




# 2020 第三届安洵杯 MISC Writeup

原创

末初  于 2020-11-26 01:05:04 发布  3599  收藏 6

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/110151315>

版权



[CTF\\_MISC\\_Writeup](#) 专栏收录该内容

246 篇文章 46 订阅

订阅专栏

## 题目名称

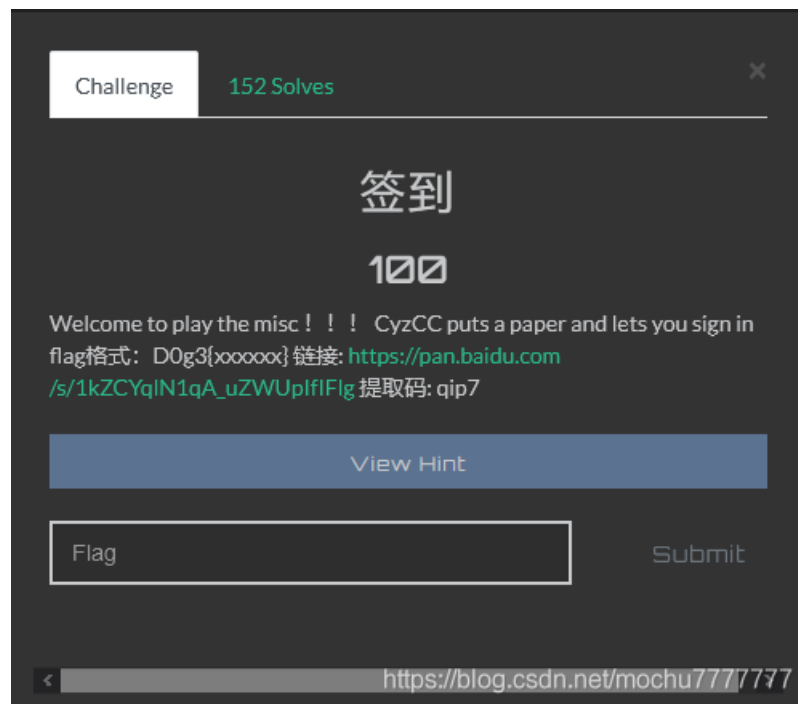
签到

王牌特工

套娃

BeCare4

## 签到



Hint: 哥哥们注意文件名

大声说出f14g.jpg



向公众号回复: `f14g`



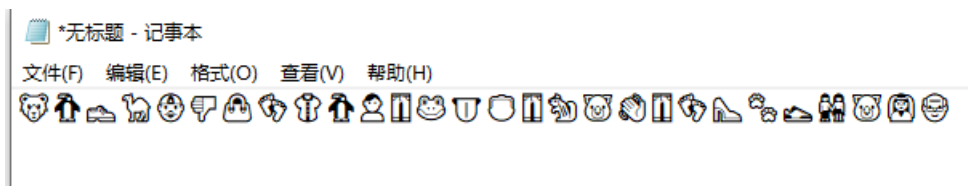
下载是 `flag.docx`

V1cuna hides the flag, try to be concentrate on getting the score from CyzCC

??


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

复制那串特殊符号到记事本



Emojiencode : <http://www.atoolbox.net/Tool.php?id=937>

# Emoji表情符号编码/解码

```
D0g3{Welc0m_AND_H1T_liGht1y}
```

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

```
D0g3{Welc0m_AND_H1T_liGht1y}
```

## 王牌特工

Challenge 64 Solves

### 王牌特工

100

Recently, Agent CyzCC has got one secret file from Trump's disk and cracked it successfully without Wushu morality. Can u do the same thing?

