Bugku-web-web基础$_POST writeup

原创

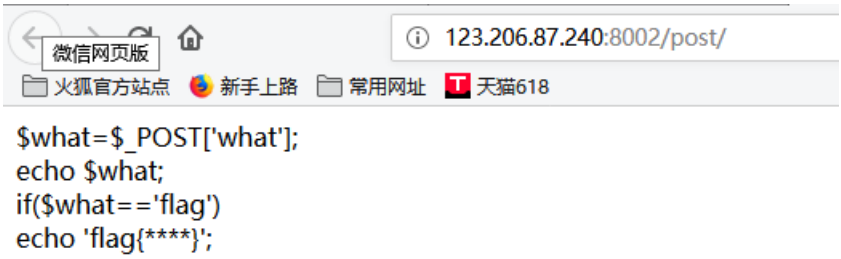
MoonBack明月归 于 2019-06-07 21:38:52 发布 2357 收藏 8

分类专栏： BugKu 文章标签： CTF web BugKu

本文链接：https://blog.csdn.net/weixin_43826194/article/details/91152998

题目网址

```
http://123.206.87.240:8002/post/
```



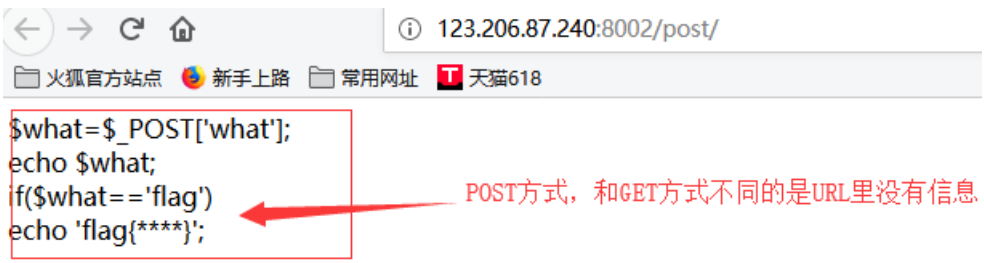
题解

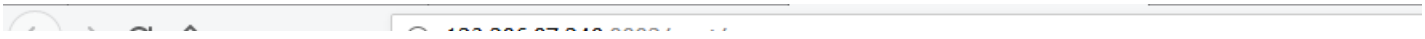
方法

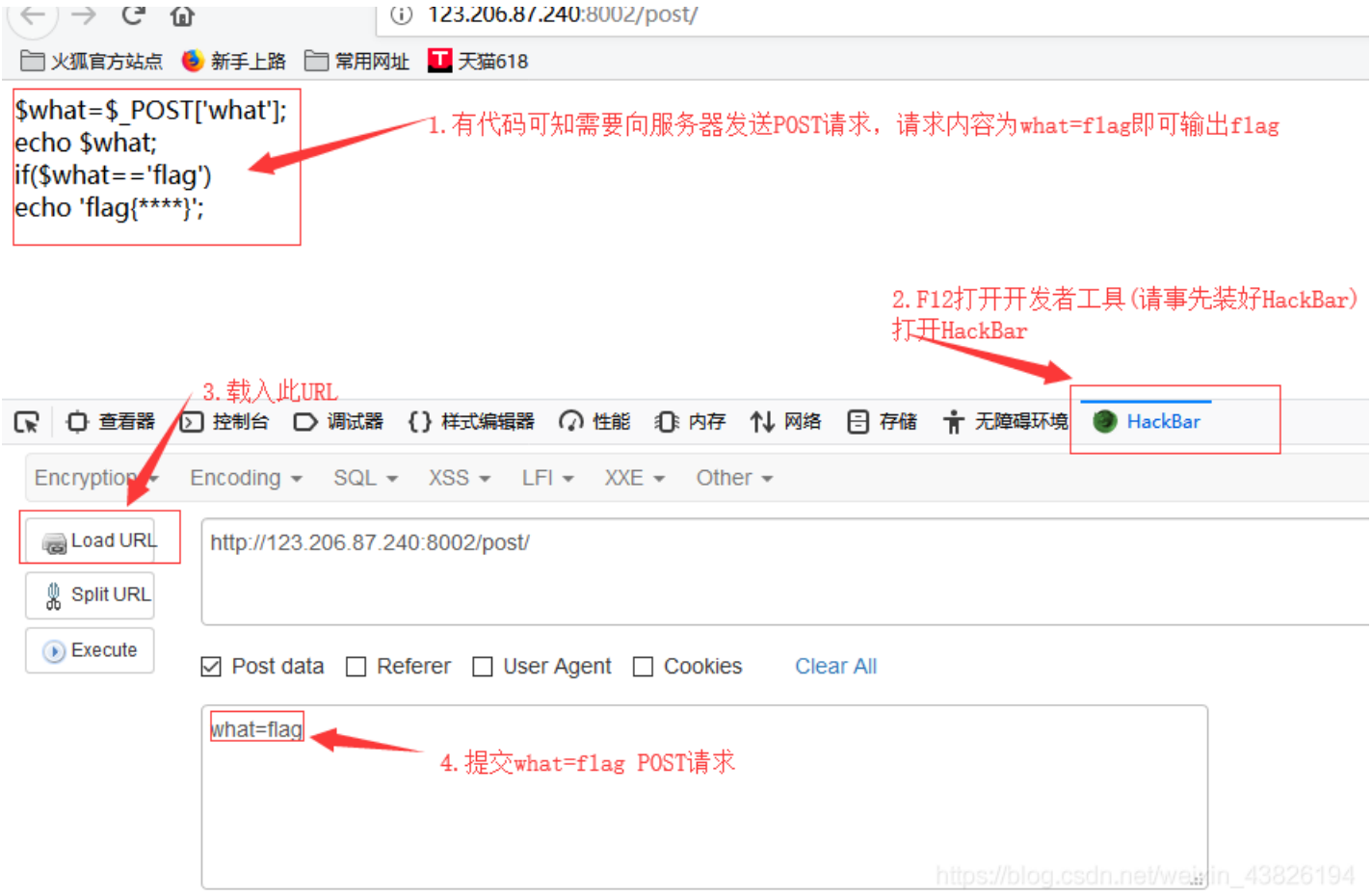
```
由POST请求方法可知只要传递相应参数即可获得相应内容
```

图解

方式一：HackBar

