Xp0intCTF 2017 writeup

原创

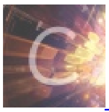
P2017118 于 2017-10-23 18:28:16 发布 1014 收藏 1

分类专栏： ctf 文章标签： ctf

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/P2017118/article/details/78321669

版权


ctf 专栏收录该内容

2 篇文章 0 订阅

订阅专栏

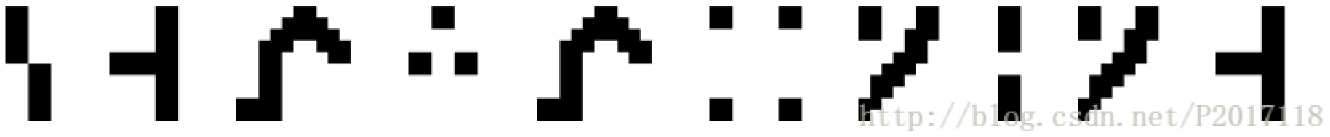
记录第一场ctf

SGA

看起来好像是一种神秘的文字…（得到的内容加flag{}提交，且全部小写）

hint:Encyclopedia is your good friend！

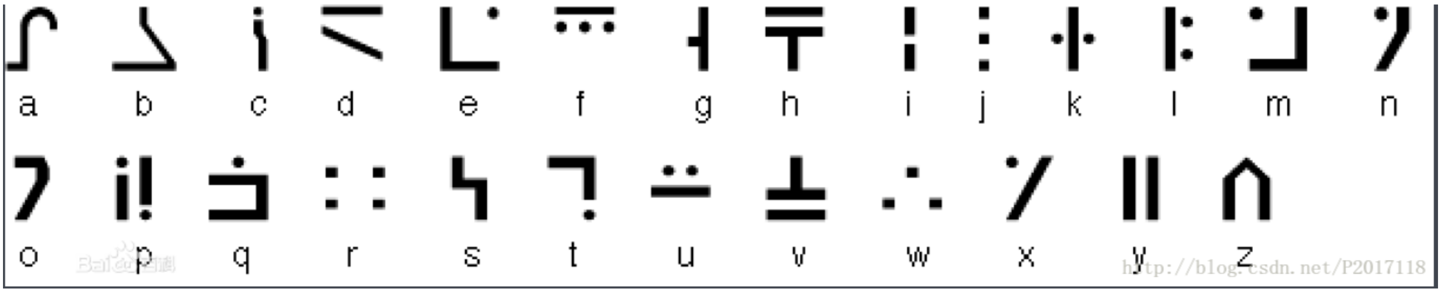
- 去掉后缀，得到zip，解压得到一串文字



- hint提示,通过wiki搜索SGA，且提示是一种神秘文字

- Standard Galactic Alphabet, the writing system in the *Commander Keen* fictional universe

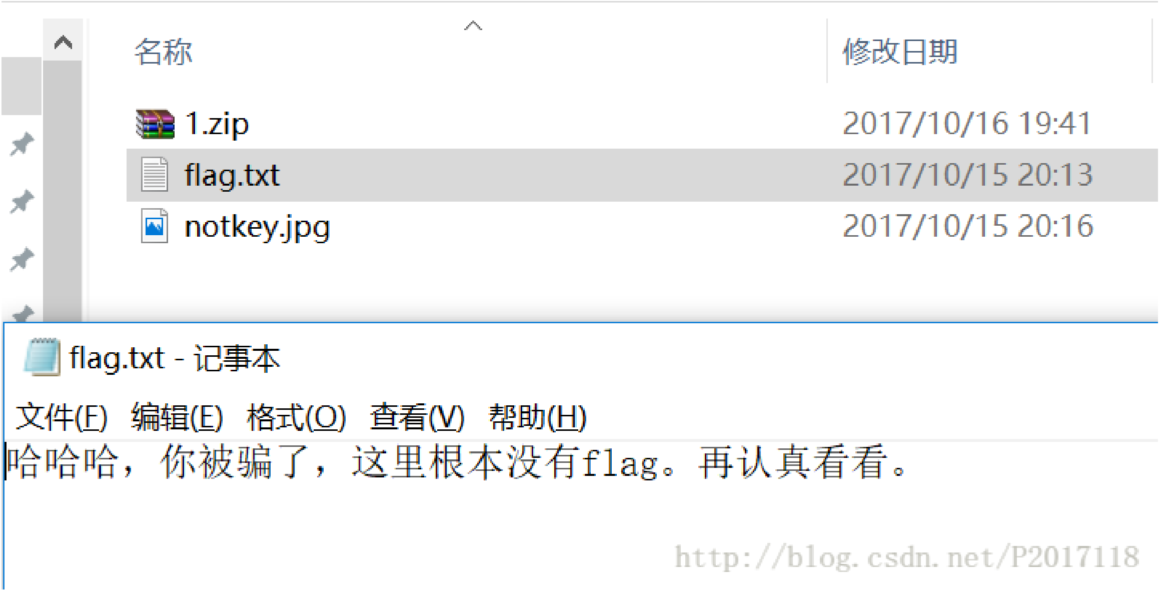
- 一一对应，得到flag


a
b
c
d
e
f
g
h
i
j
k
l
m
n
o
p
q
r
s
t
u
v
w
x
y
z
Baidu百科
http://blog.csdn.net/P2017118

弗拉戈在哪里？

小明整蛊舍友，将他舍友的兰博基尼钥匙锁在zip里面了，你能帮他找回钥匙吗？

- 解压，以1.zip着手（出题人调皮）



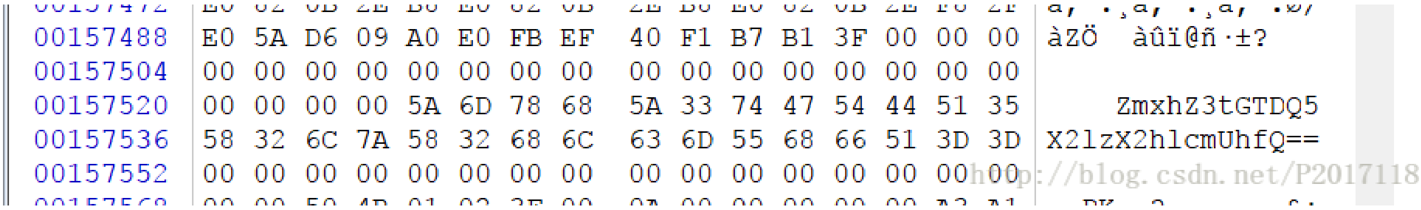
名称	修改日期
1.zip	2017/10/16 19:41
flag.txt	2017/10/15 20:13
notkey.jpg	2017/10/15 20:16

flag.txt - 记事本

哈哈哈，你被骗了，这里根本没有flag。再认真看看。

http://blog.csdn.net/P2017118

- winhex打开1.zip



```
00157488  E0 5A D6 09 A0 E0 FB EF  40 F1 B7 B1 3F 00 00 00  àZÖ  àûï@ñ·±?
00157504  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
00157520  00 00 00 00 5A 6D 78 68  5A 33 74 47 54 44 51 35      ZmxhZ3tGTDQ5
00157536  58 32 6C 7A 58 32 68 6C  63 6D 55 68 66 51 3D 3D  X2lzX2hlcmUhfQ==
00157552  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
```

http://blog.csdn.net/P2017118

- base64解码得到flag

- 补充-常见码制

o Base 64编码：

dGVybWluYXRvcg==

oMD5：9adb6a0e0003fe1293737c39acc824

oSHA-1：ebabb7d2d2120312c0e7c9

o URL编码： %05 %37 %08

o HEX编码：74 65 72 6d 69 6e 61 74 6f 72

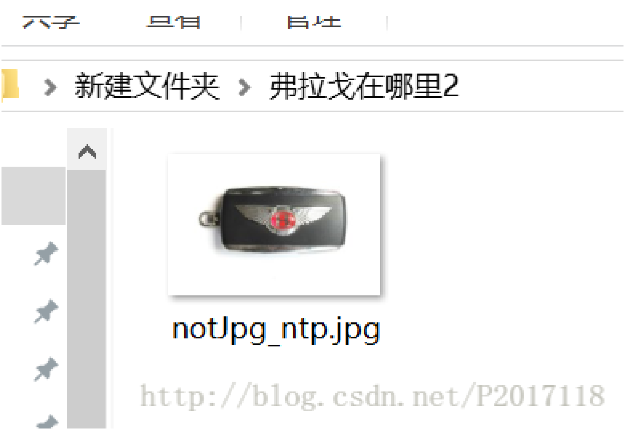
o JsFuck：[]+[+[]]+(![]+[])[!+[]+!+[]]+(!![]+[]

o Html编码：T&#917

o Unicode编码：r《》&#10

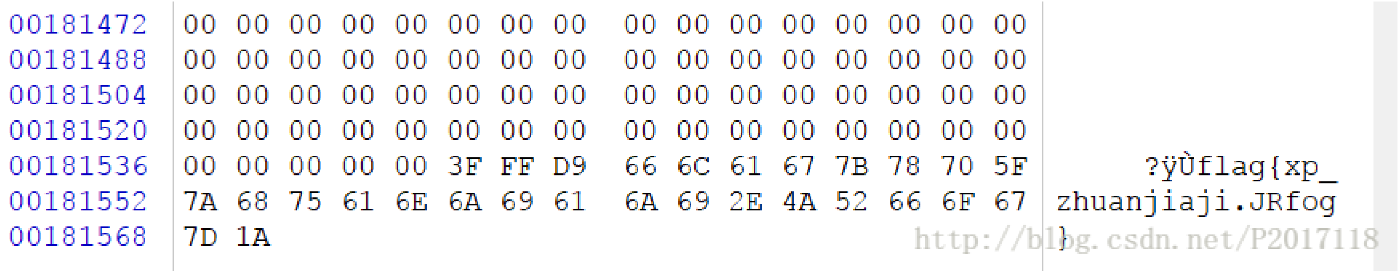
弗拉戈在哪里2?

