




ctf.bugku.com web_WriteUp

原创

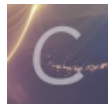
[lbabysit](#)  于 2021-05-02 11:58:24 发布  21  收藏

分类专栏: [ctf学习笔记](#) 文章标签: [web unctf](#)

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_53525138/article/details/116352417

版权



[ctf学习笔记](#) 专栏收录该内容

10 篇文章 0 订阅

订阅专栏

ctf.bugku.com web_WriteUp

web1

web1

WEB

已解决

分数: 10 金

题目作者: harry

一血: CyberFI0wer

一血奖励: 1金币

解决: 6923

提示: 官方交流群: 830263119

描述: flag{}

<http://114.67.246.176:15102>

02:59:48

删除场景

延时场景

https://blog.csdn.net/qq_53525138



F12解决

web2

web2 WEB 已解决

分数: 10 金币: 1

题目作者: harry

— 血: CyberFI0wer

— 血奖励: 1金币

解 决: 6354

提 示:

描 述: 输入验证码即可得到flag

<http://114.67.246.176:13731>

02:59:47

删除场景

延时场景

请输入flag

https://blog.csdn.net/hq_58585138 提交

84+58=? 验证

来源: BugKu-ctf

```
<html xmlns="http://www.w3.org/1999/xhtml">
  <head>...</head>
  <body> ...
    <span id="code" class="code" style="background: rgb(237, 189, 21); color: 252);">84+58=?</span>
    <input type="text" class="input" maxlength="1">
    <button id="check">验证</button>
  </div style="text-align:center;">
  <script src="js/jquery-1.12.4.min.js"></script>
  <script type="text/javascript" src="js/code.js"></script>
  <div id="qb-sougou-search" style="display: none; opacity: 0;">...</div>
</body>
</html>
```

html body

Filter: show .cls +

element.style {

body {

display: block;

margin: 8px;

margin: 8

border: -

padding: -

964 × 63

F12,修改html表单限制。

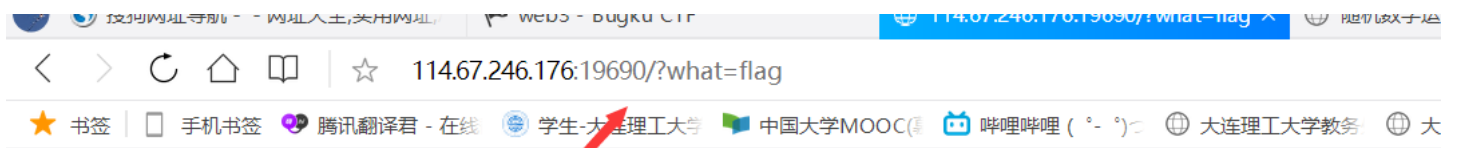
web3



```
!what=$_GET['what'];
!cho $what;
f($what=='flag')
!cho 'flag{****}';
```

https://blog.csdn.net/qq_53525138

增加get请求参数



```
$what=$_GET['what'];
echo $what;
if($what=='flag')
echo 'flag{****}';
flagflag{d348070cbcdfec3aab20c14fd65be9} flag{d348070cbcdfec3aab20c14fd65be9}
```