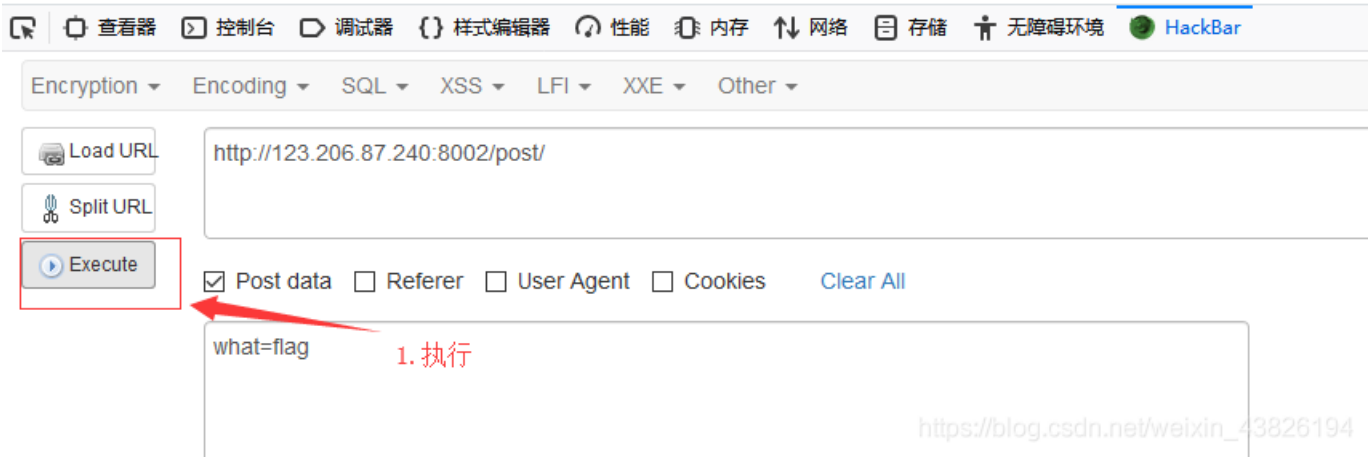




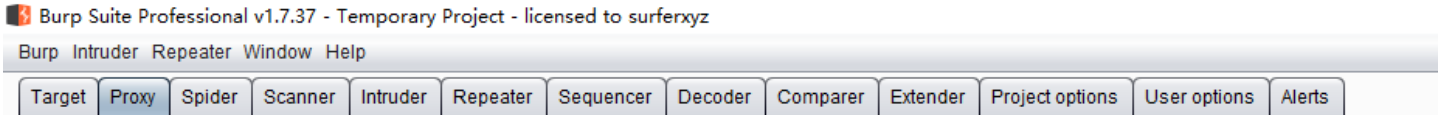


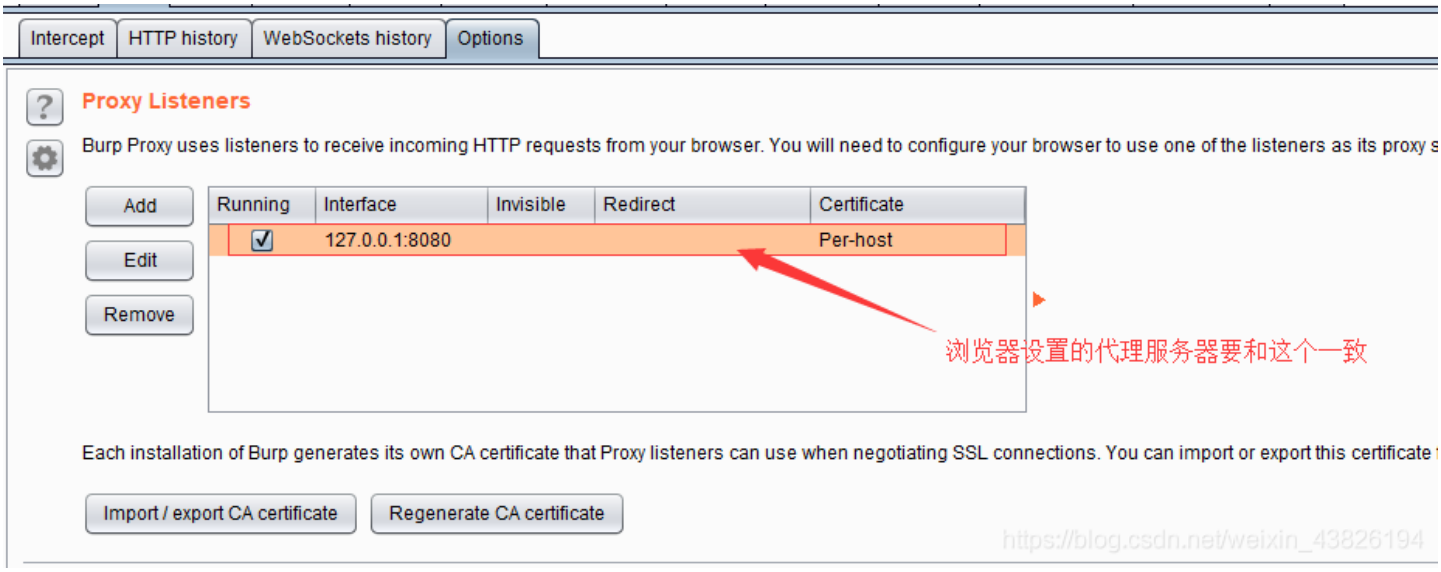

```
$what=$_POST['what'];
echo $what;
if($what=='flag')
echo 'flag{****}';
flagflag{bugku_get_ssseint67se}
```