flag格式: flag{xxxxxx}

题目链接: <https://pan.baidu.com/s/17XnERTFyOUI9c2TFHO1FmA> 密码: 3sjq

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

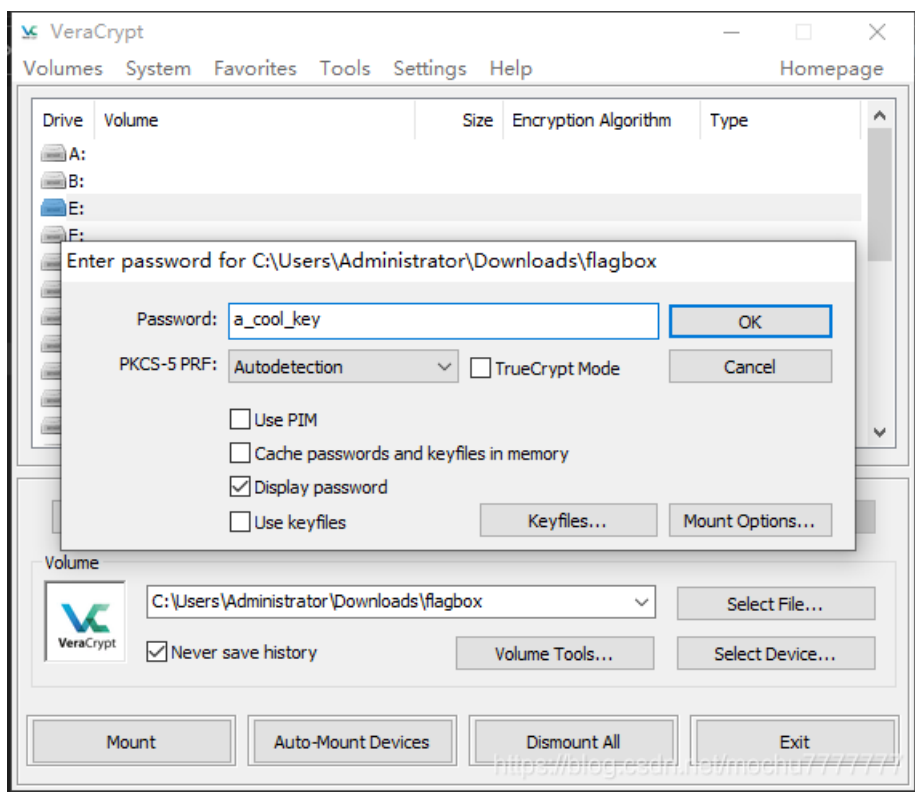
file 查看，发现是 ext3 文件系统，直接挂载

```
root@kali /home/mochu7/Desktop % ls
findme tools
root@kali /home/mochu7/Desktop % file findme
findme: Linux rev 1.0 ext3 filesystem data, UUID=f2b1e8fa-29a6-454b-b6df-6182044790bc (needs journal recovery) (large files)
root@kali /home/mochu7/Desktop % mount findme /mnt
root@kali /home/mochu7/Desktop % ls -lha /mnt
total 1.1M
drwxr-xr-x  3 root root 1.0K Nov 21 06:13 .
drwxr-xr-x 19 root root 4.0K Nov 25 05:07 ..
-rw-r--r--  1 root root 1.0M Nov 21 05:49 flagbox
-rw-r--r--  1 root root 29 Nov 21 05:49 key.txt
drwx----- 2 root root 12K Nov 21 06:09 lost+found
root@kali /home/mochu7/Desktop %
```

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

```
root@kali /mnt % ls
flagbox key.txt lost+found
root@kali /mnt % file flagbox
flagbox: data
root@kali /mnt % cat key.txt
key:a_cool_key
use Veracrypt
root@kali /mnt %
```

使用 Veracrypt 挂载 flagbox，密码：a\_cool\_key



打开挂载目录，只有一个 flag.txt



回到 `findme`，使用 `extundelete` 恢复磁盘文件

```
extundelete findme --restore-all
```

```
root@kali /home/mochu7/Desktop % ls
findme tools
root@kali /home/mochu7/Desktop % extundelete findme --restore-all
NOTICE: Extended attributes are not restored.
WARNING: EXT3_FEATURE_INCOMPAT_RECOVER is set.
The partition should be unmounted to undelete any files without further data loss.
If the partition is not currently mounted, this message indicates
it was improperly unmounted, and you should run fsck before continuing.
If you decide to continue, extundelete may overwrite some of the deleted
files and make recovering those files impossible. You should unmount the
file system and check it with fsck before using extundelete.
Would you like to continue? (y/n)
y
Loading filesystem metadata ... 2 groups loaded.
Loading journal descriptors ... 31 descriptors loaded.
Searching for recoverable inodes in directory / ...
1 recoverable inodes found.
Looking through the directory structure for deleted files ...
0 recoverable inodes still lost.
root@kali /home/mochu7/Desktop % ls
findme RECOVERED_FILES tools
root@kali /home/mochu7/Desktop % cd RECOVERED_FILES
root@kali /home/mochu7/Desktop/RECOVERED_FILES % ls
root@kali /home/mochu7/Desktop/RECOVERED_FILES % ls -lha
total 276K
drwxr-xr-x 2 root root 4.0K Nov 25 11:03 .
drwxr-xr-x 4 mochu7 mochu7 256K Nov 25 11:03 ..
-rw-r--r-- 1 root root 12K Nov 25 11:03 .coolboy.swp
root@kali /home/mochu7/Desktop/RECOVERED_FILES % file .coolboy.swp
.coolboy.swp: Vim swap file, version 8.2, pid 2046, user root, host kali, file ~root/cool/coolboy, modified
root@kali /home/mochu7/Desktop/RECOVERED_FILES %
```

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

发现个隐藏文件 `.coolboy.swp`，查看下，发现一串base64

```
root@kali /home/mochu7/Desktop/RECOVERED_FILES % ls
root@kali /home/mochu7/Desktop/RECOVERED_FILES % ls -la
total 276
drwxr-xr-x 2 root root 4096 Nov 25 11:03 .
drwxr-xr-x 4 mochu7 mochu7 262144 Nov 25 11:03 ..
-rw-r--r-- 1 root root 12288 Nov 25 11:03 .coolboy.swp
root@kali /home/mochu7/Desktop/RECOVERED_FILES % cat .coolboy.swp
U3210#! Utpad0000you find me55yf55qE5a+G56CB0nRoaxNfaXNfYV90cnVlX2tleQ==#
root@kali /home/mochu7/Desktop/RECOVERED_FILES %
```

```
55yf55qE5a+G56CB0nRoaxNfaXNfYV90cnVlX2tleQ==
```