小明又回来整蛊舍友了，不过这次钥匙他直接归还给舍友了，他说很喜欢这首歌，你知道小明说的是哪一首吗？



http://blog.csdn.net/P2017118

- 用winhex打开



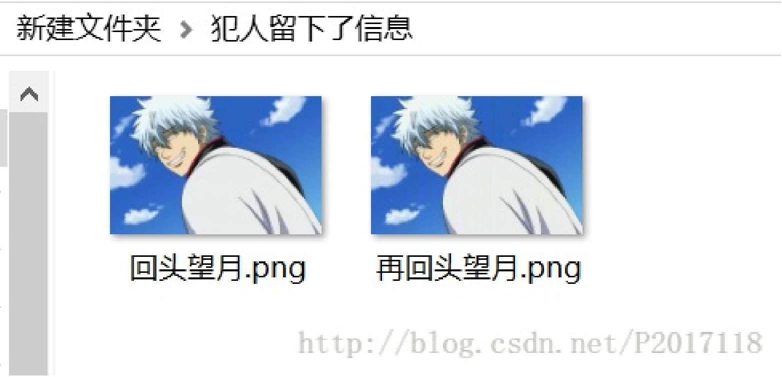
```
00181472  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
00181488  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
00181504  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
00181520  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
00181536  00 00 00 00 00 3F FF D9  66 6C 61 67 7B 78 70 5F        ?ÿÙflag{xp_
00181552  7A 68 75 61 6E 6A 69 61  6A 69 2E 4A 52 66 6F 67   zhuanjiaji.JRfog
00181568  7D 1A                                              }
```

http://blog.csdn.net/P2017118

犯人留下了信息

密室中有三个人，不是你，也不是我，好吧，是他们之中留下了信息而你却看不见，你快要被污死了，怎么办，选择自救吗，擦亮眼睛，答案就在眼前。

Hint1: 盲水印



http://blog.csdn.net/P2017118

解题参考链接：
http://blog.csdn.net/linyacool/article/details/71506638

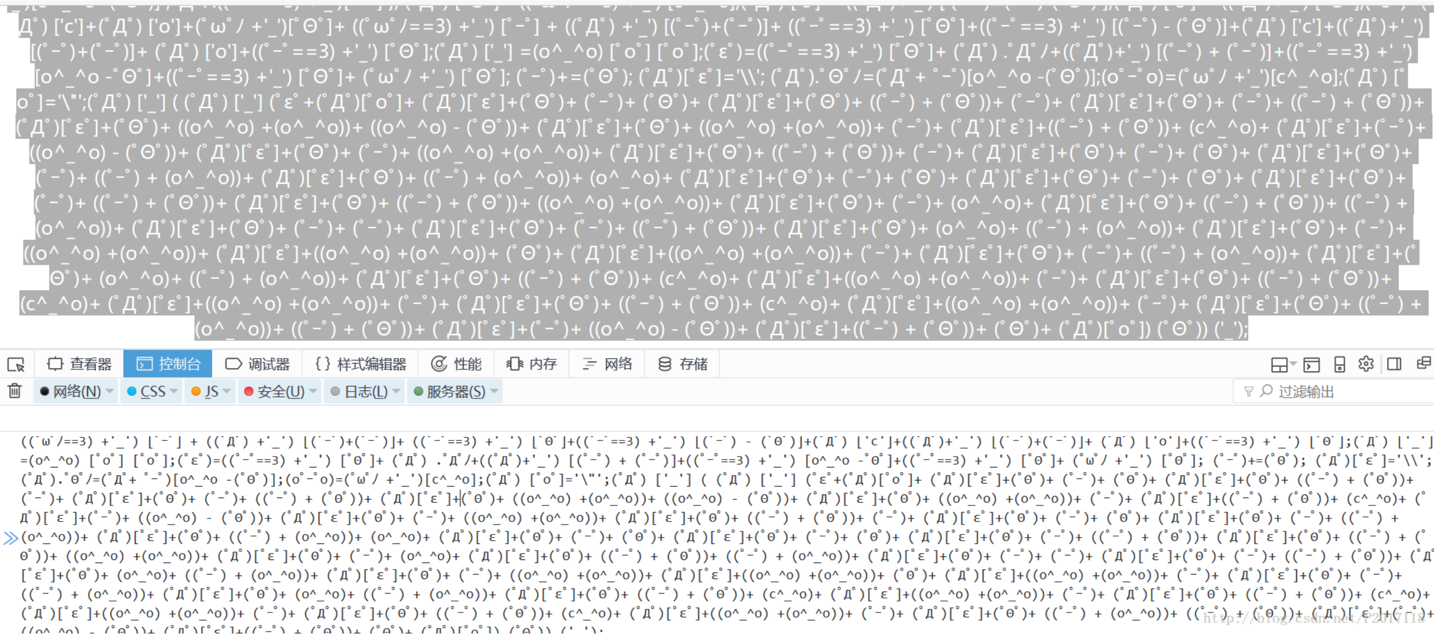
一开始找的是双图隐写，在查资料的时候发现了很多新思路，顺便贴一下链接
http://www.jianshu.com/p/02fdd5edd9fc

