

BUUCTF misc zip

原创

[Warning](#) 于 2019-10-05 10:35:10 发布 2895 收藏 6

分类专栏: [杂项](#)

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/destiny1507/article/details/102133268>

版权



[杂项 专栏收录该内容](#)

15 篇文章 1 订阅

订阅专栏

这道题跟之前在bugku上做的“好多压缩包”是一样的, 但当时做并没有好好理解, 现在再总结一下。

涉及到的知识点:

- CRC校验爆破
- rar文件头尾的熟悉
- notepad++插件的使用

首先解压发现题目给了68个压缩包.....68个, 提示的是:



拼在一起解下base64就有flag
提交

好吧, 那我们就看看压缩包里是什么, 然后发现压缩包有密码, 无法解压, 用winhex查看后发现也并不是伪加密, 而文中也没有关于压缩包密码的提示。

关于加密的zip压缩包, 一般有以下几种情况(后续会慢慢补充):

- 伪加密, 用winhex查看全局加密标志和局部加密标志
- 弱密码, 题目中会有提示或者给出字典, 直接爆破
- zip + 图片, 一般是隐写题目, 从图片中找出密码
- CRC32爆破, 一般用于压缩包里文件内容较短时

查看压缩包里的文件, 发现只有4个字节, 考虑CRC32校验爆破

名称	压缩后大小	原始大小	类型	修改日期	循环冗余检验(CRC)	注释
data.txt*	18	4	文本文档	2016/8/2...	75f90d3a	

CRC32校验爆破原理说明:

CRC32:CRC本身是“冗余校验码”的意思, CRC32则表示会产生一个32bit(8位十六进制数)的校验值。

在产生CRC32时，源数据块的每一位都参与了运算，因此即使数据块中只有一位发生改变也会得到不同的CRC32值，利用这个原理我们可以直接爆破出加密文件的内容。

爆破脚本如下（来自网上的大牛）：

```
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()
```

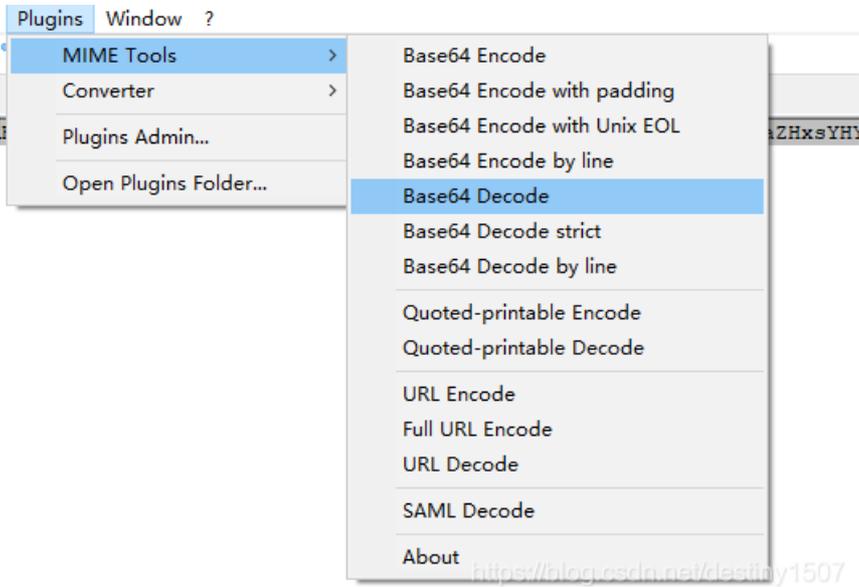
然后我们发现得到了一串base64编码的字符串：



The screenshot shows a Notepad window titled 'out.txt - 记事本'. The text content is a long base64 encoded string: z5BzAAAANAAAAAANKo+egCAIwBJAAAAVAAAAKGNKv+a2MdSR0zAwABAAAAQ01UCRUUy91BT5UkSNPoj5hFEVFBRvefHSBCfG0ruGnKnygsMyj8SBaZHxsYHY84LEZ24cXtZ01y3k1K1YJ0vpK9HwqUzb6u9z8igEr3dCCQLQAdAAAAHQAAAAJi0efVT2MdSR0wCAAgAAAAZmxhZy50eHQAsDRpZmZpeCB0aGUgZmlsZSBhbmQgZ2V0IHRoZSBmbGFnxD17AEAHAA==

这里有一个知识点，如果在线base64解码之后再复制，会出现误差，如果用脚本进行解码，总是会多一个字节。（我就是卡在这里卡了好久.....）

后来百度知道notepad++有一个解码的插件，解码后直接保存就不会有问题了：



发现文件内容中能看清的：有一个flag.txt和一段话

UP NUL STX x86: xAB xFB kc CSI GS 3 ETX NUL SOP NUL NUL NUL CMT NUL CC4 xCB xDD x0 x95 x8D3 # xF0C1 QAF xF7 x9B GS B|m+ xB8 iL(,3
 TX xD1 xE7 xD9 Oc CSI GS 0 BS NUL NUL NUL NUL flag.txt NUL xB0 4iffix the file and get the flag: C4={NUL@BS NUL

提示我们接下来需要修复文件，用winhex打开，发现了rar文件的文件尾，但是没有文件头，加上之后修改文件后缀，在注释里就可以看到flag;

名称	大小	压缩后大小	类型	修改时间	CRC32	
..			文件夹			
flag.txt	29	29	文本文档	2016/8/29 12...	D5E7D1...	flag{nev3r_enc0de_t00_sm4ll_fil3_wlth_zip}

文件头：526172211A0700

文件尾：C43D7B00400700