 KB |
| f5b197ea50fd3dc064237c312eeae285.txt | 2016/4/12 17:28 | 文本文档 | 1 KB |
| f5d33ca894f21a8a34cc46a98a242b3c.txt | 2016/4/12 17:28 | 文本文档 | 1 KB |
| f5e2515ace69b3acc0c22ee00f92a04f.txt | 2016/4/12 17:28 | 文本文档 | 1 KB |
| f434e27014b5ec594701a85ef3924a93.txt | 2016/4/12 17:28 | 文本文档 | 1 KB |
| f1986d839a012d681626f762e3c0f943.txt | 2016/4/12 17:28 | 文本文档 | 1 KB |
| fb97e82bb12a522dae0719aefa4ef438.txt | 2016/4/12 17:28 | 文本文档 | 1 KB |
| fd6b6353a97da80afb00b2bd726eeb1.txt | 2016/4/12 17:28 | 文本文档 | 1 KB |
| fecc4796ebaa77d86ad37b21634fb2fc.txt | 2016/4/12 17:28 | 文本文档 | 1 KB |
| ff5a9aea120fb89759bfe3c1c09c50fc.txt | 2016/4/12 17:28 | 文本文档 | 1 KB |
| start.txt | 2016/4/12 17:28 | 文本文档 | 1 KB |

1个项目 56字节

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

| 行 | 列 | 大小 | 格式 |
|-------|-------|------|----------------------|
| 第 1 行 | 第 1 列 | 100% | Windows (CRLF) UTF-8 |

