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

本文链接：https://blog.csdn.net/mochu7777777/article/details/110151315

题目名称

签到


```
Hint: 哥哥们注意文件名
```

`大声说出fl4g.jpg`

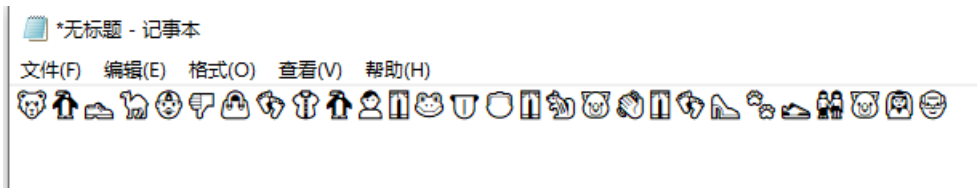
向公众号回复：`fl4g`

下载是`flag.docx`

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

□□□□□□□□□□□□□□□□□□□□□□□□□□□□□

复制那串特殊符号到记事本



`Emojiencode`：http://www.atoolbox.net/Tool.php?Id=937


```
D0g3{Welc0m_ANd_H1T_liGht1y}
```

王牌特工

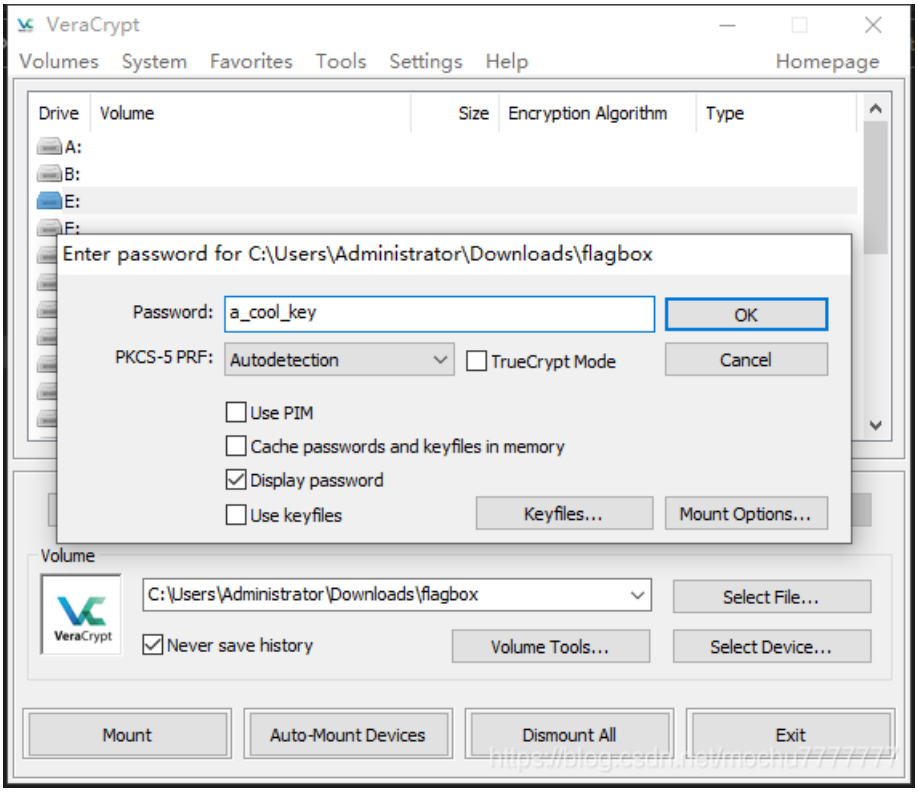
`file`查看，发现是`ext3`文件系统，直接挂载

```
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 %
```