Xp0int大家庭

Xp0int日常，跑一下我们在干什么？

题目地址：
http://119.29.191.200/ctf/7fcdb7ba6de74b6e007efe1079540e0228817d26/

- 好多颜文字，复制粘贴后，f12打开开发者工具控制台，得到flag



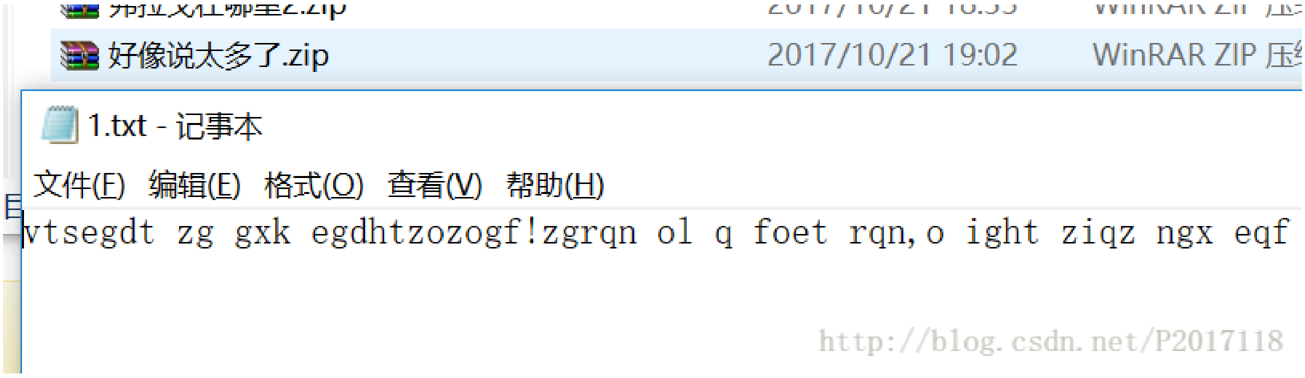
```
Дﾟ) ['c']+(ﾟДﾟ) ['o']+(ﾟωﾟﾉ +'_')[ﾟΘﾟ]+ ((ﾟωﾟﾉ==3) +'_') [ﾟｰﾟ] + ((ﾟДﾟ) +'_') [(ﾟｰﾟ)+(ﾟｰﾟ)]+ ((ﾟｰﾟ==3) +'_') [ﾟΘﾟ]+((ﾟｰﾟ==3) +'_') [(ﾟｰﾟ) - (ﾟΘﾟ)]+(ﾟДﾟ) ['c']+((ﾟДﾟ)+'_')
[(ﾟｰﾟ)+(ﾟｰﾟ)]+ (ﾟДﾟ) ['o']+((ﾟｰﾟ==3) +'_') [ﾟΘﾟ];(ﾟДﾟ) ['_'] =(o^_^o) [ﾟoﾟ] [ﾟoﾟ];(ﾟεﾟ)=((ﾟｰﾟ==3) +'_') [ﾟΘﾟ]+ (ﾟДﾟ) .ﾟДﾟﾉ+((ﾟДﾟ)+'_') [(ﾟｰﾟ) + (ﾟｰﾟ)]+((ﾟｰﾟ==3) +'_')
[o^_^o -ﾟΘﾟ]+((ﾟｰﾟ==3) +'_') [ﾟΘﾟ]+ (ﾟωﾟﾉ +'_') [ﾟΘﾟ]; (ﾟｰﾟ)+=(ﾟΘﾟ); (ﾟДﾟ)[ﾟεﾟ]='\\'; (ﾟДﾟ).ﾟΘﾟﾉ=(ﾟДﾟ+ ﾟｰﾟ)[o^_^o -(ﾟΘﾟ)];(oﾟｰﾟo)=(ﾟωﾟﾉ +'_')[c^_^o];(ﾟДﾟ) [ﾟ
oﾟ]='\"';(ﾟДﾟ) ['_'] ( (ﾟДﾟ) ['_'] (ﾟεﾟ+(ﾟДﾟ)[ﾟoﾟ]+ (ﾟДﾟ)[ﾟεﾟ]+(ﾟΘﾟ)+ (ﾟｰﾟ)+ (ﾟΘﾟ)+ (ﾟДﾟ)[ﾟεﾟ]+(ﾟΘﾟ)+ ((ﾟｰﾟ) + (ﾟΘﾟ))+ (ﾟｰﾟ)+ (ﾟДﾟ)[ﾟεﾟ]+(ﾟΘﾟ)+ (ﾟｰﾟ)+ ((ﾟｰﾟ) + (ﾟΘﾟ))+
(ﾟДﾟ)[ﾟεﾟ]+(ﾟΘﾟ)+ ((o^_^o) +(o^_^o))+ ((o^_^o) - (ﾟΘﾟ))+ (ﾟДﾟ)[ﾟεﾟ]+(ﾟΘﾟ)+ ((o^_^o) +(o^_^o))+ (ﾟｰﾟ)+ (ﾟДﾟ)[ﾟεﾟ]+((ﾟｰﾟ) + (ﾟΘﾟ))+ (c^_^o)+ (ﾟДﾟ)[ﾟεﾟ]+(ﾟｰﾟ)+
((o^_^o) - (ﾟΘﾟ))+ (ﾟДﾟ)[ﾟεﾟ]+(ﾟΘﾟ)+ (ﾟｰﾟ)+ ((o^_^o) +(o^_^o))+ (ﾟДﾟ)[ﾟεﾟ]+(ﾟΘﾟ)+ ((ﾟｰﾟ) + (ﾟΘﾟ))+ (ﾟｰﾟ)+ (ﾟДﾟ)[ﾟεﾟ]+(ﾟΘﾟ)+ (ﾟｰﾟ)+ (ﾟΘﾟ)+ (ﾟДﾟ)[ﾟεﾟ]+(ﾟΘﾟ)+
(ﾟｰﾟ)+ ((ﾟｰﾟ) + (o^_^o))+ (ﾟДﾟ)[ﾟεﾟ]+(ﾟΘﾟ)+ ((ﾟｰﾟ) + (o^_^o))+ (o^_^o)+ (ﾟДﾟ)[ﾟεﾟ]+(ﾟΘﾟ)+ (ﾟｰﾟ)+ (ﾟΘﾟ)+ (ﾟДﾟ)[ﾟεﾟ]+(ﾟΘﾟ)+ (ﾟｰﾟ)+ (ﾟΘﾟ)+ (ﾟДﾟ)[ﾟεﾟ]+(ﾟΘﾟ)+
(ﾟｰﾟ)+ ((ﾟｰﾟ) + (ﾟΘﾟ))+ (ﾟДﾟ)[ﾟεﾟ]+(ﾟΘﾟ)+ ((ﾟｰﾟ) + (ﾟΘﾟ))+ ((o^_^o) +(o^_^o))+ (ﾟДﾟ)[ﾟεﾟ]+(ﾟΘﾟ)+ (ﾟｰﾟ)+ (o^_^o)+ (ﾟДﾟ)[ﾟεﾟ]+(ﾟΘﾟ)+ ((ﾟｰﾟ) + (ﾟΘﾟ))+ ((ﾟｰﾟ) +
(o^_^o))+ (ﾟДﾟ)[ﾟεﾟ]+(ﾟΘﾟ)+ (ﾟｰﾟ)+ (ﾟｰﾟ)+ (ﾟДﾟ)[ﾟεﾟ]+(ﾟΘﾟ)+ (ﾟｰﾟ)+ ((ﾟｰﾟ) + (ﾟΘﾟ))+ (ﾟДﾟ)[ﾟεﾟ]+(ﾟΘﾟ)+ (o^_^o)+ ((ﾟｰﾟ) + (o^_^o))+ (ﾟДﾟ)[ﾟεﾟ]+(ﾟΘﾟ)+ (ﾟｰﾟ)+
((o^_^o) +(o^_^o))+ (ﾟДﾟ)[ﾟεﾟ]+((o^_^o) +(o^_^o))+ (ﾟΘﾟ)+ (ﾟДﾟ)[ﾟεﾟ]+((o^_^o) +(o^_^o))+ (ﾟｰﾟ)+ (ﾟДﾟ)[ﾟεﾟ]+(ﾟΘﾟ)+ (ﾟｰﾟ)+ ((ﾟｰﾟ) + (o^_^o))+ (ﾟДﾟ)[ﾟεﾟ]+(ﾟ
Θﾟ)+ (o^_^o)+ ((ﾟｰﾟ) + (o^_^o))+ (ﾟДﾟ)[ﾟεﾟ]+(ﾟΘﾟ)+ ((ﾟｰﾟ) + (ﾟΘﾟ))+ (c^_^o)+ (ﾟДﾟ)[ﾟεﾟ]+((o^_^o) +(o^_^o))+ (ﾟｰﾟ)+ (ﾟДﾟ)[ﾟεﾟ]+(ﾟΘﾟ)+ ((ﾟｰﾟ) + (ﾟΘﾟ))+
(c^_^o)+ (ﾟДﾟ)[ﾟεﾟ]+((o^_^o) +(o^_^o))+ (ﾟｰﾟ)+ (ﾟДﾟ)[ﾟεﾟ]+(ﾟΘﾟ)+ ((ﾟｰﾟ) + (ﾟΘﾟ))+ (c^_^o)+ (ﾟДﾟ)[ﾟεﾟ]+((o^_^o) +(o^_^o))+ (ﾟｰﾟ)+ (ﾟДﾟ)[ﾟεﾟ]+(ﾟΘﾟ)+ ((ﾟｰﾟ) +
(o^_^o))+ ((ﾟｰﾟ) + (ﾟΘﾟ))+ (ﾟДﾟ)[ﾟεﾟ]+(ﾟｰﾟ)+ ((o^_^o) - (ﾟΘﾟ))+ (ﾟДﾟ)[ﾟεﾟ]+((ﾟｰﾟ) + (ﾟΘﾟ))+ (ﾟΘﾟ)+ (ﾟДﾟ)[ﾟoﾟ]) (ﾟΘﾟ)) ('_');
```

```
((ﾟωﾟﾉ==3) +'_') [ﾟｰﾟ] + ((ﾟДﾟ) +'_') [(ﾟｰﾟ)+(ﾟｰﾟ)]+ ((ﾟｰﾟ==3) +'_') [ﾟΘﾟ]+((ﾟｰﾟ==3) +'_') [(ﾟｰﾟ) - (ﾟΘﾟ)]+(ﾟДﾟ) ['c']+((ﾟДﾟ)+'_') [(ﾟｰﾟ)+(ﾟｰﾟ)]+ (ﾟДﾟ) ['o']+((ﾟｰﾟ==3) +'_') [ﾟΘﾟ];(ﾟДﾟ) ['_']
=(o^_^o) [ﾟoﾟ] [ﾟoﾟ];(ﾟεﾟ)=((ﾟｰﾟ==3) +'_') [ﾟΘﾟ]+ (ﾟДﾟ) .ﾟДﾟﾉ+((ﾟДﾟ)+'_') [(ﾟｰﾟ) + (ﾟｰﾟ)]+((ﾟｰﾟ==3) +'_') [o^_^o -ﾟΘﾟ]+((ﾟｰﾟ==3) +'_') [ﾟΘﾟ]+ (ﾟωﾟﾉ +'_') [ﾟΘﾟ]; (ﾟｰﾟ)+=(ﾟΘﾟ); (ﾟДﾟ)[ﾟεﾟ]='\\';
(ﾟДﾟ).ﾟΘﾟﾉ=(ﾟДﾟ+ ﾟｰﾟ)[o^_^o -(ﾟΘﾟ)];(oﾟｰﾟo)=(ﾟωﾟﾉ +'_')[c^_^o];(ﾟДﾟ) [ﾟoﾟ]='\"';(ﾟДﾟ) ['_'] ( (ﾟДﾟ) ['_'] (ﾟεﾟ+(ﾟДﾟ)[ﾟoﾟ]+ (ﾟДﾟ)[ﾟεﾟ]+(ﾟΘﾟ)+ (ﾟｰﾟ)+ (ﾟΘﾟ)+ (ﾟДﾟ)[ﾟεﾟ]+(ﾟΘﾟ)+ ((ﾟｰﾟ) + (ﾟΘﾟ))+
(ﾟｰﾟ)+ (ﾟДﾟ)[ﾟεﾟ]+(ﾟΘﾟ)+ (ﾟｰﾟ)+ ((ﾟｰﾟ) + (ﾟΘﾟ))+ (ﾟДﾟ)[ﾟεﾟ]+(ﾟΘﾟ)+ ((o^_^o) +(o^_^o))+ ((o^_^o) - (ﾟΘﾟ))+ (ﾟДﾟ)[ﾟεﾟ]+(ﾟΘﾟ)+ ((o^_^o) +(o^_^o))+ (ﾟｰﾟ)+ (ﾟДﾟ)[ﾟεﾟ]+((ﾟｰﾟ) + (ﾟΘﾟ))+ (c^_^o)+ (ﾟ
Дﾟ)[ﾟεﾟ]+(ﾟｰﾟ)+ ((o^_^o) - (ﾟΘﾟ))+ (ﾟДﾟ)[ﾟεﾟ]+(ﾟΘﾟ)+ (ﾟｰﾟ)+ ((o^_^o) +(o^_^o))+ (ﾟДﾟ)[ﾟεﾟ]+(ﾟΘﾟ)+ ((ﾟｰﾟ) + (ﾟΘﾟ))+ (ﾟｰﾟ)+ (ﾟДﾟ)[ﾟεﾟ]+(ﾟΘﾟ)+ (ﾟｰﾟ)+ (ﾟΘﾟ)+ (ﾟДﾟ)[ﾟεﾟ]+(ﾟΘﾟ)+ (ﾟｰﾟ)+ ((ﾟｰﾟ) +
(o^_^o))+ (ﾟДﾟ)[ﾟεﾟ]+(ﾟΘﾟ)+ ((ﾟｰﾟ) + (o^_^o))+ (o^_^o)+ (ﾟДﾟ)[ﾟεﾟ]+(ﾟΘﾟ)+ (ﾟｰﾟ)+ (ﾟΘﾟ)+ (ﾟДﾟ)[ﾟεﾟ]+(ﾟΘﾟ)+ (ﾟｰﾟ)+ (ﾟΘﾟ)+ (ﾟДﾟ)[ﾟεﾟ]+(ﾟΘﾟ)+ (ﾟｰﾟ)+ ((ﾟｰﾟ) + (ﾟΘﾟ))+ (ﾟДﾟ)[ﾟεﾟ]+(ﾟΘﾟ)+ ((ﾟｰﾟ) + (ﾟ
Θﾟ))+ ((o^_^o) +(o^_^o))+ (ﾟДﾟ)[ﾟεﾟ]+(ﾟΘﾟ)+ (ﾟｰﾟ)+ (o^_^o)+ (ﾟДﾟ)[ﾟεﾟ]+(ﾟΘﾟ)+ ((ﾟｰﾟ) + (ﾟΘﾟ))+ ((ﾟｰﾟ) + (o^_^o))+ (ﾟДﾟ)[ﾟεﾟ]+(ﾟΘﾟ)+ (ﾟｰﾟ)+ (ﾟｰﾟ)+ (ﾟДﾟ)[ﾟεﾟ]+(ﾟΘﾟ)+ (ﾟｰﾟ)+ ((ﾟｰﾟ) + (ﾟΘﾟ))+ (ﾟДﾟ)
[ﾟεﾟ]+(ﾟΘﾟ)+ (o^_^o)+ ((ﾟｰﾟ) + (o^_^o))+ (ﾟДﾟ)[ﾟεﾟ]+(ﾟΘﾟ)+ (ﾟｰﾟ)+ ((o^_^o) +(o^_^o))+ (ﾟДﾟ)[ﾟεﾟ]+((o^_^o) +(o^_^o))+ (ﾟΘﾟ)+ (ﾟДﾟ)[ﾟεﾟ]+((o^_^o) +(o^_^o))+ (ﾟｰﾟ)+ (ﾟДﾟ)[ﾟεﾟ]+(ﾟΘﾟ)+ (ﾟｰﾟ)+
((ﾟｰﾟ) + (o^_^o))+ (ﾟДﾟ)[ﾟεﾟ]+(ﾟΘﾟ)+ (o^_^o)+ ((ﾟｰﾟ) + (o^_^o))+ (ﾟДﾟ)[ﾟεﾟ]+(ﾟΘﾟ)+ ((ﾟｰﾟ) + (ﾟΘﾟ))+ (c^_^o)+ (ﾟДﾟ)[ﾟεﾟ]+((o^_^o) +(o^_^o))+ (ﾟｰﾟ)+ (ﾟДﾟ)[ﾟεﾟ]+(ﾟΘﾟ)+ ((ﾟｰﾟ) + (ﾟΘﾟ))+ (c^_^o)+
(ﾟДﾟ)[ﾟεﾟ]+((o^_^o) +(o^_^o))+ (ﾟｰﾟ)+ (ﾟДﾟ)[ﾟεﾟ]+(ﾟΘﾟ)+ ((ﾟｰﾟ) + (ﾟΘﾟ))+ (c^_^o)+ (ﾟДﾟ)[ﾟεﾟ]+((o^_^o) +(o^_^o))+ (ﾟｰﾟ)+ (ﾟДﾟ)[ﾟεﾟ]+(ﾟΘﾟ)+ ((ﾟｰﾟ) + (o^_^o))+ ((ﾟｰﾟ) + (ﾟΘﾟ))+ (ﾟДﾟ)[ﾟεﾟ]+(ﾟｰﾟ)+
((o^_^o) - (ﾟΘﾟ))+ (ﾟДﾟ)[ﾟεﾟ]+((ﾟｰﾟ) + (ﾟΘﾟ))+ (ﾟΘﾟ)+ (ﾟДﾟ)[ﾟoﾟ]) (ﾟΘﾟ)) ('_');
```

