

## Web

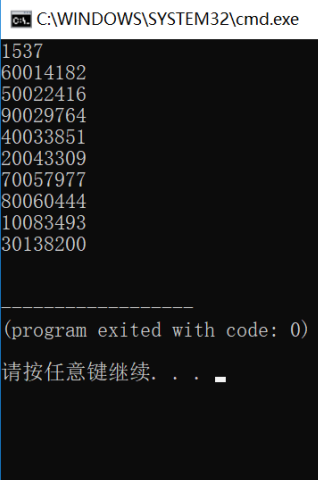
### sqli-1

URL: <http://118.89.111.179:3000/>

sql 注入的题目。

但是首先要解决这个 code 的问题。审计一下代码，大概意思是从 code 传入一个数字，使它的 MD5 值的前四个字符符合一定的条件。而这个条件每刷新一次网页都会变【这就很烦】。网上搜 hash 截断爆破，现成的类似脚本还蛮多的，我改了一下细节就直接用了。虽然是拿了现成的脚本，但是这里还是放一下吧（语言是 python）【我忘了来源是哪里了，不过还是感谢原作者】：

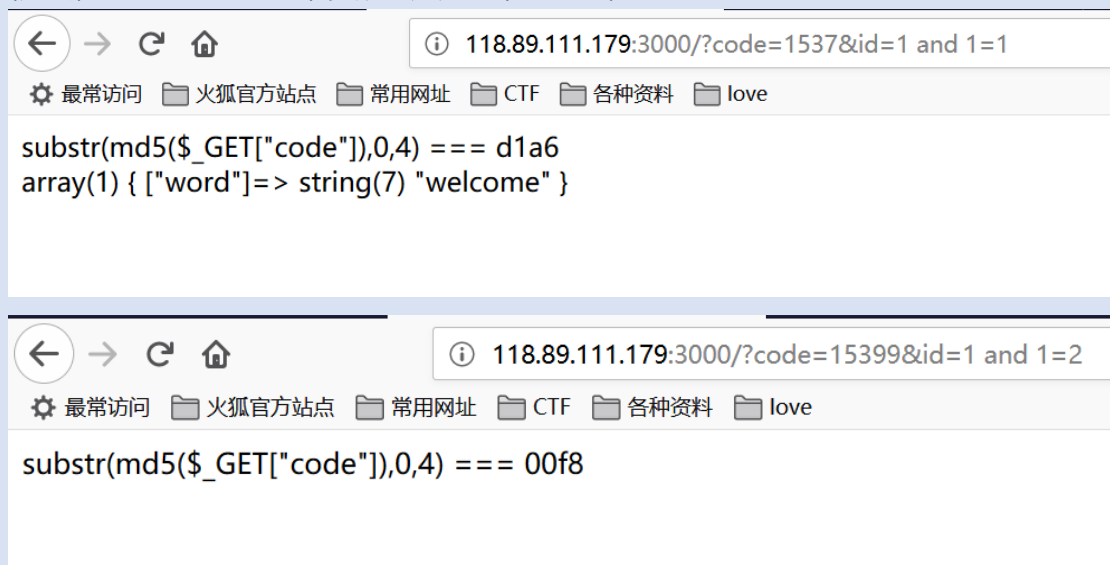
```
1 import hashlib
2 from multiprocessing.dummy import Pool as ThreadPool
3
4 def md5(s):
5     return hashlib.md5(str(s).encode('utf-8')).hexdigest()
6
7 keymd5 = 'd1a6'
8 md5start = 0
9 md5length = 4
10
11 def findmd5(sss):
12     key = sss.split(':')
13     start = int(key[0])
14     end = int(key[1])
15     result = 0
16     for i in range(start, end):
17         if md5(i)[0:4] == keymd5:
18             result = i
19             print(result)
20             break
21
22 list=[]
23 for i in range(10):
24     list.append(str(10000000*i) + ':' + str(10000000*(i+1)))
25 pool = ThreadPool()
26 pool.map(findmd5, list)
27 pool.close()
28 pool.join()
```



