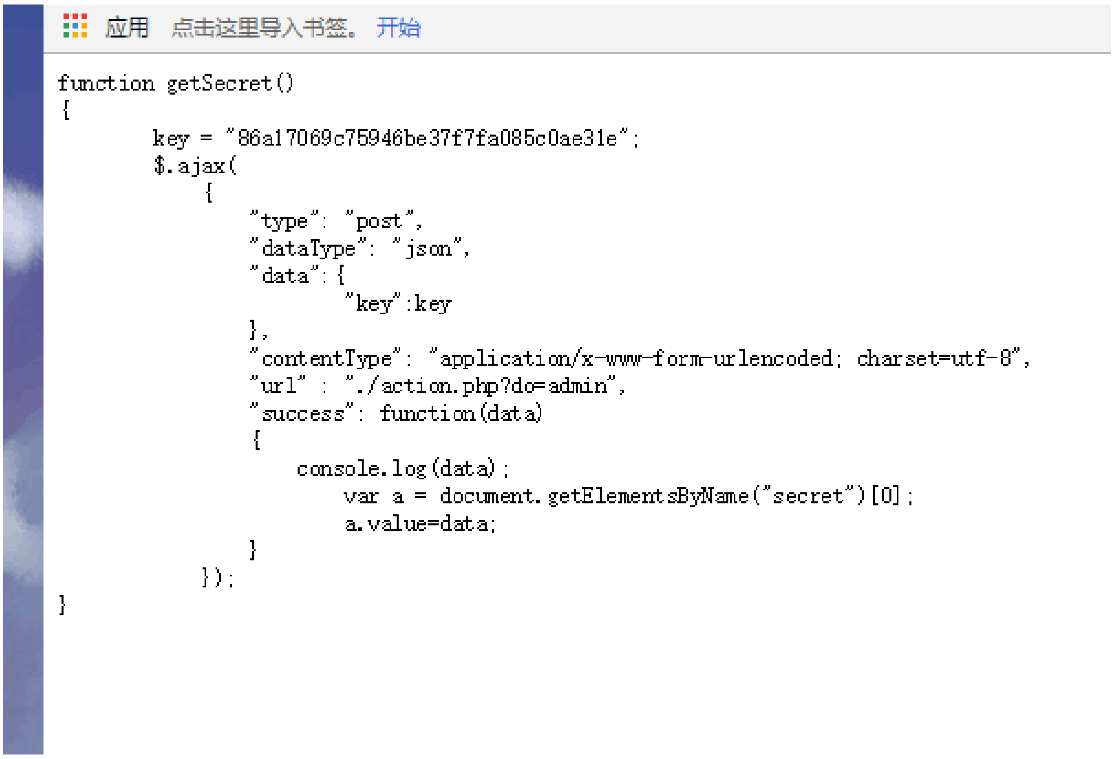
1-1

php 的精度问题 2016.999999999999=2017 谷歌浏览器输入

?year=2016.9999999999999 访问得到 flag

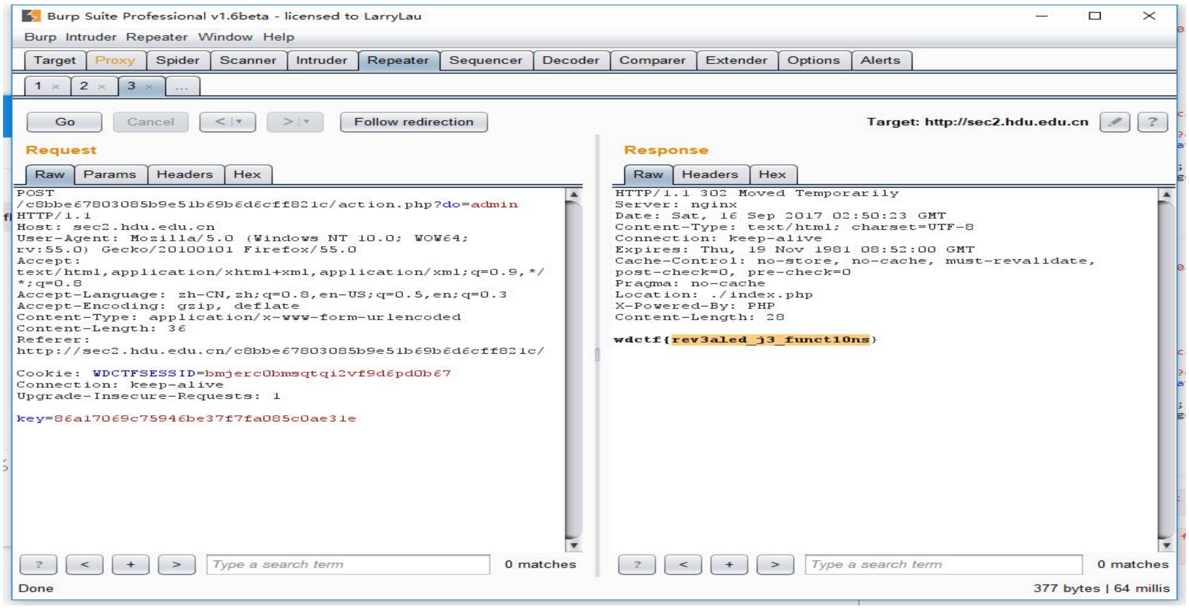
1-2

探测到存在 admin.php，访问查看源码有一段 js



```
function getSecret()
{
        key = "86a17069c75946be37f7fa085c0ae31e";
        $.ajax(
            {
                "type": "post",
                "dataType": "json",
                "data":{
                        "key":key
                },
                "contentType": "application/x-www-form-urlencoded; charset=utf-8",
                "url" : "./action.php?do=admin",
                "success": function(data)
                {
                    console.log(data);
                        var a = document.getElementsByName("secret")[0];
                        a.value=data;
                }
            });
}
```

Post 传入 key 得到 flag


Burp Suite Professional v1.6beta - licensed to LarryLau
Burp Intruder Repeater Window Help
Target Proxy Spider Scanner Intruder Repeater Sequencer Decoder Comparer Extender Options Alerts
1 × 2 × 3 × ...
Go Cancel < > Follow redirection
Target: http://sec2.hdu.edu.cn
Request
Raw Params Headers Hex
Response
Raw Headers Hex
? < + > Type a search term 0 matches
? < + > Type a search term 0 matches
Done
377 bytes | 64 millis

```
POST
/c8bbe67803085b9e51b69b6d6cff821c/action.php?do=admin
HTTP/1.1
Host: sec2.hdu.edu.cn
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64;
