i春秋 WEB fuzzing

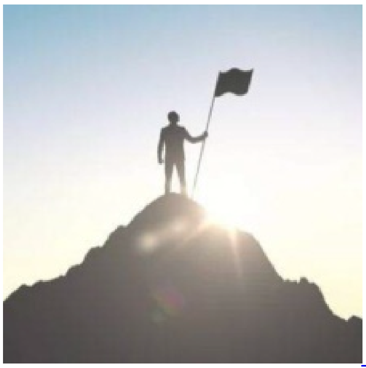
原创

A_dmins 于 2019-06-16 12:56:21 发布 1246 收藏 2

分类专栏： CTF题 一天一道CTF i春秋CTF

本文链接：https://blog.csdn.net/qq_42967398/article/details/92389151

版权


CTF题 同时被 3 个专栏收录

115 篇文章 11 订阅

订阅专栏

一天一道CTF

52 篇文章 5 订阅

订阅专栏

i春秋CTF

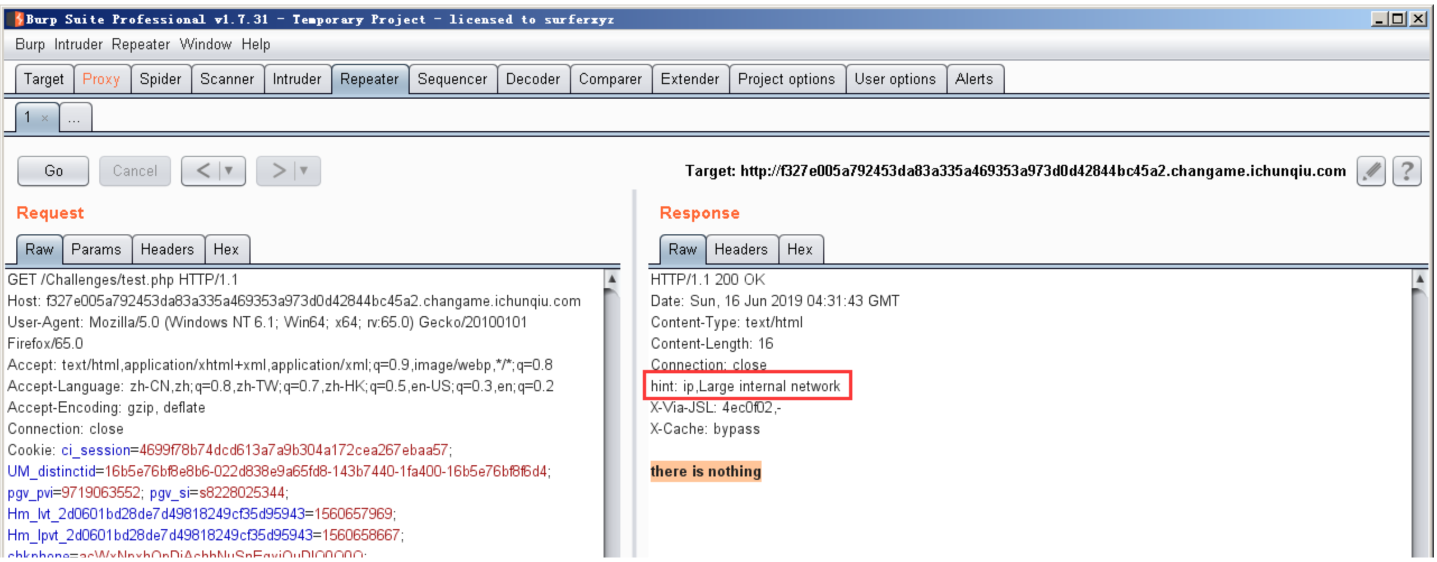
21 篇文章 1 订阅

订阅专栏

i春秋 WEB fuzzing

一天一道CTF题目，能多不能少

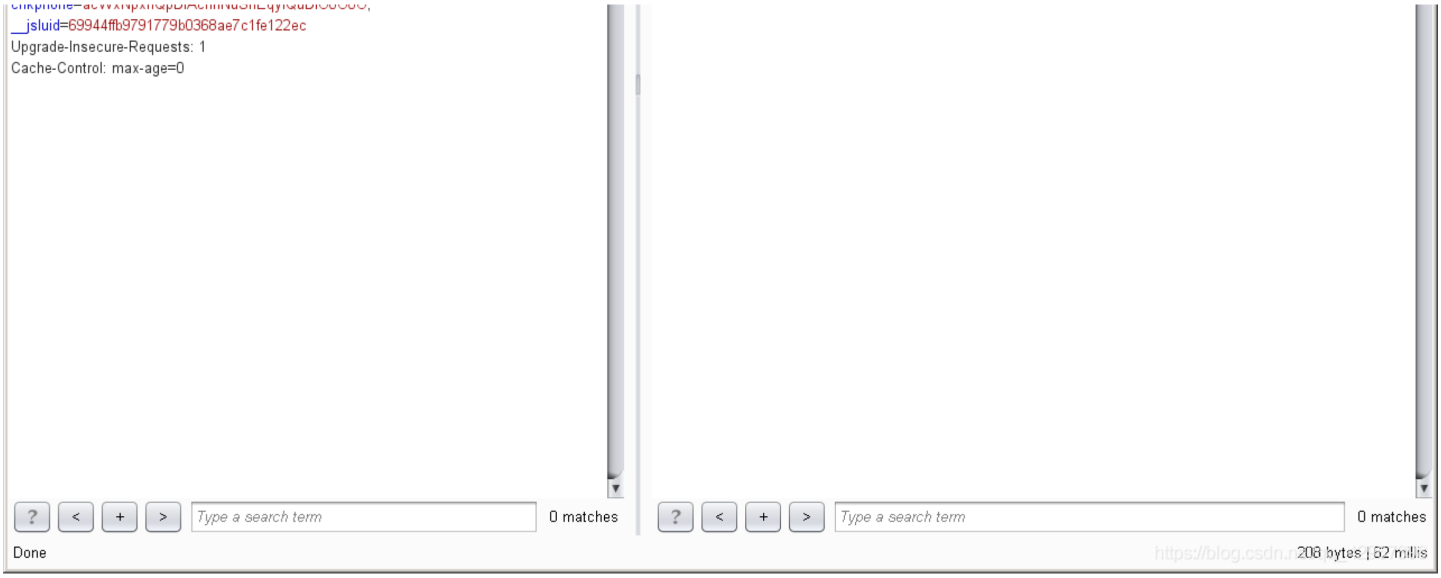
打开网页发现`there is nothing`,最后一通折腾什么都没有，最后进行抓包，得到提示：