https://blog.csdn.net/qq_53525138

web4

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

HackBar 查看器 控制台 调试器 网络 样式编辑器 性能 内存 存储 无障碍环境 应用

Encryption Encoding SQL XSS Other

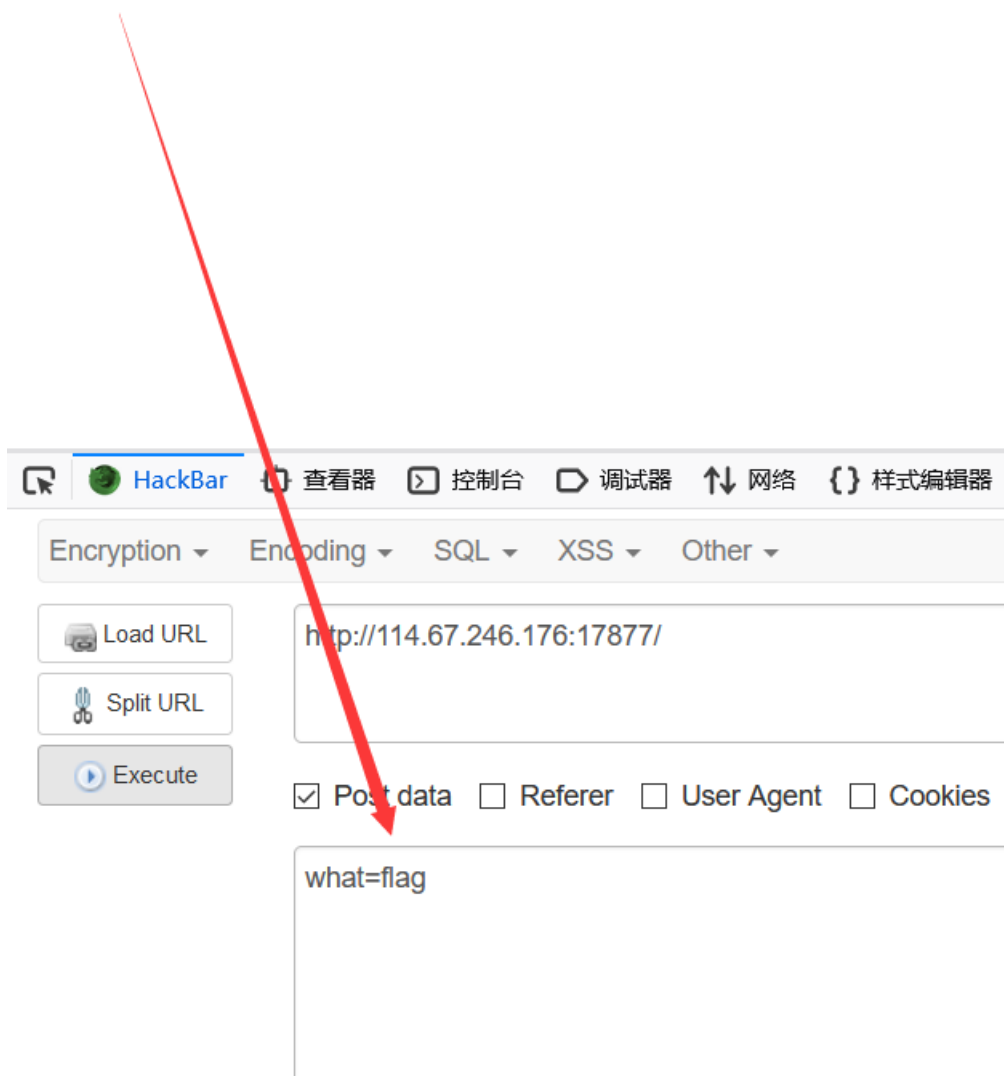
Load URL Split URL Execute

http://114.67.246.176:17877/

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

在火狐浏览器hackbar插件中输入打开网页，使用POST请求方式

```
$what=$_POST['what'];  
echo $what;  
if($what=='flag')  
echo 'flag{****}';  
flagflag{88a0f6ec0eb703e2c262a747bc99bf1b}
```



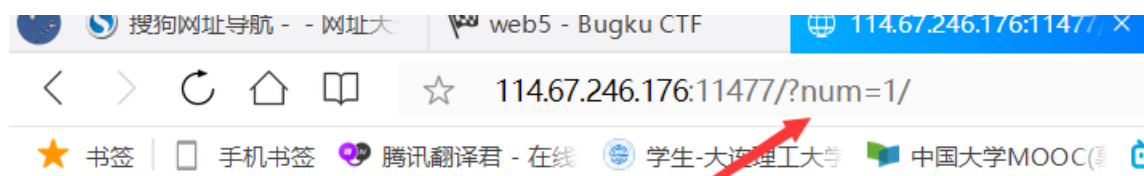
https://blog.csdn.net/qq_53525138

web5

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

https://blog.csdn.net/qq_53525138

增加get请求参数，注意url最后的/



```
$num=$_GET['num'];
if(!is_numeric($num))
{
echo $num;
if($num==1)
echo 'flag{*****}';
}
1/flag{a6bdb79b51af81d4db46a6bc35c5d515}
```

https://blog.csdn.net/qq_53525138

web6



114.67.246.176:10278 显示

flag就在这里

确定

https://blog.csdn.net/qq_53525138

火狐浏览器查看源代码，在注释中有一段数字，使用Unicode解码



unicode编码转换器

好词好句，次阅读

欢迎使用汉字转化unicode编码工具，此程序将一段中文字转换成unicode编码，也能将unicode编码转换为汉字，还具有汉字转十六进制功能，只需要在内容源文本框中输入汉字、unicode汉字编码、十六进制汉字编码即可转换为相应内容。

内容源文本框: Ascii字符补齐4位

```
&#102;&#108;&#97;&#103;&#123;&#97;&#48;&#54;&#98;&#57;&#51;&#54;&#97;&#49;&#49;&#51;&#50;&#53;&#54;&#54;&#56;&#97;&#57;&#49;&#98;&#48;&#52;&#100;&#54;&#97;&#53;&#54;&#48;&#52;&#57;&#49;&#57;&#125;
```

转Unicode编码(\uXXXX)

转换为(&#DDDDDD)

转换为&#XXXX

转换为汉字

转换结果:

```
flag{a06b936a11325668a91b04d6a5604919}
```

https://blog.csdn.net/qq_53525138