每个 txt 的关键点是 前面的数字

计算器

程序员

20,555

HEX 504B

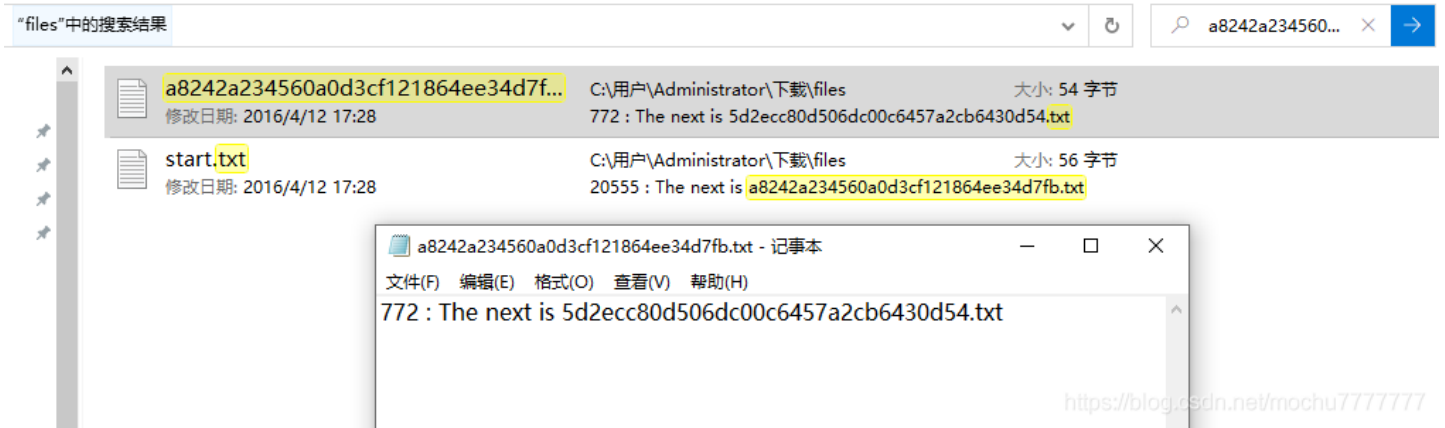
DEC 20,555

OCT 50 113

BIN 0101 0000 0100 1011

<https://blog.csdn.net/mochu7777777>

第一个 txt 文件内容中的数字是 20555 转换为十六进制发现是 504b，再看看这个 txt 给的下一个文件内容



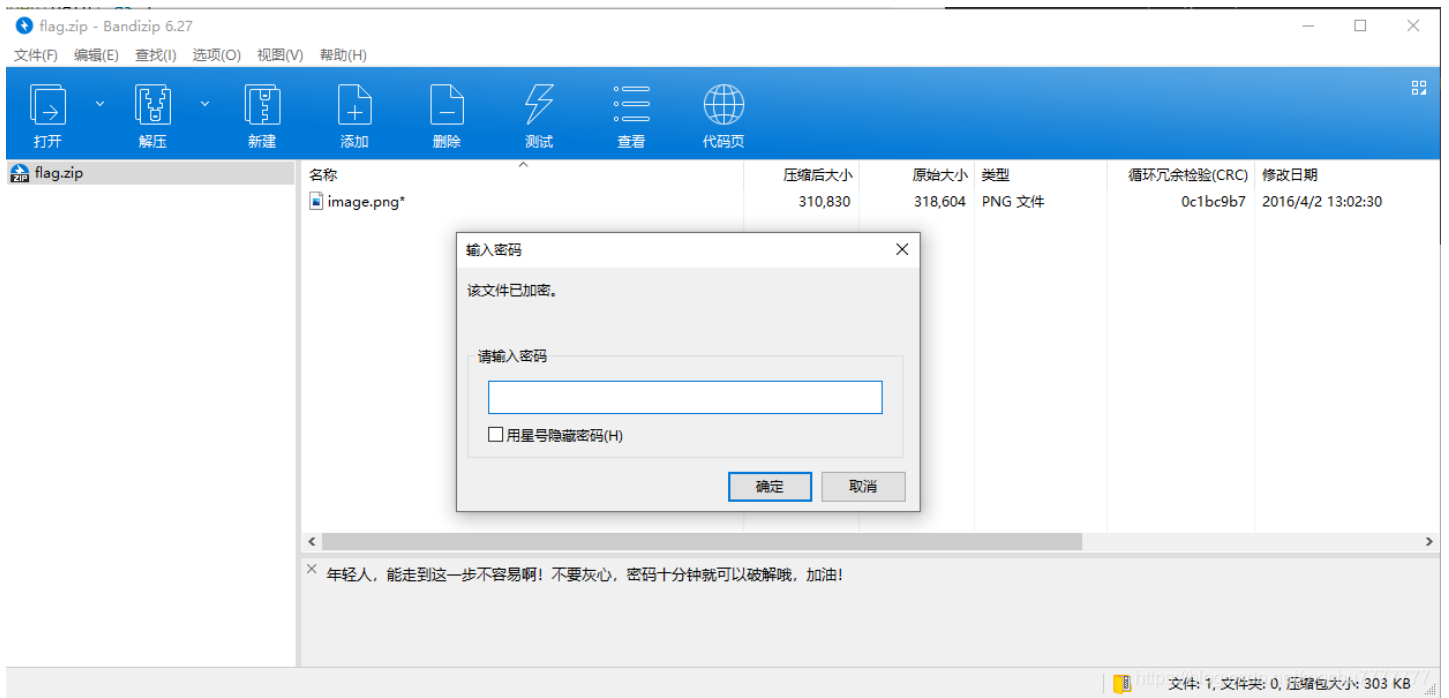
寻找提示找到第二个txt中的数字是 772 转换为十六进制为 304，这里应该还需要十六进制补高的，也就是 0304。504b0304 是 zip 的十六进制文件头，利用py脚本按照给的提示依次取出所有的数字，转换为十六进制再以字节流的形式写入 flag.zip

```
import binascii

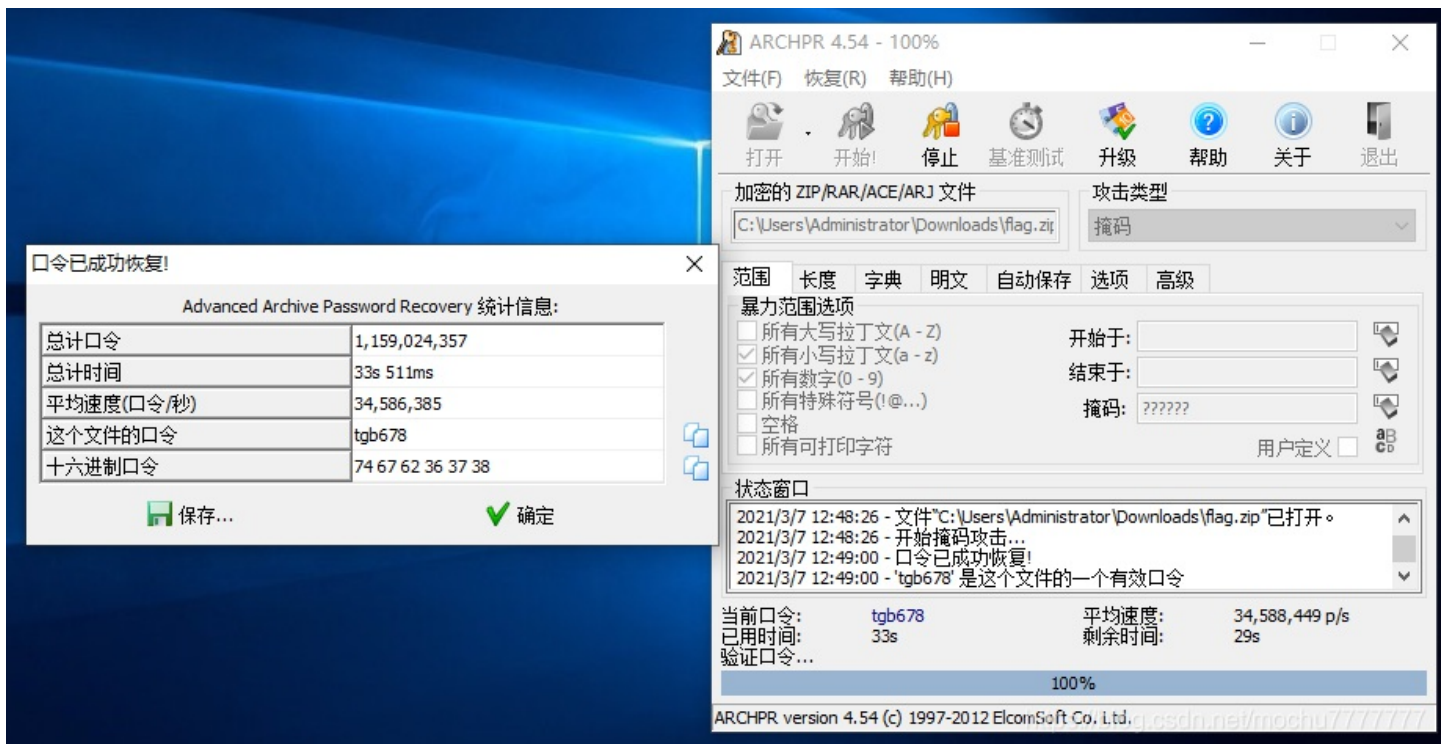
hexdata = ''
with open('./files/start.txt') as f:
    cont = f.read()
    nexttxt = cont[-36:]
    hexdata += '{:04x}'.format(int(cont[0:cont.find(':')-1]))
    while True:
        path = './files/' + nexttxt
        try:
            with open(path) as f:
                cont = f.read()
                nexttxt = cont[-36:]
                hexdata += '{:04x}'.format(int(cont[0:cont.find(':')-1]))
        except:
            break

with open('flag.zip', 'wb') as f:
    f.write(binascii.unhexlify(hexdata))
```