http://blog.csdn.net/P2017118

解题参考链接：
http://blog.csdn.net/u012763794/article/details/50959166基础篇第5点

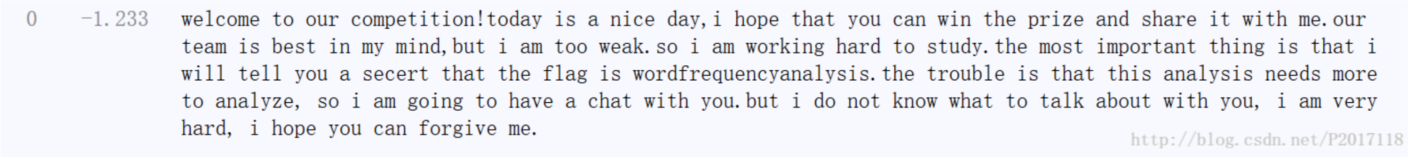
好像说太多了



```
vtsegdt zg gxk egdhtzozogf!zgrqn ol q foet rqn,o ight ziqz ngx eqf
```

http://blog.csdn.net/P2017118

- 打开文件发现是一串乱序英文字母，且有标点，猜测是一段话打乱，替代解密。（话痨，鉴定完毕）

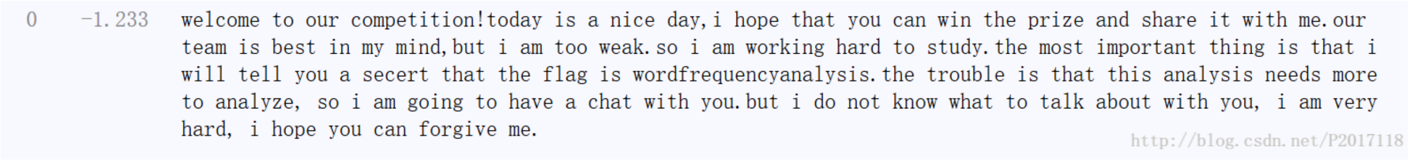


```
0    -1.233    welcome to our competition!today is a nice day,i hope that you can win the prize and share it with me.our
               team is best in my mind,but i am too weak.so i am working hard to study.the most important thing is that i
               will tell you a secert that the flag is wordfrequencyanalysis.the trouble is that this analysis needs more
               to analyze, so i am going to have a chat with you.but i do not know what to talk about with you, i am very
               hard, i hope you can forgive me.
```

http://blog.csdn.net/P2017118

解题参考链接:
https://quipqiup.com/

EasyRSA



```
0    -1.233    welcome to our competition!today is a nice day,i hope that you can win the prize and share it with me.our
               team is best in my mind,but i am too weak.so i am working hard to study.the most important thing is that i
               will tell you a secert that the flag is wordfrequencyanalysis.the trouble is that this analysis needs more
               to analyze, so i am going to have a chat with you.but i do not know what to talk about with you, i am very
               hard, i hope you can forgive me.
```

