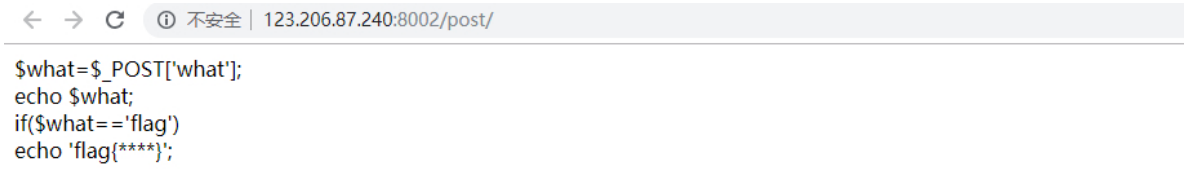
web基础$_POST-writeup

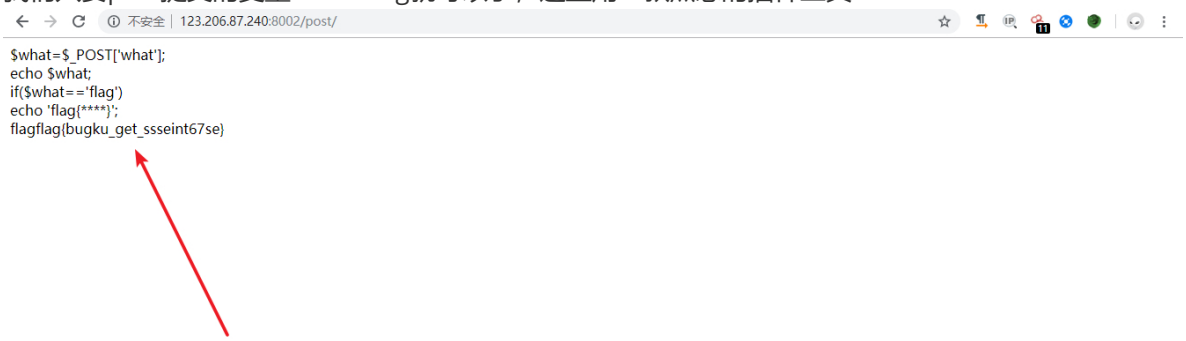
打开题目，这是一道简单的post题

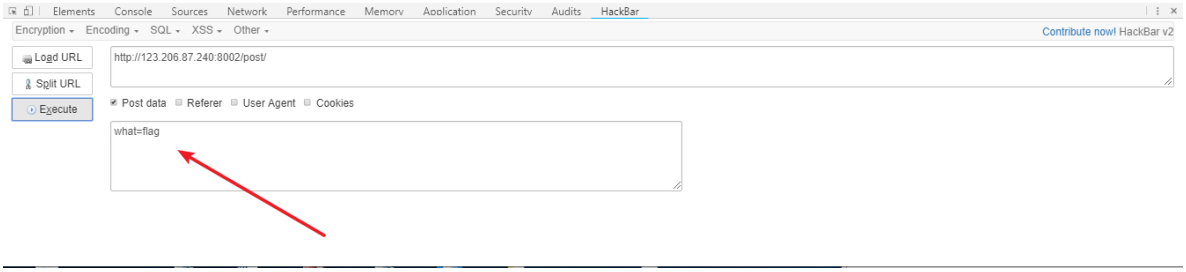
还是老规矩，点击访问链接，提示给出一串代码，分析代码，一道简单的代码审计。




```php
$what=$_POST['what']; //post提交数据赋值给变量
echo $what;
if($what=='flag') //判断post提交的数据是否等于flag，如果true输出flag
echo 'flag{****}';
```

我们只要post提交的变量what=falg就可以了，这里用一款熟悉的插件工具HackBak





点击Execute提交，flag就出来了。

> POST提交：向指定的资源提交要被处理的数据。

浅析get与post的区别：

定义了与服务器交互的不同方法，最基本的方法有4种，分别是GET，POST，PUT，DELETE（查、改、增、删）四个操作。

对资源的增，删，改，查操作，其实都可以通过GET/POST完成，不需要用到PUT和DELETE。

GET请求一般不应产生副作用。就是说，它仅仅是获取资源信息，就像数据库查询一样，不会修改，增加数据，不会影响资源的状态。

GET请求的数据会附在URL之后（就是把数据放置在HTTP协议头中），以?分割URL和传输数据，参数之间以&相连。

POST把提交的数据则放置在是HTTP包的包体中。

POST的安全性要比GET的安全性高。

get是从服务器上获取数据，post是向服务器传送数据。

get 和 post只是一种传递数据的方式，get也可以把数据传到服务器，他们的本质都是发送请求和接收结果。只是组织格式和数据量上面有差别，GET和POST只是发送机制不同，并不是一个取一个发！