Target: http://f327e005a792453da83a335a469353a973d0d42844bc45a2.changame.ichunqiu.com

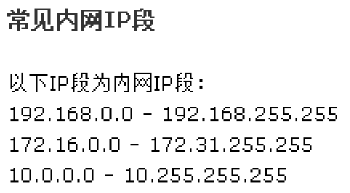
```
GET /Challenges/test.php HTTP/1.1
Host: f327e005a792453da83a335a469353a973d0d42844bc45a2.changame.ichunqiu.com
User-Agent: Mozilla/5.0 (Windows NT 6.1; Win64; x64; rv:65.0) Gecko/20100101
Firefox/65.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Accept-Encoding: gzip, deflate
Connection: close
Cookie: ci_session=4699f78b74dcd613a7a9b304a172cea267ebaa57;
UM_distinctid=16b5e76bf8e8b6-022d838e9a65fd8-143b7440-1fa400-16b5e76bf8f6d4;
pgv_pvi=9719063552; pgv_si=s8228025344;
Hm_lvt_2d0601bd28de7d49818249cf35d95943=1560657969;
Hm_lpvt_2d0601bd28de7d49818249cf35d95943=1560658667;
chkphone=acWxNpxhQpDiAchhNuSnEgxiQuDIQ0Q0O;
```

```
HTTP/1.1 200 OK
Date: Sun, 16 Jun 2019 04:31:43 GMT
Content-Type: text/html
Content-Length: 16
Connection: close
hint: ip,Large internal network
X-Via-JSL: 4ec0f02,-
X-Cache: bypass

there is nothing
```



```
chkphone=acWxNpxhQpDiAchhNuSnEqyiQuDIO0O0O;
__jsluid=69944ffb9791779b0368ae7c1fe122ec
Upgrade-Insecure-Requests: 1
Cache-Control: max-age=0
```

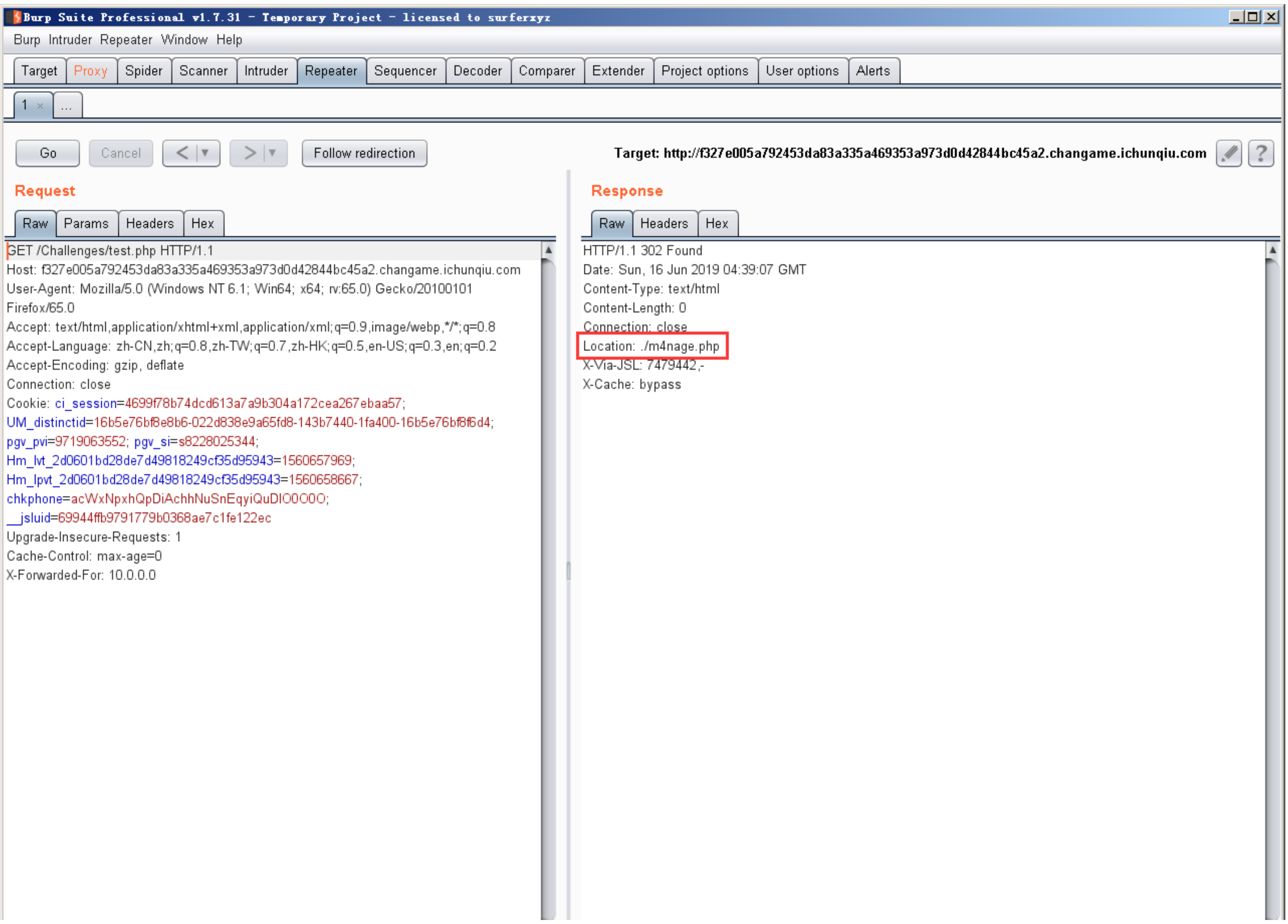
按照提示应该是要构造ip，使用X-Forwarded-For
还有个提示是它要大的内部网络，直接将常用内网IP段都试下