rv:55.0) Gecko/20100101 Firefox/55.0
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,*/
*;q=0.8
Accept-Language: zh-CN,zh;q=0.8,en-US;q=0.5,en;q=0.3
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded
Content-Length: 36
Referer:
http://sec2.hdu.edu.cn/c8bbe67803085b9e51b69b6d6cff821c/

Cookie: WDCTFSESSID=bmjerc0bmsqtqi2vf9d6pd0b67
Connection: keep-alive
Upgrade-Insecure-Requests: 1

key=86a17069c75946be37f7fa085c0ae31e
```

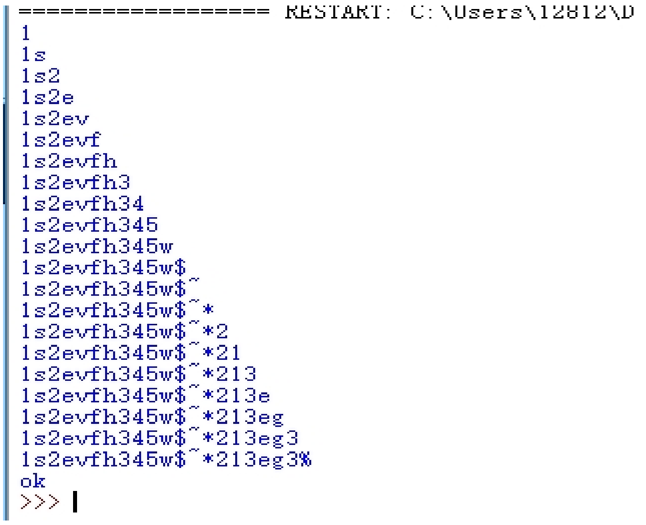
```
HTTP/1.1 302 Moved Temporarily
Server: nginx
Date: Sat, 16 Sep 2017 02:50:23 GMT
Content-Type: text/html; charset=UTF-8
Connection: keep-alive
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate,
post-check=0, pre-check=0
Pragma: no-cache
Location: ./index.php
X-Powered-By: PHP
Content-Length: 28

wdctf{rev3aled_j3_funct10ns}
```

2-1

提示说，账号密码都在博客里，账号为邮箱，那么只有一个 qq 邮箱，密码经过测试，得到是车牌号，登录之后在评论管理里面找到一个评论为 php 链接地址，访问得到 flag

2-2

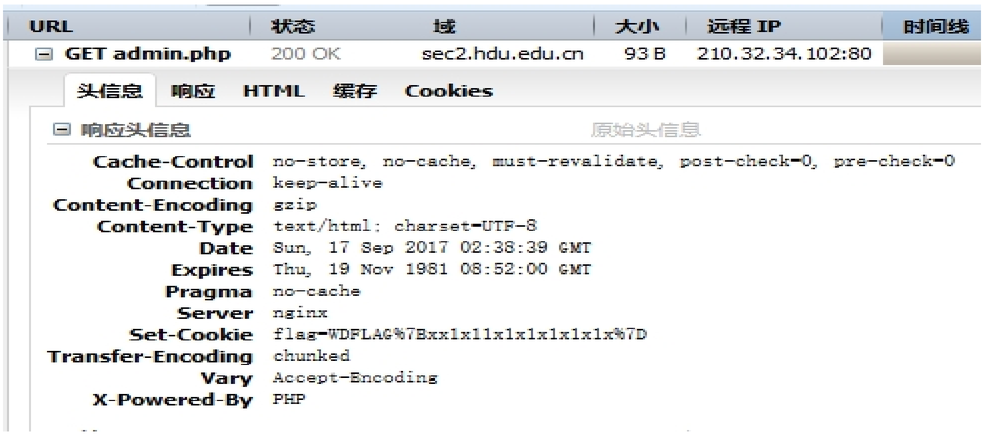
这道题是一个盲注，注入点在 username，过滤了单引号，空格，发现并没有过滤双引号，而且 username="^1^"时为 username error ， username="^0^"时，为 password error，说明是双引号闭合注入，写脚本，跑出密码



```
================== RESTART: C:\Users\12812\D
1
1s
1s2
1s2e
1s2ev
1s2evf
1s2evfh
1s2evfh3
1s2evfh34
1s2evfh345
1s2evfh345w
1s2evfh345w$
1s2evfh345w$~
1s2evfh345w$~*
1s2evfh345w$~*2
1s2evfh345w$~*21
1s2evfh345w$~*213
1s2evfh345w$~*213e
1s2evfh345w$~*213eg
1s2evfh345w$~*213eg3
1s2evfh345w$~*213eg3%
ok
>>> 
```

