

# CTF-Bugku-Web\$\_GET && \$\_POST基础

原创

fzykn06 于 2019-03-22 21:06:13 发布 717 收藏 1

分类专栏: [CTF\\_writeup](#) 文章标签: [bugku writeup](#)

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/fzykn06/article/details/88745789>

版权



[CTF\\_writeup](#) 专栏收录该内容

4 篇文章 0 订阅

订阅专栏

第一次在Bugku有点抓狂, 挺多方法不会使用, 导致做题很慢, 哪怕是简单的题目都挺解, 以后要多熟悉这些方法。首先先讲讲一些简单的签到题, 十分的基础的题目。

## web 2

<http://123.206.87.240:8002/web2/>

这是一道有趣的签到题, 答案只要在源码中就能找到, 但是如果没想到找源码的话就有点麻烦, 因为它是一个动态图, 越看越晕。

按F12查看源码

```
<!doctype html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN"
"http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd">
<html xmlns="http://www.w3.org/1999/xhtml">
  <head>...</head>
  <body id="body" onload="init()" >
    <!--flag KEY{Web-2-bugKssNNik1s9100}-->
    <script type="text/javascript" src="js/ThreeCanvas.js"></script>
    <script type="text/javascript" src="js/Snow.js"></script>
    <script type="text/javascript">
      var SCREEN_WIDTH = window.innerWidth;//
      var SCREEN_HEIGHT = window.innerHeight;
```

就能找到flag啦~

## 计算器

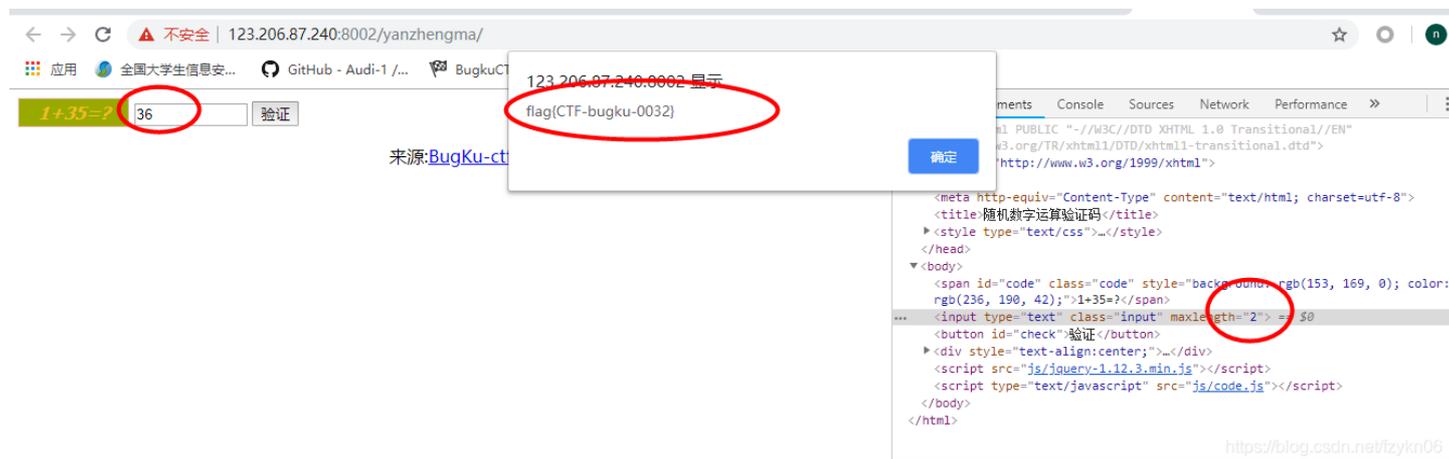
<http://123.206.87.240:8002/yanzhengma/>

这道题有点意思，我们如果没接触到解法的话，或许真的有点难知道，因为它是将要填的地方限定在一个字符，但是答案都是两个字符以上的，有点难受啊当初，想到了就是按F12将空格改为需要大小的字符就好啦

```
<!doctype html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN"
"http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd">
<html xmlns="http://www.w3.org/1999/xhtml">
  <head>
    <meta http-equiv="Content-Type" content="text/html; charset=utf-8">
    <title>随机数字运算验证码</title>
    <style type="text/css">...</style> == $0
  </head>
  <body>
    <span id="code" class="code" style="background: rgb(153, 169, 0); color:
    rgb(236, 190, 42);">1+35=?</span>
    <input type="text" class="input" maxlength="1">
    <button id="check">验证</button>
    <script src="js/jquery-1.12.3.min.js"></script>
    <script type="text/javascript" src="js/code.js"></script>
  </body>
</html>
```

