

BugKu ——WP (WEB[一])

原创

[窝窝头_233](#) 于 2019-11-26 10:45:11 发布 173 收藏

分类专栏: [CTFwriteup](#) 文章标签: [ctf BugKuCTF](#)

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/hahaha233330/article/details/103251179>

版权



[CTFwriteup](#) 专栏收录该内容

20 篇文章 1 订阅

订阅专栏

【持续更新】BugKu ——WriteUp (一)

BugKu ——WEB

- [0] 工具:

①hackbar: web渗透的经典工具。

使用说明:

WEB

- 1、web2

题目地址

听说聪明的人都能找到答案

链接一打开, 满屏幕的滑稽, 简直是精神污染, 直接F12查看页面源代码得到flag。

- 2、计算器

题目地址



乍一看这多简单，直接输入结果，发现只能输

1位数，F12看一下源代码。

```
<body>
  <span id="code" class="code" style="background: rgb(153, 163, 61) none repeat scroll 0% 0%; color: rgb(72, 242, 135);">75+66=?</span>
  <input class="input" type="text" maxlength="1">
  <button id="check">验证</button>
  <div style="text-align:center;">
    <p>
      来源:
      <a href="http://ctf.bugku.com/" target="_blank">BugKu-ctf</a>
    </p>
  </div>
</body>
```

发现最

大长度动了手脚，双击一下修改长度，再输入正确结果即可拿到flag。

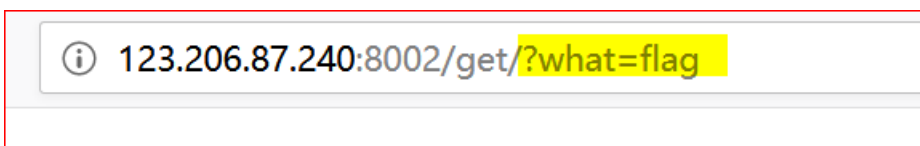
• 3、WEB \$GET

题目地址

这是一道 **get**传参 问题，阅读源代码可知：在参数 `what=flag` 的时候会回写 `flag{*****}`。

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

在url后面加上: `? what=flag`即可得到 `flag{*****}`。



**注意一定要加上 '?' 才可以get参数。

相关知识:

\$_GET :

- 1、预定义的 \$_GET 变量用于收集来自 method="get" 的表单中的值。
- 2、从带有 GET 方法的表单发送的信息，对任何人都是可见的（会显示在浏览器的地址栏），并且对发送信息的量也有限制。!

• 4、WEB \$POST

题目地址

阅读代码后可知是 **post** 传参，所以可构造一个 post 传参。使用 hackbar。

The screenshot shows a web browser window with the address bar containing `123.206.87.240:8002/post/?what=flag`. The page content displays a shell script:

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

Below the script, the Hackbar tool interface is visible. The 'Load URL' field contains `http://123.206.87.240:8002/post/?what=flag`. The 'Execute' button is circled in red. The 'Post data' checkbox is checked, and the 'Post data' field contains `what=flag`, with the word 'input' written in red next to it. The 'Referer', 'User Agent', and 'Cookies' checkboxes are unchecked. A 'Clear All' button is also present.

<https://blog.csdn.net/hahaha233330>

相关知识:

\$_POST:

- 1、预定义的 \$_POST 变量用于收集来自 method="post" 的表单中的值。
- 2、从带有 POST 方法的表单发送的信息，对任何人都是不可见的（不会显示在浏览器的地址栏），并且对发送信息的量也没有限制。

• 6、web3

题目地址

flag就在这里快来找找吧