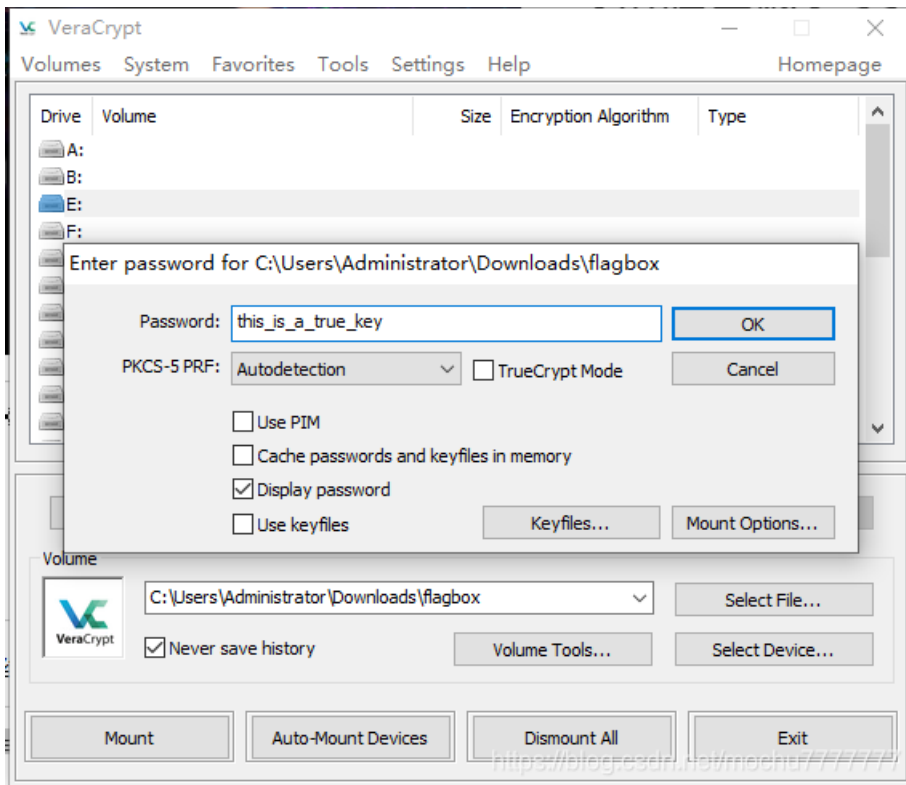
55yf55qE5a+G56CBOnRoaxNfaXNfYV90cnV1X2t1eQ==

清空 加密 解密  解密结果以16进制显示

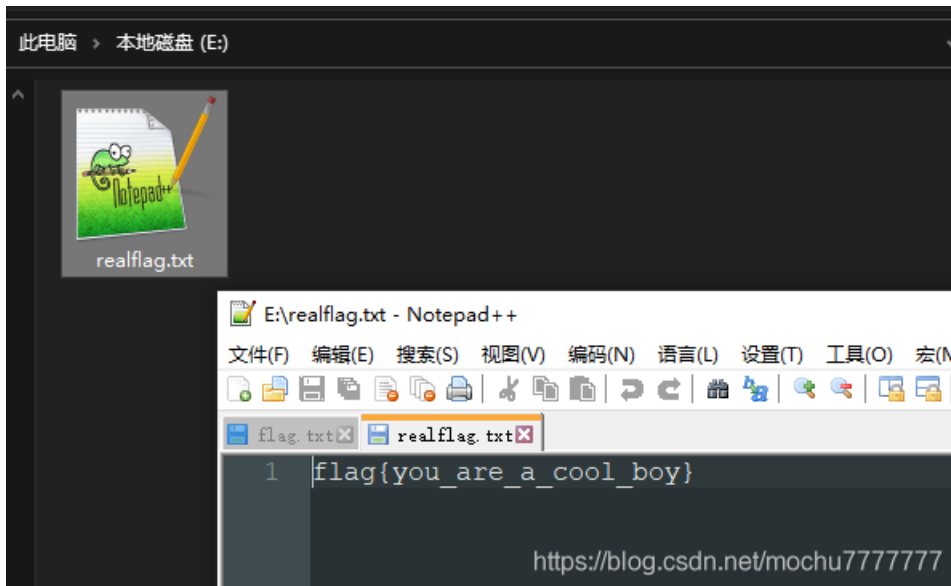
真的密码:this\_is\_a\_true\_key

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

得到真的密码，使用这个密码再去挂载 **flagbox**



再次打开挂载目录，得到真的flag



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

flag{you\_are\_a\_cool\_boy}

# 套娃

Challenge 44 Solves

## 套娃

### 100

CyzCC usually compresses his love into something locked and send it to the one who he loves. Give him love and he will give you more.

flag格式: flag{xxxxxx} 题目链接: <https://pan.baidu.com/s/1fNMtoLji9IkFFT4WCgFgLA> 提取码: faa4

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

## hardzip.zip 需要密码

名称	压缩后大小	原始大小	类型	循环冗余检验(CRC)	修改日期
password1	84	12			2020/10/19 2:48:52
easyzip.zip*	929	1,144	ZIP 压缩文件	db6a2cb0	2020/11/21 19:51:26

