【BugKu-CTF论坛writeup(杂项)】好多压缩包

原创

Kingyo12 于 2018-03-15 22:19:33 发布 1718 收藏
分类专栏： BugKu-CTF论坛writeup(杂项)

本文链接：https://blog.csdn.net/preserphy/article/details/79473094

excuse me???68个压缩包

out62.zip
out63.zip
out64.zip
out65.zip
out66.zip
out67.zip

而且每个里面都有一个名为data的txt文件。那么我们需要写脚本解压。（根据CRC碰撞原理）（代码是借鉴自网上大神的，我一个python小白没写出来...）

```
#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):
                        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
        CrackCrc(crc)

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

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

这个脚本运行时间，请给我一首歌的时间。

最后得到一个输出文件内容如下

z5BzAAANAAAAAAAAAAKo+egCAIwBJAAAAVAAAAAKGNKv
+a2MdSR0zAwABAAAAQ01UCRUUy91BT5UkSNPoj5hFEVFBRvefHSBCfG0ruGnKnygsMyj8SBaZHxsYHY84LEZ24cXtZ01y3k1K1YJ0vp
K9HwqUzb6u9z8igEr3dCCQLQAdAAAAHQAAAAJi0efVT2MdSR0wCAAgAAAAZmxhZy50eHQAsDRpZmZpeCB0aGUgZmlsZSBhbmQgZ2V0I
HRoZSBmbGFnxD17AEAHAA==

使用NotePad++自带的插件来进行BASE64解码

```
LSOHNULNULNULCMT NAKDC4xCBxDDAOx95$HxD3菘EDC1QAFxF7x9FGS B|m+xB8iL(,3(xFCHSYNx
LNULflag.txtNULxB04iffix the file and get the flagxC4={NUL@BELNUL
```

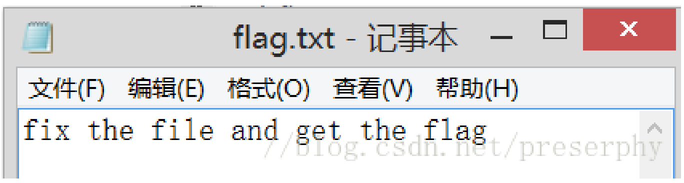

发现里面有flag字样，而且给了提示说是如果能修复这个文件就可以得到flag。保存一下文件。

那我们就试着来修复一下，将刚刚保存的文件用HxD打开，观察一下

```
Offset(h) 00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F

00000000  CF 90 73 00 00 0D 00 00 00 00 00 00 00 AA 3E 7A  Ï.s..........ª>z
00000010  00 80 23 00 49 00 00 00 54 00 00 00 02 86 34 AB  .€#.I...T....†4«
00000020  FE 6B 63 1D 49 1D 33 03 00 01 00 00 00 43 4D 54  þkc.I.3......CMT
00000030  09 15 14 CB DD 41 4F 95 24 48 D3 E8 8F 98 45 11  ...ËÝAO•$HÓè.˜E.
00000040  51 41 46 F7 9F 1D 20 42 7C 6D 2B B8 69 CA 9F 28  QAF÷Ÿ. B|m+¸iÊŸ(
00000050  2C 33 28 FC 48 16 99 1F 1B 18 1D 8F 38 2C 46 76  ,3(üH.™.....8,Fv
00000060  E1 C5 ED 67 4D 72 DE 4D 4A D5 82 74 BE 92 BD 1F  áÅígMrÞMJÕ‚t¾'½.
00000070  0A 94 CD BE AE F7 3F 22 80 4A F7 74 20 90 2D 00  ."Í¾®÷?"€J÷t .-.
00000080  1D 00 00 00 1D 00 00 00 02 62 D1 E7 D5 4F 63 1D  .........bÑçÕOc.
00000090  49 1D 30 08 00 20 00 00 00 66 6C 61 67 2E 74 78  I.0.. ...flag.tx
000000A0  74 00 B0 34 69 66 66 69 78 20 74 68 65 20 66 69  t.°4iffix the fi
000000B0  6C 65 20 61 6E 64 20 67 65 74 20 74 68 65 20 66  le and get the f
000000C0  6C 61 67 C4 3D 7B 00 40 07 00                    lagÄ={.@..
```


对照十六进制文件头尾格式我们可以发现这是一个rar文件，因为有RAR文件的结尾标志C43D7B00400700，那么我们给它加上标志头526172211A0700。保存一下。改文件后缀，解压。得到一个flag.txt文件

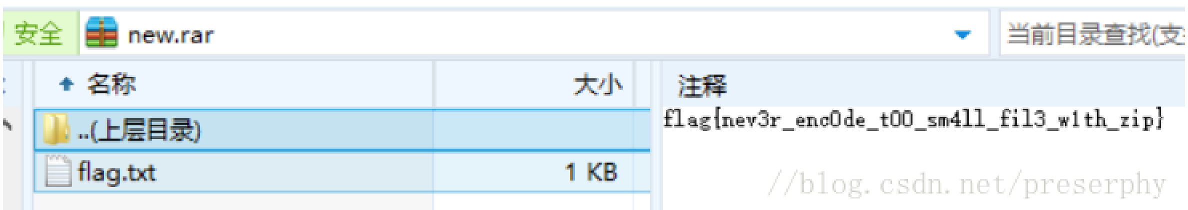


emmmm……flag不在这里。又看了txt和rar的属性，但是还是没有找到flag。

在这里卡了好久……明天再搞……

==

不得不佩服出题人想为难我们的脑洞，因为今天用电脑一起看文件的时候，被同学无意中双击了一下之前那个修复好了的rar文件，蹦出来了压缩软件的窗口——



行吧，我找到flag了，它就在rar文件的注释里面呵呵呵呵呵。