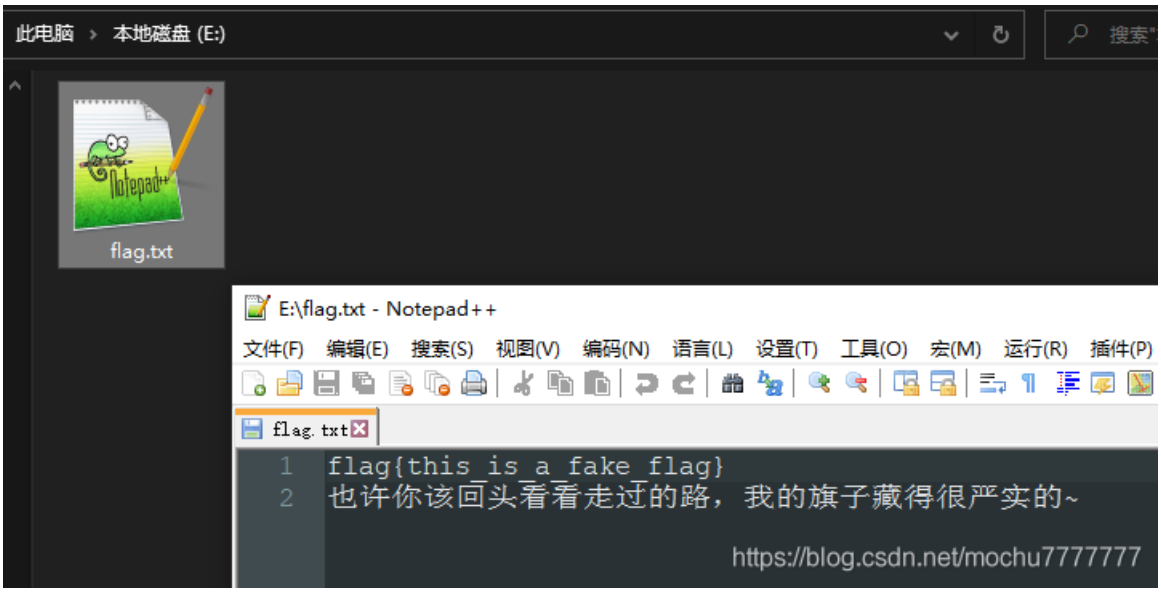


```
root@kali /mnt % ls
flagbox  key.txt  lost+found
root@kali /mnt % file flagbox
flagbox: data
root@kali /mnt % cat key.txt
key:a_cool_key
use Veracrypt
root@kali /mnt %
```

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

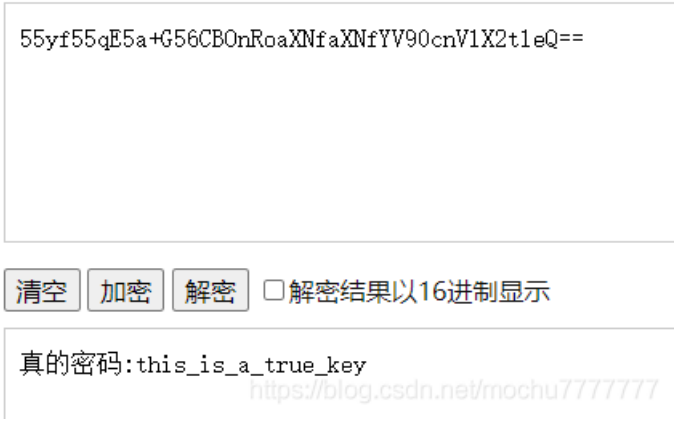
```
extundelete findme --restore-all
```

```
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/mochu7777777
```

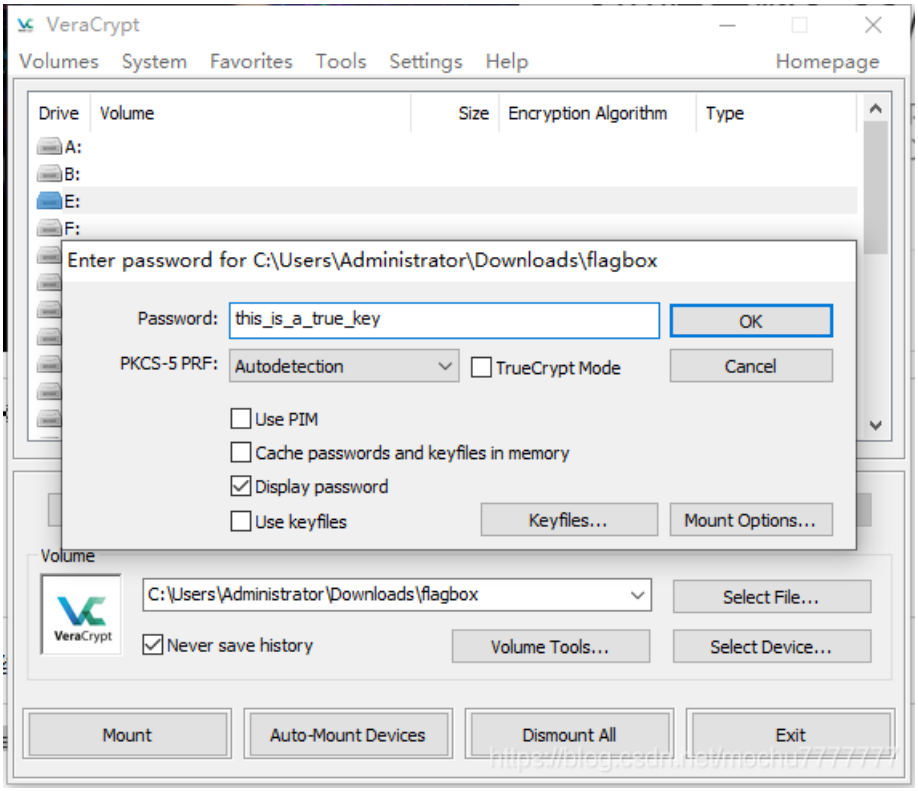
发现个隐藏文件`.coolboy.swp`，查看下，发现一串base64

```
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#"! Utpad@@@@@you find me55yf55qE5a+G56CBOnRoaXNfaXNfYV90cnVlX2tleQ==#
root@kali /home/mochu7/Desktop/RECOVERED_FILES %
```

