

Bugku-web-web基础\$_POST writeup

原创

MoonBack明月归 于 2019-06-07 21:38:52 发布 2357 收藏 8

分类专栏: [BugKu](#) 文章标签: [CTF web BugKu](#)

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/weixin_43826194/article/details/91152998

版权



[BugKu 专栏收录该内容](#)

9 篇文章 0 订阅

订阅专栏

题目网址

<http://123.206.87.240:8002/post/>

```
123.206.87.240:8002/post/
$what=$_POST['what'];
echo $what;
if($what=='flag')
echo 'flag{****}';
```

题解

方法

由POST请求方法可知只要传递相应参数即可获得相应内容

图解

方式一: HackBar

```
123.206.87.240:8002/post/
$what=$_POST['what'];
echo $what;
if($what=='flag')
echo 'flag{****}';
```

POST方式, 和GET方式不同的是URL里没有信息

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

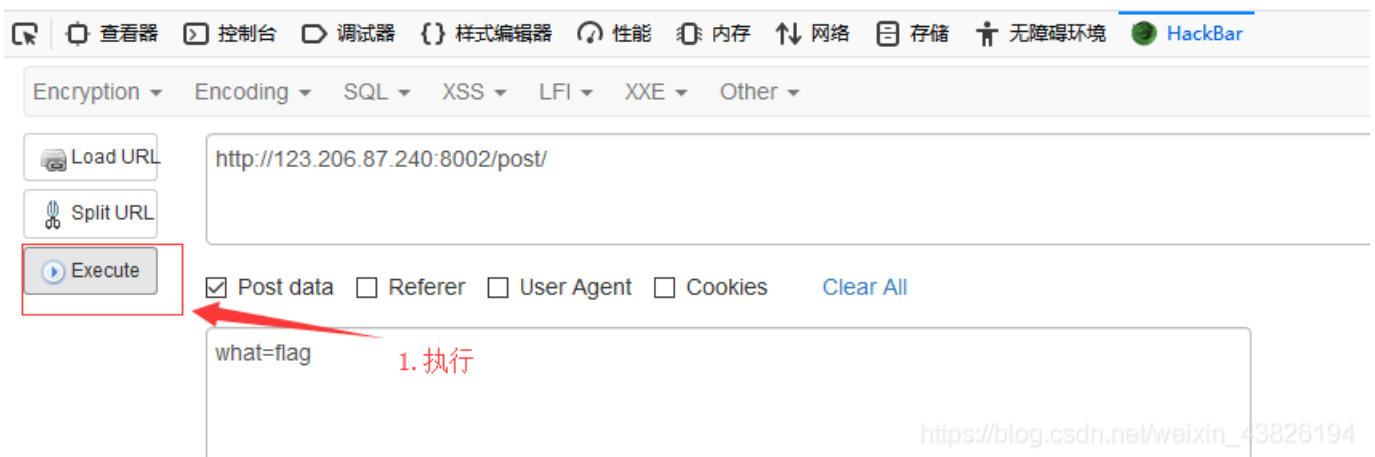
1. 有代码可知需要向服务器发送POST请求，请求内容为what=flag即可输出flag

2. F12打开开发者工具(请事先装好HackBar) 打开HackBar



```
$what=$_POST['what'];  
echo $what;  
if($what=='flag')  
echo 'flag{****}';  
flagflag{bugku_get_ssseint67se}
```

2. 得到flag



方式二：Burpsuite抓包

Intercept HTTP history WebSockets history Options

Proxy Listeners

Burp Proxy uses listeners to receive incoming HTTP requests from your browser. You will need to configure your browser to use one of the listeners as its proxy server.

Running	Interface	Invisible	Redirect	Certificate
<input checked="" type="checkbox"/>	127.0.0.1:8080			Per-host

浏览器设置的代理服务器要和这个一致

Each installation of Burp generates its own CA certificate that Proxy listeners can use when negotiating SSL connections. You can import or export this certificate:

Import / export CA certificate Regenerate CA certificate

https://blog.csdn.net/weixin_43826194

连接设置

配置访问互联网的代理服务器

不使用代理服务器(Y)
 自动检测此网络的代理设置(W)
 使用系统代理设置(U)
 手动代理配置(M)

HTTP 代理(X) 127.0.0.1 端口(P) 8080

为所有协议使用相同代理服务器(S)

SSL 代理 127.0.0.1 端口(O) 8080

FTP 代理 127.0.0.1 端口(R) 8080

SOCKS 主机 127.0.0.1 端口(I) 8080

SOCKS v4 SOCKS v5

自动代理配置的 URL (PAC)

重新载入(E)

不使用代理(N)

确定 取消 帮助(H)

https://blog.csdn.net/weixin_43826194

Burp Suite Professional v1.7.37 - Temporary Project - licensed to surferxyz

Burp Intruder Repeater Window Help

Target Proxy Spider Scanner Intruder Repeater Sequencer Decoder Comparer Extender Project options User options Alerts

Intercept HTTP history WebSockets history Options

Request to http://123.206.87.240:8002

Forward Drop Intercept is on Action

Raw Headers Hex

GET /post/ HTTP/1.1
Host: 123.206.87.240:8002

1. 打开浏览器时应先关闭，防止从其他URL抓到的包干扰。
2. 开启这个，访问试题网址，得到以下的请求头
3. 发现并不是我们想要的POST类型，改变类型

```
Host: 123.206.87.240:8002
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:67.0) Gecko/20100101 Firefox/67.0
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
Upgrade-Insecure-Requests: 1
```

https://blog.csdn.net/weixin_43826194

Burp Suite Professional v1.7.37 - Temporary Project - licensed to surferxyz

Request to http://123.206.87.240:8002 3. 推送数据包

Forward Drop Intercept is on Action

Raw Headers Hex

```
POST /post/ HTTP/1.1
Host: 123.206.87.240:8002
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:67.0) Gecko/20100101 Firefox/67.0
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
Upgrade-Insecure-Requests: 1
Content-Type: application/x-www-form-urlencoded
Content-Length: 0
```

what=flag

2. 在末尾加上参数
要与前面的内容空一行

- Send to Spider
- Do an active scan
- Send to Intruder Ctrl+I
- Send to Repeater Ctrl+R
- Send to Sequencer
- Send to Comparer
- Send to Decoder
- Request in browser ▶
- Engagement tools ▶
- Change request method
- Change body encoding
- Copy URL
- Copy as curl command
- Copy to file

1. 改变请求方式 (图为改过的)

https://blog.csdn.net/weixin_43826194

123.206.87.240:8002/post/

```
$what=$_POST['what'];
echo $what;
if($what=='flag')
echo 'flag{****}';
flagflag{bugku_get_sseint67se}
```

得到flag

https://blog.csdn.net/weixin_43826194

方法三: python的requests模块

```
import requests

s = requests.Session()
values={'what':'flag'}
r = s.post("http://123.206.87.240:8002/post/", values)
print(r.text)
```

成功解题