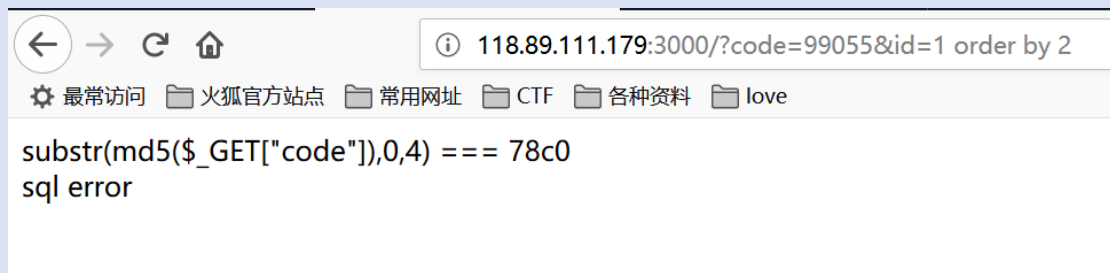
每次刷新页面我都是手动改 keymd5 的变量值然后运行程序出结果的。

下面专注于 sql 注入的过程吧。

根据错误回显发现 id 这个参数果然是一个注入途径



用 order by 语句判断字段值，以便后面的联合查询注入操作：

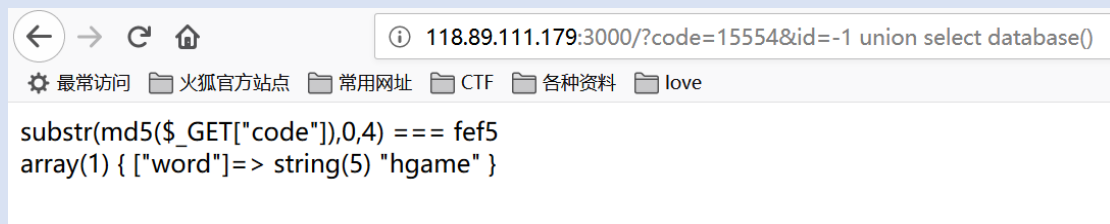


order by 2 返回错误页面了



说明只有一个字段，那么后面的构造就很方便了

使用联合查询注入（id 设为 -1 报错使之执行后面的语句。也可以构造为 id=1 and 1=2）：  
?id=-1 union select database()



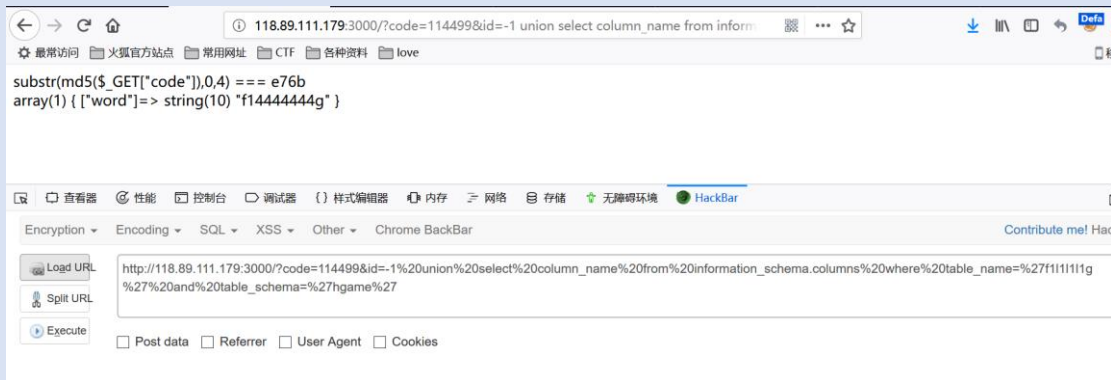
得到数据库名 hgame。

然后继续构造 id 参数=-1 union select table\_name from information\_schema.tables where table\_shema='hgame'