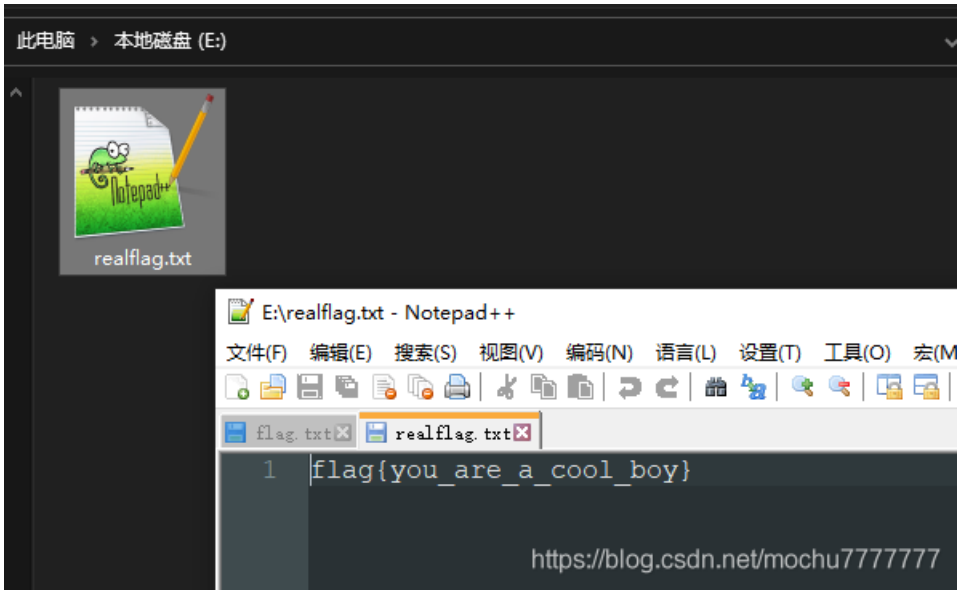
```
55yf55qE5a+G56CBOnRoaXNfaXNfYV90cnVlX2tleQ==
```