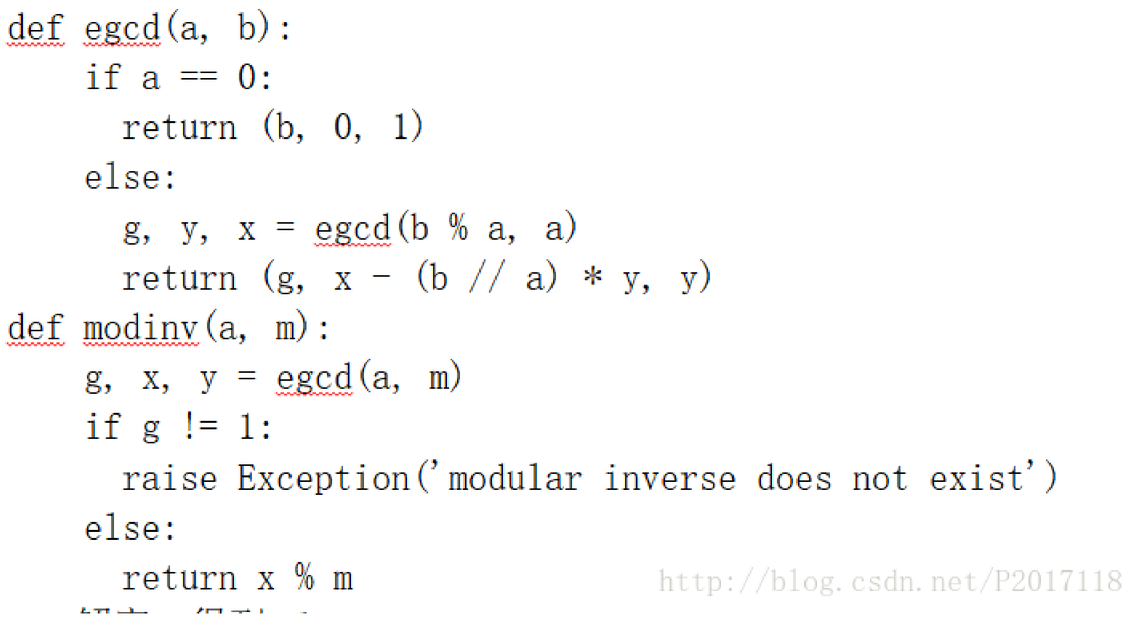
http://blog.csdn.net/P2017118

• 模数分解

o 如果n比较小，那么可以通过工具进行直接n分解，从而得到私钥。如果n的大小小于256bit，那么我们通过本地工具即可爆破成功。例如采用windows平台的RSATool2v17，可以在几分钟内完成256bit的n的分解。

o 如果n在768bit或者更高，可以尝试使用一些在线的n分解网站，这些网站会存储一些已经分解成功的n，比如：http://factordb.com

• 知道e，p，q的情况下，可以解出d：



```
def egcd(a, b):
    if a == 0:
      return (b, 0, 1)
    else:
      g, y, x = egcd(b % a, a)
      return (g, x - (b // a) * y, y)
def modinv(a, m):
    g, x, y = egcd(a, m)
    if g != 1:
      raise Exception(’modular inverse does not exist’)
    else:
      return x % m
```

http://blog.csdn.net/P2017118

• RSA解密，得到flag

• 解题参考链接：
http://bobao.360.cn/learning/detail/3058.html

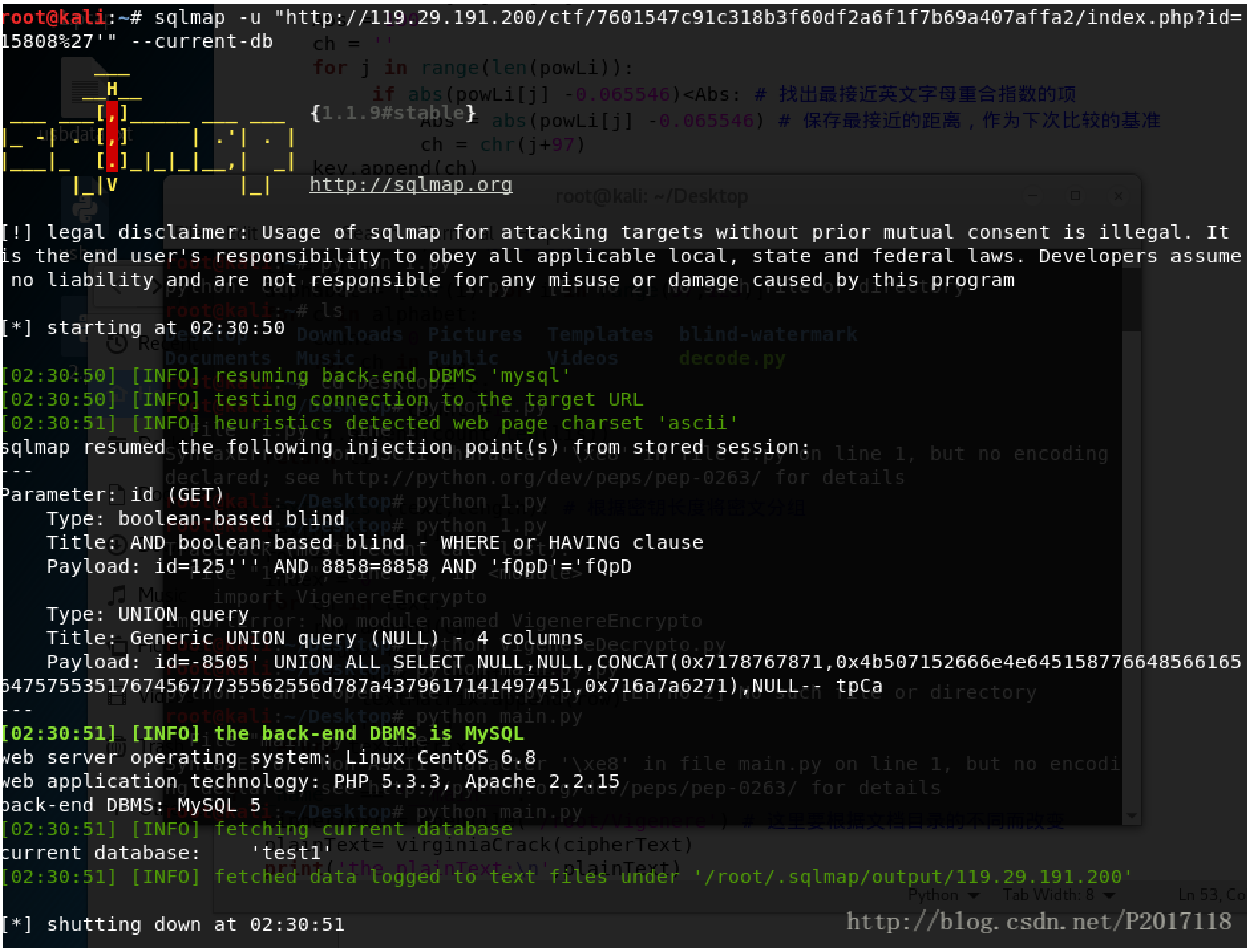
一个简陋的博客 Web

前端的X同学做一半跑路了，反正功能实现了，能上传文章就行（逃。。。

题目地址：
http://119.29.191.200/ctf/7601547c91c318b3f60df2a6f1f7b69a407affa2/

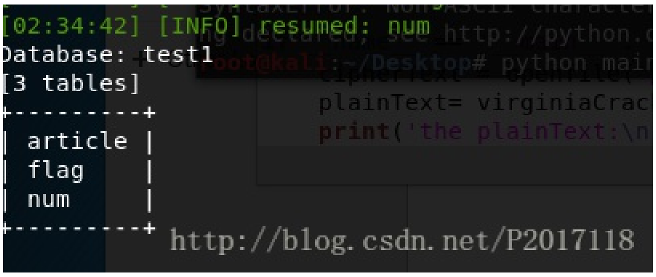
• sql注入，尝试后发现未过滤单引号，找到注入点

- 使用sqlmap，发现database是test1



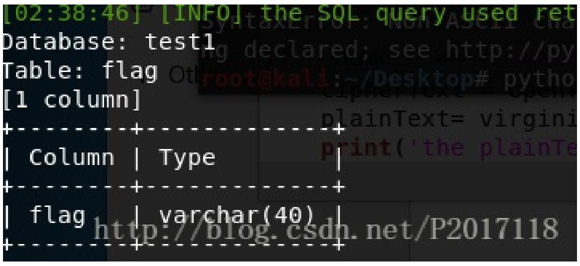
```
root@kali:~# sqlmap -u "http://119.29.191.200/ctf/7601547c91c318b3f60df2a6f1f7b69a407affa2/index.php?id=
15808%27'" --current-db
        ___
       __H__
 ___ ___[,]_____ ___ ___  {1.1.9#stable}
|_ -| . [,]     | .'| . |
|___|_  [.]_|_|_|__,|  _|
      |_|V          |_|   http://sqlmap.org

[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal. It
is the end user's responsibility to obey all applicable local, state and federal laws. Developers assume
 no liability and are not responsible for any misuse or damage caused by this program

[*] starting at 02:30:50

[02:30:50] [INFO] resuming back-end DBMS 'mysql'
[02:30:50] [INFO] testing connection to the target URL
[02:30:51] [INFO] heuristics detected web page charset 'ascii'
sqlmap resumed the following injection point(s) from stored session:
---
Parameter: id (GET)
    Type: boolean-based blind
    Title: AND boolean-based blind - WHERE or HAVING clause
    Payload: id=125''' AND 8858=8858 AND 'fQpD'='fQpD

    Type: UNION query
    Title: Generic UNION query (NULL) - 4 columns
    Payload: id=-8505' UNION ALL SELECT NULL,NULL,CONCAT(0x7178767871,0x4b507152666e4e6451587766485661656
4757553517674567773556256d787a4379617141497451,0x716a7a6271),NULL-- tpCa
---
[02:30:51] [INFO] the back-end DBMS is MySQL
web server operating system: Linux CentOS 6.8
web application technology: PHP 5.3.3, Apache 2.2.15
back-end DBMS: MySQL 5
[02:30:51] [INFO] fetching current database
current database:    'test1'
[02:30:51] [INFO] fetched data logged to text files under '/root/.sqlmap/output/119.29.191.200'

[*] shutting down at 02:30:51
```