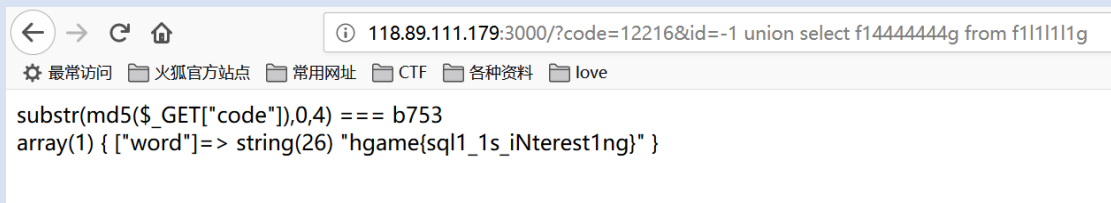


得到表名。有两个表，我们查看那个 f1l1l1l1g 的表，查询里面的列名（这个看起来比较像藏了 flag 的地方）

union select column\_name from information\_schema.columns where table\_name='f1l1l1l1g' and table\_shema='hgame'



里面只有一个列 f14444444g



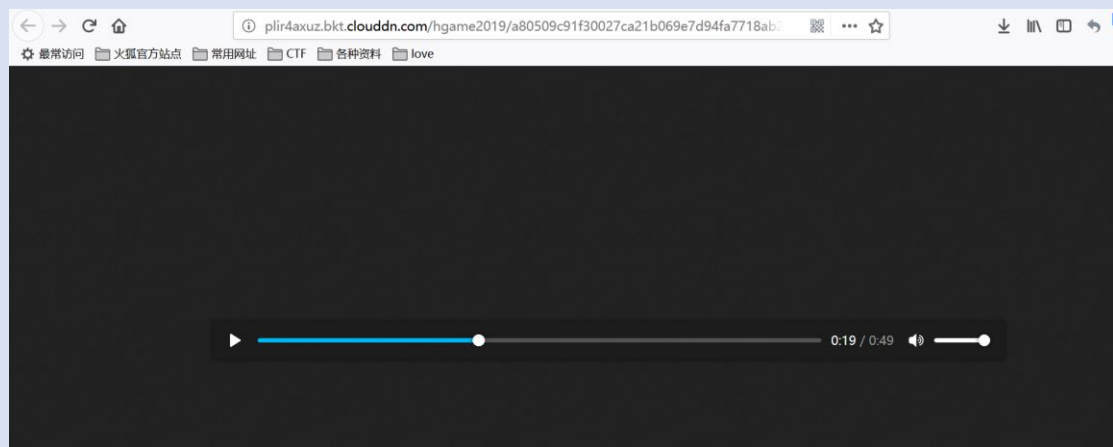
查看此列的内容，得到 flag

## Misc

### 听听音乐

URL:<http://plir4axuz.bkt.clouddn.com/hgame2019/a80509c91f30027ca21b069e7d94fa7718ab2e40684628c41943bf647f3d7c6a/stego.mp3>

从第 19 秒开始是摩斯电码的音频



我是直接用耳朵听然后手记下来，放到在线解码工具里解码的（最后一个单词 wav 那里反复听了很多次，长短有点听不清，尝试了很多组合试了好几次不同的 flag 然后出来的）。

