BUUCTF：zip

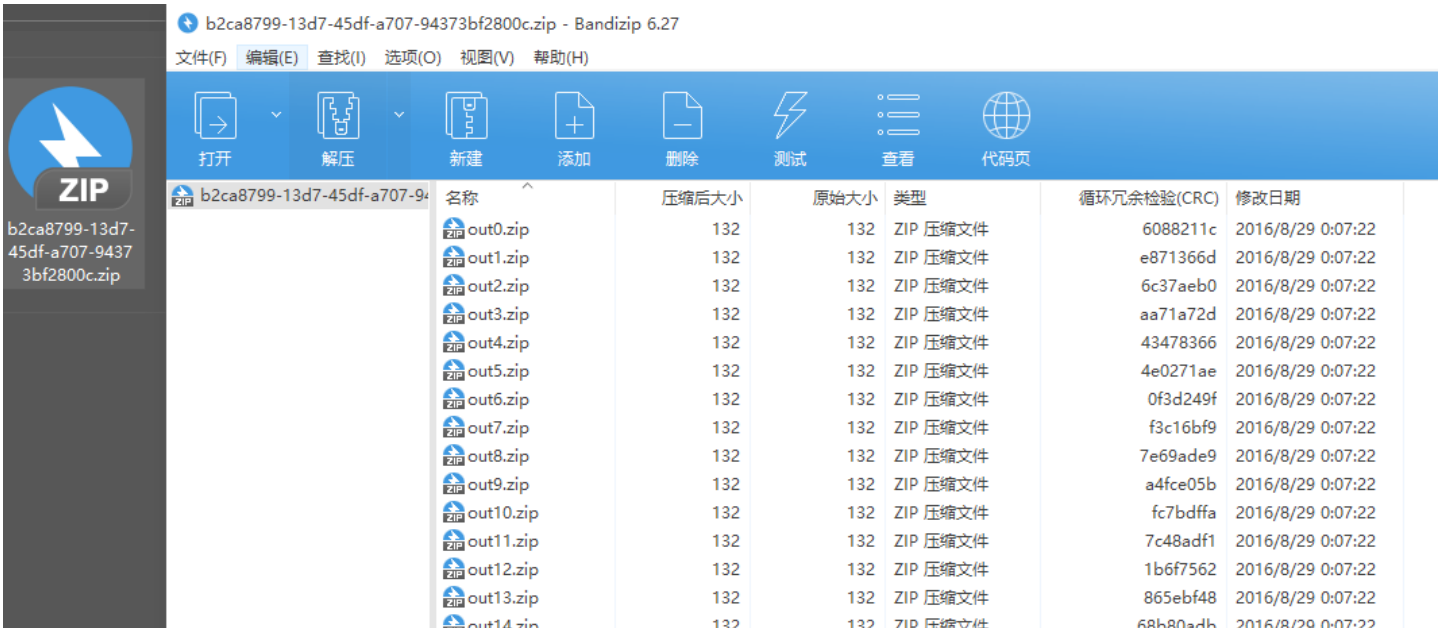
原创

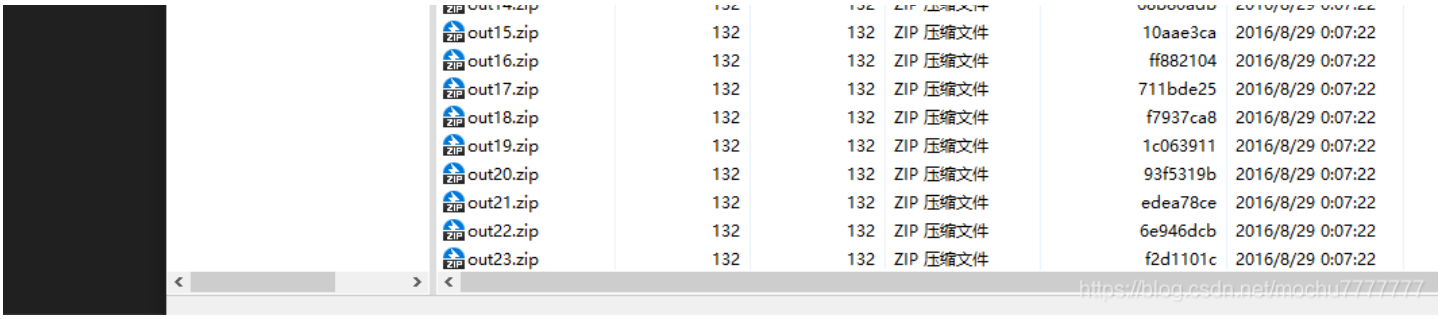
末 初 于 2020-11-01 21:11:23 发布 1164 收藏 1

分类专栏： CTF_MISC_Writeup

本文链接：https://blog.csdn.net/mochu7777777/article/details/109435117

> 题目地址：https://buuoj.cn/challenges#zip





很多压缩包，但是里面的内容非常小，小于5字节，可以尝试使用`CRC32爆破`得到其内容

先以`out0.zip`做个例子，`out0.zip`的`CRC32`校验码为：`0x75f90d3a`

```
PS D:\Tools\Misc\crc32> python .\crc32.py reverse 0x75f90d3a
4 bytes: {0x7a, 0x35, 0x42, 0x7a}
verification checksum: 0x75f90d3a (OK)
alternative: 2BHS9N (OK)
alternative: 4zPLa0 (OK)
alternative: 7gJsJx (OK)
alternative: 9hUCvv (OK)
alternative: Gzefs4 (OK)
alternative: MqgWNY (OK)
alternative: QoY76E (OK)
alternative: RORDuU (OK)
alternative: VKOEt6 (OK)
alternative: XDPuH8 (OK)
alternative: bmE3S_ (OK)
alternative: guV_H1 (OK)
alternative: j6113k (OK)
alternative: jgSP_w (OK)
alternative: zV8BCl (OK)
PS D:\Tools\Misc\crc32> php -r "var_dump(hex2bin('7a35427a'));"
string(4) "z5Bz"
```

这样就可以爆破出`out0.zip`中`data.txt`的内容，然后利用网上找的一个脚本