，

登录发现并没有反应，也不提示 password error，队友说还存在一个 admin.php，访问查看 php 响应头得到 flag



URL	状态	域	大小	远程 IP	时间线
⊟ GET admin.php	200 OK	sec2.hdu.edu.cn	93 B	210.32.34.102:80	

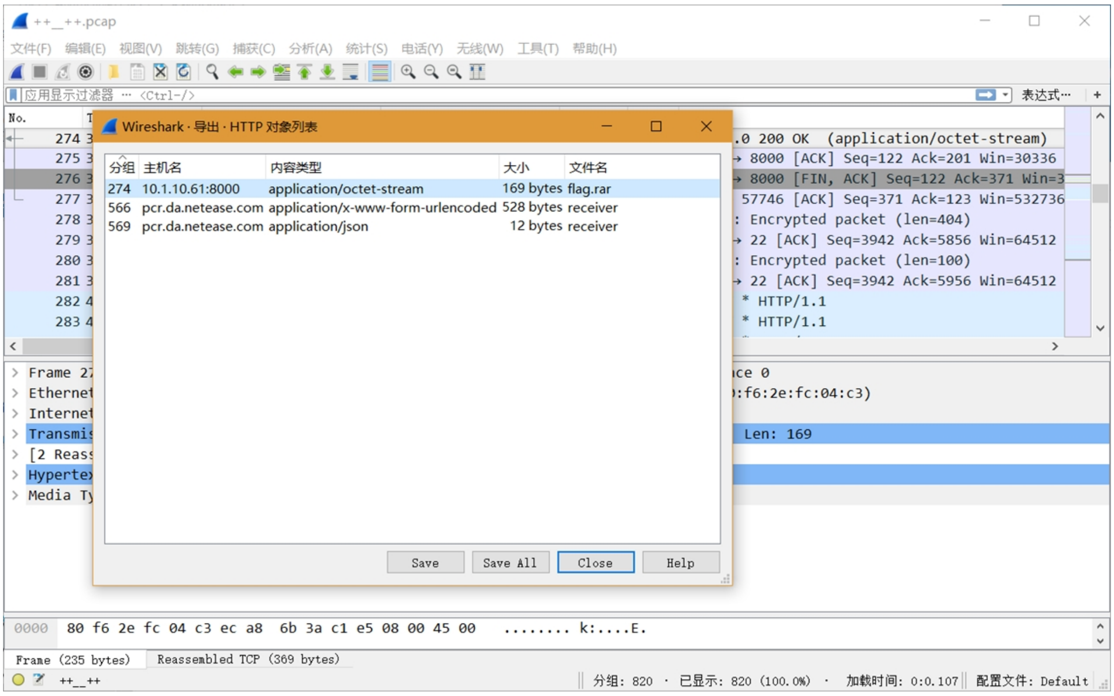
头信息　响应　HTML　缓存　Cookies

⊟ 响应头信息　　原始头信息

```
    Cache-Control  no-store, no-cache, must-revalidate, post-check=0, pre-check=0
       Connection  keep-alive
 Content-Encoding  gzip
     Content-Type  text/html; charset=UTF-8
             Date  Sun, 17 Sep 2017 02:38:39 GMT
          Expires  Thu, 19 Nov 1981 08:52:00 GMT
           Pragma  no-cache
           Server  nginx
       Set-Cookie  flag=WDFLAG%7Bxx1x11x1x1x1x1x%7D
Transfer-Encoding  chunked
             Vary  Accept-Encoding
     X-Powered-By  PHP
```