【后来查了下好像有音频直接转文字的方法？



至少像那雪一样

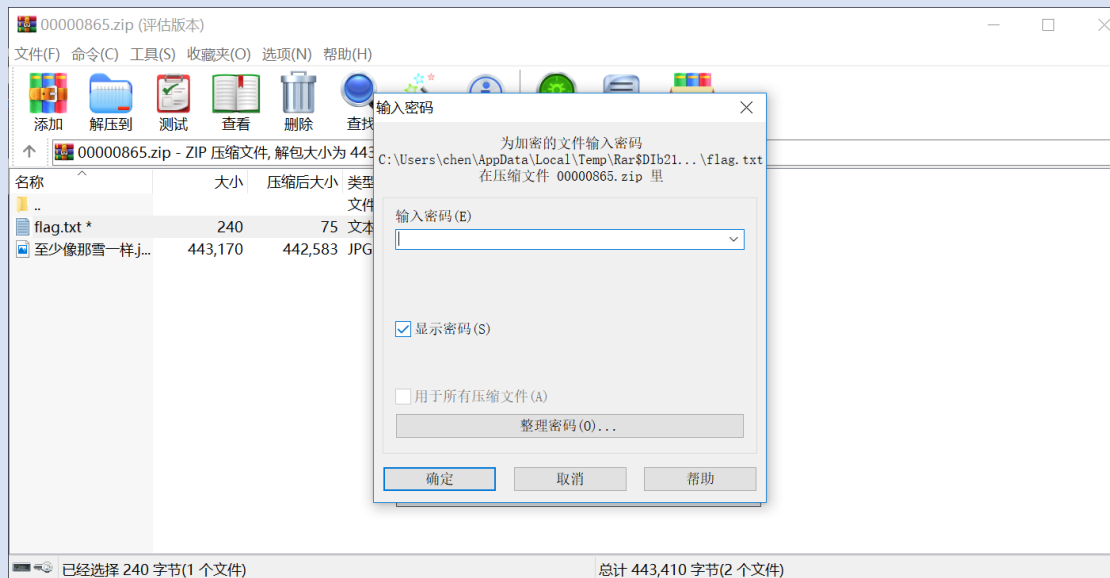
URL:<http://plqfgjy5a.bkt.clouddn.com/%E8%87%B3%E5%B0%91%E5%83%8F%E9%82%A3%E9%9B%AA%E4%B8%80%E6%A0%B7.jpg>

是张 jpg 图片，查看属性和源码无果之后用 binwalk 分析了一下，发现 jpg 后面还隐藏一个 zip 压缩包。于是用 foremost 把 jpg 图片和 zip 压缩包分离开来：

```
chen537@chen537-virtual-machine:~/桌面$ binwalk 至少像那雪一样.jpg
DECIMAL      HEXADECEMAL  DESCRIPTION
-----
0            0x0         JPEG image data, JFIF standard 1.01
30           0x1E       TIFF image data, big-endian, offset of first image directory: 8
885851       0xD845B    Zip archive data, encrypted at least v2.0 to extract, compressed size: 75, uncompressed size: 240, name: flag.txt
886204       0xD85BC    End of Zip archive, footer length: 22

chen537@chen537-virtual-machine:~/桌面$ foremost 至少像那雪一样.jpg
ERROR: /home/chen537/桌面/output is not empty
Please specify another directory or run with -T.
chen537@chen537-virtual-machine:~/桌面$ foremost -T 至少像那雪一样.jpg
Processing: 至少像那雪一样.jpg
|foundat=*****hoo.jpgup|
*|
chen537@chen537-virtual-machine:~/桌面$
```

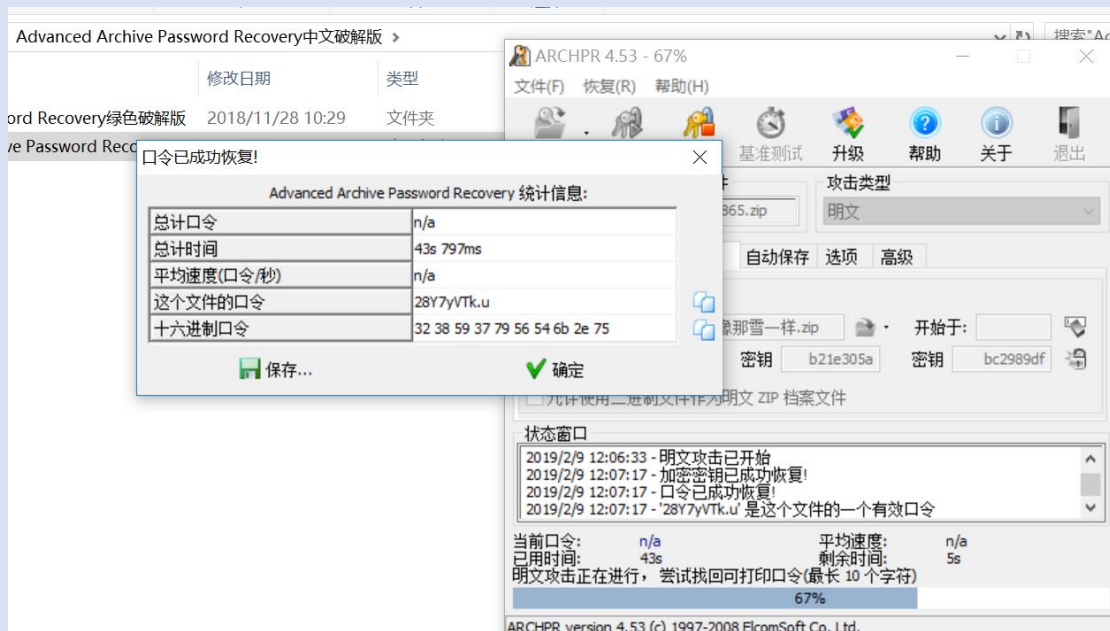
压缩包里也有一张 至少像那雪一样.jpg，除此之外还有 flag.txt。但是解压需要密码。