<https://blog.csdn.net/fzykn06>

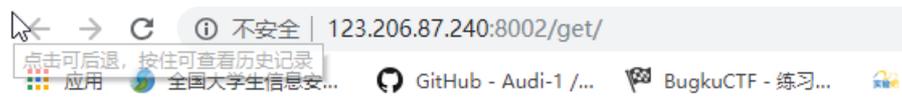
将最大长度改为2就能输入两个字符，然后输入答案就能得到我们的flag啦



## web基础\$\_GET

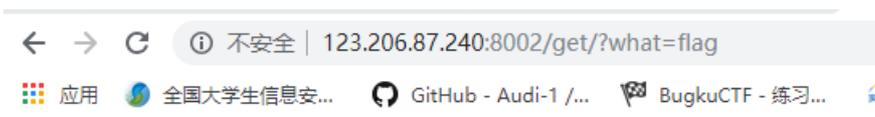
<http://123.206.87.240:8002/get/>

这题考察php的get变量，\$\_GET获取参数其实很简单，在浏览器中进行url改一下就好了，打开网址，我们获得以下信息：



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

如果能看懂php代码就很好做了，这是通过\$\_GET来获取参数，输出\$what,如果说\$what=flag,就能输出flag，这就很简单了，只需要在url上增加? what=flag就能出答案了，就是将what值为flag传入：



```
$what=$_GET['what'];
echo $what;
if($what=='flag')
echo 'flag{****}';
flagflag{bugku_get_su8kej2en}
```