http://blog.csdn.net/P2017118



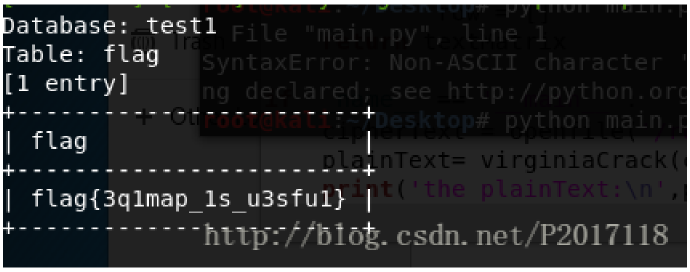
```
[02:34:42] [INFO] resumed: num
Database: test1
[3 tables]
+---------+
| article |
| flag    |
| num     |
+---------+
```

http://blog.csdn.net/P2017118



```
[02:38:46] [INFO] the SQL query used ret
Database: test1
Table: flag
[1 column]
+--------+-------------+
| Column | Type        |
+--------+-------------+
| flag   | varchar(40) |
+--------+-------------+
```

http://blog.csdn.net/P2017118



```
Database: test1
Table: flag
[1 entry]
+-----------------------+
| flag                  |
+-----------------------+
| flag{3q1map_1s_u3sful} |
+-----------------------+
```

http://blog.csdn.net/P2017118

- 补充-sqlmap基本命令

o sqlmap -u “http://119.29.191.200/ctf/7601547c91c318b3f60df2a6f1f7b69a407affa2/index.php?id=15808%27‘” –current-db

o qlmap -u “http://119.29.191.200/ctf/7601547c91c318b3f60df2a6f1f7b69a407affa2/index.php?id=15808%27‘” -D test1 –tables

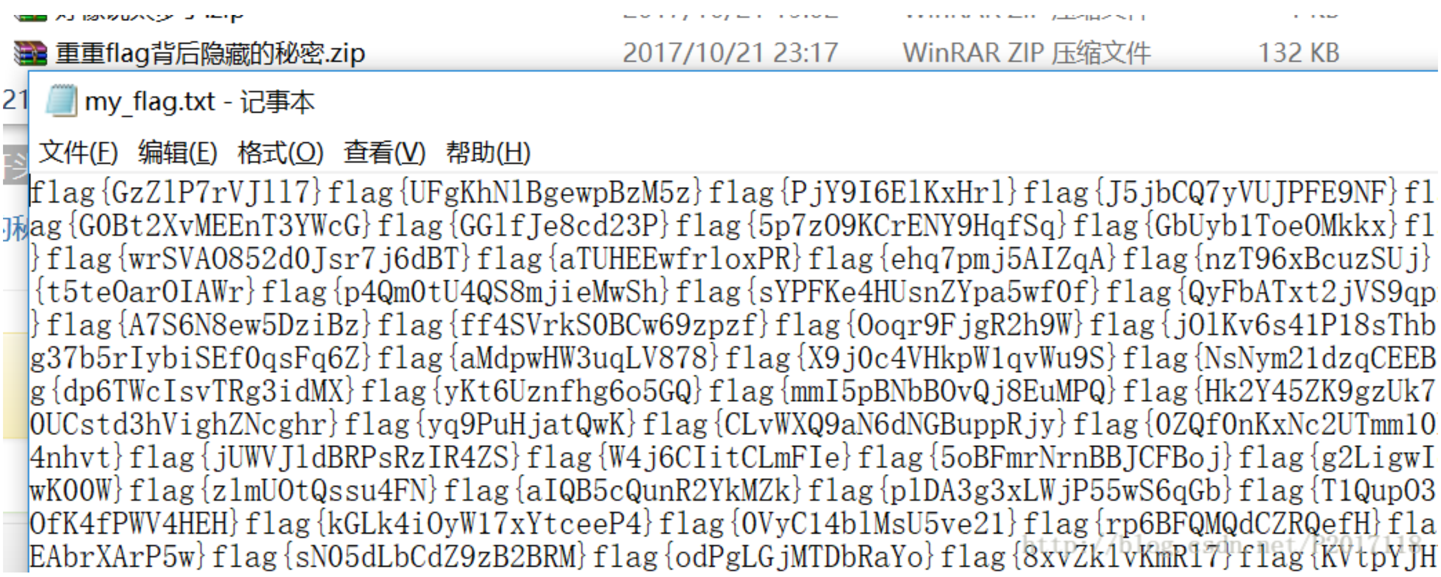
o sqlmap -u “http://119.29.191.200/ctf/7601547c91c318b3f60df2a6f1f7b69a407affa2/index.php?id=15808%27‘” -D test1 -T flag –columns

o sqlmap -u “http://119.29.191.200/ctf/7601547c91c318b3f60df2a6f1f7b69a407affa2/index.php?id=15808%27‘” -D test1 -T flag -C flag –dump