输入密码  
该文件已加密。  
请输入密码  
 用星号隐藏密码(H)  
确定 取消

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

## password1 目录可查看

名称	压缩后大小	原始大小	类型	循环冗余检验(CRC)	修改日期
..					
密码 - 副本 (0).txt*	14	2	TXT 文件	ea4446b6	2020/10/19 2:46:24
密码 - 副本 (1).txt*	14	2	TXT 文件	ed7987de	2020/10/19 2:46:34
密码 - 副本 (2).txt*	14	2	TXT 文件	46fe0943	2020/10/19 2:46:42
密码 - 副本 (3).txt*	14	2	TXT 文件	4be30989	2020/10/19 2:46:48
密码 - 副本 (4).txt*	14	2	TXT 文件	b31975c0	2020/10/19 2:47:00
密码 - 副本 (5).txt*	14	2	TXT 文件	d6bb1bef	2020/10/19 2:47:42

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

6个文件，全都只有 2 字节，使用 [CRC32爆破脚本](#) 爆破内容

按顺序取出每个文件的 [CRC](#)

```
0xea4446b6
0xed7987de
0x46fe0943
0x4be30989
0xb31975c0
0xd6bb1bef
```

## 编写爆破 2 字节内容Python脚本

```
#Written by: Mochu7
import binascii
import string

def crack_crc():
    crc_list = [0xea4446b6,0xed7987de,0x46fe0943,0x4be30989,0xb31975c0,0xd6bb1bef]
    chars = string.printable
    for res_crc in crc_list:
        for str_1 in chars:
            for str_2 in chars:
                comment = str_1 + str_2
                test_crc = binascii.crc32(comment.encode())
                calc_crc = test_crc & 0xffffffff
                if calc_crc == res_crc:
                    print(comment)

if __name__ == '__main__':
    crack_crc()
```

```
1  #Written by: Mochu7
2  import binascii
3  import string
4
5  def crack_crc():
6      crc_list = [0xea4446b6,0xed7987de,0x46fe0943,0x4be30989,0xb31975c0,0xd6bb1bef]
7      chars = string.printable
8      for res_crc in crc_list:
9          for str_1 in chars:
10             for str_2 in chars:
11                 comment = str_1 + str_2
12                 test_crc = binascii.crc32(comment.encode())
13                 calc_crc = test_crc & 0xffffffff
14                 if calc_crc == res_crc:
15                     print(comment)
16
17 if __name__ == '__main__':
18     crack_crc()
```

PROBLEMS 1 OUTPUT TERMINAL DEBUG CONSOLE

```
[Running] D:/Python/Python3/python.exe "c:\Users\Administrator\Downloads\code1.py"
!q
QI
dE
a@
#!
z)

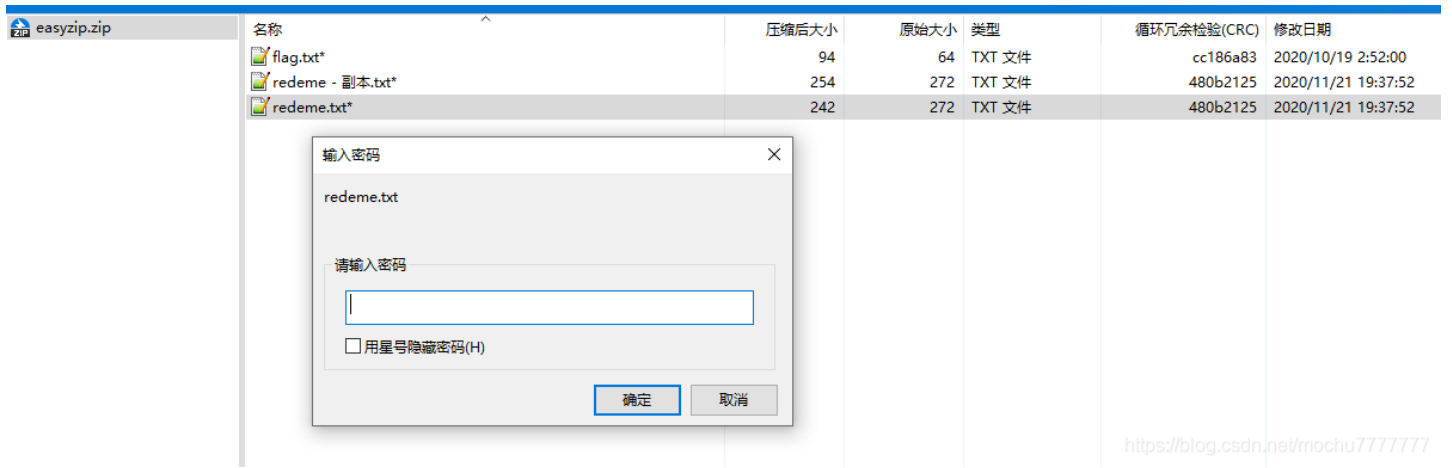
[Done] exited with code=0 in 0.098 seconds
```

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

得到 `hardzip.zip` 的密码: `!qQIdEa@#!z)`

`easyzip.zip` 有密码





7zip 可直接从 `easyzip.zip` 中解压出 `redeme.txt`，然后即可进行明文攻击，注意这里 `flag.txt` 加密方式不一样，不能放在明文攻击的目标 `zip` 中