3-1

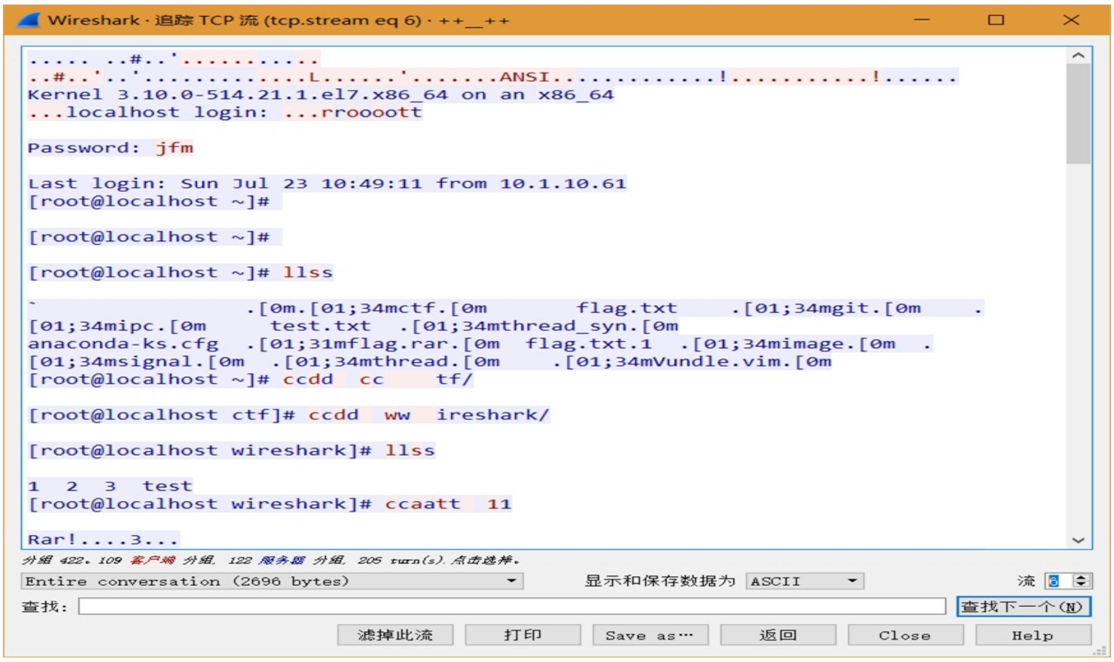
附件下载下来一个没有后缀名的 文件，改后缀名 rar，把解压后的文件后缀名改成 pcap，导出 http 对象


++_++.pcap
文件(F) 编辑(E) 视图(V) 跳转(G) 捕获(C) 分析(A) 统计(S) 电话(Y) 无线(W) 工具(T) 帮助(H)
应用显示过滤器 … <Ctrl-/>
表达式…
Wireshark · 导出 · HTTP 对象列表
Save
Save All
Close
Help

分组	主机名	内容类型	大小	文件名
274	10.1.10.61:8000	application/octet-stream	169 bytes	flag.rar
566	pcr.da.netease.com	application/x-www-form-urlencoded	528 bytes	receiver
569	pcr.da.netease.com	application/json	12 bytes	receiver

```
No.    T
 274 3   .0 200 OK  (application/octet-stream)
 275 3   → 8000 [ACK] Seq=122 Ack=201 Win=30336
 276 3   → 8000 [FIN, ACK] Seq=122 Ack=371 Win=3
 277 3   57746 [ACK] Seq=371 Ack=123 Win=532736
 278 3   : Encrypted packet (len=404)
 279 3   → 22 [ACK] Seq=3942 Ack=5856 Win=64512
 280 3   : Encrypted packet (len=100)
 281 3   → 22 [ACK] Seq=3942 Ack=5956 Win=64512
 282 4   * HTTP/1.1
 283 4   * HTTP/1.1

> Frame 27                 ice 0
> Ethernet                 ):f6:2e:fc:04:c3)
> Internet
> Transmis                  Len: 169
> [2 Reass
> Hypertex
> Media Ty

0000  80 f6 2e fc 04 c3 ec a8  6b 3a c1 e5 08 00 45 00   ........ k:....E.

Frame (235 bytes)   Reassembled TCP (369 bytes)
++_++        分组: 820 · 已显示: 820 (100.0%) · 加载时间: 0:0.107   配置文件: Default
```

flag.rar 需要解压密码，先用工具爆破下密码，没爆破出来，然后开始追踪 tcp 看看有没有一些线索，追钟到第 6 个流时，发现



```
.....  ..#..'...........
..#..'..'..............L......'.......ANSI..............!............!......
Kernel 3.10.0-514.21.1.el7.x86_64 on an x86_64
...localhost login: ...rroooott

Password: jfm

Last login: Sun Jul 23 10:49:11 from 10.1.10.61
[root@localhost ~]#

[root@localhost ~]#

[root@localhost ~]# llss

`                 .[0m.[01;34mctf.[0m        flag.txt     .[01;34mgit.[0m     .
[01;34mipc.[0m      test.txt   .[01;34mthread_syn.[0m
anaconda-ks.cfg   .[01;31mflag.rar.[0m  flag.txt.1   .[01;34mimage.[0m   .
[01;34msignal.[0m   .[01;34mthread.[0m      .[01;34mVundle.vim.[0m
[root@localhost ~]# ccdd  cc     tf/

[root@localhost ctf]# ccdd  ww  ireshark/

[root@localhost wireshark]# llss

1  2  3  test
[root@localhost wireshark]# ccaatt  11

Rar!....3...
```