常见内网IP段

以下IP段为内网IP段：
192.168.0.0 - 192.168.255.255
172.16.0.0 - 172.31.255.255
10.0.0.0 - 10.255.255.255

尝试到10.0.0.0的时候得到一个新的提示：



Burp Suite Professional v1.7.31 - Temporary Project - licensed to surferxyz
Burp Intruder Repeater Window Help
Target Proxy Spider Scanner Intruder Repeater Sequencer Decoder Comparer Extender Project options User options Alerts
1 ×
...
Go
Cancel
< | ▾
> | ▾
Follow redirection
Request
Raw Params Headers Hex
Response
Raw Headers Hex

Target: http://f327e005a792453da83a335a469353a973d0d42844bc45a2.changame.ichunqiu.com

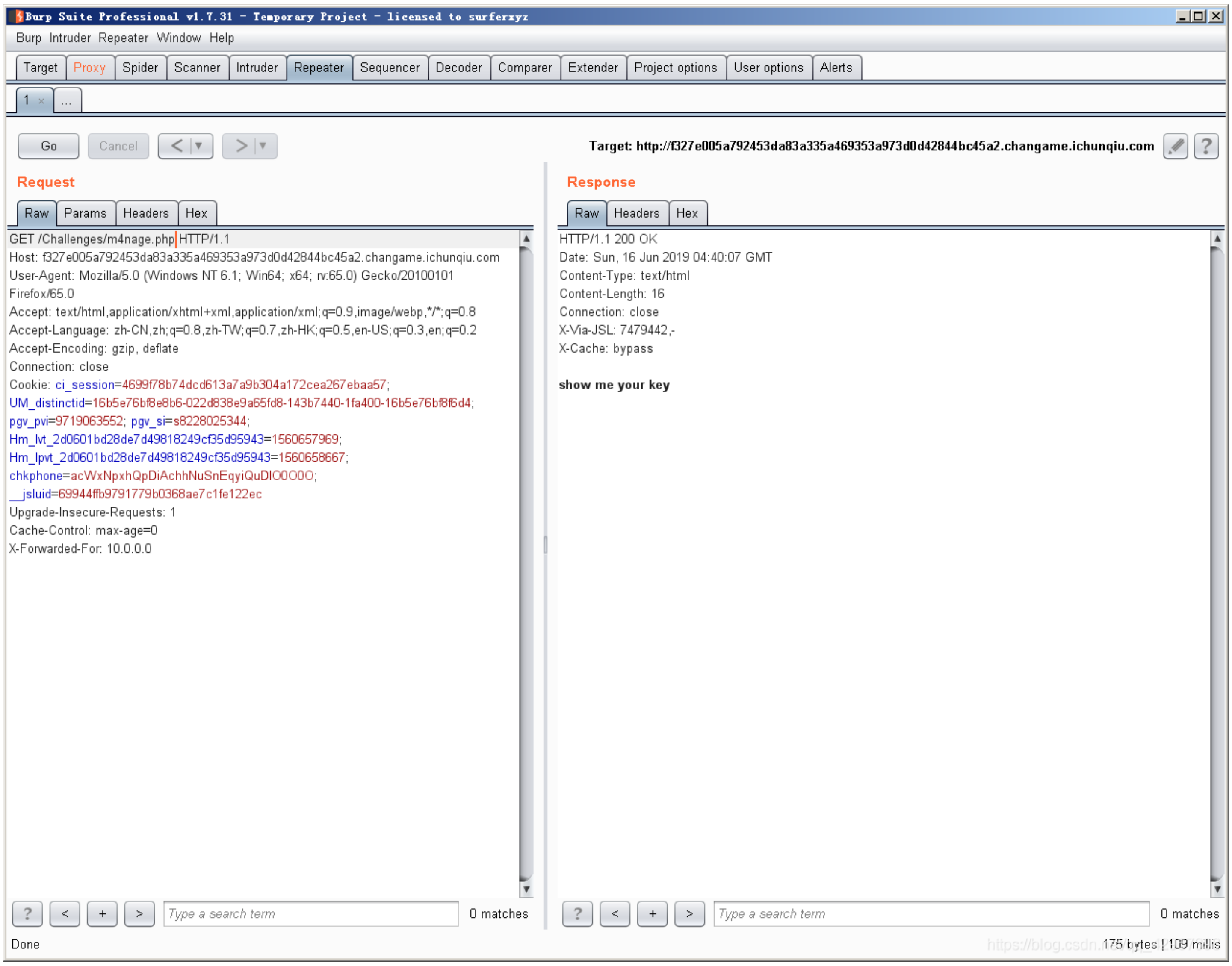
```
GET /Challenges/test.php HTTP/1.1
Host: f327e005a792453da83a335a469353a973d0d42844bc45a2.changame.ichunqiu.com
User-Agent: Mozilla/5.0 (Windows NT 6.1; Win64; x64; rv:65.0) Gecko/20100101
Firefox/65.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Accept-Encoding: gzip, deflate
Connection: close
Cookie: ci_session=4699f78b74dcd613a7a9b304a172cea267ebaa57;
UM_distinctid=16b5e76bf8e8b6-022d838e9a65fd8-143b7440-1fa400-16b5e76bf8f6d4;
pgv_pvi=9719063552; pgv_si=s8228025344;
Hm_lvt_2d0601bd28de7d49818249cf35d95943=1560657969;
Hm_lpvt_2d0601bd28de7d49818249cf35d95943=1560658667;
chkphone=acWxNpxhQpDiAchhNuSnEqyiQuDIO0O0O;
__jsluid=69944ffb9791779b0368ae7c1fe122ec
Upgrade-Insecure-Requests: 1
Cache-Control: max-age=0
X-Forwarded-For: 10.0.0.0
```

```
HTTP/1.1 302 Found
Date: Sun, 16 Jun 2019 04:39:07 GMT
Content-Type: text/html
Content-Length: 0
Connection: close
Location: ./m4nage.php
X-Via-JSL: 7479442,-
X-Cache: bypass
```

Done

185 bytes | 109 millis

进入得到新的提示，需要传递一个key?