得到真的密码，使用这个密码再去挂载 `flagbox`



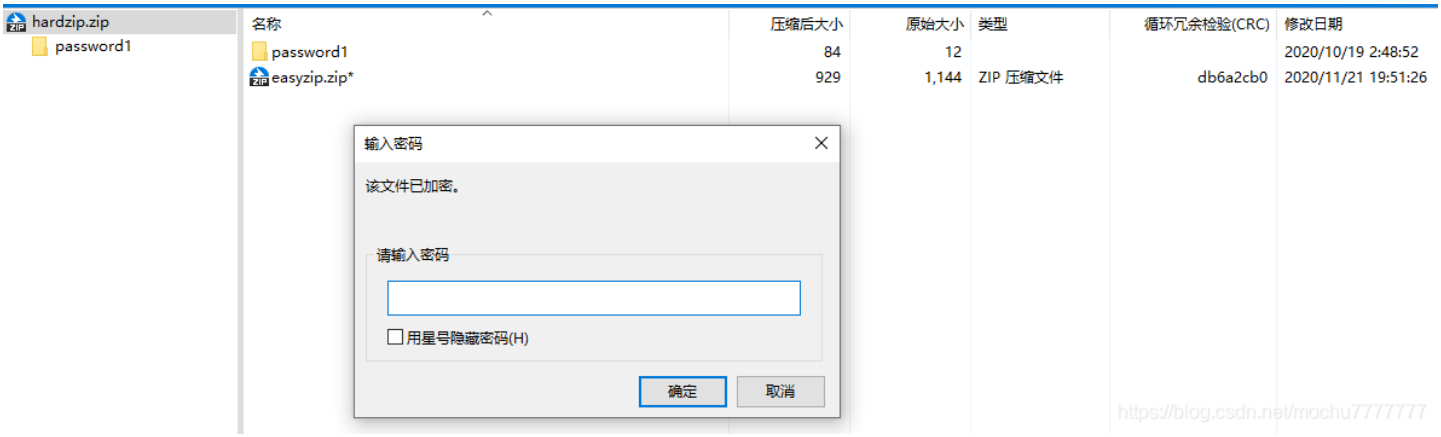
再次打开挂载目录，得到真的flag



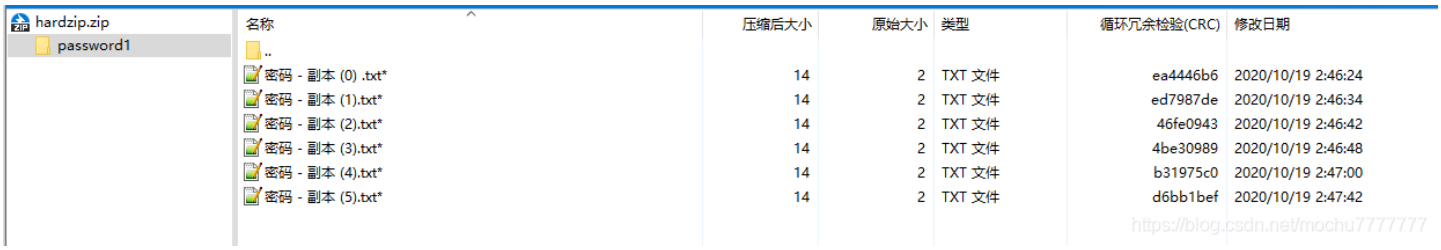

```
flag{you_are_a_cool_boy}
```

套娃

`hardzip.zip` 需要密码



`password1` 目录可查看



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

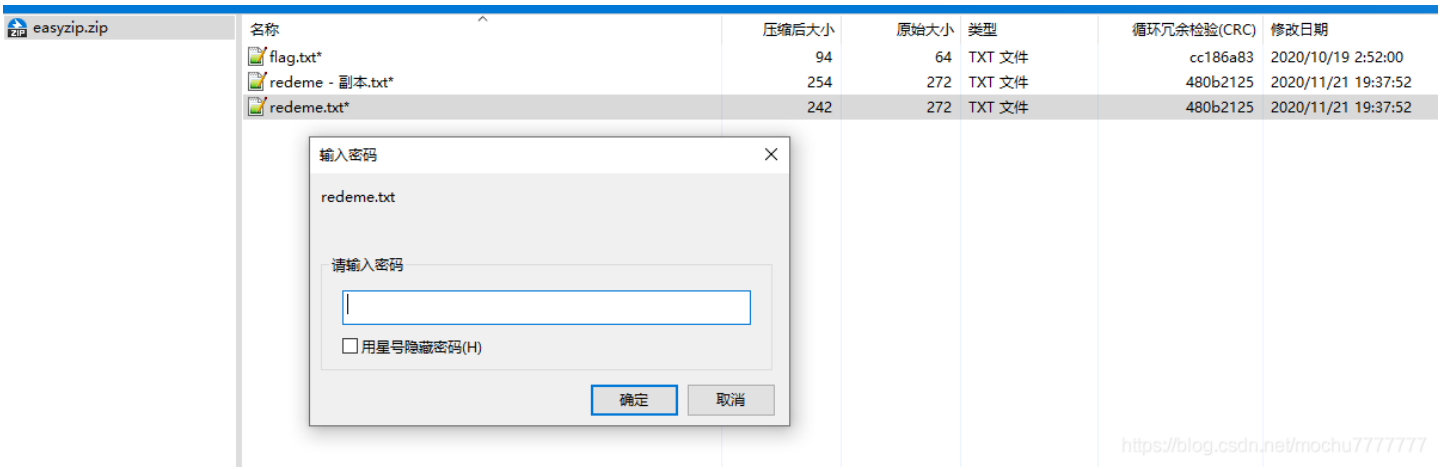
```python
#Written by: Mochu7
import binascii
import string

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()
```

得到`hardzip.zip`的密码：`!qQIdEa@#!z)`

`easyzip.zip`有密码

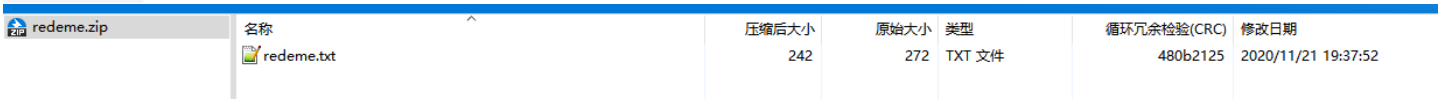


`7zip` 可直接从 `easyzip.zip` 中解压出 `redeme.txt`，然后即可进行明文攻击，注意这里 `flag.txt` 加密方式不一样，不能放在明文攻击的目标 `zip` 中