分组 422。109 客户端 分组, 122 服务器 分组, 205 turn(s). 点击选择。

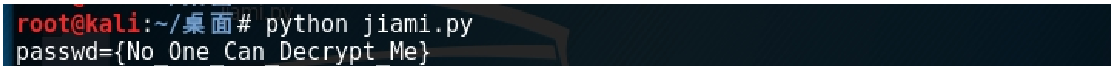
Entire conversation (2696 bytes)　　显示和保存数据为 ASCII　　流 6

查找：

一些对 flag.rar 进行操作，一共有 1 ,2, 3,test 三个文件，文件 1 是 flag.rar，文件 2 是一串字符串 19aaFYsQQKr+hVX6hl2smAUQ5a767TsULEUebWSajEo=

文件 3 是一个 aes 加密解密脚本 test 是出题人的 zhunichenggong。猜测，这串字符串就是 flag.rar 解压密码的密文

```
# coding:utf-8
__author__ = 'YFP'
from Crypto import Random
from Crypto.Cipher import AES
import sys
import base64
IV = 'QWERTYUIOPASDFGH'


def decrypt(encrypted):
  aes = AES.new(IV, AES.MODE_CBC, IV)
  return aes.decrypt(encrypted)


def encrypt(message):
  length = 16
  count = len(message)
  padding = length - (count % length)
  message = message + '\0' * padding
  aes = AES.new(IV, AES.MODE_CBC, IV)
  return aes.encrypt(message)


a = '19aaFYsQQKr+hVX6hl2smAUQ5a767TsULEUebWSajEo='
b = base64.b64decode(a)
print(decrypt(b))
```

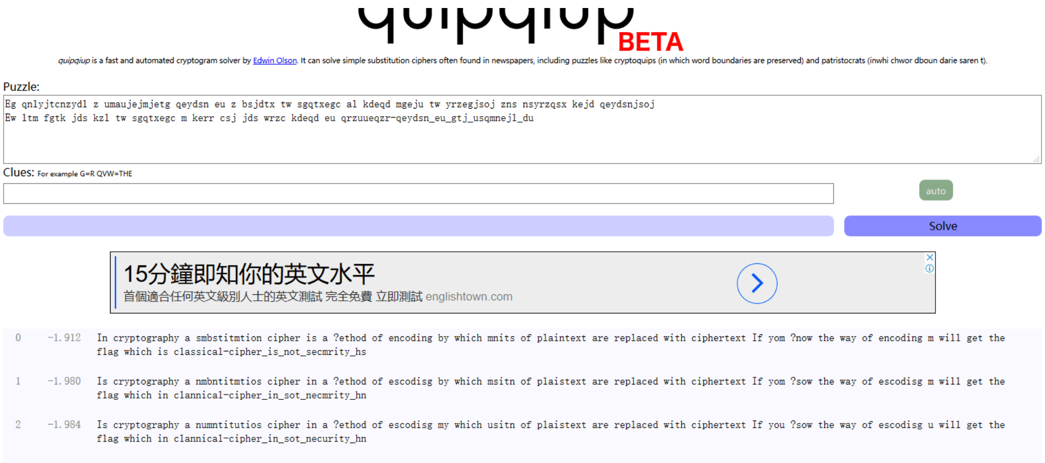


```
root@kali:~/桌面# python jiami.py
passwd={No_One_Can_Decrypt_Me}
```

然后打开 flag.rar 里面就是 flag

3-2

打开链接是一串不规则的字母，直接想到单表替换，



quipqiup is a fast and automated cryptogram solver by Edwin Olson. It can solve simple substitution ciphers often found in newspapers, including puzzles like cryptoquips (in which word boundaries are preserved) and patristocrats (inwhi chwor dboun darie saren t).

Puzzle:

```
Eg qnlyjtcnzydl z umaujejmjetg qeydsn eu z bsjdtx tw sgqtxegc al kdeqd mgeju tw yrzegjsoj zns nsyrzqsx kejd qeydsnjsoj
Ew ltm fgtk jds kzl tw sgqtxegc m kerr csj jds wrzc kdeqd eu qrzuueqzr-qeydsn_eu_gtj_usqmnejl_du
```