<https://blog.csdn.net/fzykn06>

这样我们就获取到该题的flag

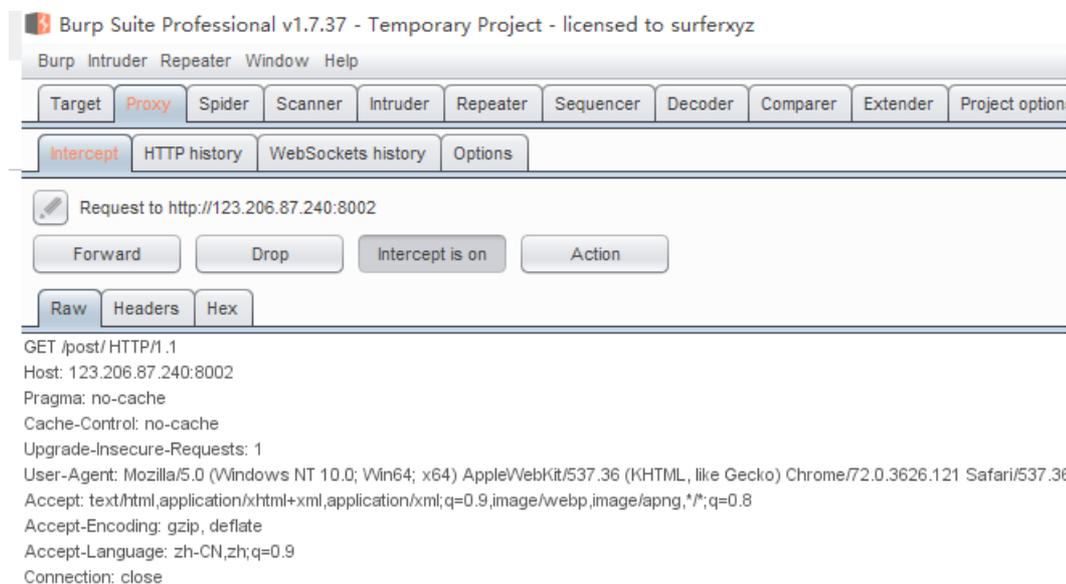
## web基础\$\_POST

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

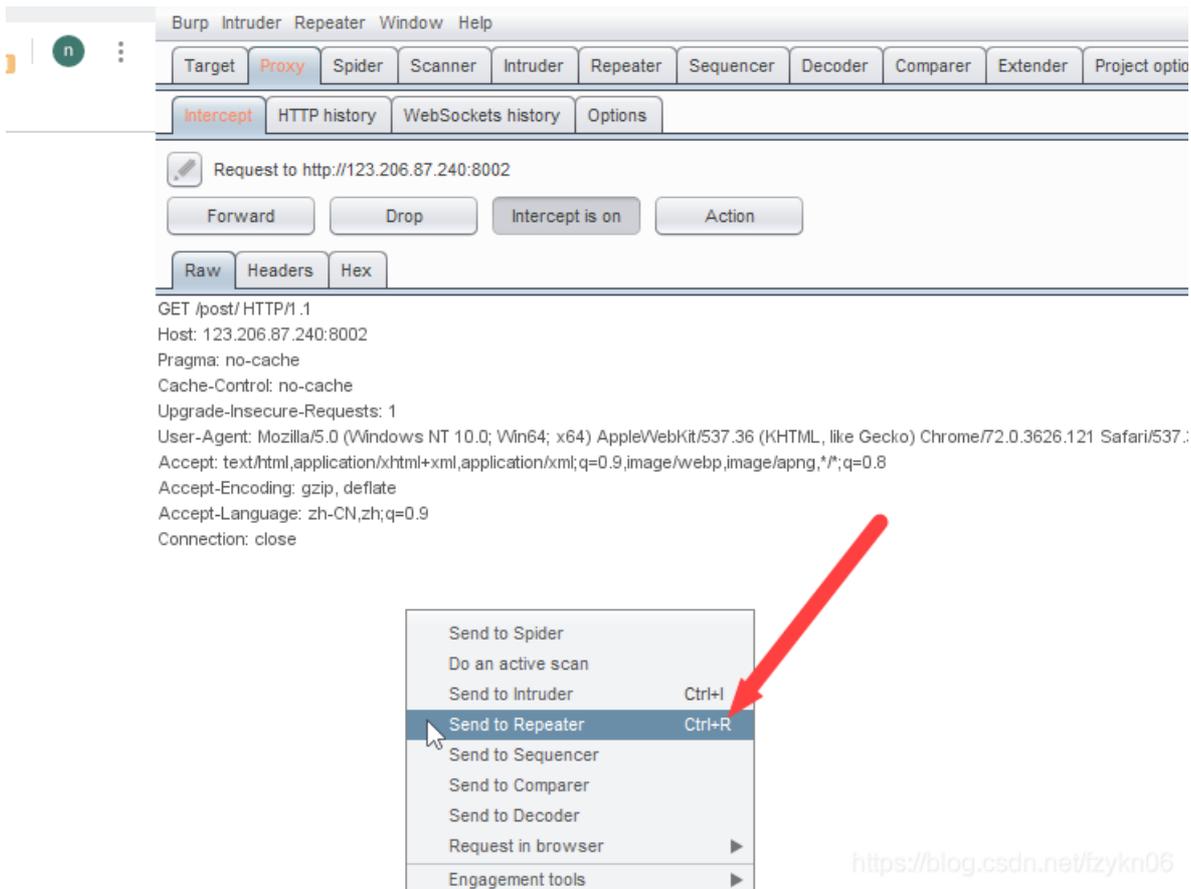
这题很有意思啊，跟上题很像，就是请求方式不同，如果小白接触这题，做完上面这道题，很容易的就是将? what=flag直接在url上改了，其实post请求方式不是这样，post是将参数在数据包内进行传递。在看了一些writeup后有三种方法：