找不到密码的相关线索，简单的爆破也尝试了下不行。于是去网上查了下各种压缩包密码破解方法，发现有种方法叫做“明文攻击”。

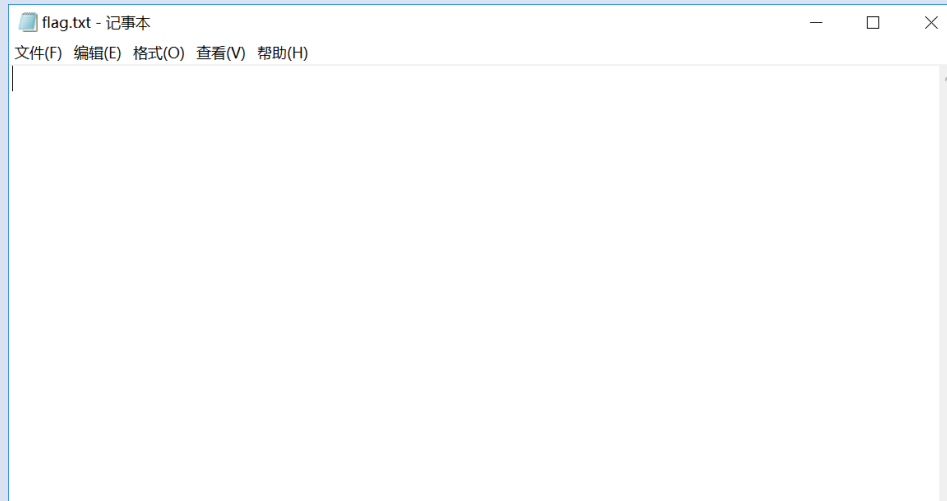
能够使用明文攻击的前提条件是我们已有加密压缩包里的一部分源文件。比如这里我们有的就是“至少像那雪一样.jpg”，通过文件大小能猜到加密压缩包里的图片和我们之前分离出来的 jpg 图片应该是一样的。

明文攻击可以下这个工具，叫 Advanced Archive Password Recovery 【好像只有正版才能显示正确密码，免费版只能帮你解压加密压缩包里的第一个文件，我一开始用免费版结果解压出来只有 jpg 图片……正版太贵了只好下了破解版】。完成攻击只需要把那部分已知的源文件也压缩成 zip 包，然后在 AAPR 里打开它，以及打开要解密的压缩包就行了。（使用方法百度到的）解密过程很快：

