

# 安全-POST (BugkuCTF)

原创

小狐狸FM 于 2021-07-05 11:46:48 发布 95 收藏

分类专栏: [安全 # CTF夺旗](#) 文章标签: [post ctf web php](#)

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/smallfox233/article/details/118486965>

版权



[安全](#) 同时被 2 个专栏收录

91 篇文章 9 订阅

订阅专栏



[CTF夺旗](#)

38 篇文章 0 订阅

订阅专栏

## 文章目录

- 一、题目
- 二、WriteUp

## 一、题目

原题链接

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

## 二、WriteUp

可以使用 [Firefox](#) 浏览器的请求提交插件 [Poster](#) 或者是抓包软件 [Burpsuite](#) 提交 `post` 请求  
`php` 代码中, 对 `what` 参数进行了判断, 当值为 `flag` 时就会显示 `flag`

获取附加组件

- 扩展
- 外观
- 插件

### NETCRATT EXTENSION

Comprehensive site information and protection

### Poster

A developer tool for interacting with URLs [更改](#)

INT

SQL BASICS- UNION BASED- ERROR/DOUBLE QUERY- TOOLS- WAF BYPA!

Load URL

Split URL

Execute

Post data

Post data  Referrer  0xHEX  %URL  BASE64

<https://blog.csdn.net/smallfox233>

```
$what=$_POST['what'];  
echo $what;  
if($what=='flag')  
echo 'flag{****}';  
flagflag{c303a9e8b6c6d17fdc1ef41aac3bb802}
```