

# BUUCTF：九连环

原创

未初 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://buujoj.cn/challenges#%E4%B9%9D%E8%BF%9E%E7%8E%AF>

Challenge 876 Solves ×

## 九连环

1

注意：得到的 flag 请包上 flag{} 提交

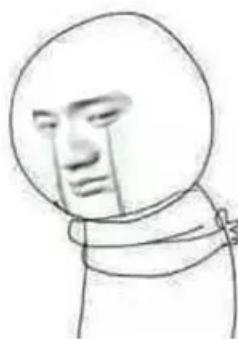
389a0c11-d...

Flag Submit

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

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
```

```

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        0xBD46        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

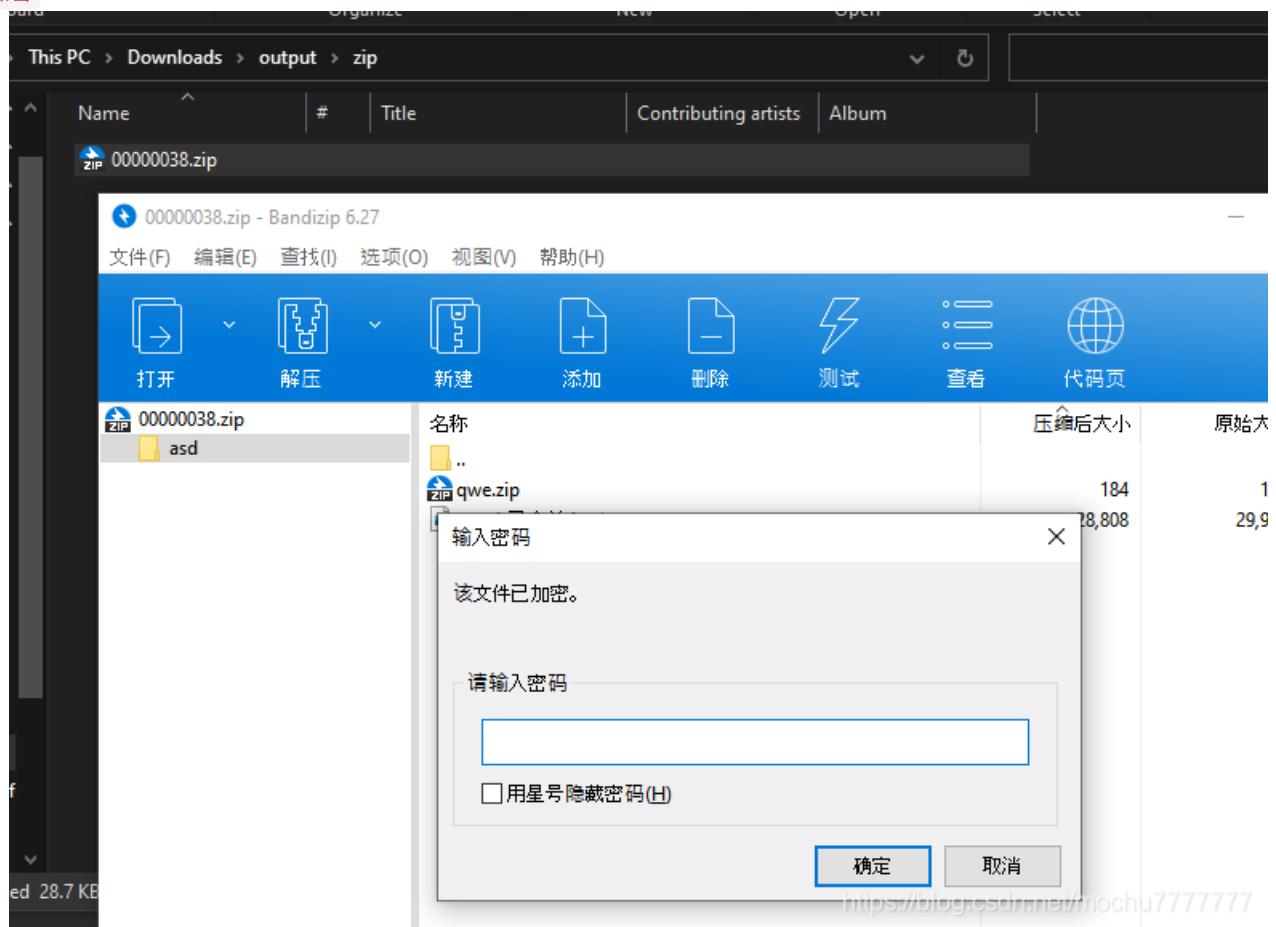
m0c1nu7@Seanz7:/mnt/c/Users/Administrator/Downloads$ foremost 123456cry.jpg
Processing: 123456cry.jpg
|foundat=asd/PK0000
foundat=asd/good-已合并.jpg<+a+6++++WF0
rfelI*!+T+DR+We++[+LQI+B>+"Kvf!}+2nf+0++}++{++}++++3++u_+u+q0+u++1+++.Z+X+XX@+10:+++++ON++++h      ++++++00da0dat+ +q+000
foundat=asd/qwe.zipPK00