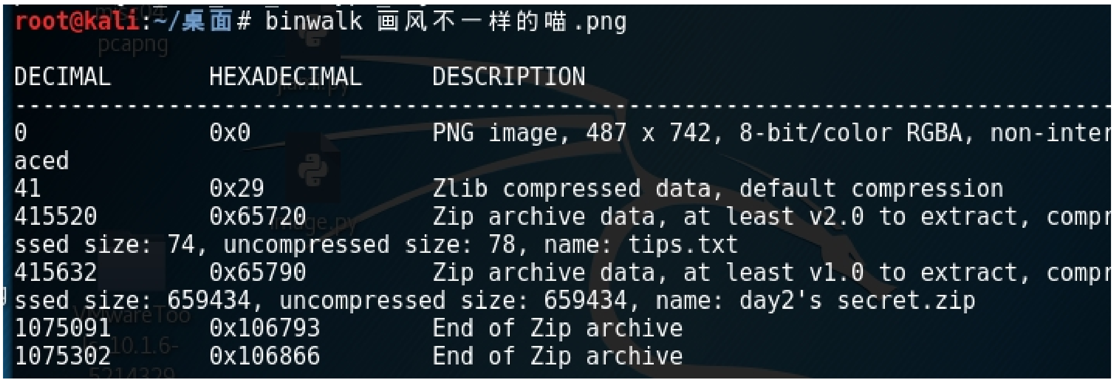
Clues: For example G=R QVW=THE

```
0    -1.912   In cryptography a smbstitmtion cipher is a ?ethod of encoding by which mnits of plaintext are replaced with ciphertext If yom ?now the way of encoding m will get the
              flag which is classical-cipher_is_not_secmrity_hs

1    -1.980   Is cryptography a nmbntitmtios cipher in a ?ethod of escodisg by which msitn of plaistext are replaced with ciphertext If yom ?sow the way of escodisg m will get the
              flag which in clannical-cipher_in_sot_necmrity_hn

2    -1.984   Is cryptography a numntitutios cipher in a ?ethod of escodisg my which usitn of plaistext are replaced with ciphertext If you ?sow the way of escodisg u will get the
              flag which in clannical-cipher_in_sot_necurity_hn
```

得到 flag

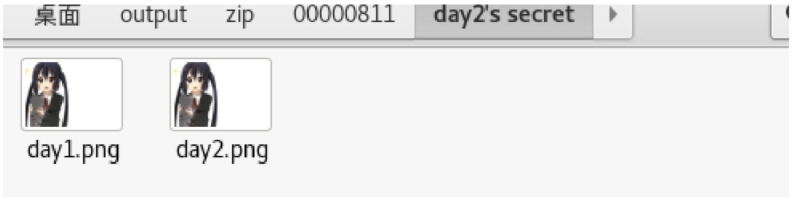
4-1

上来就是一张图片，用 binwalk 分析

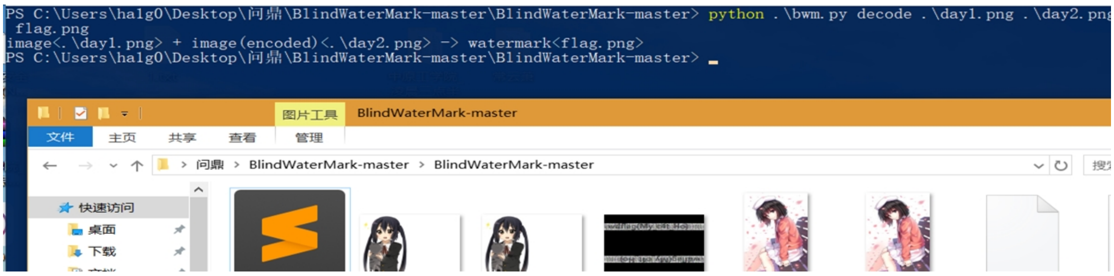


```
root@kali:~/桌面# binwalk 画风不一样的喵.png

DECIMAL       HEXADECIMAL     DESCRIPTION
--------------------------------------------------------------------------------
0             0x0             PNG image, 487 x 742, 8-bit/color RGBA, non-inter
aced
41            0x29            Zlib compressed data, default compression
415520        0x65720         Zip archive data, at least v2.0 to extract, compr
ssed size: 74, uncompressed size: 78, name: tips.txt
415632        0x65790         Zip archive data, at least v1.0 to extract, compr
ssed size: 659434, uncompressed size: 659434, name: day2's secret.zip
1075091       0x106793        End of Zip archive
1075302       0x106866        End of Zip archive
```