```python
#python3
import zipfile
import string
import binascii

def CrackCrc(crc):
 for i in dic:
  for j in dic:
   for k in dic:
    for h in dic:
     s = i + j + k + h
     if crc == (binascii.crc32(s.encode())):
      f.write(s)
      return

def CrackZip():
 for i in range(0,68):
  file = 'out'+str(i)+'.zip'
  crc = zipfile.ZipFile(file,'r').getinfo('data.txt').CRC
  CrackCrc(crc)
  print('\r'+"loading: {:%}".format(float((i+1)/68)),end='')

dic = string.ascii_letters + string.digits + '+/='
f = open('out.txt','w')
print("\nCRC32begin")
CrackZip()
print("CRC32finished")
f.close()
```

得到所有压缩包的`data.txt`中的内容。并拼接在一起

```
z5BzAAANAAAAAAAAAKo+egCAIwBJAAAAVAAAAAKGNKv+a2MdSR0zAwABAAAAQ01UCRUUy91BT5UkSNPoj5hFEVFBRvefHSBCfG0ruGnKnygsMyj8
SBaZHxsYHY84LEZ24cXtZ01y3k1K1YJ0vpK9HwqUzb6u9z8igEr3dCCQLQAdAAAAHQAAAAJi0efVT2MdSR0wCAAgAAAAZmxhZy50eHQAsDRpZmZp
eCB0aGUgZmlsZSBhbmQgZ2V0IHRoZSBmbGFnxD17AEAHAA==
```

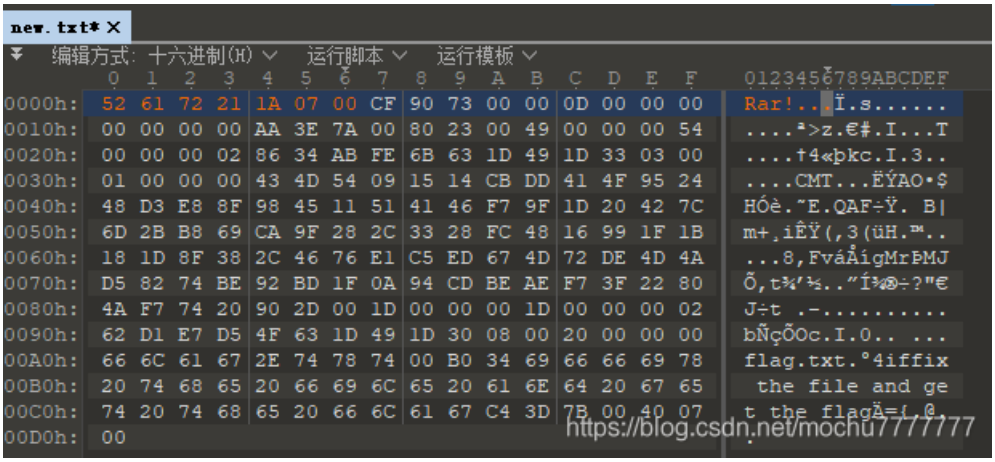
使用这个网站在线解密base64：https://the-x.cn/base64

