bugkuflag.php,bugku web所有writeup_超详细讲解_持续更新

转载

十字苗刀 于 2021-04-08 05:36:47 发布 23 收藏
文章标签： bugkuflag.php

首先说一下我的主用工具，在windows下，主要是用这些，用到其他特定的工具会在题里说。

0.浏览器：火狐，配合Max hackbar插件 (这个是免费的)

1.web2:这题查看源代码即可，在url前加上 view-source: 。或者按F12也行。

view-source:http://123.206.87.240:8002/web2/

2.计算器

这个输入框只能输入一位数字，把它改大即可。任何的前端验证都是不安全的。

按F12, 用选区器选取文本框，在maxlength那个把1改大，然后就能正常输入了。

3。web基础$_GET

这个确实是基础，在get请求时，传入参数形式是在url后面加 ?参数=值。多个参数用 ?参数1=值1&参数2=值1……

源代码含义：

$what=$_GET['what'];//读取参数what，把值存到变量what里

echo $what; //输出

if($what=='flag')//如果值是flag

echo 'flag{****}';//打印flag

payload：

http://123.206.87.240:8002/get/?what=flag

4. web基础$_POST

POST请求没办法写在url里，需要用hackbar或者burp修改，格式就是在最下面Content里写 参数1=值&参数2=值

如果用hackbar就没这么麻烦了，直接在框里填就行。

源代码：

$what=$_POST['what']; //接受post过来的参数what，存到what里

echo $what; //打印

if($what=='flag') //如果值是flag

echo 'flag{****}';// 打印flag

payload：

5.矛盾

```
$num=$_GET['num']; //获取参数num

if(!is_numeric($num))// 如果num不是数字

{

echo $num;

if($num==1)              //如果num是数字1

echo 'flag{**********}'; //打印flag

}
```

这个要求不是数字且为1，有点矛盾是不是？其实有绕过的办法。下面num==1的判定是两个等号，这是弱类型比较，如果等号两边类型不同，会转换成相同类型再比较。与之对应的是强类型比较，用的是三个等号===，如果类型不同就直接不相等了。在弱类型比较下，当一个字符串与数字比较时，会把字符串转换成数字，具体是保留字母前的数字。例如123ab7c会转成123，ab7c会转成0.(字母前没数字就是0)

所以payload：

http://123.206.87.240:8002/get/index1.php?num=1a

待续