重重flag背后隐藏的秘密

据说：真正的flag开头三位和结尾均为数字，第4位和倒数第3位为大写字母，聪明的你能找到它吗？

- 打开文件，猜测是使用正则表达式找到符合要求的flag

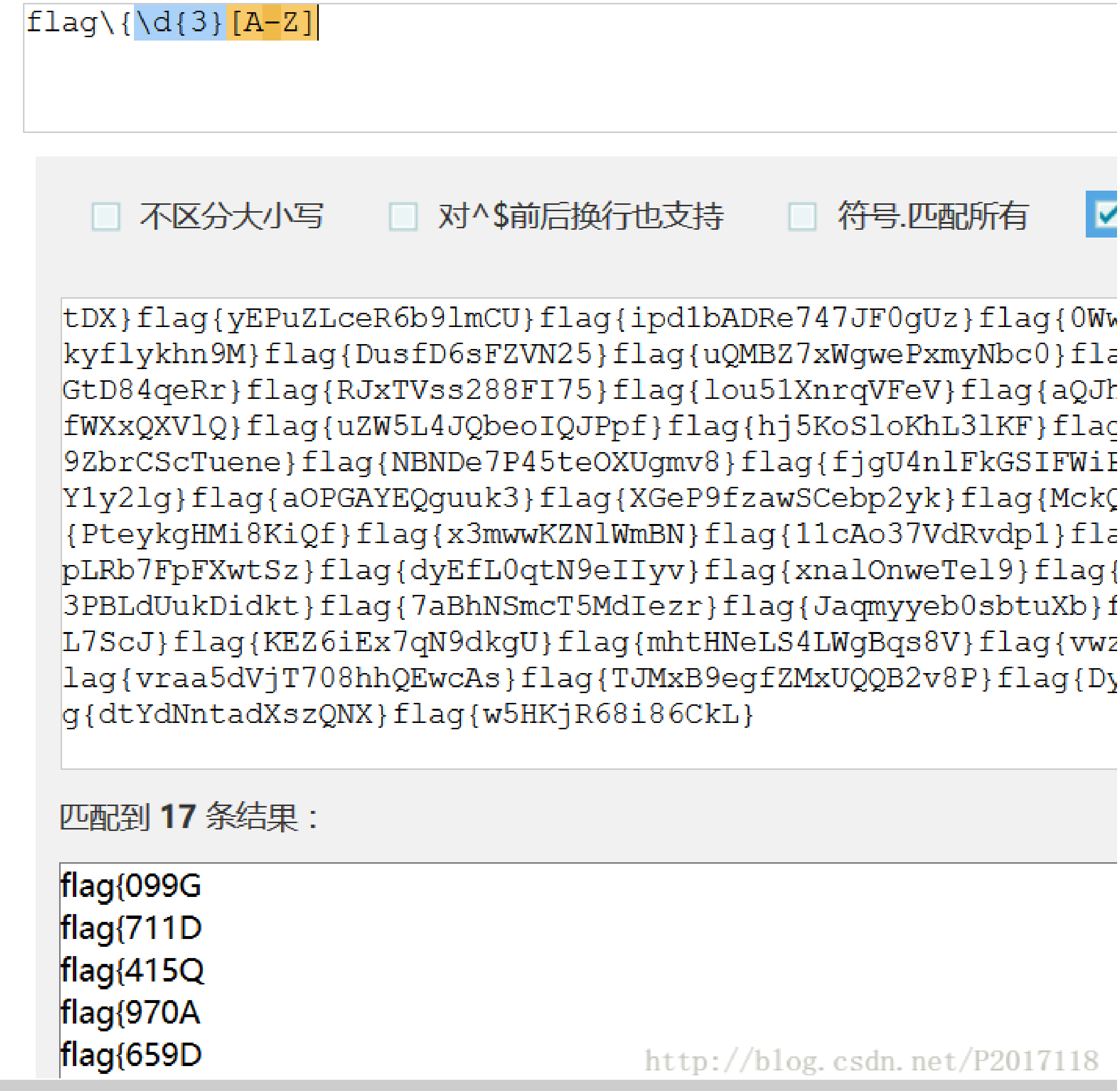


重重flag背后隐藏的秘密.zip
2017/10/21 23:17
WinRAR ZIP 压缩文件
132 KB
my_flag.txt - 记事本
文件(F) 编辑(E) 格式(O) 查看(V) 帮助(H)

```
flag{GzZ1P7rVJ117}flag{UFgKhN1BgewpBzM5z}flag{PjY9I6E1KxHr1}flag{J5jbCQ7yVUJPFE9NF}fl
ag{G0Bt2XvMEEnT3YWcG}flag{GG1fJe8cd23P}flag{5p7z09KCrENY9HqfSq}flag{GbUyb1Toe0Mkkx}fl
}flag{wrSVA0852d0Jsr7j6dBT}flag{aTUHEEwfrloxPR}flag{ehq7pmj5AIZqA}flag{nzT96xBcuzSUj}
{t5te0ar0IAWr}flag{p4Qm0tU4QS8mjieMwSh}flag{sYPFKe4HUsnZYpa5wf0f}flag{QyFbATxt2jVS9qp
}flag{A7S6N8ew5DziBz}flag{ff4SVrkS0BCw69zpzf}flag{0oqr9FjgR2h9W}flag{j01Kv6s41P18sThb
g37b5rIybiSEf0qsFq6Z}flag{aMdpwHW3uqLV878}flag{X9j0c4VHkpW1qvWu9S}flag{NsNym21dzqCEEB
g{dp6TWcIsvTRg3idMX}flag{yKt6Uznfhg6o5GQ}flag{mmI5pBNbB0vQj8EuMPQ}flag{Hk2Y45ZK9gzUk7
0UCstd3hVighZNcghr}flag{yq9PuHjatQwK}flag{CLvWXQ9aN6dNGBuppRjy}flag{0ZQf0nKxNc2UTmm10
4nhvt}flag{jUWVJ1dBRPsRzIR4ZS}flag{W4j6CIitCLmFIe}flag{5oBFmrNrnBBJCFBoj}flag{g2LigwI
wK00W}flag{z1mU0tQssu4FN}flag{aIQB5cQunR2YkMZk}flag{p1DA3g3xLWjP55wS6qGb}flag{T1Qup03
0fK4fPWV4HEH}flag{kGLk4i0yW17xYtceeP4}flag{0VyC14b1MsU5ve21}flag{rp6BFQMQdCZRQefH}fla
EAbrXArP5w}flag{sN05dLbCdZ9zB2BRM}flag{odPgLGjMTDbRaYo}flag{8xvZk1vKmR17}flag{KVtpYJH
```

http://blog.csdn.net/P2017118

- 不会正则，只能筛到17条flag，接下来就是ctrl+f了



```
flag\{\d{3}[A-Z]
```

□ 不区分大小写 □ 对^$前后换行也支持 □ 符号.匹配所有 ☑

```
tDX}flag{yEPuZLceR6b9lmCU}flag{ipd1bADRe747JF0gUz}flag{0Ww
kyflykhn9M}flag{DusfD6sFZVN25}flag{uQMBZ7xWgwePxmyNbc0}fla
GtD84qeRr}flag{RJxTVss288FI75}flag{lou51XnrqVFeV}flag{aQJ
fWXxQXV1Q}flag{uZW5L4JQbeoIQJPpf}flag{hj5KoSloKhL31KF}flag
9ZbrCScTuene}flag{NBNDe7P45teOXUgmv8}flag{fjgU4nlFkGSIFWi
Y1y2lg}flag{aOPGAYEQguuk3}flag{XGeP9fzawSCebp2yk}flag{Mck
{PteykgHMi8KiQf}flag{x3mwwKZNlWmBN}flag{11cAo37VdRvdp1}fla
pLRb7FpFXwtSz}flag{dyEfL0qtN9eIIyv}flag{xnalOnweTel9}flag{
3PBLdUukDidkt}flag{7aBhNSmcT5MdIezr}flag{Jaqmyyeb0sbtuXb}f
L7ScJ}flag{KEZ6iEx7qN9dkgU}flag{mhtHNeLS4LWgBqs8V}flag{vwz
lag{vraa5dVjT708hhQEwcAs}flag{TJMxB9egfZMxUQQB2v8P}flag{Dy
g{dtYdNntadXszQNX}flag{w5HKjR68i86CkL}
```

匹配到 **17** 条结果：

```
flag{099G
flag{711D
flag{415Q
flag{970A
flag{659D
```

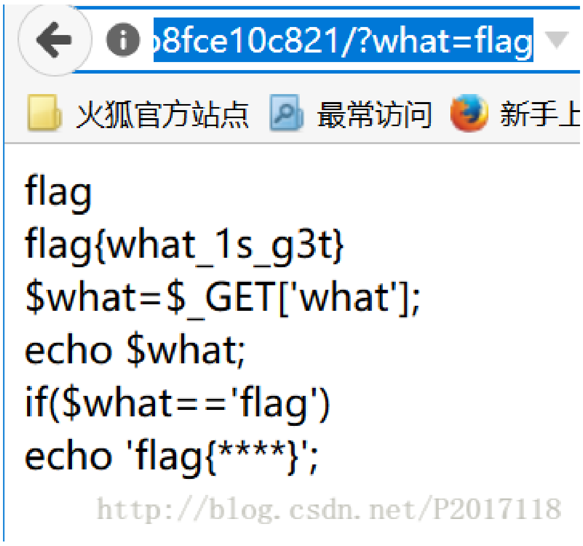
http://blog.csdn.net/P2017118

《web安全入门第一课》

X同学不懂什么是get请求，请教Y同学，Y同学叫他上网看，并丢给他一个网站实践…

题目地址：
http://119.29.191.200/ctf/2f83ff6a6a77e7aca11c87d1ee6f9b8fce10c821/

- Get请求，在url中使what=flag即可



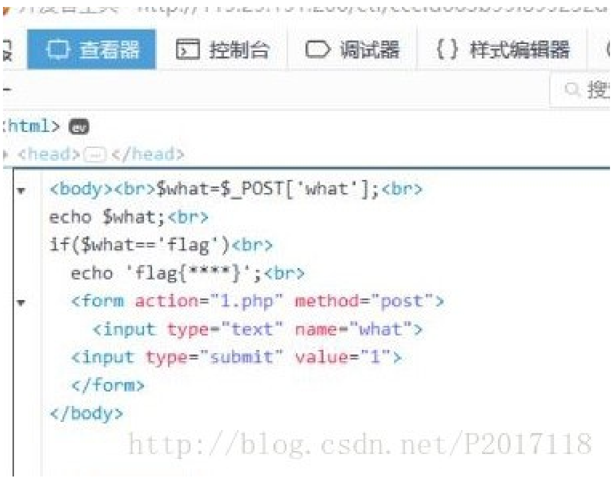
```
flag
flag{what_1s_g3t}
$what=$_GET['what'];
echo $what;
if($what=='flag')
echo 'flag{****}';
```

http://blog.csdn.net/P2017118

《web安全入门第二课》

X同学学完了get请求，又开始好奇什么是post请求，请教y同学，y同学又丢给他一个网站实践….

题目地址：
http://119.29.191.200/ctf/cccfd063b99f899232d571d89d3f832308c0d0bc/

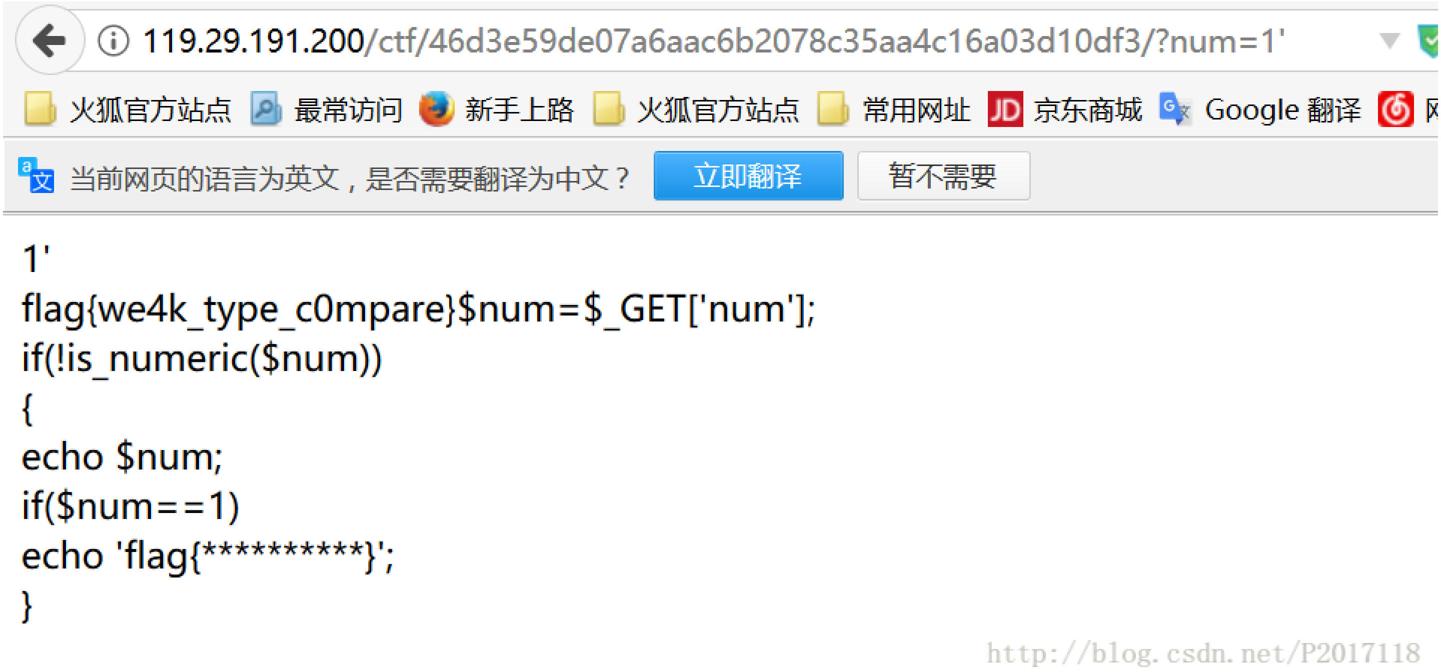


```
<html>
  <head></head>
  <body><br>$what=$_POST['what'];<br>
  echo $what;<br>
  if($what=='flag')<br>
    echo 'flag{****}';<br>
    <form action="1.php" method="post">
      <input type="text" name="what">
    <input type="submit" value="1">
    </form>
  </body>
```