- 火狐浏览器的hackbar插件
- bp抓包，然后添加参数发送
- python爆破

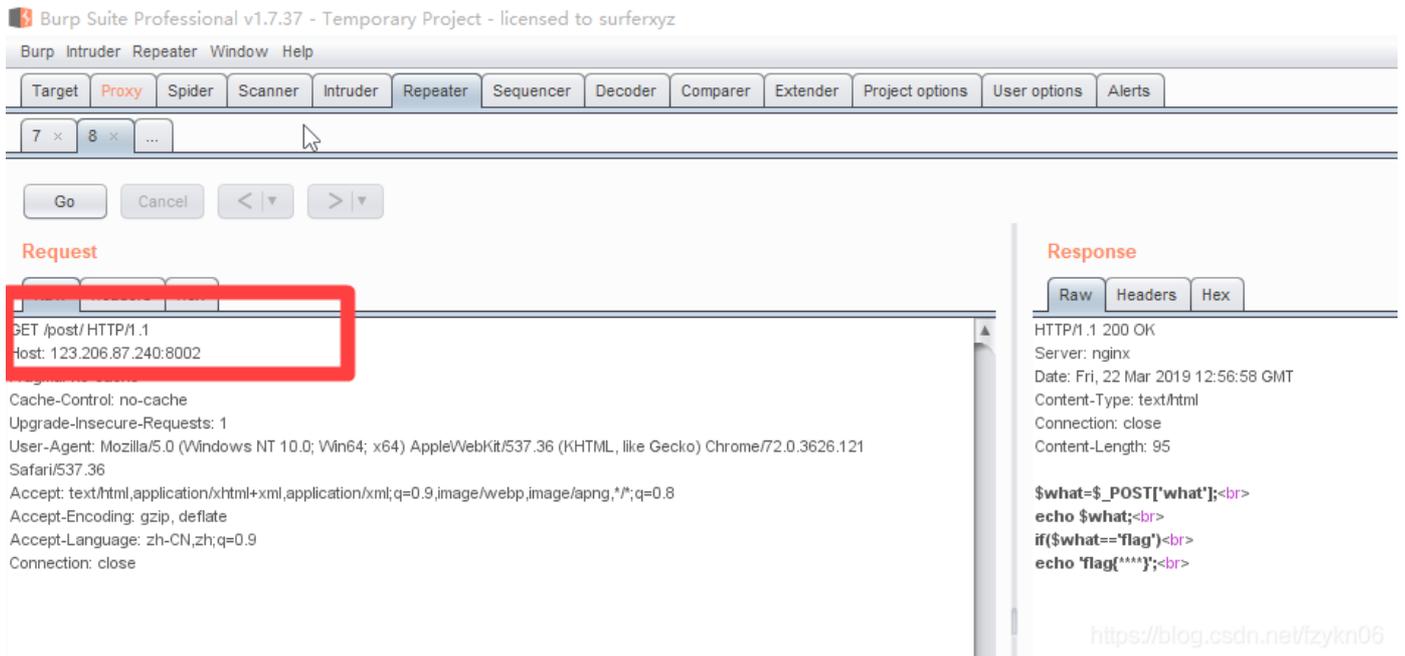
在这边我使用了bp的方式



右键将截取到的包扔到Repeater,

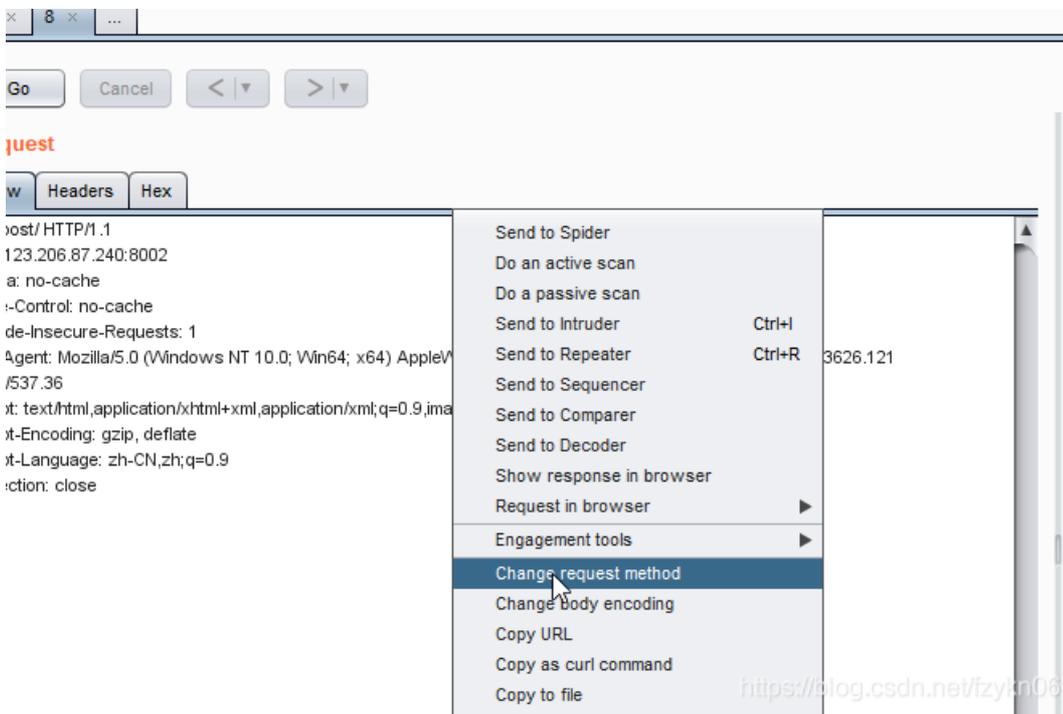


此时你可以看到，这边变红了，那就是包扔过去了

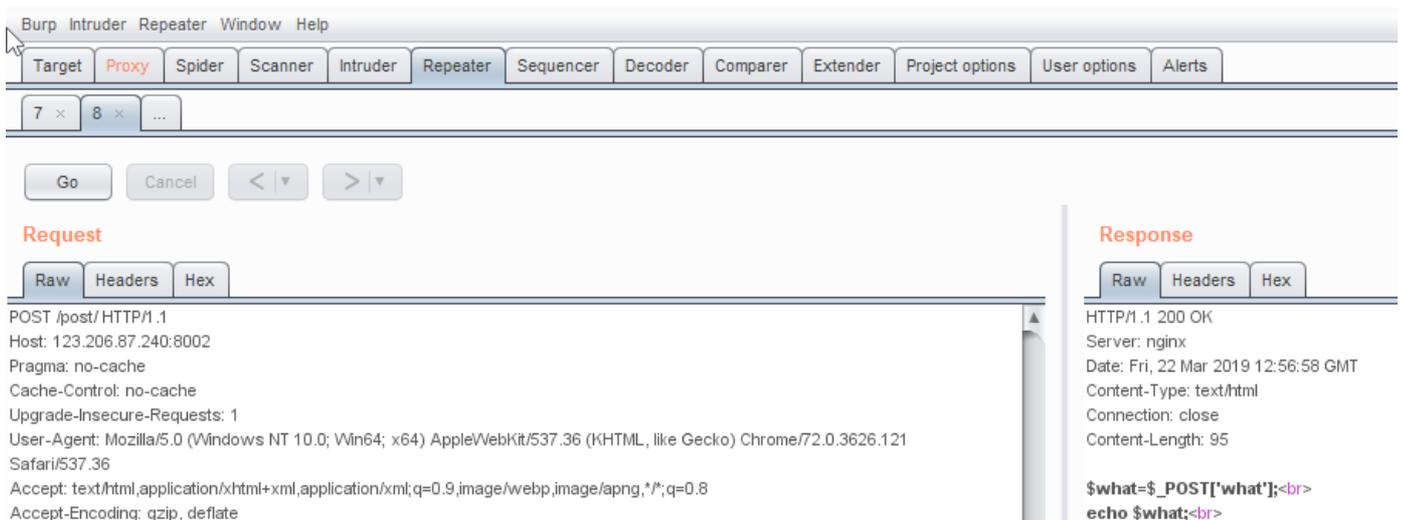


go一下你就可以看到旁边的回复报文，并且我们看到请求方式并不是POST,而是GET,这时候我们就需要将GET换为POST, 右键更换请求方式:





这样我们就更换了请求方式，， 接下来就是将我们的参数进行传送， 直接在报文底下写入参数：



```
Accept-Language: zh-CN,zh;q=0.9
Connection: close
Content-Type: application/x-www-form-urlencoded
Content-Length: 0
```

what=flag

```
if($what=='flag')<br>
echo 'flag{****}';<br>
```

<https://blog.csdn.net/fzykn06>

这边写入参数记得几个点，空一行写参数，语句结束不需要分号，写完参数直接go一下，就能得到flag了：

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

Request

```
POST /post/ HTTP/1.1
Host: 123.206.87.240:8002
Pragma: no-cache
Cache-Control: no-cache
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/72.0.3626.121 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Connection: close
Content-Type: application/x-www-form-urlencoded
Content-Length: 9

what=flag
```

Response

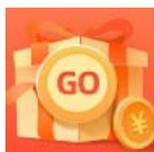
```
HTTP/1.1 200 OK
Server: nginx
Date: Fri, 22 Mar 2019 13:03:07 GMT
Content-Type: text/html
Connection: close
Content-Length: 126

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

flagflag(bugku_get_sseint67se)
```

<https://blog.csdn.net/fzykn06>

这四道应该我是bugku里面web方面最简单的题目，但是我作为小白确实花了点时间去做，哈哈，以后得加油了！



[创作打卡挑战赛](#) >

[赢取流量/现金/CSDN周边激励大奖](#)