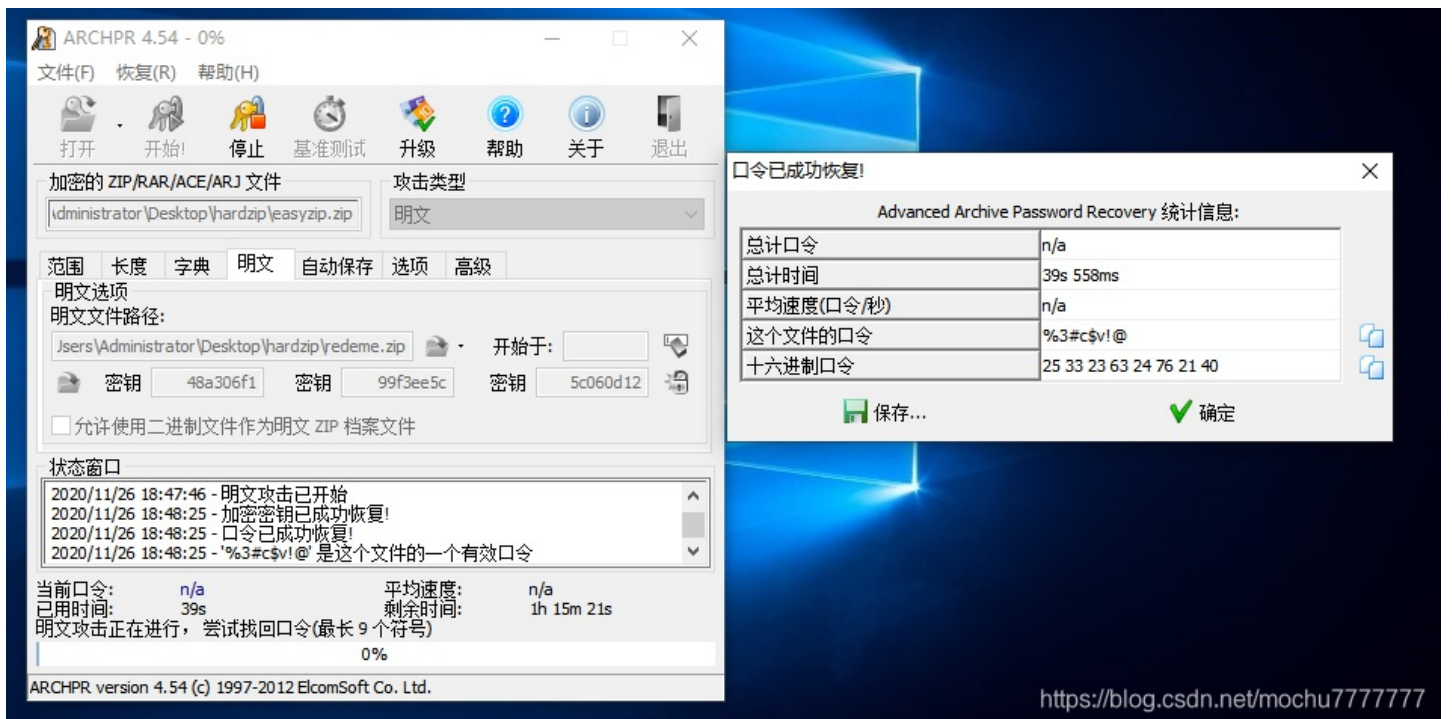
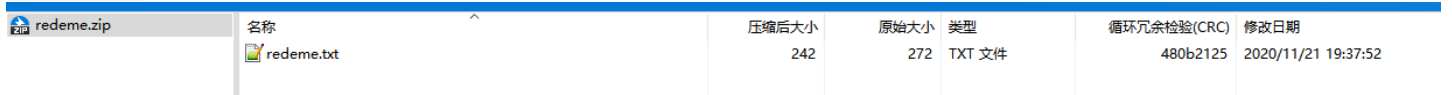


先备份一份 `easyzip.zip`，接着使用 WinRAR 打开 `easyzip.zip`，删除掉 `flag.txt` 和 `redeme.txt`，只留 `redeme-副本.txt`，然后再用 WinRAR 压缩之前解压出来的 `redeme.txt` 得到明文压缩包 `redeme.zip`

### easyzip.zip



### redeme.zip



%3#c\$v!@

使用这个密码直接解 `flag.txt`

名称	压缩后大小	原始大小	类型	循环冗余检验(CRC)	修改日期
flag.txt*	94	64	TXT 文件	cc186a83	2020/10/19 2:52:00
redeme - 副本.txt*	254	272	TXT 文件	480b2125	2020/11/21 19:37:52
redeme.txt*	242	272	TXT 文件	480b2125	2020/11/21 19:37:52

```
C:\Users\Administrator\AppData\Local\Temp\BNZ.5fbf91588fdc5e\flag.txt - Notepad++
文件(F) 编辑(E) 搜索(S) 视图(V) 编码(N) 语言(L) 设置(T) 工具(O) 宏(M) 运行(R) 插件(P) 窗口(W) ?
1 |V20xa2NGa3hPV1ppYlRrd1lraDBkMk51WkdwWU1UazVXVmhm2YlZreVZtaGFSMnhC
https://blog.csdn.net/mochu7777777
```