得到如下

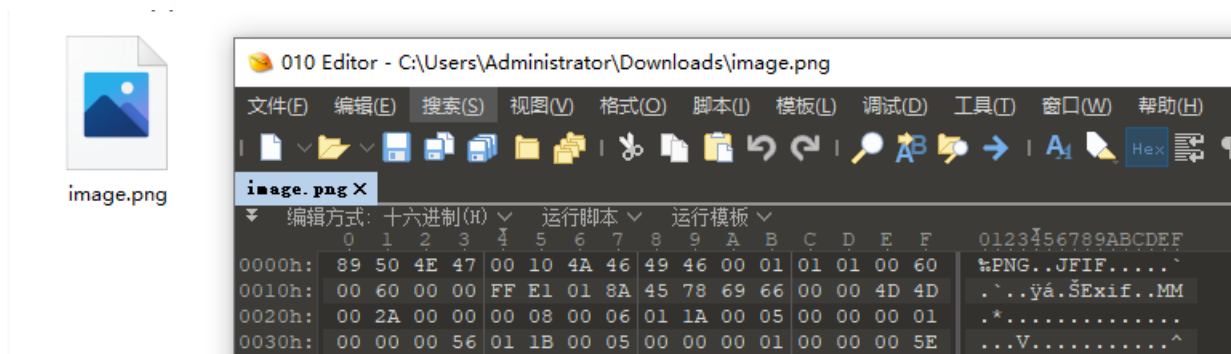


这个说实话爆破有点坑，什么提示都没，看了下 [Ga1axy师傅](#) 的wp，爆破 26字母小写+数字



得到压缩包密码: **tgb678**

解压得到 **image.png**



```
0040h: 01 28 00 03 00 00 00 01 00 02 00 00 01 31 00 02  .(.....1..
0050h: 00 00 00 0E 00 00 00 66 01 32 00 02 00 00 00 14  f.2
0060h: 00 00 00 74 87 69 00 04 00 00 00 01 00 00 00 83  ..t#1.....
```

文件头应该是jpg的，修改文件头为jpg文件头: **FF D8 FF E0**



flag{0c6b489ca956e2fd94dce12be4bf0729}