

BUUCTF: 九连环

原创

末初 于 2020-09-23 15:03:06 发布 2079 收藏 3

分类专栏: [CTF_MISC_Writeup](#)

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/mochu777777/article/details/108752016>

版权



[CTF_MISC_Writeup](#) 专栏收录该内容

246 篇文章 45 订阅

订阅专栏

题目地址: <https://buuoj.cn/challenges#%E4%B9%9D%E8%BF%9E%E7%8E%AF>



题目如下:

留下了委屈的泪水



<https://blog.csdn.net/mochu777777>

binwalk 分析, foremost 分离

```
m0c1nu7@Seanz7:/mnt/c/Users/Administrator$ cd Downloads/  
m0c1nu7@Seanz7:/mnt/c/Users/Administrator/Downloads$ ls  
123456cry.jpg 389a0c11-d0df-4180-829a-b529e6b0a1bc.zip desktop.ini  
m0c1nu7@Seanz7:/mnt/c/Users/Administrator/Downloads$ binwalk 123456cry.jpg
```

```

DECIMAL      HEXADECIMAL    DESCRIPTION
-----
0            0x0           JPEG image data, JFIF standard 1.01
19560       0x4C68       Zip archive data, at least v1.0 to extract, name: asd/
48454       0xB0D46     Zip archive data, at least v1.0 to extract, compressed size: 184, uncompressed size: 184, name: asd/qwe.zip
48657       0xBE11      End of Zip archive, footer length: 22
48962       0xBF42      End of Zip archive, footer length: 22

m0c1nu7@Seanz7:/mnt/c/Users/Administrator/Downloads$ foremost 123456cry.jpg
Processing: 123456cry.jpg
|foundat=asd/PK0000
foundat=asd/good-已合并.jpg  <aa6*****WF0
rfe!I*!T*QR*W*++[**LQI**B* >*"KVf!}*2nf*0**}*{**}*+*****3**u**u**q**u**+1**+D.Z*X*XX@ 0*/+10**+*****N*****h      r*****000da0dat* *q**00
foundat=asd/qwe.zipPK00

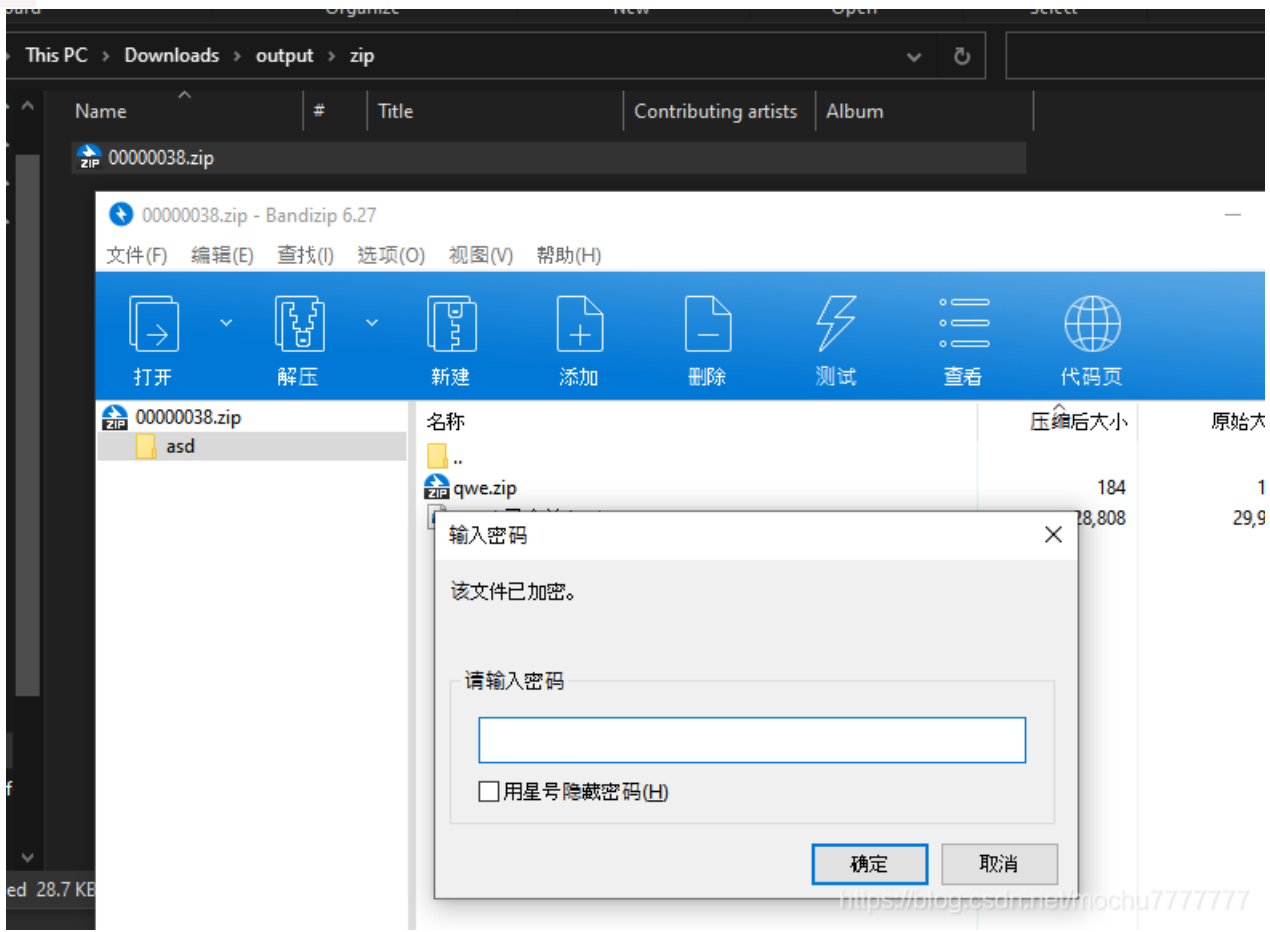
*|
m0c1nu7@Seanz7:/mnt/c/Users/Administrator/Downloads$ ls
123456cry.jpg  389a0c11-d0df-4180-829a-b529e6b0a1bc.zip  desktop.ini  00000038.zip
m0c1nu7@Seanz7:/mnt/c/Users/Administrator/Downloads$
m0c1nu7@Seanz7:/mnt/c/Users/Administrator/Downloads$ tree output/
.
├── audit.txt
├── jpg
├── zip
├── 00000000.jpg
└── 00000038.zip

2 directories, 3 files
m0c1nu7@Seanz7:/mnt/c/Users/Administrator/Downloads$