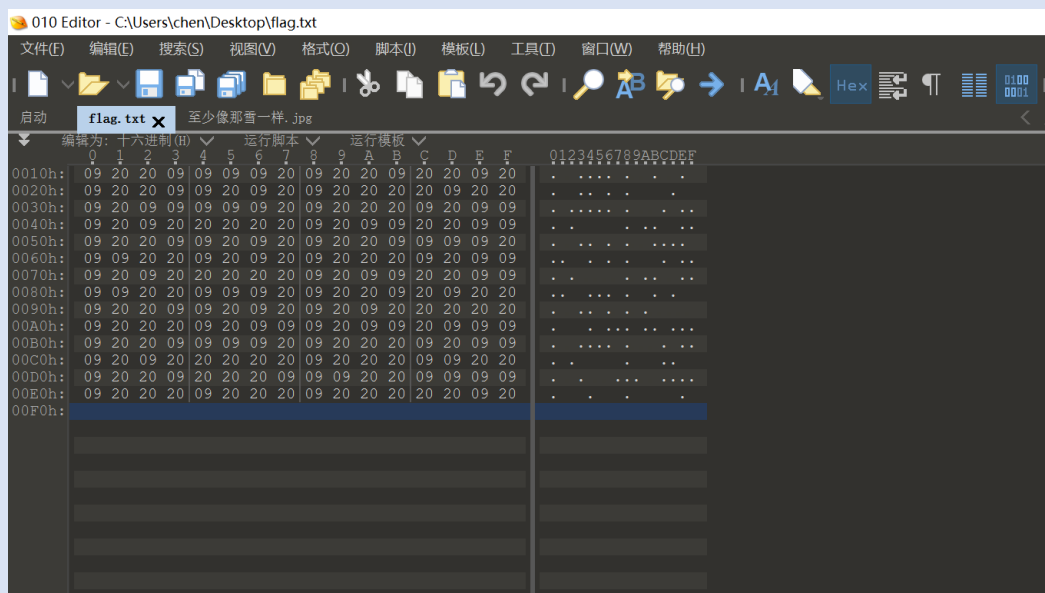


得到密码，解压压缩包，我满心欢喜地打开 flag.txt 结果发现里面一片空白：

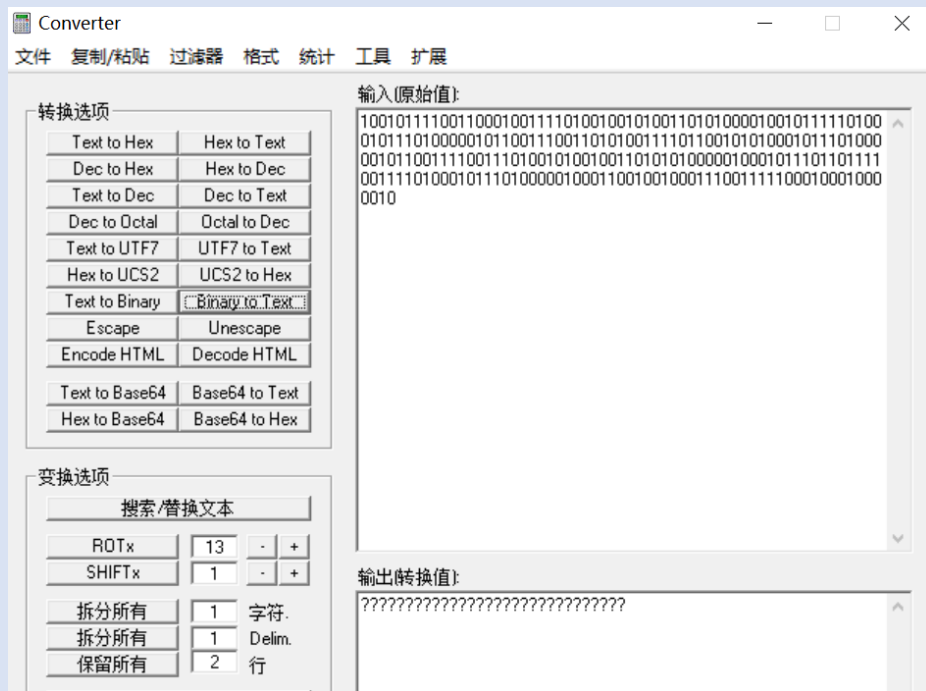
【你妈的，为什么】



冷静下来之后发现还是有内容的（十六进制 20 好像是空格，09 就不知道了，反正显示不出来）：



看到只有 09 和 20 的排列组合就脑洞大开了，想转换成二进制看看，于是手动把 09 记成 1，20 记成 0：



呃好像不太对，那么 1 和 0 调换一下：

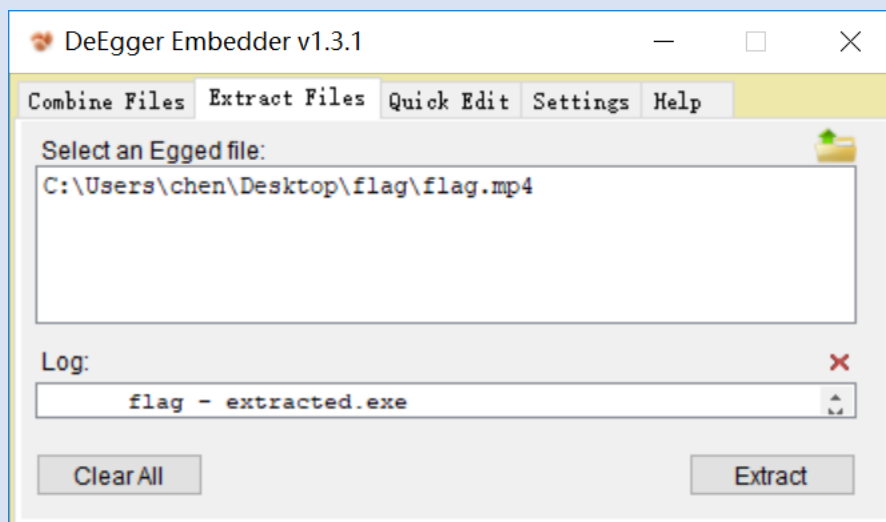


flag 出来了

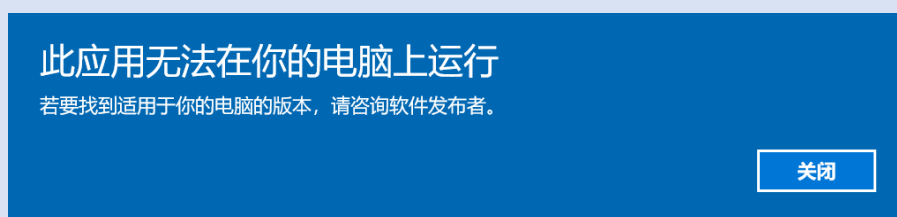
时至今日，你仍是我的光芒

URL: <http://plir4axuz.bkt.clouddn.com/hgame2019/stuff/flag.zip>

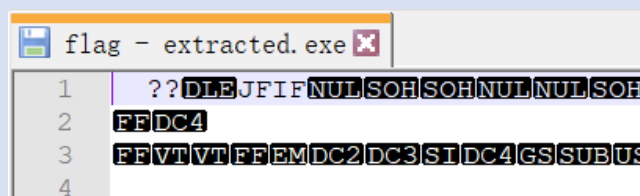
这题没做出来，卡住了。但还是想把部分过程写一下：  