Target: http://f327e005a792453da83a335a469353a973d0d42844bc45a2.changame.ichunqiu.com

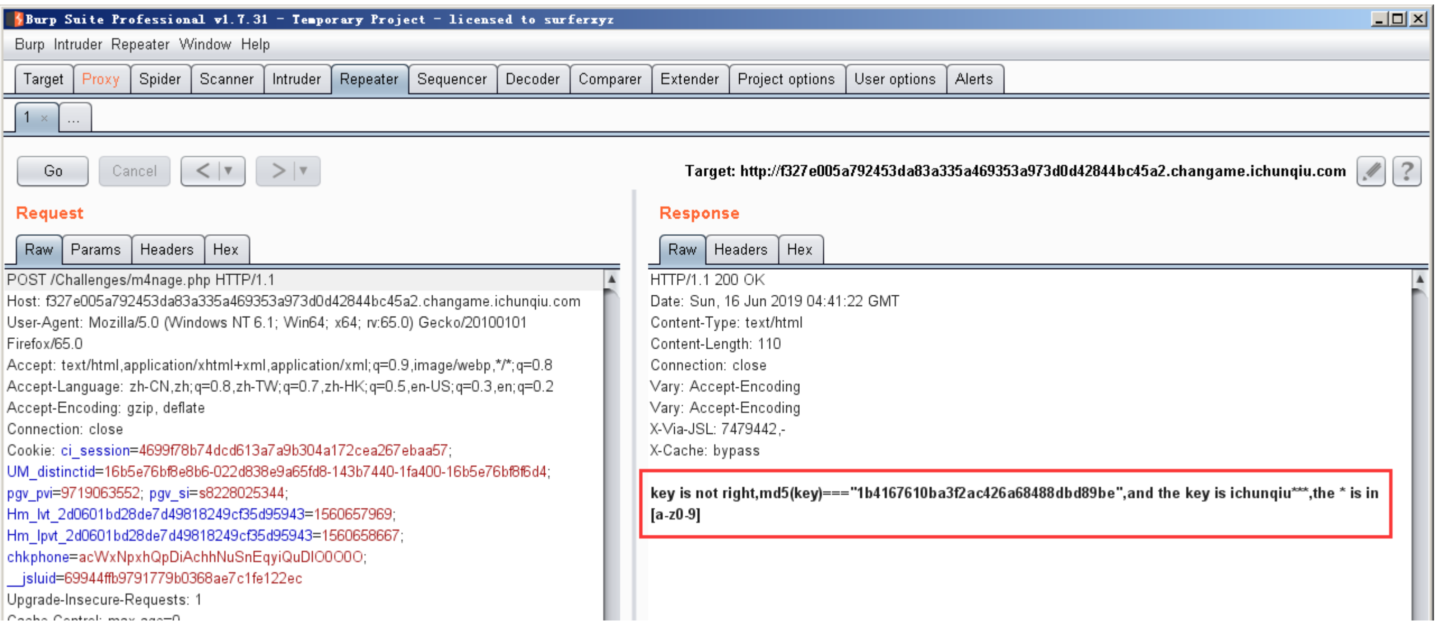
```
GET /Challenges/m4nage.php HTTP/1.1
Host: f327e005a792453da83a335a469353a973d0d42844bc45a2.changame.ichunqiu.com
User-Agent: Mozilla/5.0 (Windows NT 6.1; Win64; x64; rv:65.0) Gecko/20100101
Firefox/65.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Accept-Encoding: gzip, deflate
Connection: close
Cookie: ci_session=4699f78b74dcd613a7a9b304a172cea267ebaa57;
UM_distinctid=16b5e76bf8e8b6-022d838e9a65fd8-143b7440-1fa400-16b5e76bf8f6d4;
pgv_pvi=9719063552; pgv_si=s8228025344;
Hm_lvt_2d0601bd28de7d49818249cf35d95943=1560657969;
Hm_lpvt_2d0601bd28de7d49818249cf35d95943=1560658667;
chkphone=acWxNpxhQpDiAchhNuSnEqyiQuDIO0O0O;
__jsluid=69944ffb9791779b0368ae7c1fe122ec
Upgrade-Insecure-Requests: 1
Cache-Control: max-age=0
X-Forwarded-For: 10.0.0.0
```

```
HTTP/1.1 200 OK
Date: Sun, 16 Jun 2019 04:40:07 GMT
Content-Type: text/html
Content-Length: 16
Connection: close
X-Via-JSL: 7479442,-
X-Cache: bypass

show me your key
```