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

2 directories, 3 files
m0c1nu7@Seanz7:/mnt/c/Users/Administrator/Downloads$ |
https://blog.csdn.net/mochu7777777

```

### zip伪加密



<https://blog.csdn.net/mochu7777777>

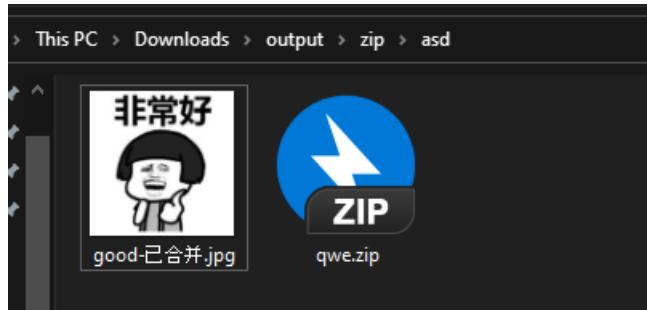
起始页 00000038 - Copy.zip*																	
编辑方式: 十六进制(H) 运行脚本(V) 运行模板: ZIP.bt D																	
0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F		
7060h:	A3	C1	BA	4D	A1	2A	54	6D	76	5C	01	39	EE	AA	42	ED	0123456789ABCDE
7070h:	41	F5	81	DC	15	0B	05	70	76	5D	86	9B	61	F2	E1	E5	£Á°M;*Tmv\.9i^Bi
7080h:	F6	5D	48	C6	1B	95	84	0F	E5	87	EF	A1	3F	AF	70	74	Aõ.Ü...pv]†>aòáå
7090h:	E2	88	97	D3	27	F8	ED	C7	9D	C9	B6	80	33	E5	8C	7E	ö]HE.*..å†i;?_pt
70A0h:	8A	34	16	4D	AC	AC	CB	7C	D7	98	28	D5	51	57	D5	F0	å^—Ó'øiÇ.Éø€3åç~
70B0h:	A5	D7	CB	FD	6C	FC	37	81	67	23	D1	32	59	0F	33	B0	Š4.M--È x~"(ÖQWÖš
70C0h:	A7	78	22	71	B5	D1	FD	60	24	03	34	56	7F	5C	C5	F0	¥×ëýlú7.g#Ñ2Y.3°
70D0h:	DB	4A	0A	B2	5E	FD	BF	5D	BB	40	31	26	FE	F5	50	4B	Sx"quÑý \$.4V.\Åø
70E0h:	03	04	0A	00	00	08	00	00	F1	52	53	4B	D3	13	C6	E0	ÛJ.^^ý]»@l&p_PK
70F0h:	B8	00	00	00	B8	00	00	00	OB	00	00	00	61	73	64	2F	.....ñRSKÓ.Eà
7100h:	71	77	65	2E	7A	69	70	50	4B	03	04	0A	00	01	08	00	.....asd/
7110h:	00	08	4E	53	4B	8A	C4	35	B6	22	00	00	00	16	00	00	.ŽNSKŠÄ5¶".....