用 foremost 提取出一个 zip



是双图隐写，想到这次国赛时候盲水印隐写，直接用 github 上的脚本尝试下



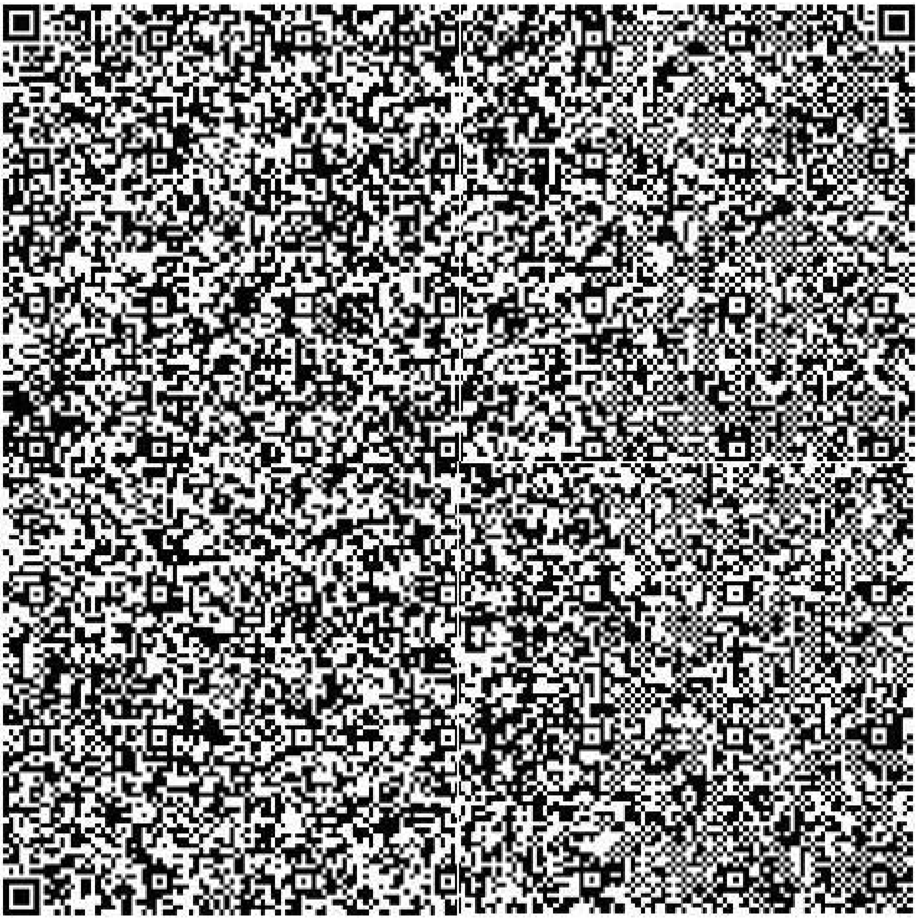
```
PS C:\Users\halg0\Desktop\问鼎\BlindWaterMark-master\BlindWaterMark-master> python .\bwm.py decode .\day1.png .\day2.png
 flag.png
image<.\day1.png> + image(encoded)<.\day2.png> -> watermark<flag.png>
PS C:\Users\halg0\Desktop\问鼎\BlindWaterMark-master\BlindWaterMark-master> _
```

得到 flag

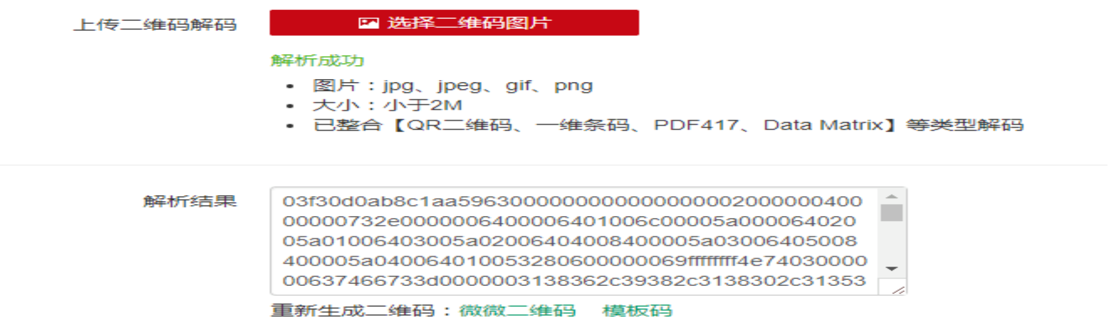
4-2

动图 gif，用 stegsolve 保存每一帧的图片

再用 ps 把图片拼接起来



手机扫不出来，用在线的二维码识别，扫描出来一串 16 进制，



解析成功

- 图片：jpg、jpeg、gif、png
- 大小：小于2M
- 已整合【QR二维码、一维条码、PDF417、Data Matrix】等类型解码

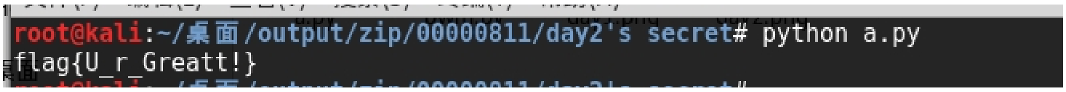
解析结果

```
03f30d0ab8c1aa596300000000000000000200000040 0
00000732e0000006400006401006c00005a000064020
05a01006403005a02006404008400005a03006405008
400005a04006401005328060000000069ffffffff4e74030000
00637466733d0000003138362c39382c3138302c31353
```

然后发现转移过来是 pyc 文件，反编译。然后直接调用函数

```
import random
key = 'ctf'
strr = '186,98,180,154,139,192,114,14,102,168,43,136,52,218,85,100,43'


def func1(str1, key):
    random.seed(key)
    str2 = ''
    for c in str1:
        str2 += str(ord(c) ^ random.randint(0, 255)) + ','
    str2 = str2.strip(',')
    return str2


def func2(str2, key):
    random.seed(key)
    str1 = ''
    for i in str2.split(','):
        i = int(i)
        str1 += chr(i ^ random.randint(0, 255))
    return str1
# print func1(strr,key)
print func2(strr,key)
```