2. 得到flag

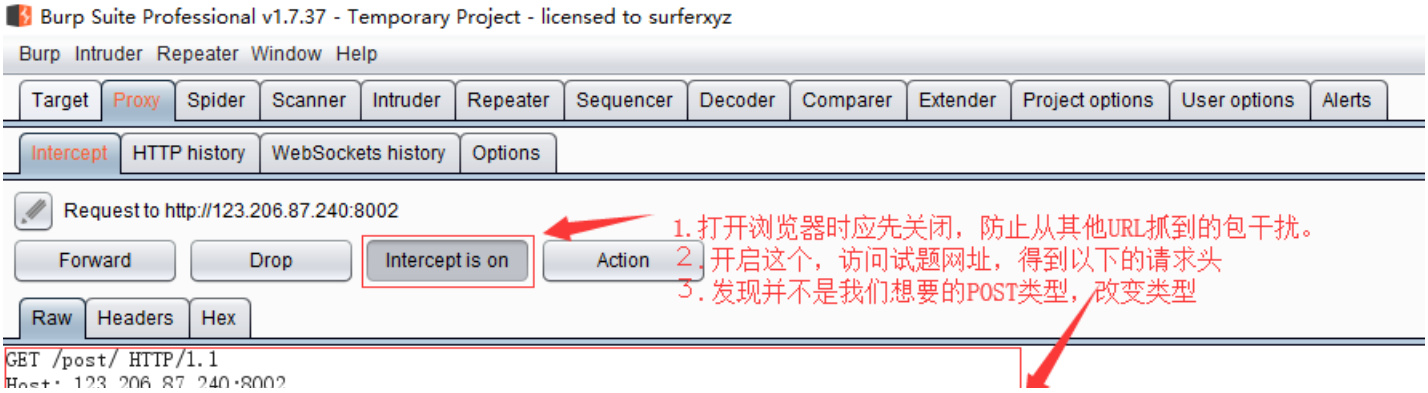


方式二：Burpsuite抓包

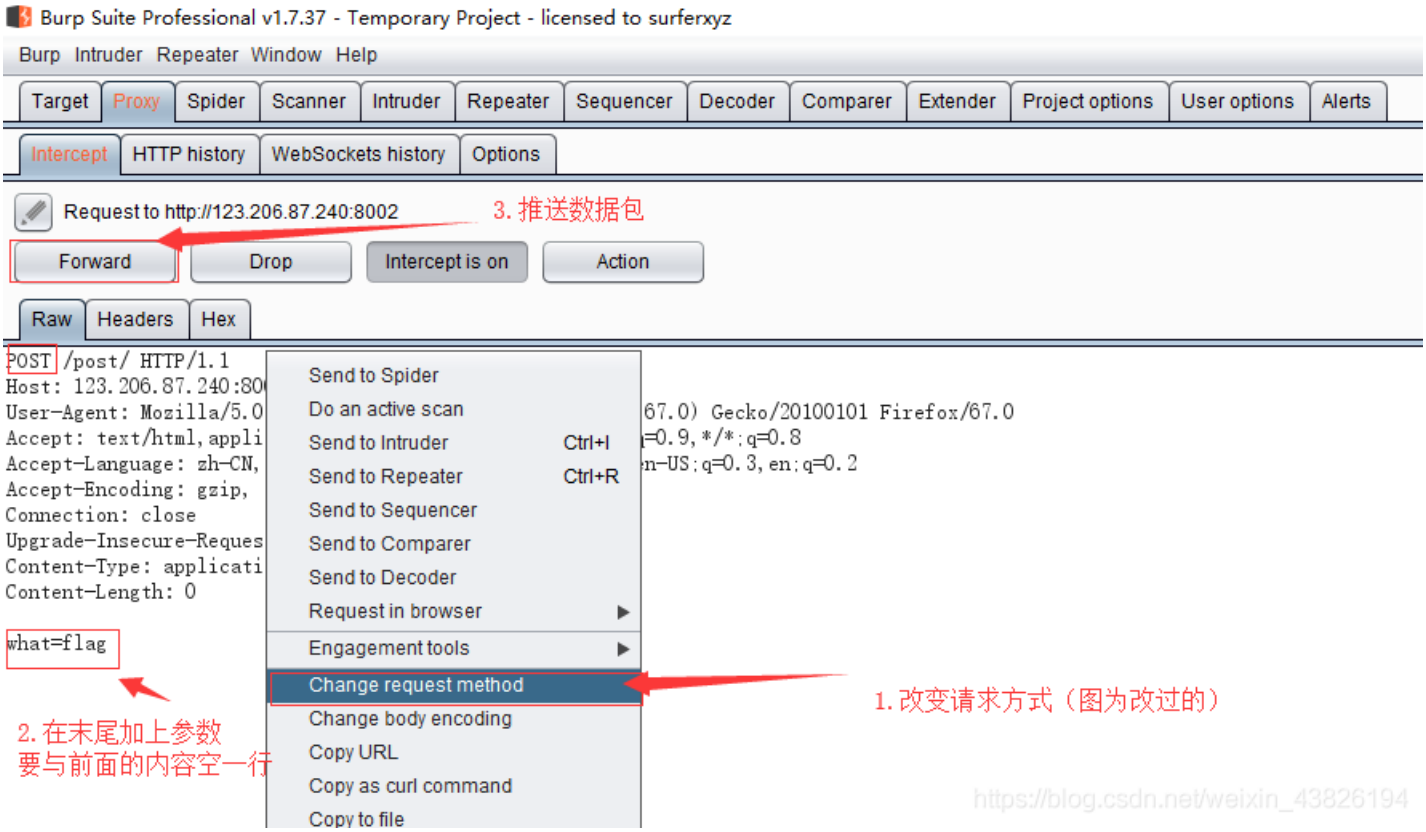


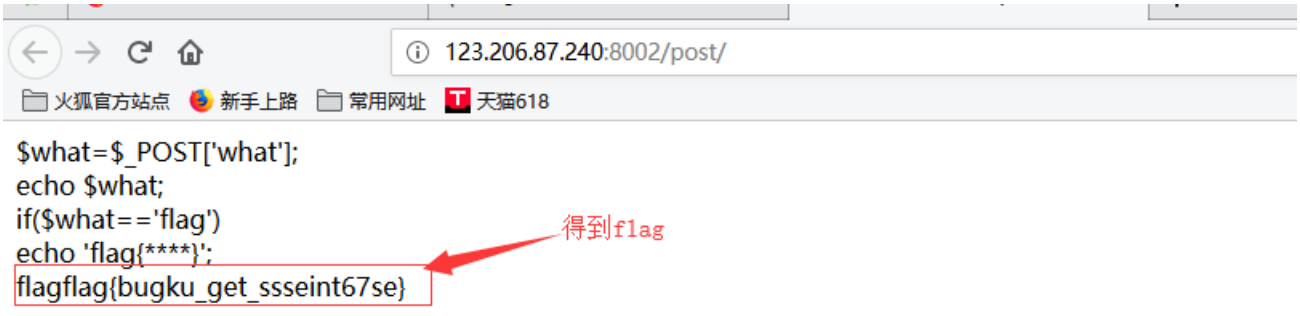

Intercept
HTTP history
WebSockets history
Options
Proxy Listeners
Burp Proxy uses listeners to receive incoming HTTP requests from your browser. You will need to configure your browser to use one of the listeners as its proxy s
Add
Edit
Remove
Running
Interface
Invisible
Redirect
Certificate
127.0.0.1:8080
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
端口(O)
FTP 代理
端口(R)
SOCKS 主机
端口(T)
SOCKS v4
SOCKS v5
自动代理配置的 URL（PAC）
重新载入(E)
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
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
Raw
Headers
Hex
GET /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
```



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