BUUCTF：一路到底

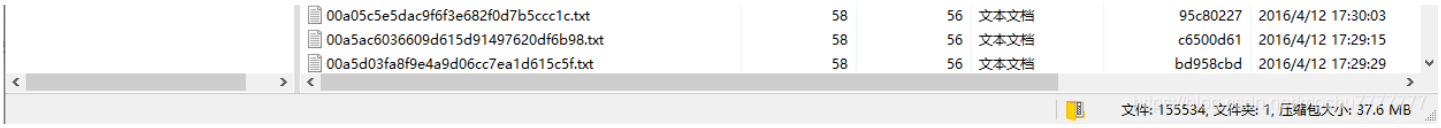
原创

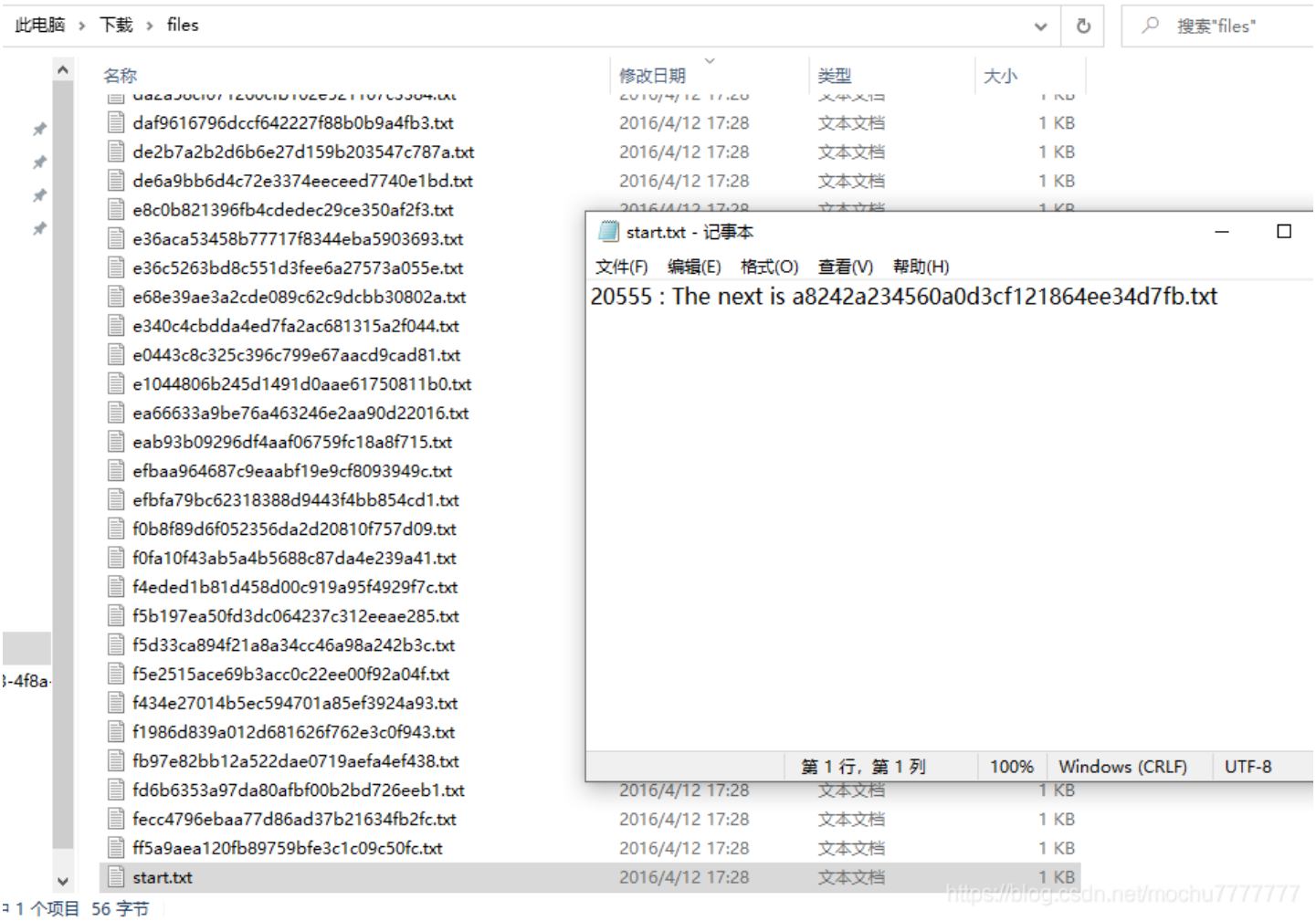
末 初 于 2021-03-07 14:24:17 发布 638 收藏 3

分类专栏： CTF_MISC_Writeup