Base64套娃

```
V20xa2NGa3hPV1ppYlRrd1lraDBkMk51WkdwWU1UazVXVmhm2YlZreVZtaGFSMnhC
```

```
import base64

base64_code = 'V20xa2NGa3hPV1ppYlRrd1lraDBkMk51WkdwWU1UazVXVmhm2YlZreVZtaGFSMnhC'

try:
    while True:
        base64_code = base64.b64decode(base64_code)
except:
    print(base64_code)
```

C: > Users > Administrator > Desktop > hardzip > code.py > ...

```
1 import base64
2
3 base64_code = 'V20xa2NGa3hPV1ppY1Rrd1lraDBkMk51WkdwWU1UazVXVmh2Y1ZreVZtaGFSMnhC'
4
5 try:
6     while True:
7         base64_code = base64.b64decode(base64_code)
8 except:
9     print(base64_code)
```

PROBLEMS OUTPUT TERMINAL DEBUG CONSOLE

[Running] D:/Python/Python3/python.exe "c:\Users\Administrator\Desktop\hardzip\code.py"  
b'fgic\_\_not1{prwc\_\_}az&ceadi@'

[Done] exited with code=0 in 0.074 seconds

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

栅栏密码解一下

fgic\_\_not1{prwc\_\_}az&ceadi@

每组字数

加密

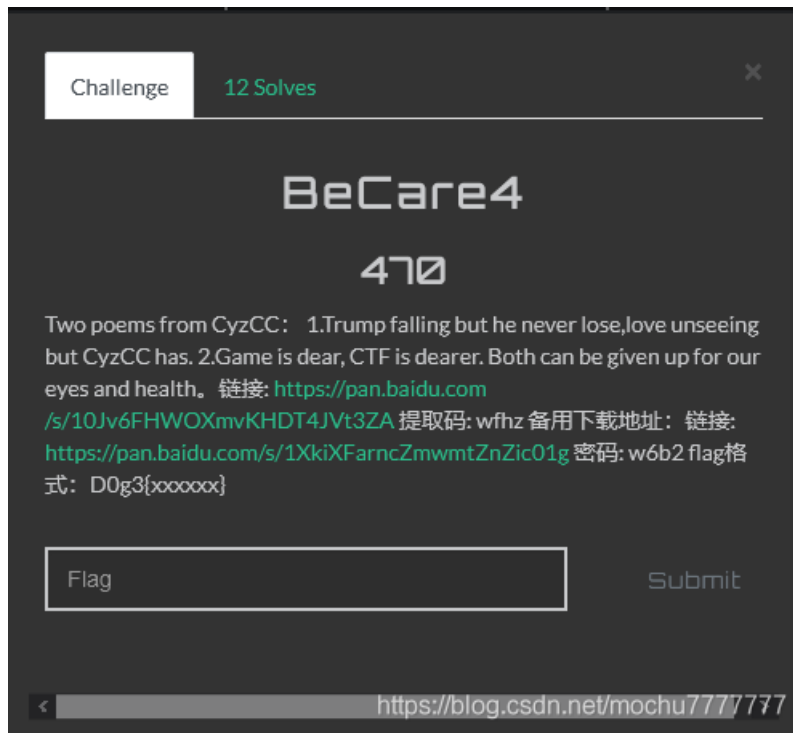
解密

flag{zip&crc\_we\_can\_do\_it}@

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

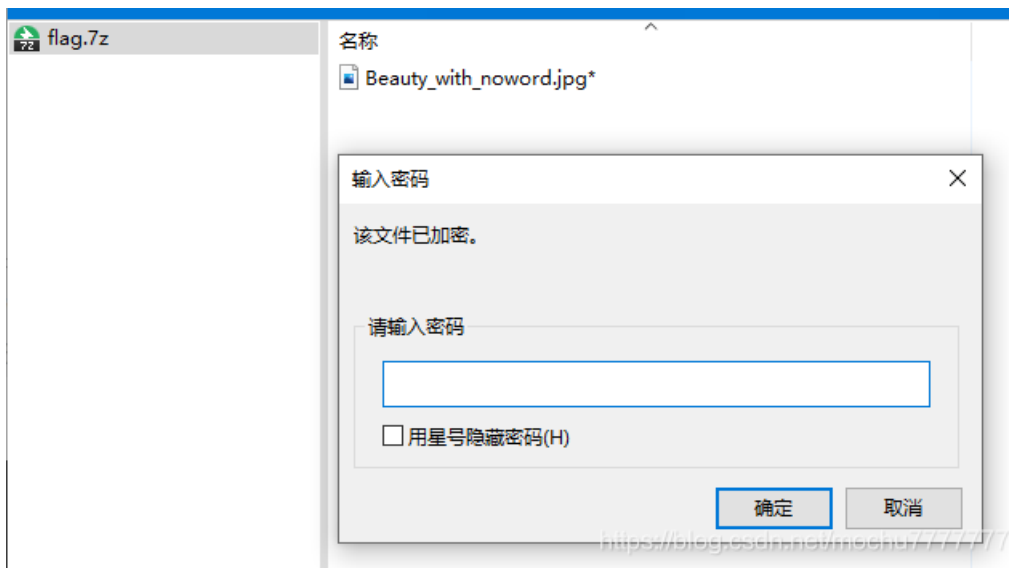
flag{zip&crc\_we\_can\_do\_it}

BeCare4



flag.7z	2020/11/25 8:11	7Z 压缩文件	126 KB
npmtxt	2020/11/22 15:57	文件	2 KB

flag.7z 有密码, 猜测要从 npmtxt 上得到解压密码



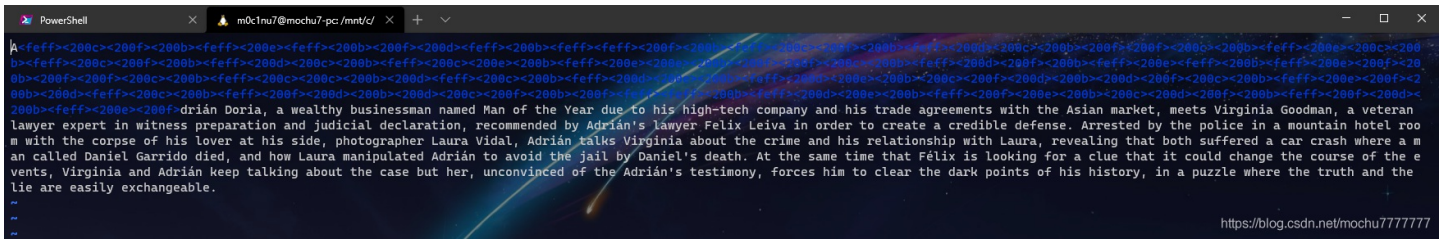
npmtxt 是 txt 文件, cat 一下发现好像有隐藏字符, 可能存在 零宽度字符隐写

```