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`

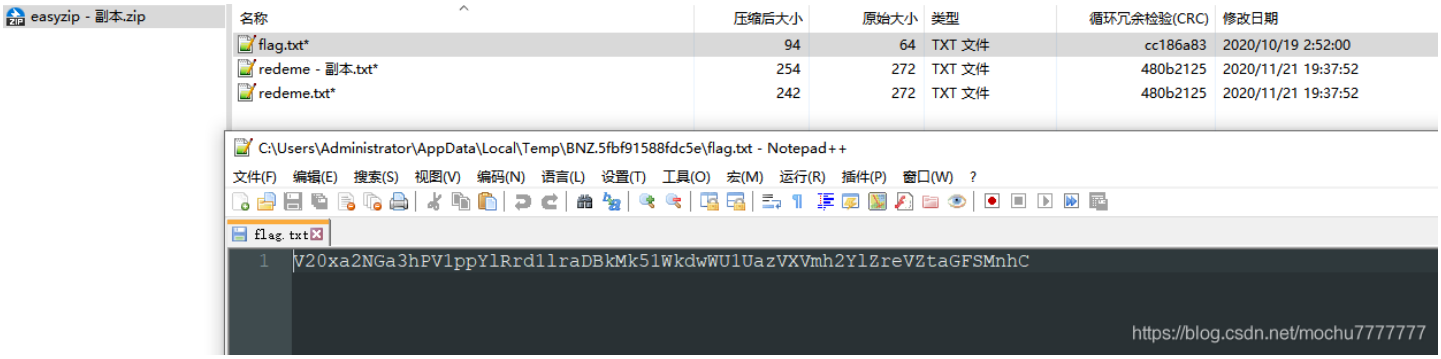
`easyzip.zip`

`redeme.zip`




```
%3#c$v!@
```

使用这个密码直接解`flag.txt`



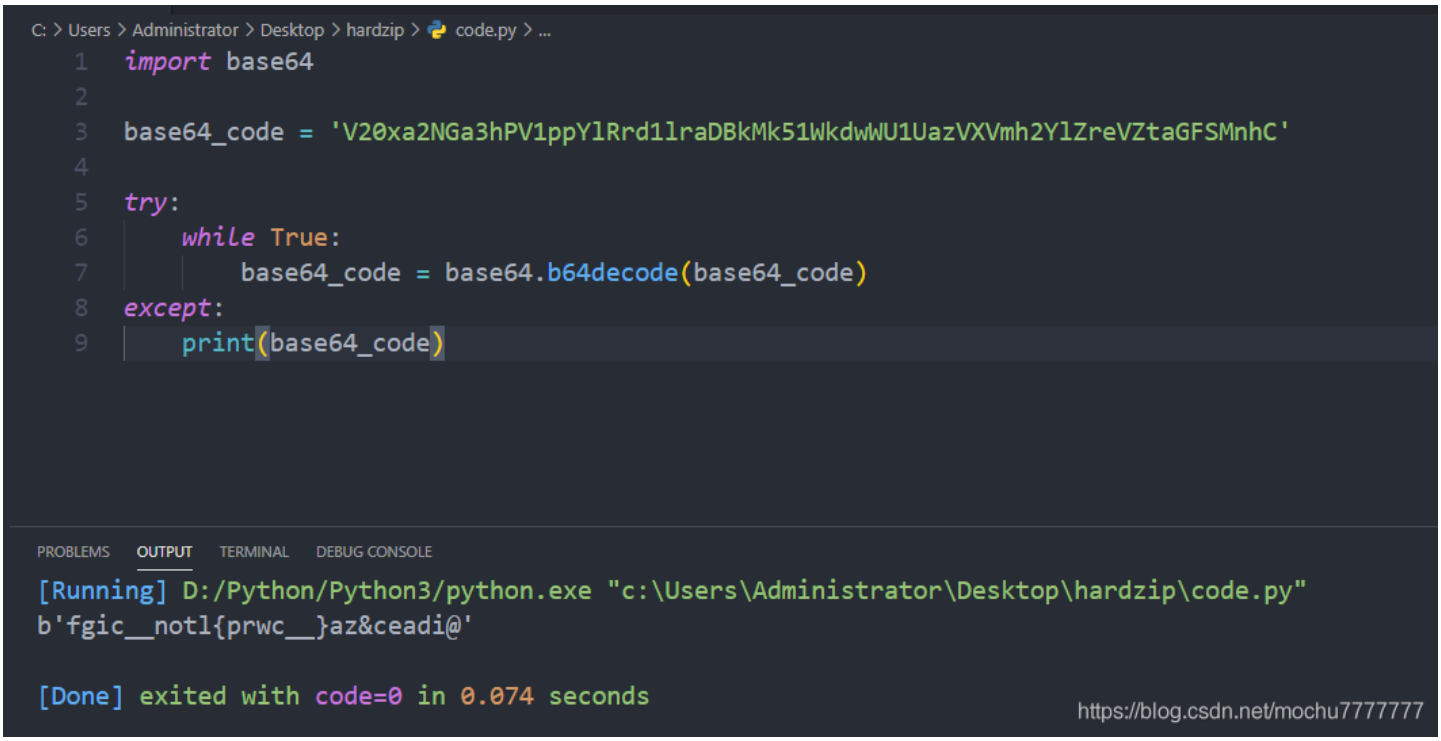
Base64套娃

```
V20xa2NGa3hPV1ppYlRrd1lraDBkMk51WkdwWU1UazVXVmh2YlZreVZtaGFSMnhC
```