Done

175 bytes | 109 millis

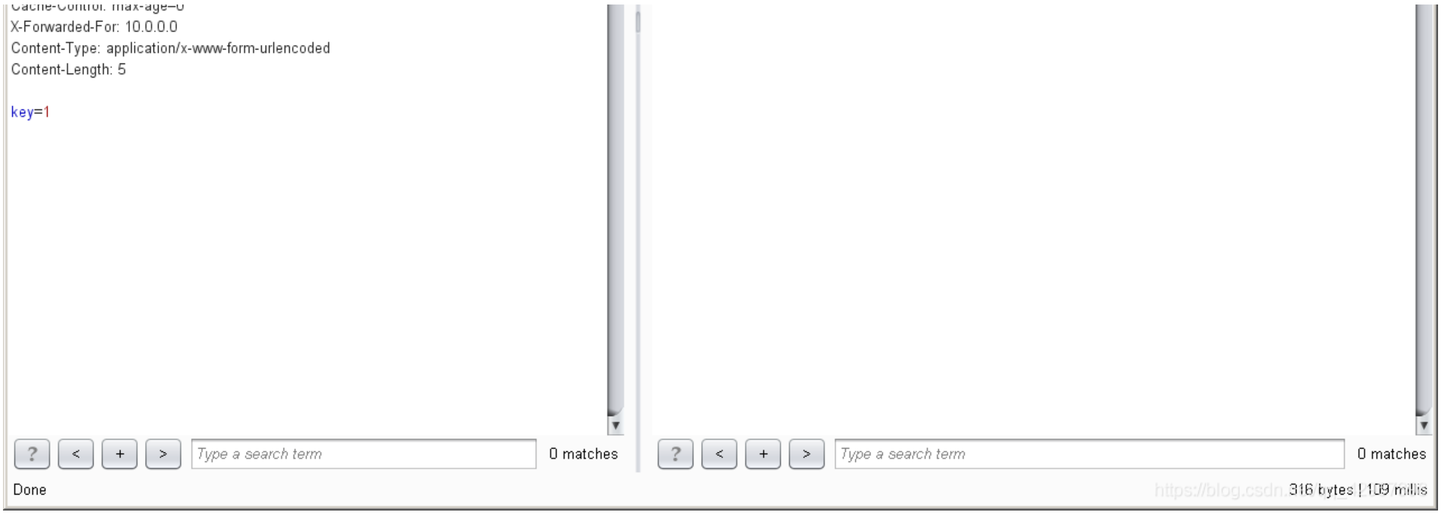
发现get传递不行，改为POST传递，得到再一个提示：



Target: http://f327e005a792453da83a335a469353a973d0d42844bc45a2.changame.ichunqiu.com

```
POST /Challenges/m4nage.php HTTP/1.1
Host: f327e005a792453da83a335a469353a973d0d42844bc45a2.changame.ichunqiu.com
User-Agent: Mozilla/5.0 (Windows NT 6.1; Win64; x64; rv:65.0) Gecko/20100101
Firefox/65.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Accept-Encoding: gzip, deflate
Connection: close
Cookie: ci_session=4699f78b74dcd613a7a9b304a172cea267ebaa57;
UM_distinctid=16b5e76bf8e8b6-022d838e9a65fd8-143b7440-1fa400-16b5e76bf8f6d4;
pgv_pvi=9719063552; pgv_si=s8228025344;
Hm_lvt_2d0601bd28de7d49818249cf35d95943=1560657969;
Hm_lpvt_2d0601bd28de7d49818249cf35d95943=1560658667;
chkphone=acWxNpxhQpDiAchhNuSnEqyiQuDIO0O0O;
__jsluid=69944ffb9791779b0368ae7c1fe122ec
Upgrade-Insecure-Requests: 1
Cache-Control: max-age=0
```

```
HTTP/1.1 200 OK
Date: Sun, 16 Jun 2019 04:41:22 GMT
Content-Type: text/html
Content-Length: 110
Connection: close
Vary: Accept-Encoding
Vary: Accept-Encoding
X-Via-JSL: 7479442,-
X-Cache: bypass

key is not right,md5(key)==="1b4167610ba3f2ac426a68488dbd89be",and the key is ichunqiu***,the * is in
[a-z0-9]
```

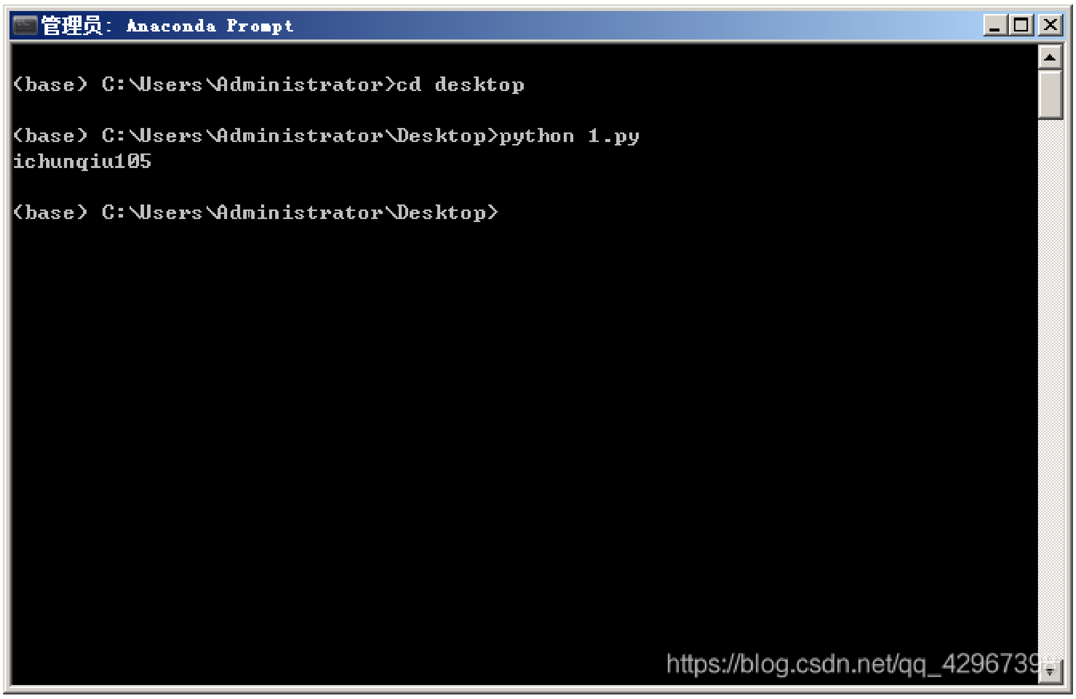


```
Cache-Control: max-age=0
X-Forwarded-For: 10.0.0.0
Content-Type: application/x-www-form-urlencoded
Content-Length: 5

key=1
```