http://blog.csdn.net/P2017118

一段矛盾的代码

这段代码好矛盾，真的能得到flag吗？

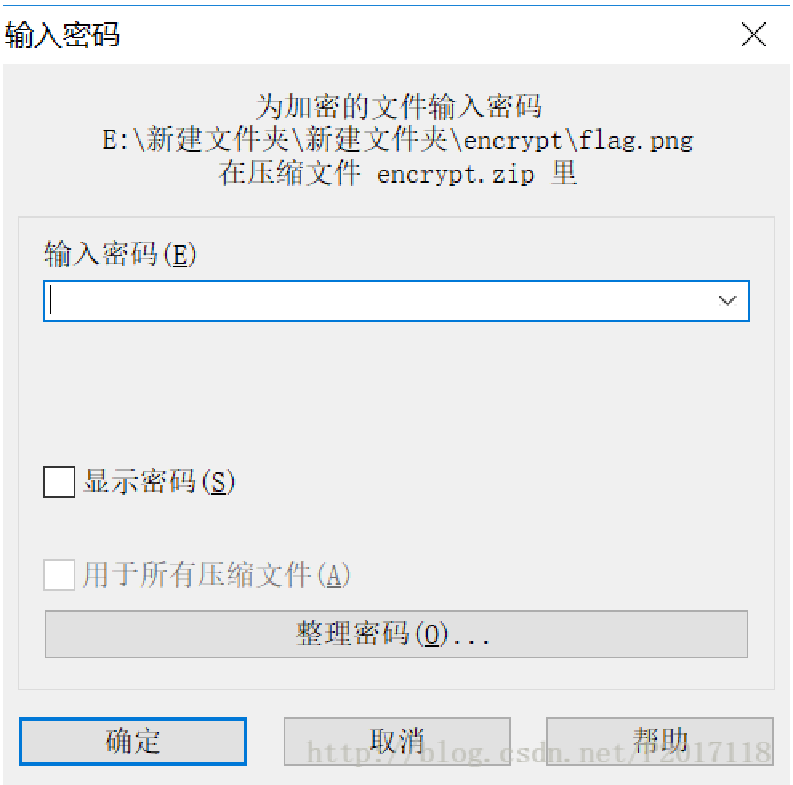

119.29.191.200/ctf/46d3e59de07a6aac6b2078c35aa4c16a03d10df3/?num=1'
火狐官方站点
最常访问
新手上路
火狐官方站点
常用网址
京东商城
Google 翻译
当前网页的语言为英文，是否需要翻译为中文？
立即翻译
暂不需要
http://blog.csdn.net/P2017118

```
1'
flag{we4k_type_c0mpare}$num=$_GET['num'];
if(!is_numeric($num))
{
echo $num;
if($num==1)
echo 'flag{**********}';
}
```

这次真的加密了

加密的压缩包，就一定安全吗？

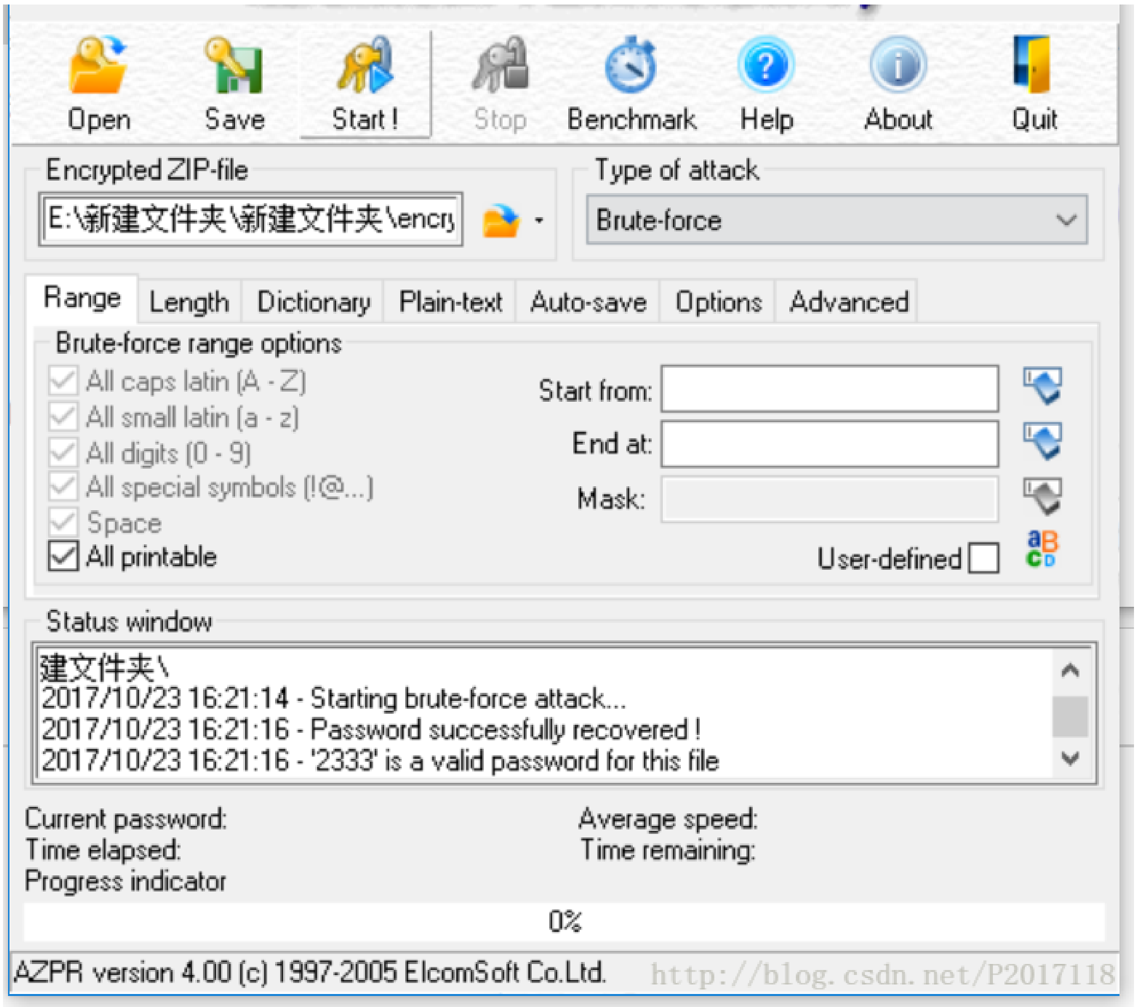
- 解压需要密码，经提示，可排除伪加密



输入密码

为加密的文件输入密码
E:\新建文件夹\新建文件夹\encrypt\flag.png
在压缩文件 encrypt.zip 里

- 使用AZPR破解密码



Encrypted ZIP-file

E:\新建文件夹\新建文件夹\encry

Type of attack

Brute-force

Brute-force range options

☑ All caps latin (A - Z)
☑ All small latin (a - z)
☑ All digits (0 - 9)
☑ All special symbols (!@...)
☑ Space
☑ All printable

Start from:

End at:

Mask:

User-defined □

Status window

```
建文件夹\
2017/10/23 16:21:14 - Starting brute-force attack...
2017/10/23 16:21:16 - Password successfully recovered !
2017/10/23 16:21:16 - '2333' is a valid password for this file
```

Current password:
Time elapsed:
Progress indicator

Average speed:
Time remaining:

0%

AZPR version 4.00 (c) 1997-2005 ElcomSoft Co.Ltd.

http://blog.csdn.net/P2017118

一张含有信息的图片

古时候打仗，友军间通信为了不被敌人发现重要的情报，用了各种各样的方法隐藏信息，延续到了现代，又有了新的变化…

- 打开发现一面全白的图片，使用StegSolve即可。