本文链接：https://blog.csdn.net/mochu7777777/article/details/114482689

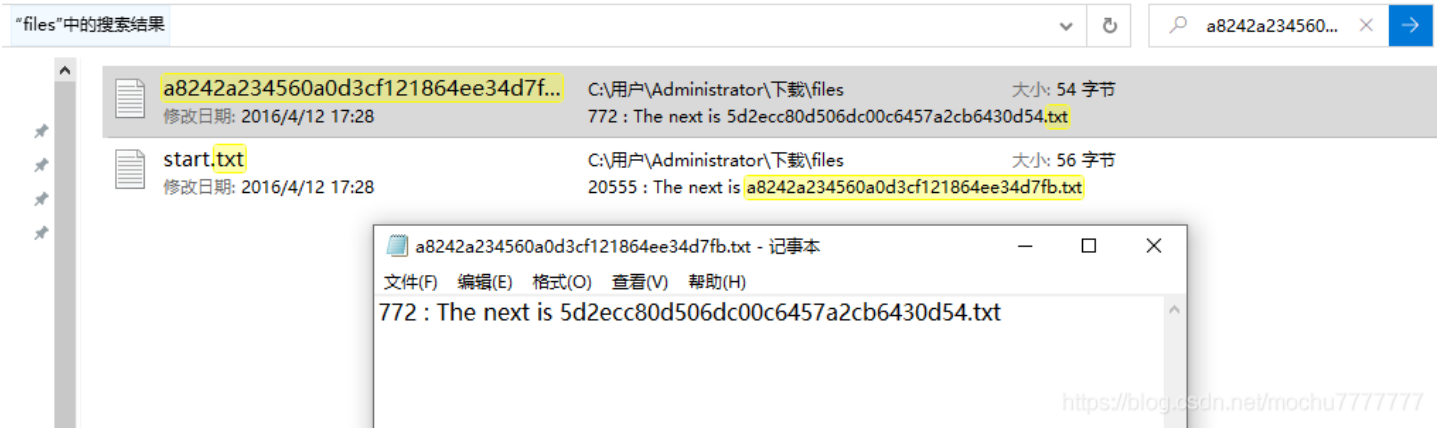

```
https://buuoj.cn/challenges#%E4%B8%80%E8%B7%AF%E5%88%B0%E5%BA%95
```





