Bugku - 好多压缩包 - Writeup

转载

baikeng3674 于 2017-06-06 13:53:00 发布 124 收藏
原文链接：http://www.cnblogs.com/WangAoBo/p/6951160.html

bugku - 好多压缩包 - Writeup

> M4x原创，转载请注明出处

> 这道题前前后后做了好几天，这里记录一下

题目

文件下载

分析

- 解压下载后的文件，发现有68个压缩文件，并且每个压缩文件里都有一个**4个字节大小**的名为**data.txt**的txt文件，于是尝试用**crc32碰撞**还原出所有压缩包中的文件内容

脚本如下：

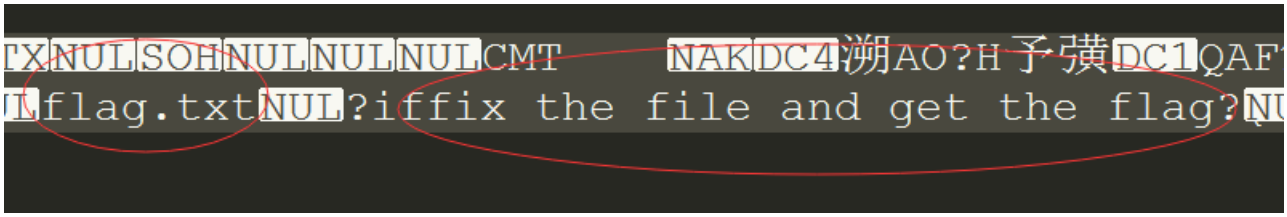
```python
#coding:utf-8
import zipfile
import string
import binascii

def CrackCrc(crc):
    for i in dic:
        for j in dic:
            for p in dic:
                for q in dic:
                    s = i + j + p + q
                    if crc == (binascii.crc32(s) & 0xffffffff):
                        #print s
                        f.write(s)
                        return

def CrackZip():
    for I in range(68):
        file = 'out' + str(I) + '.zip'
        f = zipfile.ZipFile(file, 'r')
        GetCrc = f.getinfo('data.txt')
        crc = GetCrc.CRC
        #以上3行为获取压缩包CRC32值的步骤
        #print hex(crc)
        CrackCrc(crc)

dic = string.ascii_letters + string.digits + '+/='

f = open('out.txt', 'w')
CrackZip()
f.close()
```

脚本运行时间较长

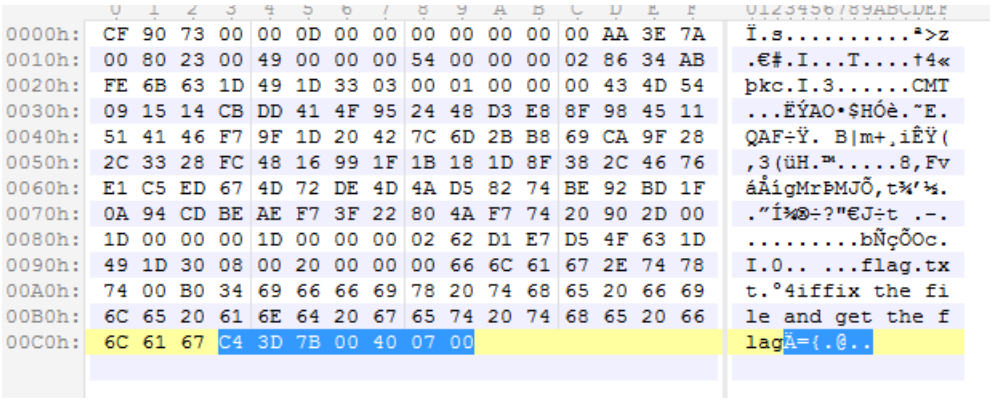
> CRC32碰撞的原理请翻到这篇文章的0x06部分

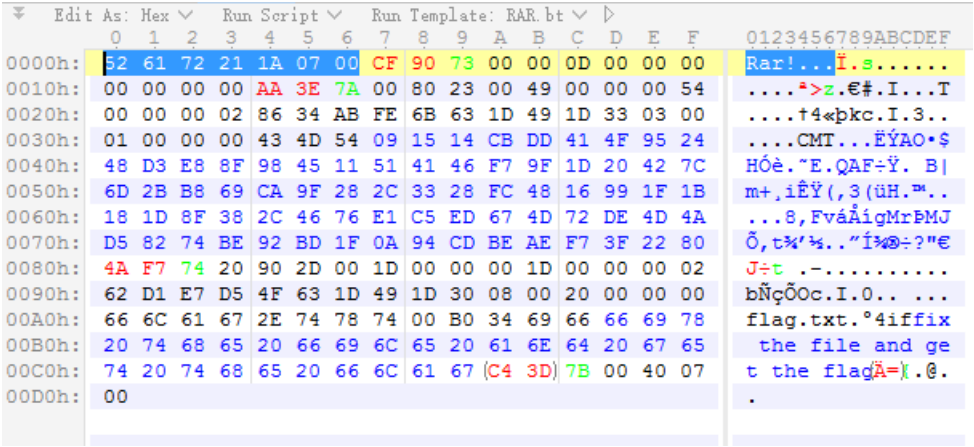
步骤

根据碰撞出内容的格式（末尾两个==）推断这段数据是base64编码过的，先解码，根据解码结果中的flag.txt推断这可能是一个压缩包，同时根据*fix the file and get the flag*知需要修复文件