也就是说key经过MD5加密之前是ichunqiu加上三位未知数，这三个可以使小写字母和数字中的任意一个
编写脚本来进行暴力：

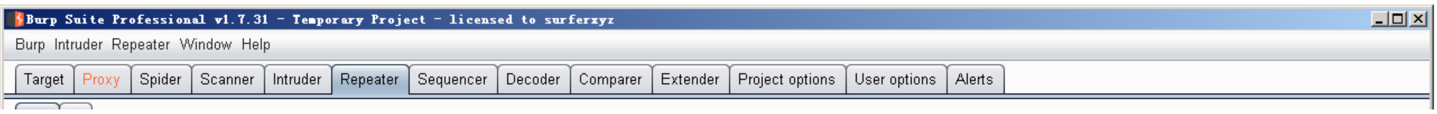
```
import hashlib

md5 = "1b4167610ba3f2ac426a68488dbd89be"
s = "abcdefghijklmnopqrstuvwxyz1234567890"

for i in s:
 for j in s:
  for k in s:
   key = "ichunqiu"+i+j+k
   if(hashlib.md5(key.encode("utf8")).hexdigest() == md5):
    print(key)
```

得到：

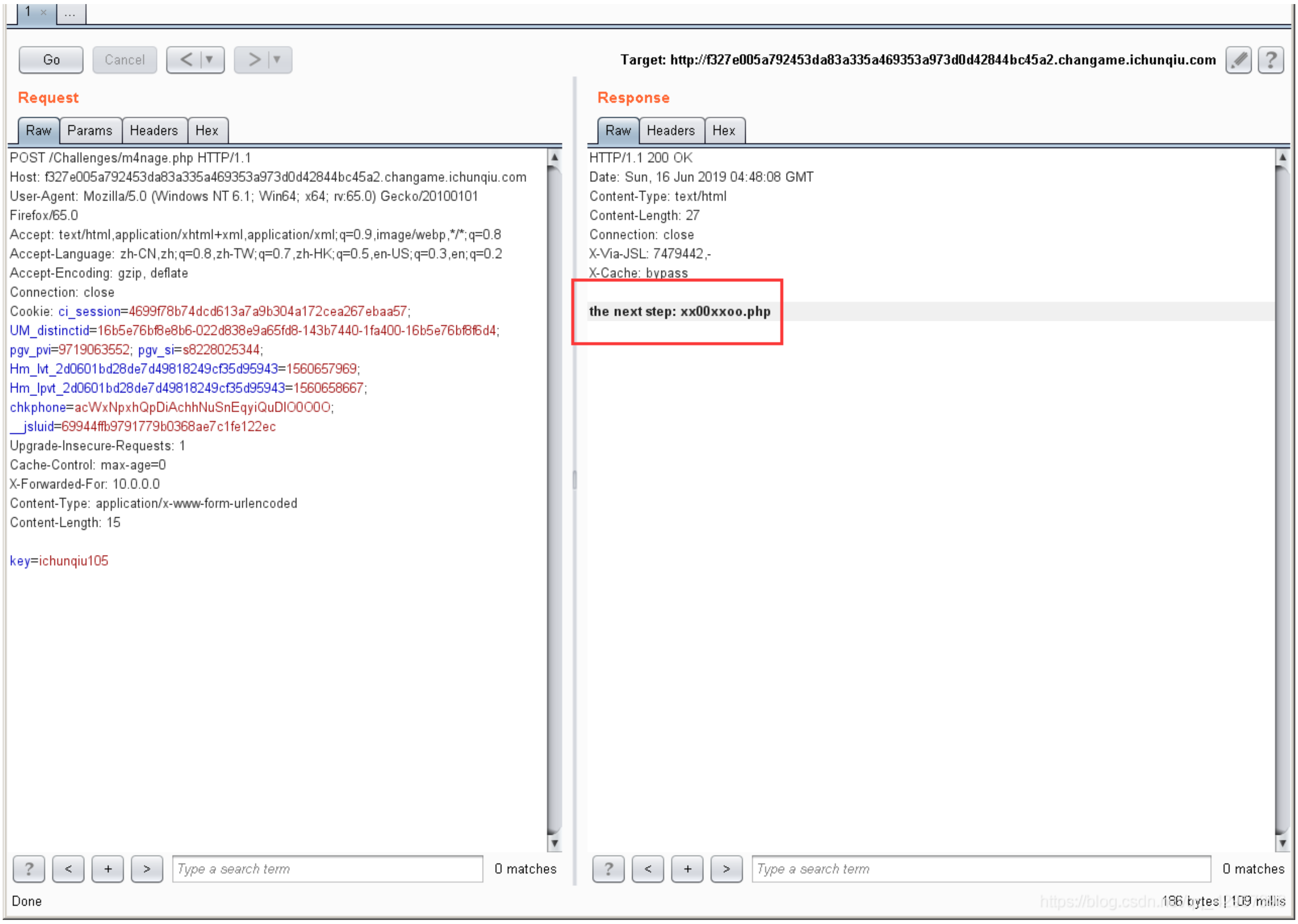


```
(base) C:\Users\Administrator>cd desktop

(base) C:\Users\Administrator\Desktop>python 1.py
ichunqiu105

(base) C:\Users\Administrator\Desktop>
```

得到一个新的提示，下一步：



Burp Suite Professional v1.7.31 - Temporary Project - licensed to surferxyz
Burp Intruder Repeater Window Help
Target
Proxy
Spider
Scanner
Intruder
Repeater
Sequencer
Decoder
Comparer
Extender
Project options
User options
Alerts