每个`txt`的关键点是`前面的数字`

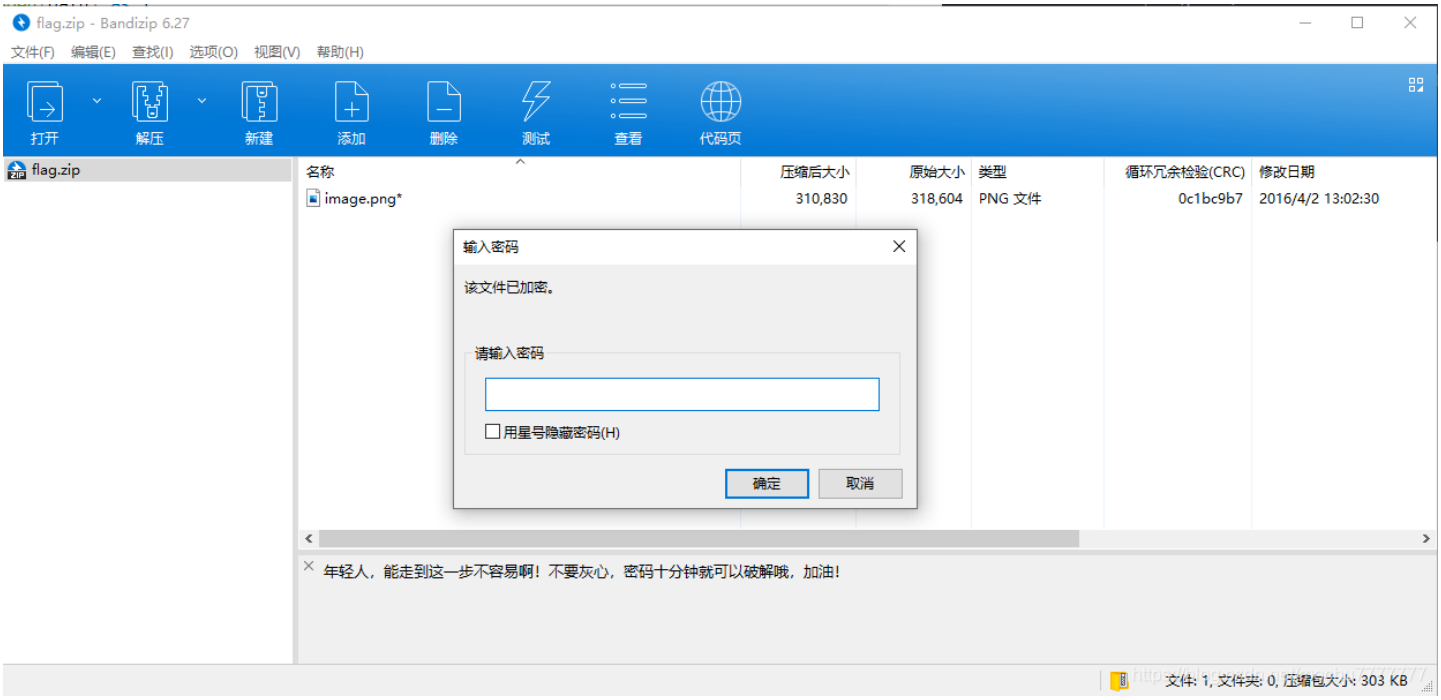
第一个`txt`文件内容中的数字是`20555`转换为十六进制发现是`504b`，再看看这个`txt`给的下一个文件内容