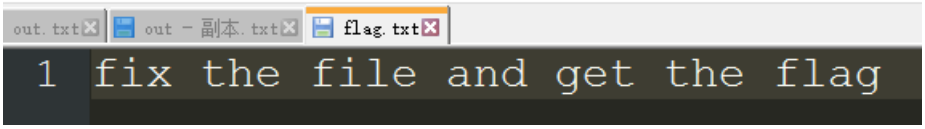


将解码后的文件导入16进制编辑器（如010editor），观察数据，发现存在rar的文件尾**C43D7B00400700**，但缺少文件头，于是补上rar的文件头**526172211A0700**。

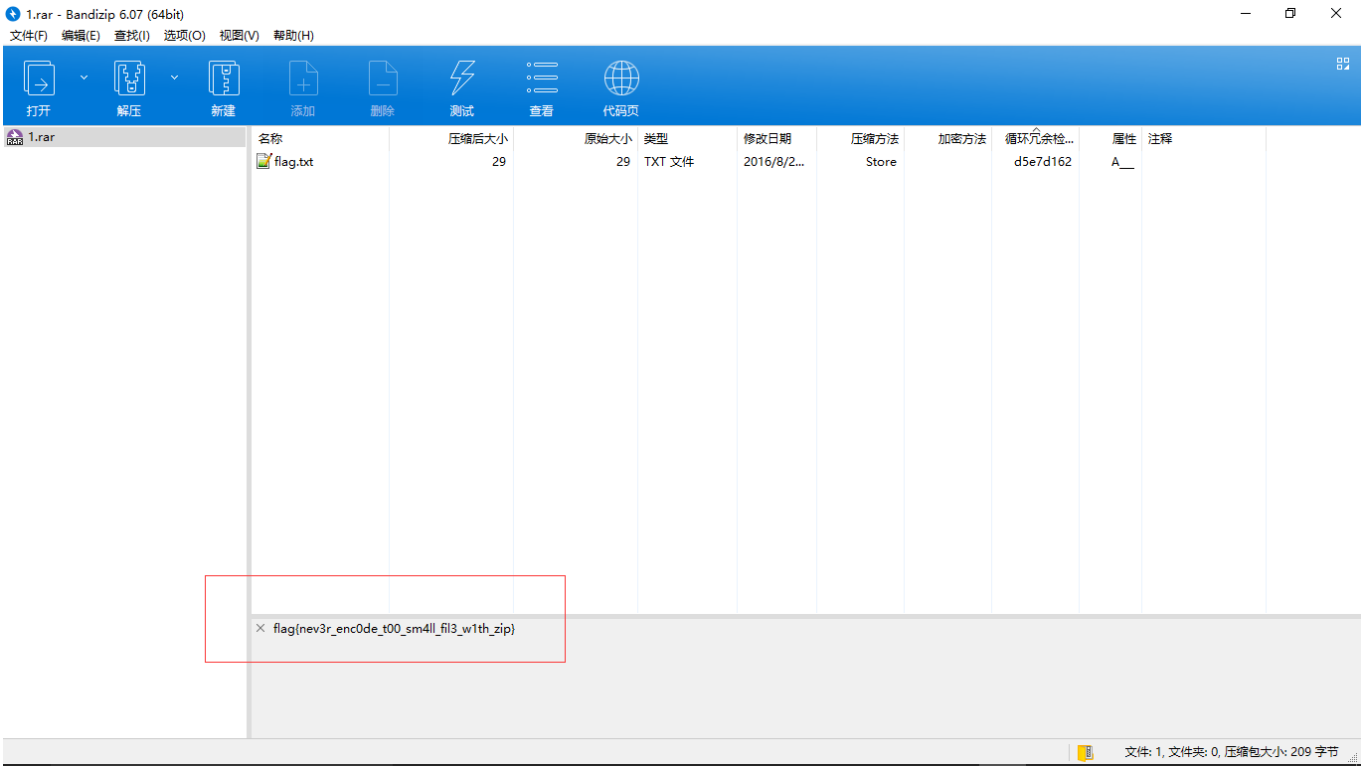




另存为rar格式，发现文件修复成功，解压后发现一个txt文档如下

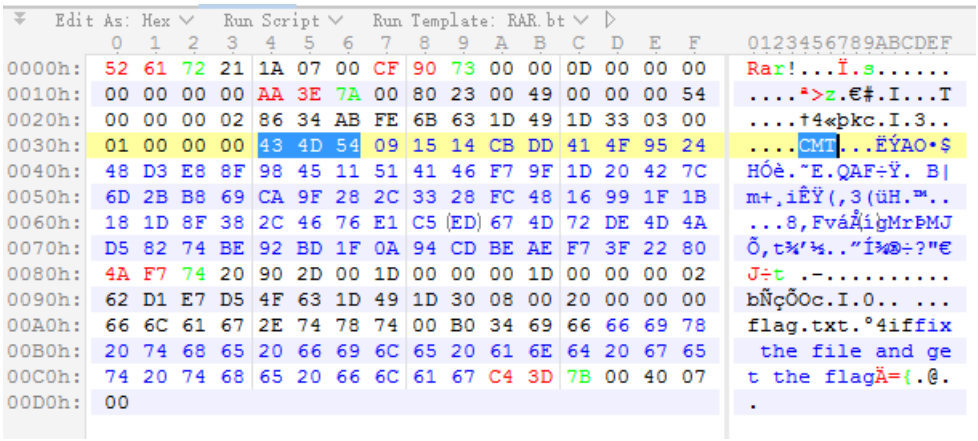


文件已经修复但还没发现flag，仔细寻找，在注释里找到了flag



于是flag即为**flag{nev3r_enc0de_t00*sm4ll_fil3*w1th_zip}**

后来经大神提示，根据rar的文件结构可以看出还存在一个名为CMT的文件，CMT即为comment，即为注释



转载于:https://www.cnblogs.com/WangAoBo/p/6951160.html