```

<https://blog.csdn.net/mochu777777>

zip伪加密

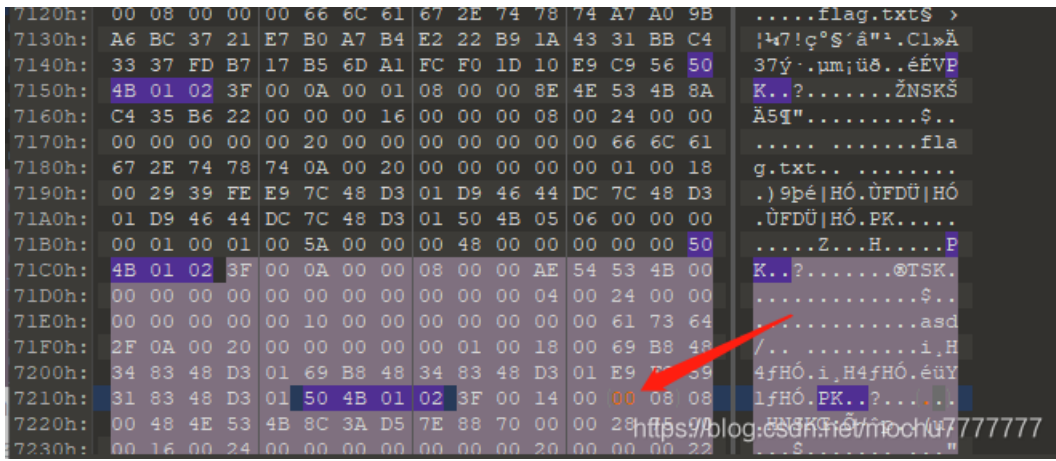


<https://blog.csdn.net/mochu777777>

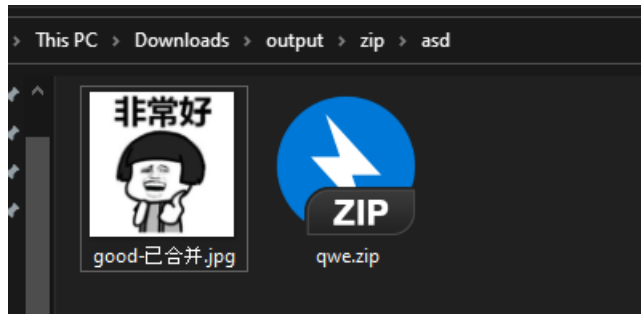
```

起始页 00000038 - Copy.zip* x
编辑方式: 十六进制(H) 运行脚本 运行模板: ZIP.bt
0 1 2 3 4 5 6 7 8 9 A B C D E F 0123456789ABCDEF
7060h: A3 C1 BA 4D A1 2A 54 6D 76 5C 01 39 EE AA 42 ED EÁ*Mj;*Tmv\.9i*Bí
7070h: 41 F5 81 DC 15 0B 05 70 76 5D 86 9B 61 F2 E1 E5 Aõ.Ü...pvj]t>adáá
7080h: F6 5D 48 C6 1B 95 84 0F E5 87 EF A1 3F AF 70 74 ö]HÆ..,..â+i;?_pt
7090h: E2 88 97 D3 27 F8 ED C7 9D C9 B6 80 33 E5 8C 7E á~ó'øiC.Éq€3á@~
70A0h: 8A 34 16 4D AC AC CB 7C D7 98 28 D5 51 57 D5 F0 Š4.M~E|*~(ÖQWÖð
