

Bugkuctf web writeup

原创

k0sec 于 2019-03-18 21:14:51 发布 219 收藏 1

分类专栏: [bugkuctf writeup](#)

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/ghx13630444675/article/details/88595267>

版权



[bugkuctf writeup](#) 专栏收录该内容

1 篇文章 0 订阅

订阅专栏

web2 writeup

Challenge

8918 Solves



web2 20

听说聪明的人都能找到答案

<http://123.206.87.240:8002/web2/> <https://blog.csdn.net/ghx13630444675>

访问 <http://123.206.87.240:8002/web2/>

一堆滑稽。。。

页面没有任何提示, 查看一下源代码。点击鼠标右键, 发现没有查看源码选项, 正常情况下应该有。



猜测flag很可能在源代码中。

按F12:

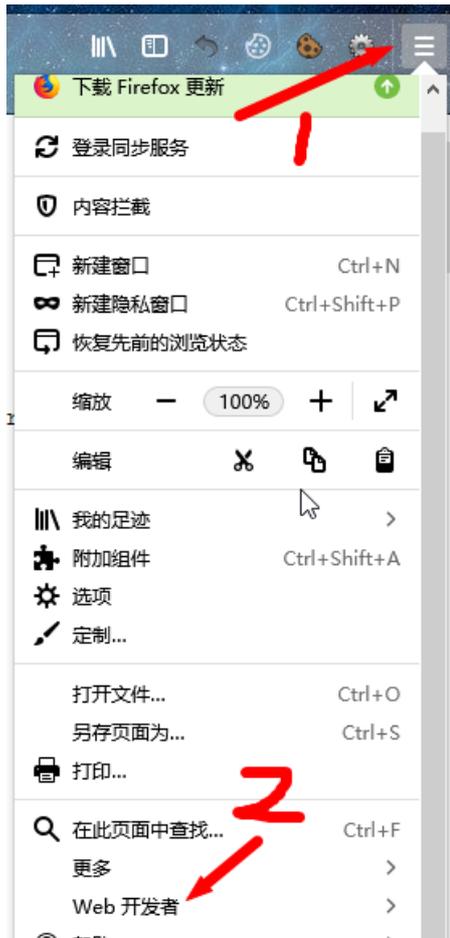


```
<html xmlns="http://www.w3.org/1999/xhtml"> event
  <head></head>
  <body id="body" onload="init()">
    <!--flag KEY{Web-2-bugKssNNikls9100}-->
    <script type="text/javascript" src="js/ThreeCanva
    <script type="text/javascript" src="js/Snow.js">
```

很显然，flag KEY{Web-2-bugKssNNikls9100}

总结，查看源代码的几种方法：

- (1) F12
- (2) Ctrl+U
- (3) 在url前面加上view-source:
- (4) 浏览器的设置菜单框中

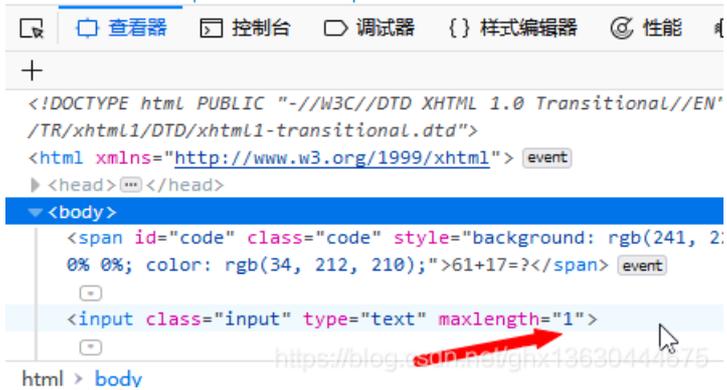


计算器 writeup

点击连接进入发现一道小学数学题。。。真的low,可是一顿操作算出78,却发现只能输入一个数字,见鬼了。。。



F12看下源代码



```
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN"
/TR/xhtml1/DTD/xhtml1-transitional.dtd">
<html xmlns="http://www.w3.org/1999/xhtml">
  <head>
  </head>
  <body>
    <span id="code" class="code" style="background: rgb(241, 241, 241); color: rgb(34, 212, 210);">61+17=?</span>
    <input class="input" type="text" maxlength="1">
```

原来是限制了只能输入一位,这可是为难我胖虎。。。

修改数值,增加输入位数



```
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional
/TR/xhtml1/DTD/xhtml1-transitional.dtd">
<html xmlns="http://www.w3.org/1999/xhtml">
  <head>
  </head>
  <body>
    <span id="code" class="code" style="background: rgb(241, 241, 241); color: rgb(136, 142, 32);">64+60=?</span>
    <input class="input" type="text" maxlength="2">
```

放回界面输入计所得的值,即得flag的值flag{CTF-bugku-0032}



web基础\$_GET

点击连接



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

<https://blog.csdn.net/ghx13630444675>

PHP程序员都想钱想疯了，所以他们喜欢在变量前面加

\$

这道题考get,不懂自己百度去

构造payload:



hat'];

回车就看到flag



```
$what=$_GET['what'];  
echo $what;  
if($what=='flag')  
echo 'flag{****}';  
flagflag{bugku_get_su8kej2en}
```