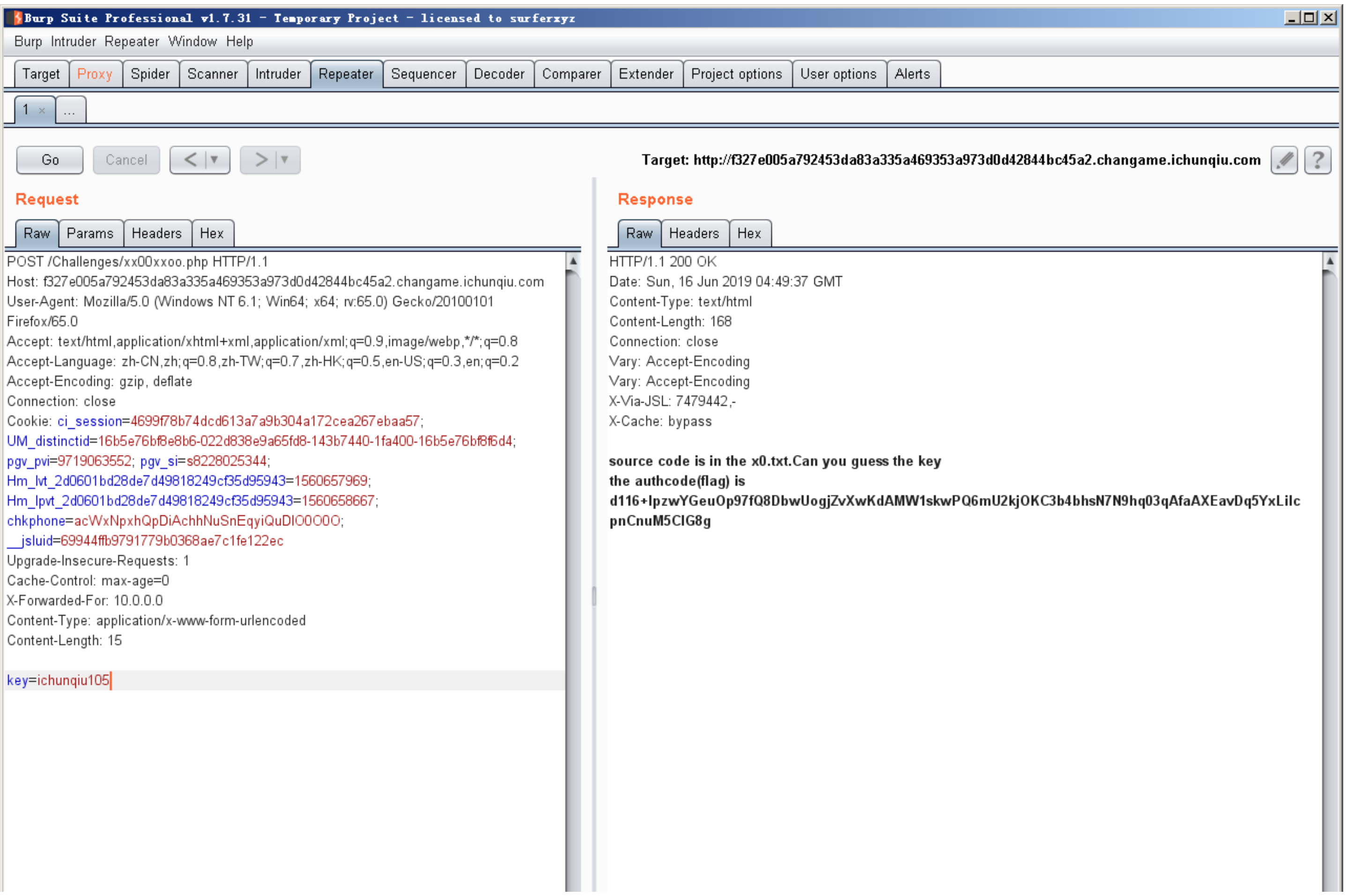


Target: http://f327e005a792453da83a335a469353a973d0d42844bc45a2.changame.ichunqiu.com

```
POST /Challenges/m4nage.php HTTP/1.1
Host: f327e005a792453da83a335a469353a973d0d42844bc45a2.changame.ichunqiu.com
User-Agent: Mozilla/5.0 (Windows NT 6.1; Win64; x64; rv:65.0) Gecko/20100101
Firefox/65.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Accept-Encoding: gzip, deflate
Connection: close
Cookie: ci_session=4699f78b74dcd613a7a9b304a172cea267ebaa57;
UM_distinctid=16b5e76bf8e8b6-022d838e9a65fd8-143b7440-1fa400-16b5e76bf8f6d4;
pgv_pvi=9719063552; pgv_si=s8228025344;
Hm_lvt_2d0601bd28de7d49818249cf35d95943=1560657969;
Hm_lpvt_2d0601bd28de7d49818249cf35d95943=1560658667;
chkphone=acWxNpxhQpDiAchhNuSnEqyiQuDIO0O0O;
__jsluid=69944ffb9791779b0368ae7c1fe122ec
Upgrade-Insecure-Requests: 1
Cache-Control: max-age=0
X-Forwarded-For: 10.0.0.0
Content-Type: application/x-www-form-urlencoded
Content-Length: 15

key=ichunqiu105
```

```
HTTP/1.1 200 OK
Date: Sun, 16 Jun 2019 04:48:08 GMT
Content-Type: text/html
Content-Length: 27
Connection: close
X-Via-JSL: 7479442,-
X-Cache: bypass

the next step: xx00xxoo.php
```

进入页面得到：



Target: http://f327e005a792453da83a335a469353a973d0d42844bc45a2.changame.ichunqiu.com

```
POST /Challenges/xx00xxoo.php HTTP/1.1
Host: f327e005a792453da83a335a469353a973d0d42844bc45a2.changame.ichunqiu.com
User-Agent: Mozilla/5.0 (Windows NT 6.1; Win64; x64; rv:65.0) Gecko/20100101
Firefox/65.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Accept-Encoding: gzip, deflate
Connection: close
Cookie: ci_session=4699f78b74dcd613a7a9b304a172cea267ebaa57;
UM_distinctid=16b5e76bf8e8b6-022d838e9a65fd8-143b7440-1fa400-16b5e76bf8f6d4;
pgv_pvi=9719063552; pgv_si=s8228025344;
Hm_lvt_2d0601bd28de7d49818249cf35d95943=1560657969;
Hm_lpvt_2d0601bd28de7d49818249cf35d95943=1560658667;
chkphone=acWxNpxhQpDiAchhNuSnEqyiQuDIO0O0O;
__jsluid=69944ffb9791779b0368ae7c1fe122ec
Upgrade-Insecure-Requests: 1
Cache-Control: max-age=0
X-Forwarded-For: 10.0.0.0
Content-Type: application/x-www-form-urlencoded
Content-Length: 15

key=ichunqiu105
```

```
HTTP/1.1 200 OK
Date: Sun, 16 Jun 2019 04:49:37 GMT
Content-Type: text/html
Content-Length: 168
Connection: close
Vary: Accept-Encoding
Vary: Accept-Encoding
X-Via-JSL: 7479442,-
X-Cache: bypass

source code is in the x0.txt.Can you guess the key
the authcode(flag) is
d116+lpzwYGeuOp97fQ8DbwUogjZvXwKdAMW1skwPQ6mU2kjOKC3b4bhsN7N9hq03qAfaAXEavDq5YxLilc
pnCnuM5ClG8g
```