发现base64解出来貌似是字节流数据，而且结尾是`RAR`文件的结尾，使用脚本将base64解码并以字节流的形式写入一个新的文件

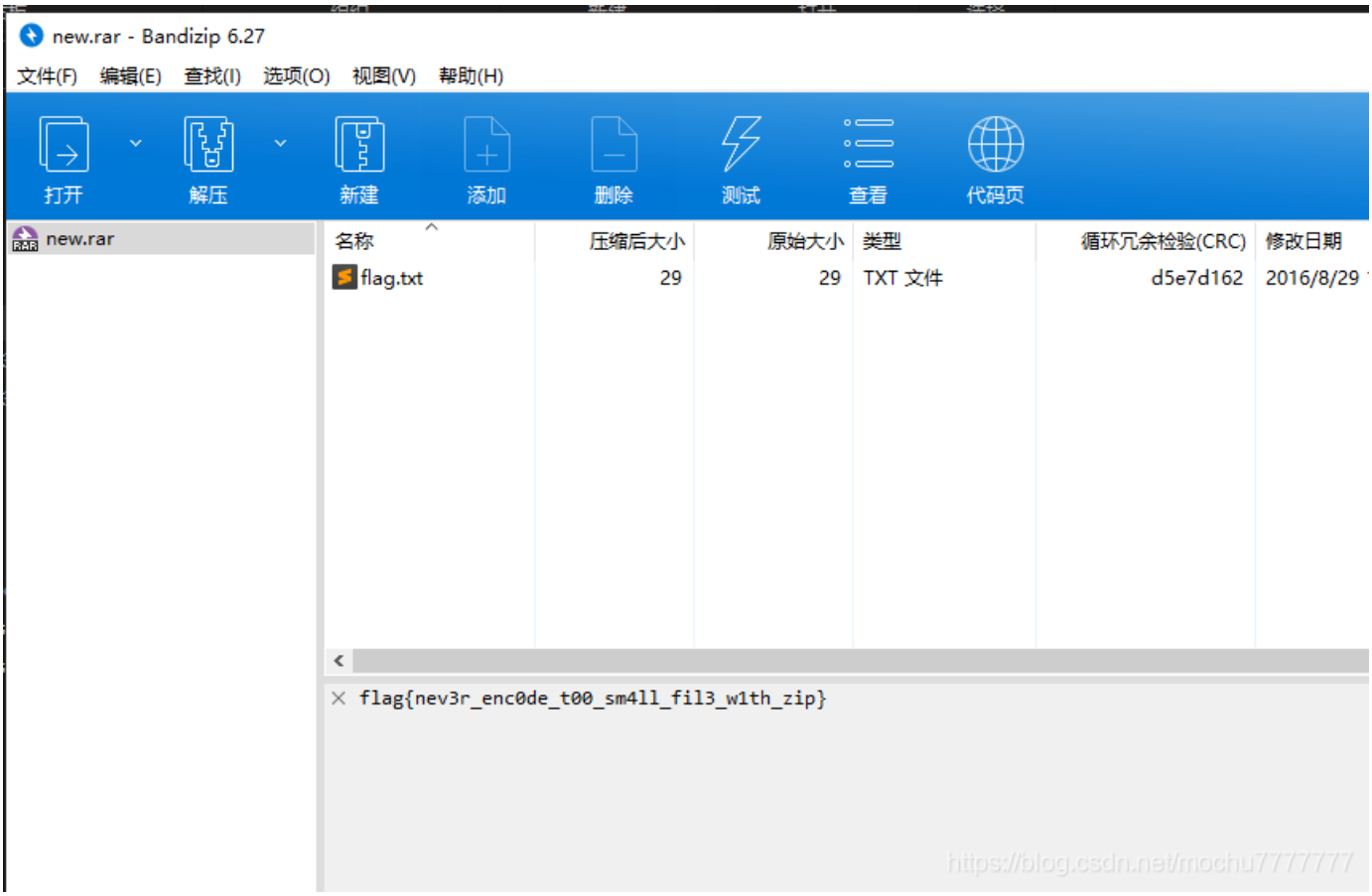
```
import base64

base64_text = open('out.txt','r').read()
byte_stream = base64.b64decode(base64_text)
open('new.txt','wb').write(byte_stream)
```

使用`010 Editor`打开，添加一个`RAR`文件的头部

```
52 61 72 21 1A 07 00
```



保存，修改后缀为`rar`



在注释中发现flag

```
flag{nev3r_enc0de_t00_sm4ll_fil3_w1th_zip}
```