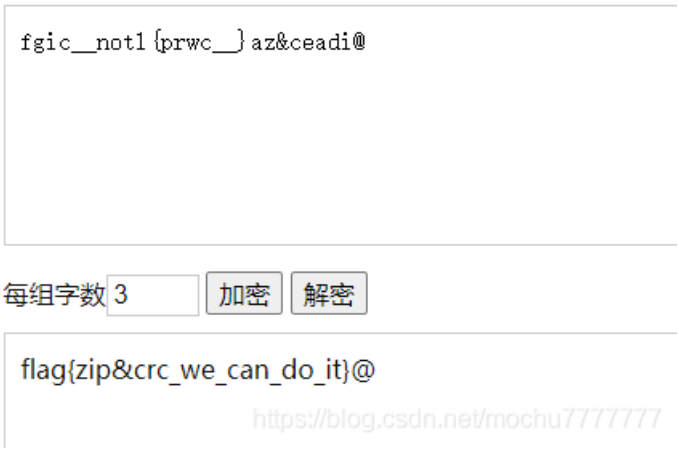
```python
import base64

base64_code = 'V20xa2NGa3hPV1ppYlRrd1lraDBkMk51WkdwWU1UazVXVmh2YlZreVZtaGFSMnhC'

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

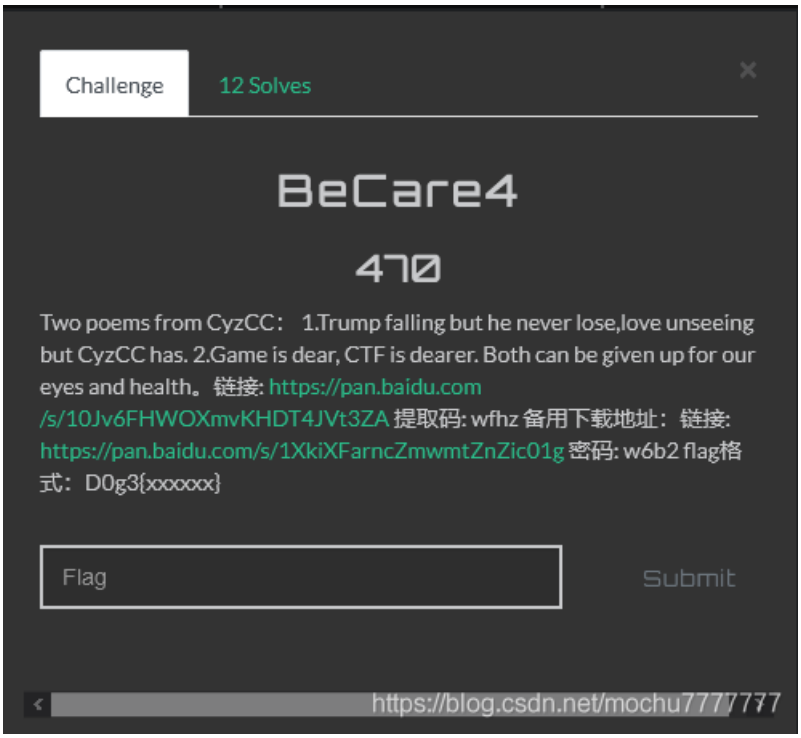


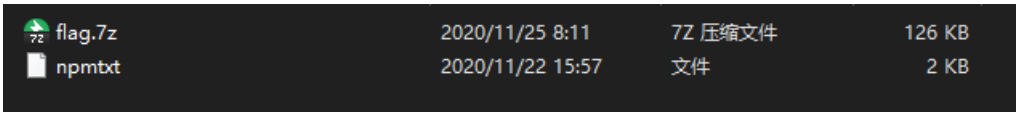
栅栏密码解一下



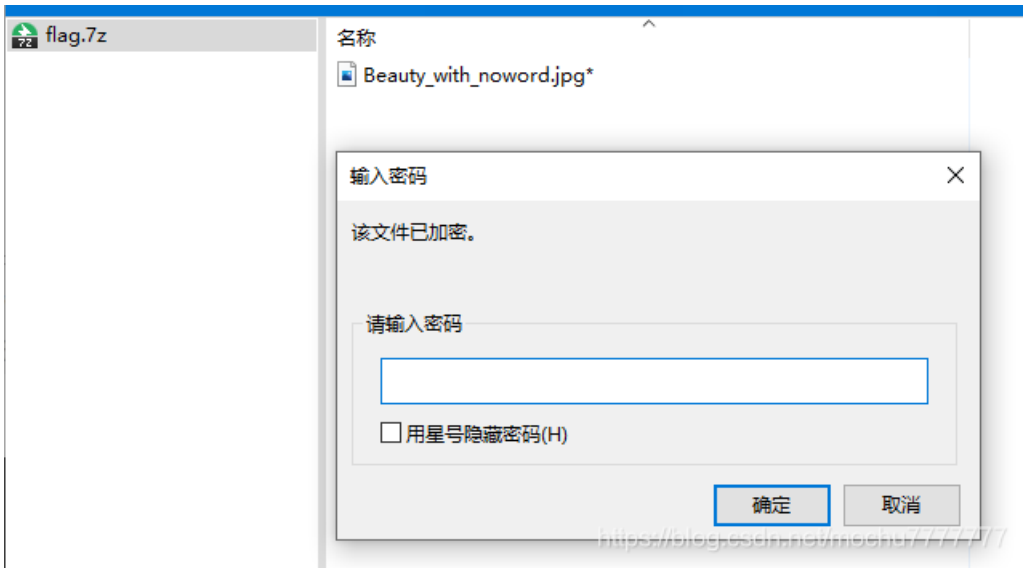