根据 hint1，去下了 deegger embedder，从 mp4 里提取出隐藏文件



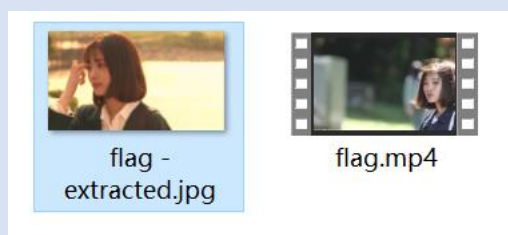
exe 文件打不开



查看源码发现文件头标志是 jpg 图片的，于是重命名，把后缀改为 jpg



再分析这张图片，好像没有隐藏文件了，stegsolve 分析出来啥也没有，binwalk 分析出来也是纯正的 jpg 图片。



第二个 hint 是 outguess，这是个隐写工具，我在 linux 里安装好，然后处理一下这张图片，好像直接 outguess -r 是不行的。题目描述里说密码是 sec.\*，于是我加了 key 选项上去：

```
outguess -k "sec.*" -r flag-extracted.jpg 1.txt
```

好像成功了。

```
cat 1.txt
```

发现是一堆乱码。

然后就卡在这了，这堆乱码实在分析不出来，也不知道是不是因为 outguess 的方法不对……



而且题目描述里说的 rockyou.txt 那个字典我也没用到，没啥头绪。

【明明已经给了两个 hint 了还是做不出来我果然还是太菜了唉】等官方 wp 出来再说吧。