70B0h: A5 D7 CB FD 6C FC 37 81 67 23 D1 32 59 0F 33 B0 Ÿ*Éýlü7.g#Ñ2Y.3°
70C0h: A7 78 22 71 B5 D1 FD 60 24 03 34 56 7F 5C C5 F0 Sx"quÑÿ`¢.4V.\\Áð
70D0h: DB 4A 0A B2 5E FD BF 5D BB 40 31 26 FE 5F 50 4B ŪJ.^`ýç]»@l&p_PK
70E0h: 03 04 0A 00 00 08 00 00 F1 52 53 4B D3 13 C6 E0 .....ñRSKÖ.Èà
70F0h: B8 00 00 00 B8 00 00 00 0B 00 00 00 61 73 64 2E .....asd/
7100h: 71 77 65 2E 7A 69 70 50 4B 03 04 0A 00 01 08 00 qwe.zipPK.....
7110h: 00 8E 4E 53 4B 8A C4 35 B6 22 00 00 00 16 00 00 .ZNSKŠA5Ÿ".....

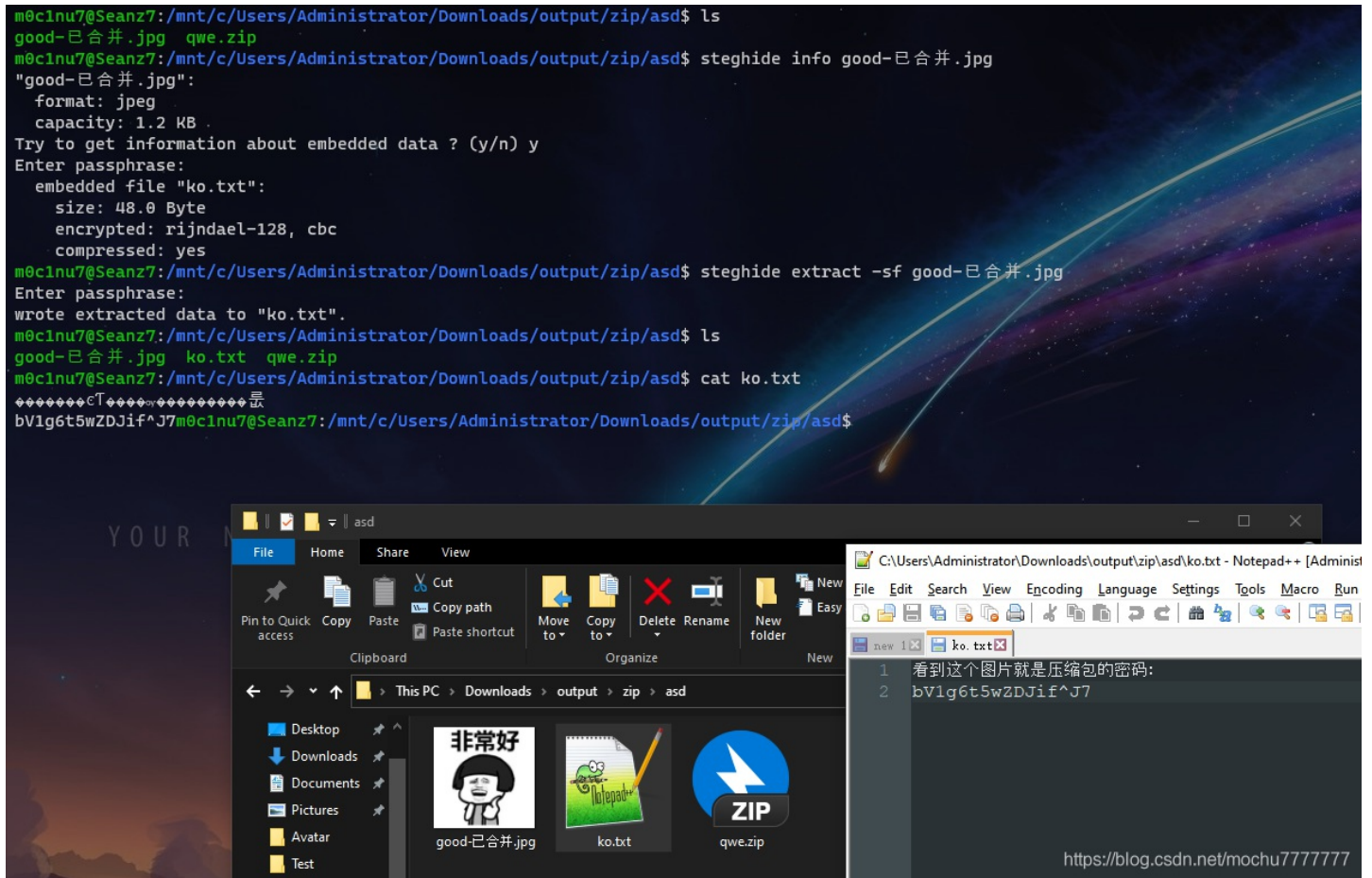
```



解压得到



使用 `steghide` 发现图片有隐写文件，使用 `steghide extract -sf good.jpg`，空密码即可



使用解密密码解压 `qwe.zip` 即可得到flag

`flag{1RTo8w@&4nK@z*XL}`