```
flag{zip&crc_we_can_do_it}
```

BeCare4

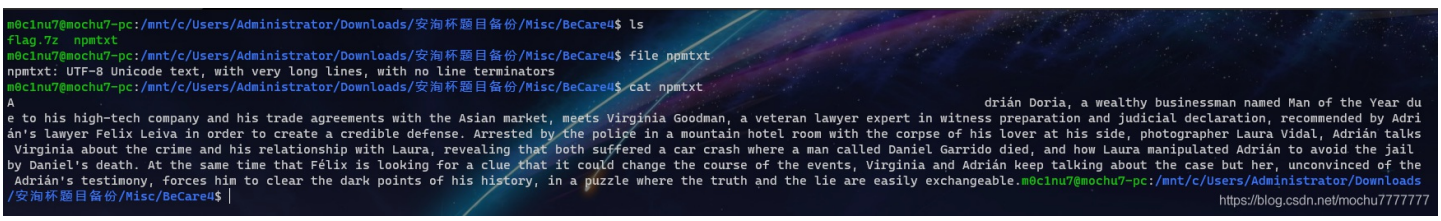




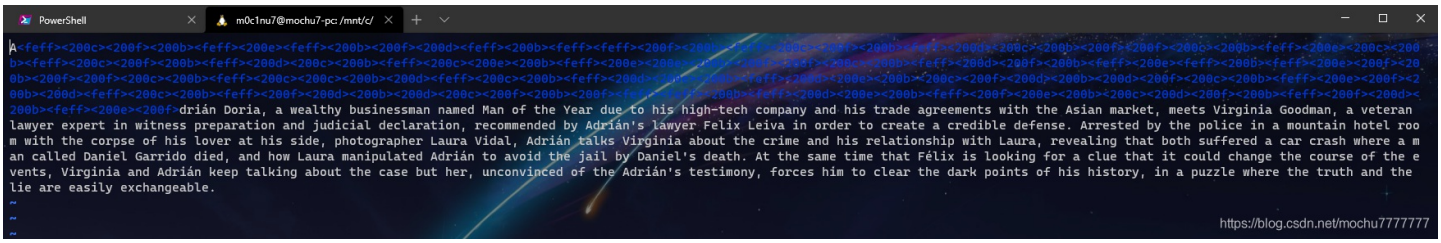
`flag.7z`有密码，猜测要从`npmtxt`上得到解压密码



`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`

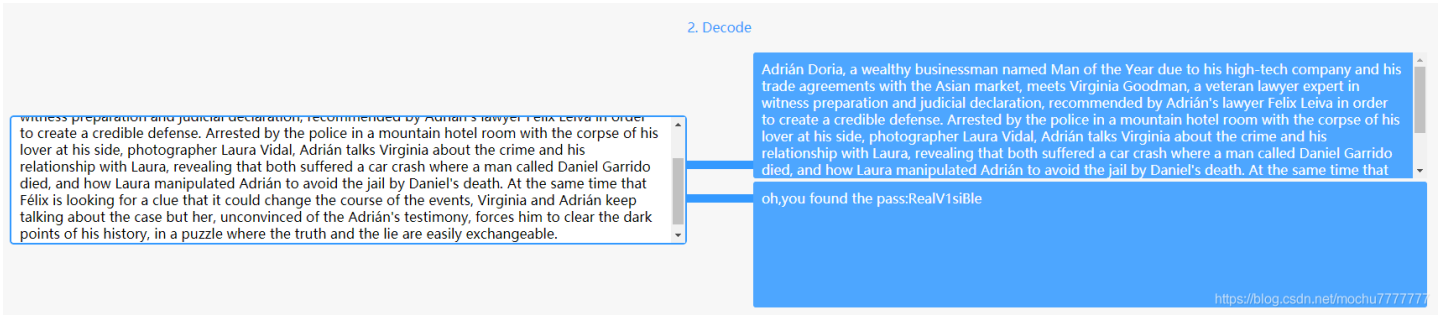


使用`Vim`验证一下，果然是零宽度字符隐写



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

Zeroi-Width-Steg-Online：https://yuanfux.github.io/zero-width-web/

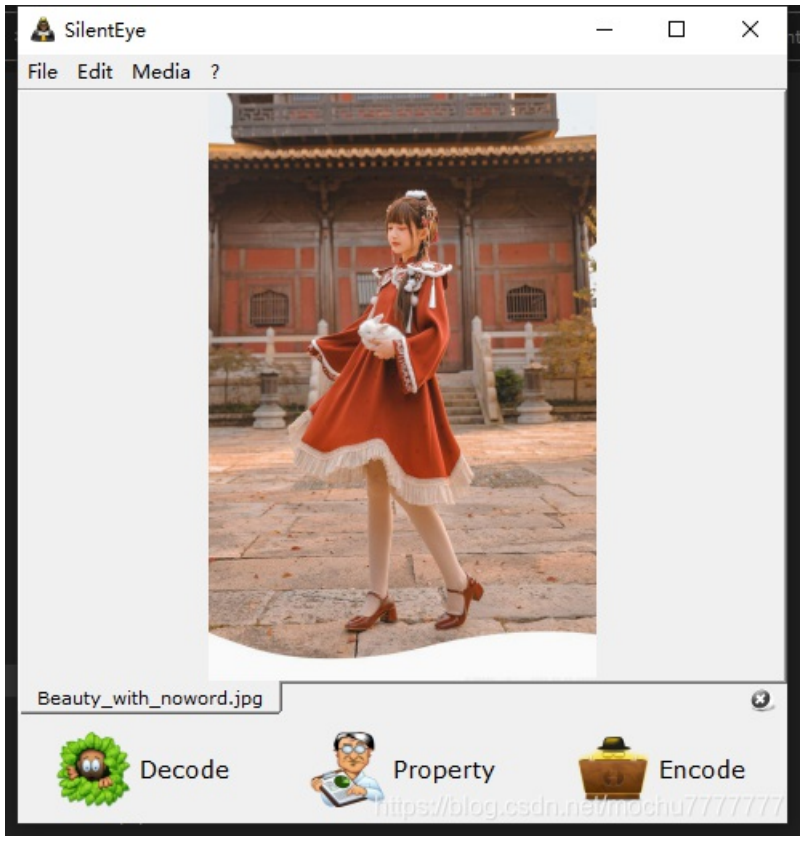