源码在x0.txt内，附上源码：

```
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);
  } else {
   return '';
  }
 } else {
  return $keyc . str_replace('=', '', base64_encode($result));
 }

}
```

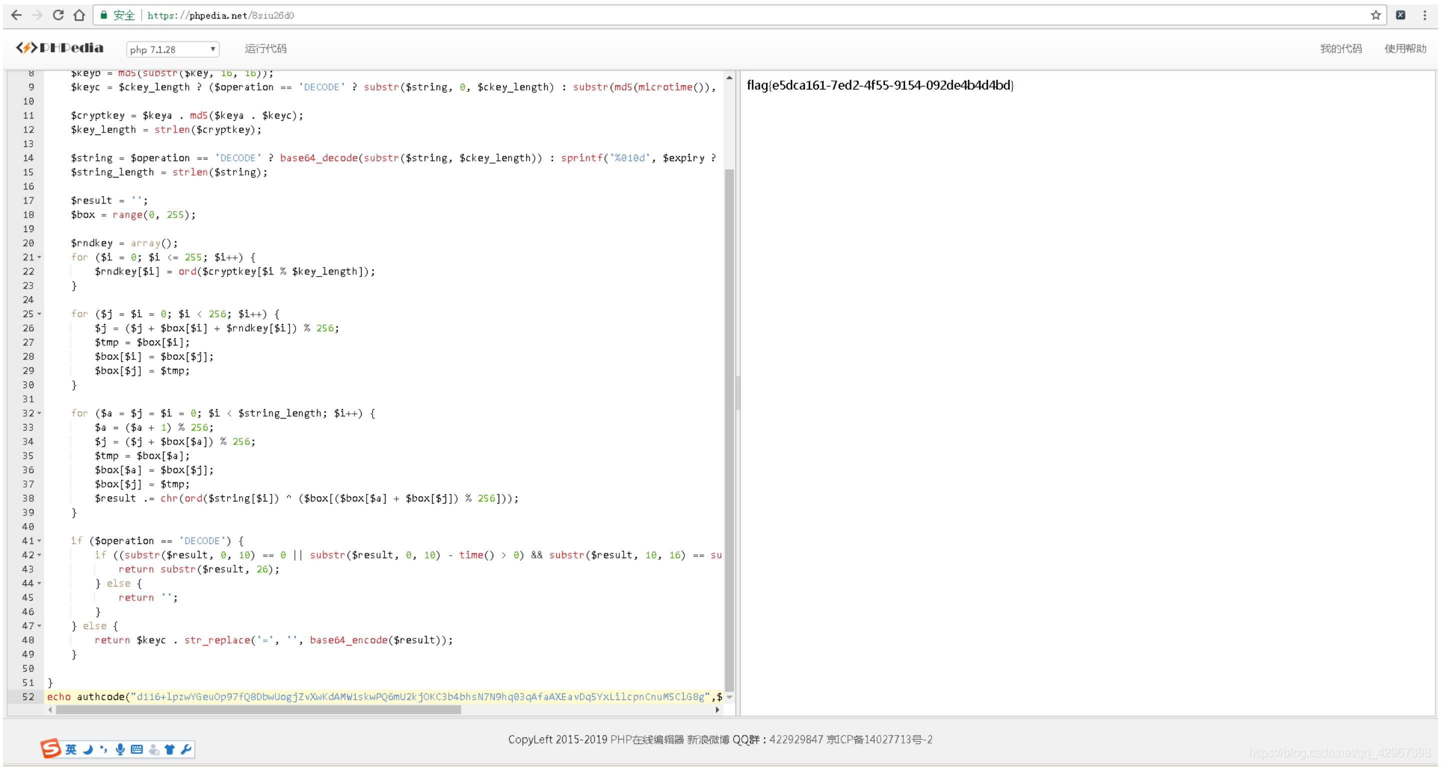
这个好像就是一个函数，而且是一个解密函数，DECODE嘛

我们直接调用这个函数来解密

直接echo

```
echo authcode("d116+lpzwYGeuOp97fQ8DbwUogjZvXwKdAMW1skwPQ6mU2kjOKC3b4bhsN7N9hq03qAfaAXEavDq5YxLilcpnCnuM5ClG8g",
$operation = 'DECODE', $key = 'ichunqiu105', $expiry = 0);
```

get flag:



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

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

    $string = $operation == 'DECODE' ? base64_decode(substr($string, $ckey_length)) : sprintf('%010d', $expiry ?
    $string_length = strlen($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) == su
            return substr($result, 26);
        } else {
            return '';
        }
    } else {
        return $keyc . str_replace('=', '', base64_encode($result));
    }

}
echo authcode("d116+lpzwYGeuOp97fQ8DbwUogjZvXwKdAMW1skwPQ6mU2kjOKC3b4bhsN7N9hq03qAfaAXEavDq5YxLilcpnCnuM5ClG8g",$
```

```
flag{e5dca161-7ed2-4f55-9154-092de4b4d4bd}
```

CopyLeft 2015-2019 PHP在线编辑器 新浪微博 QQ群：422929847 京ICP备14027713号-2

flag: `flag{e5dca161-7ed2-4f55-9154-092de4b4d4bd}`