#0c1nu7@mochu7-pc: /mnt/c/Users/Administrator/Downloads/安淘杯题目备份/Misc/BeCare4$ ls
flag.7z npmtxt
#0c1nu7@mochu7-pc: /mnt/c/Users/Administrator/Downloads/安淘杯题目备份/Misc/BeCare4$ file npmtxt
npmtxt: UTF-8 Unicode text, with very long lines, with no line terminators
#0c1nu7@mochu7-pc: /mnt/c/Users/Administrator/Downloads/安淘杯题目备份/Misc/BeCare4$ cat npmtxt
A
e to his high-tech company and his trade agreements with the Asian market, meets Virginia Goodman, a veteran lawyer expert in witness preparation and judicial declaration, recommended by Adrián's lawyer Felix Leiva in order to create a credible defense. Arrested by the police in a mountain hotel room with the corpse of his lover at his side, photographer Laura Vidal, Adrián talks Virginia about the crime and his relationship with Laura, revealing that both suffered a car crash where a man called Daniel Garrido died, and how Laura manipulated Adrián to avoid the jail by Daniel's death. At the same time that Félix is looking for a clue that it could change the course of the events, Virginia and Adrián keep talking about the case but her, unconvinced of the Adrián's testimony, forces him to clear the dark points of his history, in a puzzle where the truth and the lie are easily exchangeable.#0c1nu7@mochu7-pc: /mnt/c/Users/Administrator/Downloads/安淘杯题目备份/Misc/BeCare4$

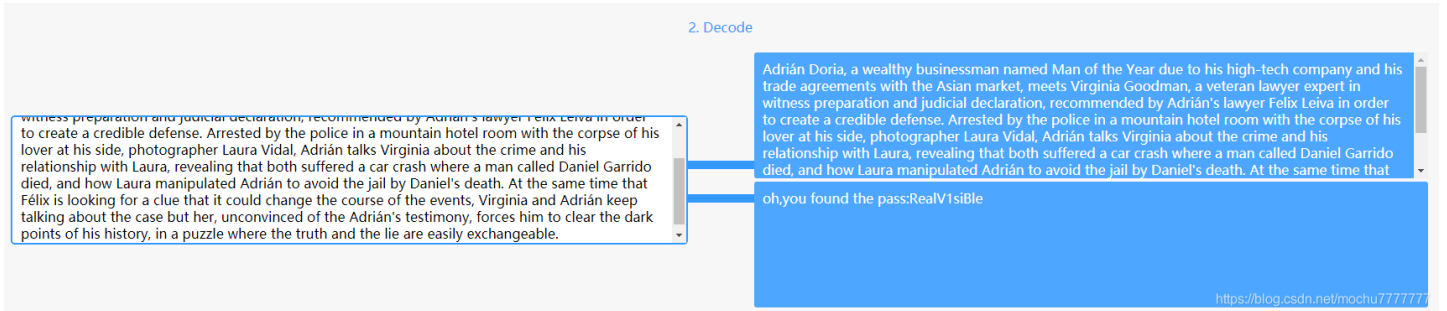
```