注意在 windows 底下是乱码，必须在 linux 底下

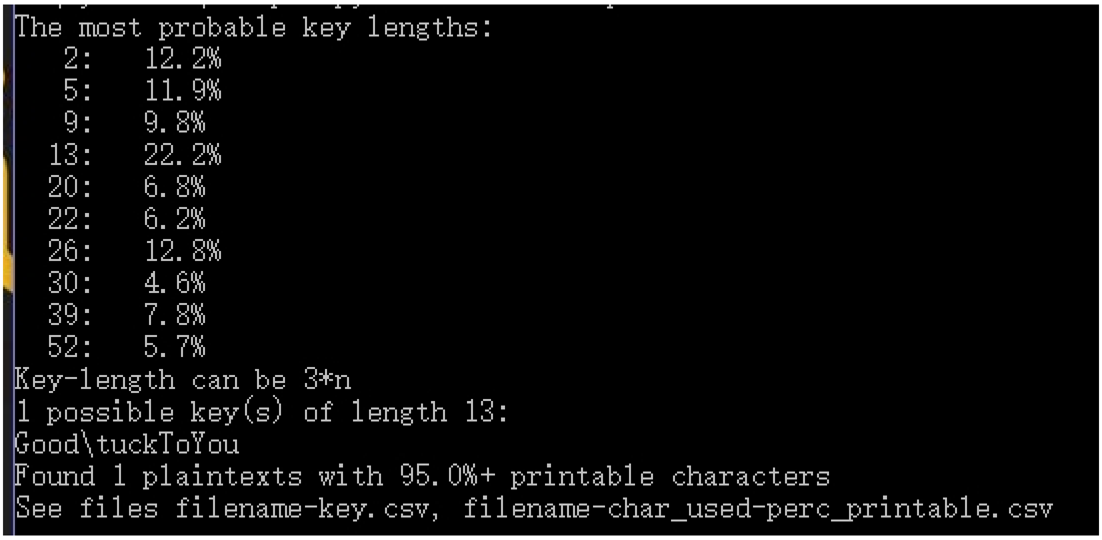


```
root@kali:~/桌面/output/zip/00000811/day2's secret# python a.py
flag{U_r_Greatt!}
```

5-1

拿到题目，cipher，提示就是一个 xor，第一个猜想是这个文件本身异或试试，然后就把文件和逆向输出的两个文件进行了 xor 操作，然后什么都没有发现前后对称嘛，就这么一直 xor 下去看看好了，额。到最后出来个笑脸。好吧，假假的套路。

第二个猜想就是 xor 的加密，用 xortool 分析一波试试；

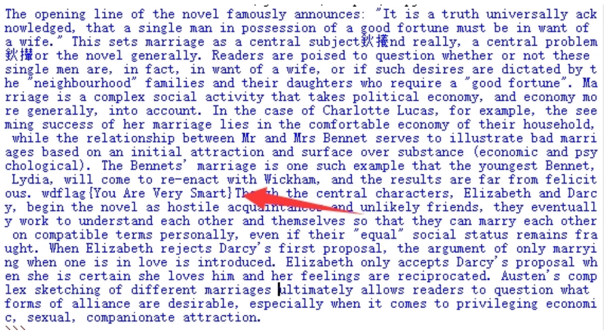


```
The most probable key lengths:
   2:   12.2%
   5:   11.9%
   9:   9.8%
  13:   22.2%
  20:   6.8%
  22:   6.2%
  26:   12.8%
  30:   4.6%
  39:   7.8%
  52:   5.7%
Key-length can be 3*n
1 possible key(s) of length 13:
Good\tuckToYou
Found 1 plaintexts with 95.0%+ printable characters
See files filename-key.csv, filename-char_used-perc_printable.csv
```

出来密钥了，一个脚本解解看吧。

```
f = open('cipher','rb')
key = "GoodLuckToYou"

txt = f.read()

flag = ""
for i in range(0,len(txt)):
    flag = flag + chr(ord(txt[i])^ord(key[i%len(key)]))
print flag
```

这就出来了。



~~~
The opening line of the novel famously announces: "It is a truth universally ack
nowledged, that a single man in possession of a good fortune must be in want of
a wife." This sets marriage as a central subject鈥攁nd really, a central problem
鈥攆or the novel generally. Readers are poised to question whether or not these
single men are, in fact, in want of a wife, or if such desires are dictated by t
he "neighbourhood" families and their daughters who require a "good fortune". Ma
rriage is a complex social activity that takes political economy, and economy mo
re generally, into account. In the case of Charlotte Lucas, for example, the see
ming success of her marriage lies in the comfortable economy of their household,
 while the relationship between Mr and Mrs Bennet serves to illustrate bad marri
ages based on an initial attraction and surface over substance (economic and psy
chological). The Bennets' marriage is one such example that the youngest Bennet,
 Lydia, will come to re-enact with Wickham, and the results are far from felicit
ous. wdflag{You Are Very Smart}Though the central characters, Elizabeth and Darc
y, begin the novel as hostile acquaintances and unlikely friends, they eventuall
y work to understand each other and themselves so that they can marry each other
 on compatible terms personally, even if their "equal" social status remains fra
ught. When Elizabeth rejects Darcy's first proposal, the argument of only marryi
ng when one is in love is introduced. Elizabeth only accepts Darcy's proposal wh
en she is certain she loves him and her feelings are reciprocated. Austen's comp
lex sketching of different marriages ultimately allows readers to question what
forms of alliance are desirable, especially when it comes to privileging economi
c, sexual, companionate attraction.
```
~~~