<https://blog.csdn.net/ghx13630444675>

web基础\$_POST

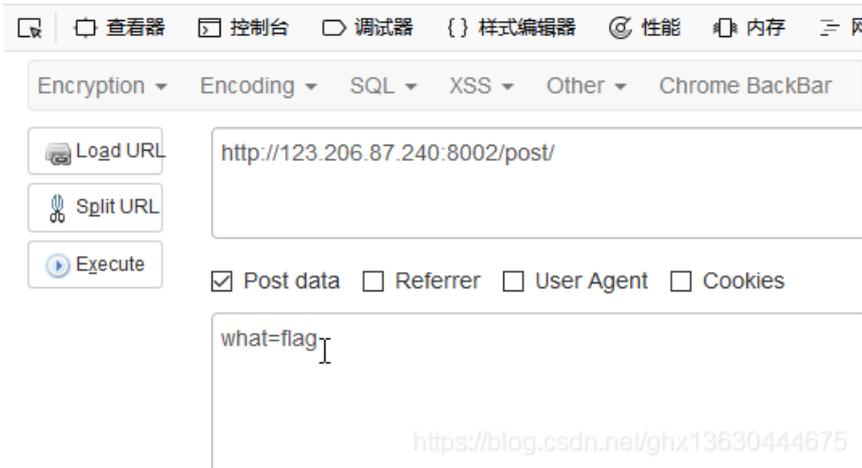
点击链接



<https://blog.csdn.net/ghx13630444675>

此时按F12启用hackbar

构造payload:



<https://blog.csdn.net/ghx13630444675>

回车可得flag



<https://blog.csdn.net/ghx13630444675>

叫个外卖，继续刷

矛盾

点击链接



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

<https://blog.csdn.net/ghx13630444675>

这段代码的意思，输入的值既不能是数字，又要和1相等

双等号==弱类型，判断的时候要进行弱类型转换，即1qweqw就转成1，而它本身又不是数字



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

<https://blog.csdn.net/ghx13630444675>

总结，网上除了以上解法，还有%00截断，%20截断

web3

点击链接



点击确定，看下什么效果





打上勾，点击确定

<https://blog.csdn.net/ghx13630444675>

F12查看源码，发现注释有点东西，跟“”类似，百度才知道后是Unicode编码

```

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"); alert("flag就在这
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");
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"); alert("flag就在这
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");
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"); alert("flag就在这
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");
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"); alert("flag就在这
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");
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>

```

所以转换成ASCLL编码，就得到flag

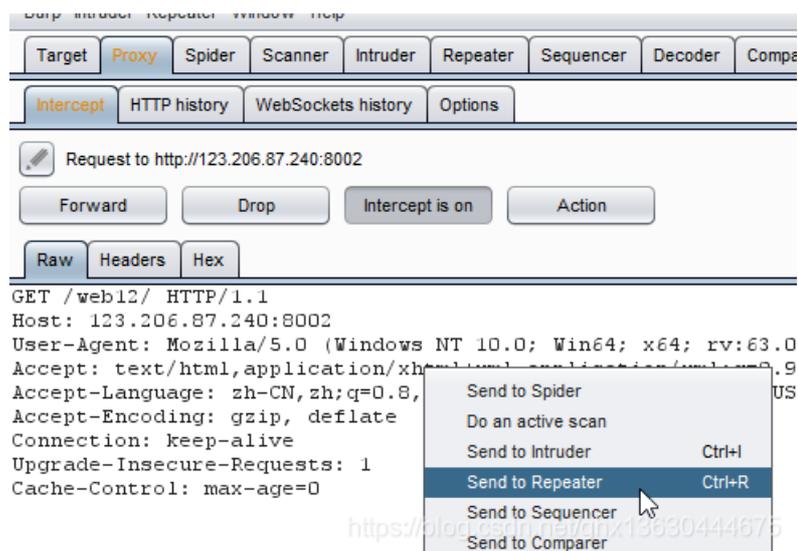
Unicode编码	UTF-8编码	URL编码/解码	Unix时间戳	Ascii/Native编码互转
<pre> &#75;&#69;&#89;&#123;&#74;&#50;&#115;&#97;&#52;&#50;&#97;&#104;&#74;&#75;&#45;&#72;&#83;&#49;&#49;&#73;&#73;&#73;&#125; </pre>				KEY{J2sa42ahJK-HS11III}

你必须让他停下

打开后，发现网址不停在跳转，遂用Burpsuite抓包



I want to play Dummy game with others; But I can't stop!
Stop at panda ! u will get flag



重放几次后得到flag

```
<script language="JavaScript">
function myrefresh(){
window.location.reload();
}
setTimeout('myrefresh()',500);
</script>
<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></center><br><a
style="display:none">flag{dummy_game_is_so_popular}</a></body>
</html>
```

变量1

[点击链接](#)



flag In the variable ! <?php

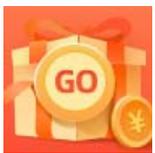
```
error_reporting(0);
include "flag1.php";
highlight_file(__file__);
if(isset($_GET['args'])){
    $args = $_GET['args'];
    if(!preg_match("/^\w+$/", $args)){
        die("args error!");
    }
    eval("var_dump($args);");
}
?>
```

<https://blog.csdn.net/ghx13630444675>

```
1 http://120.24.86.145:8004/index1.php
2 flag In the variable ! <?php
3
4
5 error_reporting(0); // 关闭php错误显示
6 include "flag1.php"; // 引入flag1.php文件代码
7 highlight_file(__file__); //对文件进行语法高亮显示
8 if(isset($_GET['args'])){ // 条件判断 get方法传递的args参数是否存在
9     $args = $_GET['args']; //赋值给变量 $args
10    if(!preg_match("/^\w+$/", $args)){ // /^开始, \w表示任意一个单词字符, 即[a-zA-Z0-9_], +将前面的字符匹
11        die("args error!"); //输出 args error!
12    }
13    eval("var_dump($args);"); // 将字符串作为php代码执行结尾加分号 var_dump()函数 显示关于一个或
14 }
15 ?>
```

复制

<https://blog.csdn.net/ghx13630444675>



[创作打卡挑战赛](#)

[赢取流量/现金/CSDN周边激励大奖](#)