```

7120h: 00 08 00 00 00 66 6C 61 67 2E 74 78 74 A7 A0 9B ....flag.txt$ >
7130h: A6 BC 37 21 E7 B0 A7 B4 E2 22 B9 1A 43 31 BB C4 !47!ç°$'â"1.Cl»À
7140h: 33 37 FD B7 17 B5 6D A1 FC F0 1D 10 E9 C9 56 50 37ý..µm;üð..éÉVP
7150h: 4B 01 02 3F 00 0A 00 01 08 00 00 8E 4E 53 4B 8A K?.....žNSKŠ
7160h: C4 35 B6 22 00 00 00 16 00 00 00 08 00 24 00 00 Ä5Í".....$...
7170h: 00 00 00 00 00 20 00 00 00 00 00 00 00 00 66 6C 61 .....fla
7180h: 67 2E 74 78 74 0A 00 20 00 00 00 00 00 00 00 01 00 18 g.txt...
7190h: 00 29 39 FE E9 7C 48 D3 01 D9 46 44 DC 7C 48 D3 .)gpé|HÓ.ÜFDÜ|HÓ
71A0h: 01 D9 46 44 DC 7C 48 D3 01 50 4B 05 06 00 00 00 .ÜFDÜ|HÓ.PK...
71B0h: 00 01 00 01 00 5A 00 00 00 48 00 00 00 00 00 50 .....Z...H....P
71C0h: 4B 01 02 3F 00 0A 00 00 08 00 00 AE 54 53 4B 00 K.?.....@TSK.
71D0h: 00 00 00 00 00 00 00 00 00 00 04 00 24 00 00 .....$...
71E0h: 00 00 00 00 00 10 00 00 00 00 00 00 00 00 61 73 64 .....asd
71F0h: 2F 0A 00 20 00 00 00 00 00 01 00 18 00 69 B8 48 /...i,H
7200h: 34 83 48 D3 01 69 B8 48 34 83 48 D3 01 E9 70 39 4fHÓ.i,H4fHÓ.éÜY
7210h: 31 83 48 D3 01 50 4B 01 02 3F 00 14 00 00 08 08 lfHÓ.PK.?...
7220h: 00 48 4E 53 4B 8C 3A D5 7E 88 70 00 00 28 15 00 HSKŠ.žñp...u7
7230h: 00 16 00 24 00 00 00 00 00 00 00 20 00 00 00 22 S

```

解压得到

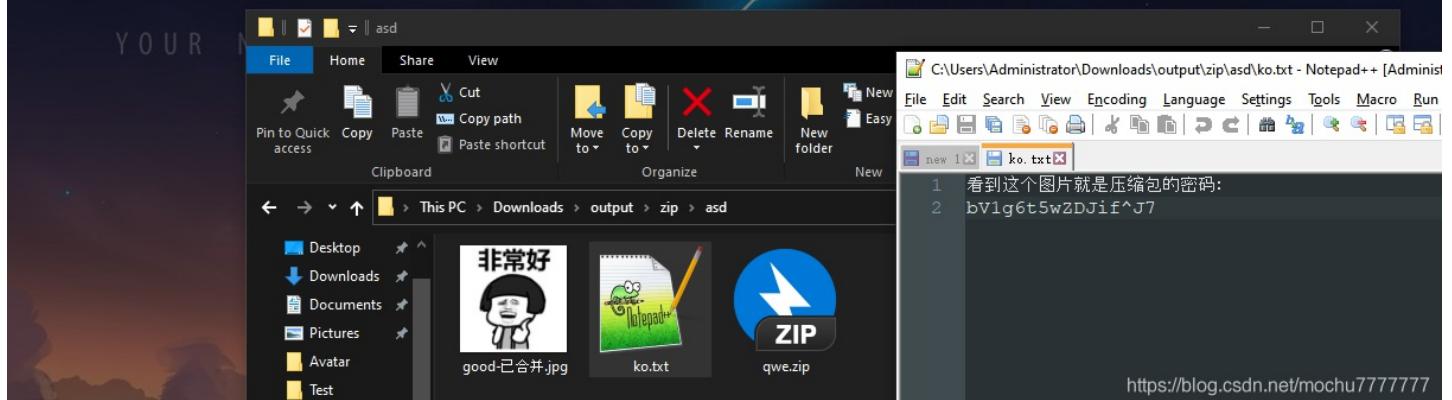


使用 `steghide` 发现图片有隐写文件，使用 `steghide extract -sf good.jpg`，空密码即可

```

m0c1nu7@Seanz7:/mnt/c/Users/Administrator/Downloads/output/zip/asd$ ls
good-已合并.jpg qwe.zip
m0c1nu7@Seanz7:/mnt/c/Users/Administrator/Downloads/output/zip/asd$ steghide info good-已合并.jpg
"good-已合并.jpg":
  format: jpeg
  capacity: 1.2 KB
Try to get information about embedded data ? (y/n) y
Enter passphrase:
embedded file "ko.txt":
  size: 48.0 Byte
  encrypted: rijndael-128, cbc
  compressed: yes
m0c1nu7@Seanz7:/mnt/c/Users/Administrator/Downloads/output/zip/asd$ steghide extract -sf good-已合并.jpg
Enter passphrase:
wrote extracted data to "ko.txt".
m0c1nu7@Seanz7:/mnt/c/Users/Administrator/Downloads/output/zip/asd$ ls
good-已合并.jpg ko.txt qwe.zip
m0c1nu7@Seanz7:/mnt/c/Users/Administrator/Downloads/output/zip/asd$ cat ko.txt
oooooooooooooCoooooooooooooo
bV1g6t5wZDJif^J7m0c1nu7@Seanz7:/mnt/c/Users/Administrator/Downloads/output/zip/asd$

```



使用解压密码解压 `qwe.zip` 即可得到flag

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