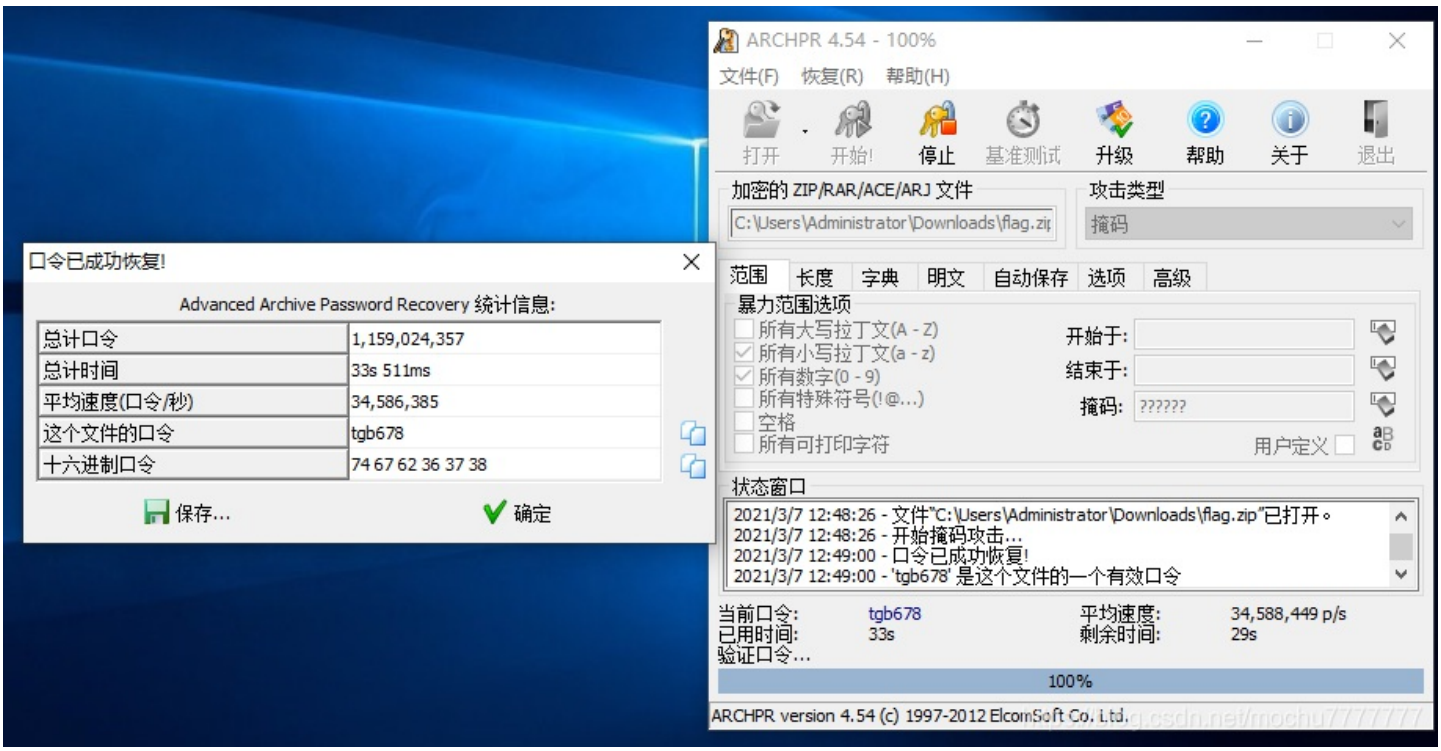
寻找提示找到第二个txt中的数字是`772`转换为十六进制为`304`，这里应该还需要十六进制补高的，也就是`0304`。`504b0304`是`zip`的十六进制文件头，利用py脚本按照给的提示依次取出所有的数字，转换为十六进制再以字节流的形式写入`flag.zip`

```
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

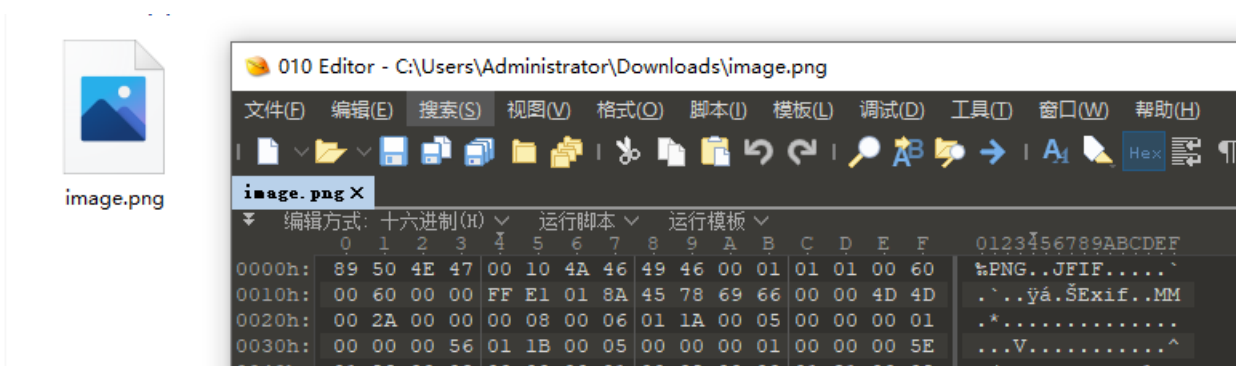


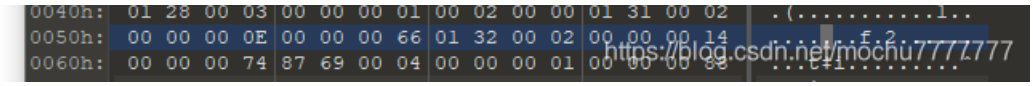
这个说实话爆破有点坑，什么提示都没，看了下`Ga1axy师傅`的wp，爆破`26字母小写+数字`



得到压缩包密码：`tgb678`

解压得到`image.png`





文件头应该是jpg的，修改文件头为jpg文件头：`FF D8 FF E0`


```
flag{0c6b489ca956e2fd94dce12be4bf0729}
```