```
oh,you found the pass:RealV1siBle
```

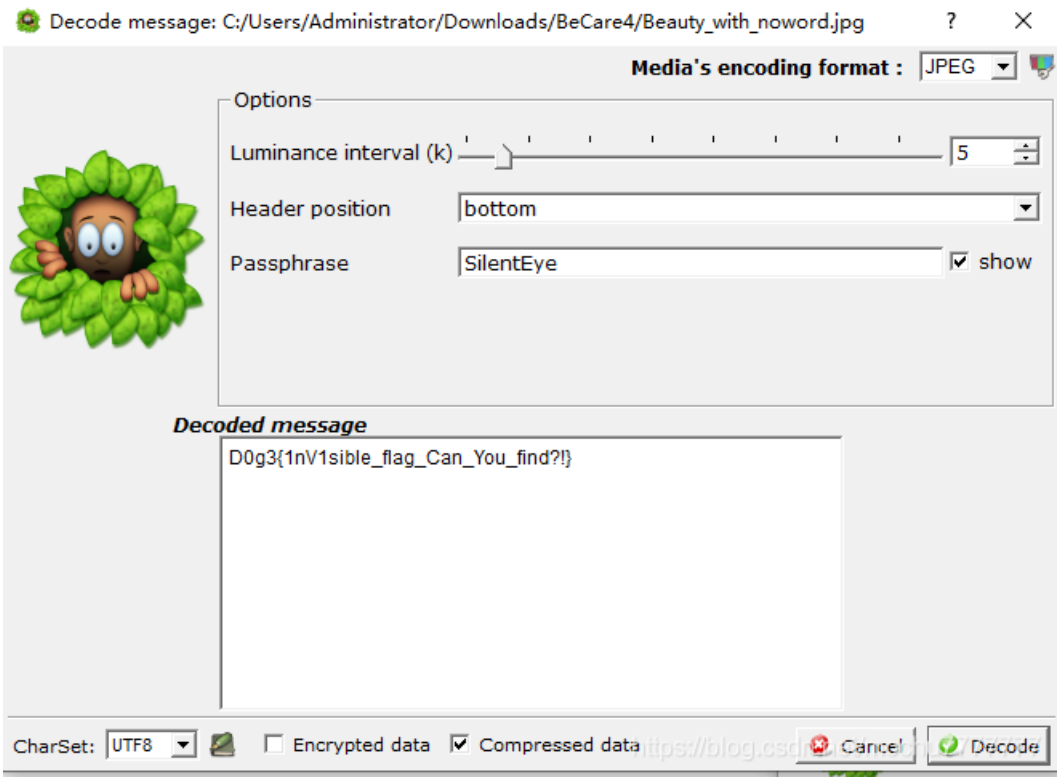
解压`flag.7z`，得到`Beauty_with_noword.jpg`

解到这里，对这张图片试了很多隐写方法，没有得到什么结果，看了题目给的描述中有提到`eye`，才想到`SilentEye`

使用`SilentEye`打开



`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?!}
```