使用 Vim 验证一下, 果然是零宽度字符隐写



这里有 `<200f>` 也就是 `U+202F`，所以有些站解出来结果不太对或者解不出来，比赛的时候找了个能解的

Zero-Width-Steg-Online: <https://yuanfux.github.io/zero-width-web/>

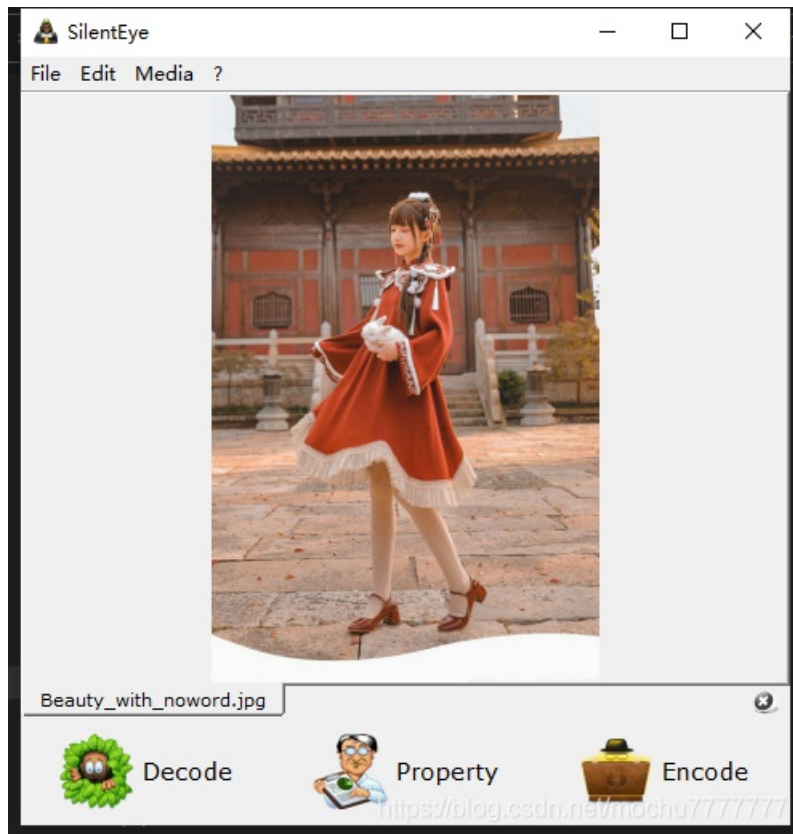


oh,you found the pass:RealV1sible

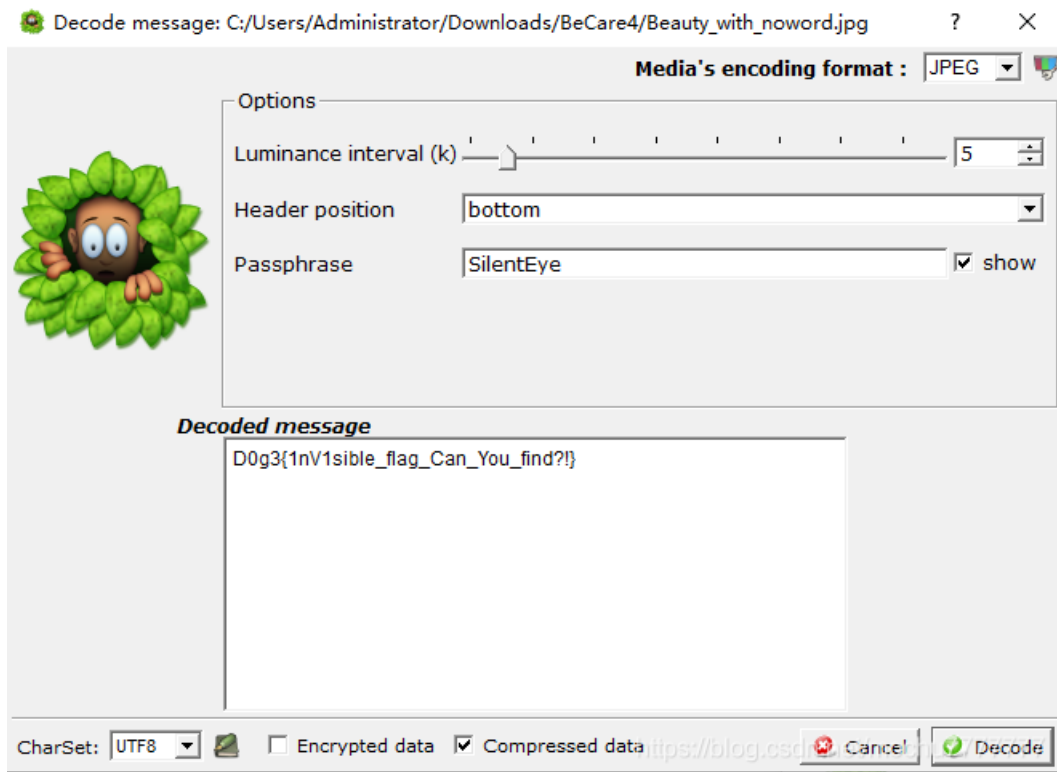
解压 `flag.7z`，得到 `Beauty_with_noword.jpg`







Decode，也没有密码，直接用默认密码



当时懵了，就这?????

```
D0g3{1nV1sible_flag_Can_You_find?!}
```