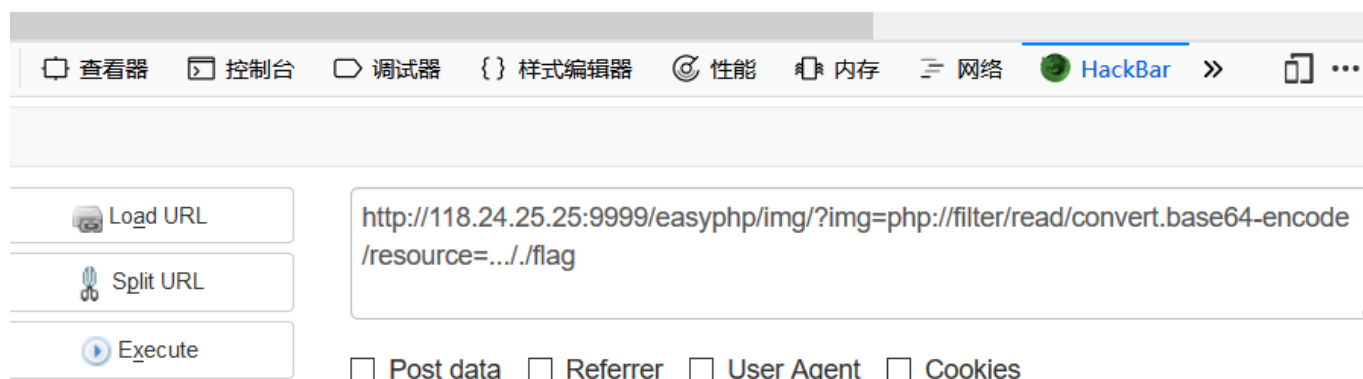


# easy\_php

提示robtos.txt,然后访问

```
http://118.24.25.25:9999/easyphp/img/index.php
```

文件包含，可以利用伪协议读源码，开始不知道读什么，卡住了。。。后来发现源目录有flag.php，用工具扫描常见文件的重要性，过滤了../双写绕过



base64解密，拿到flag

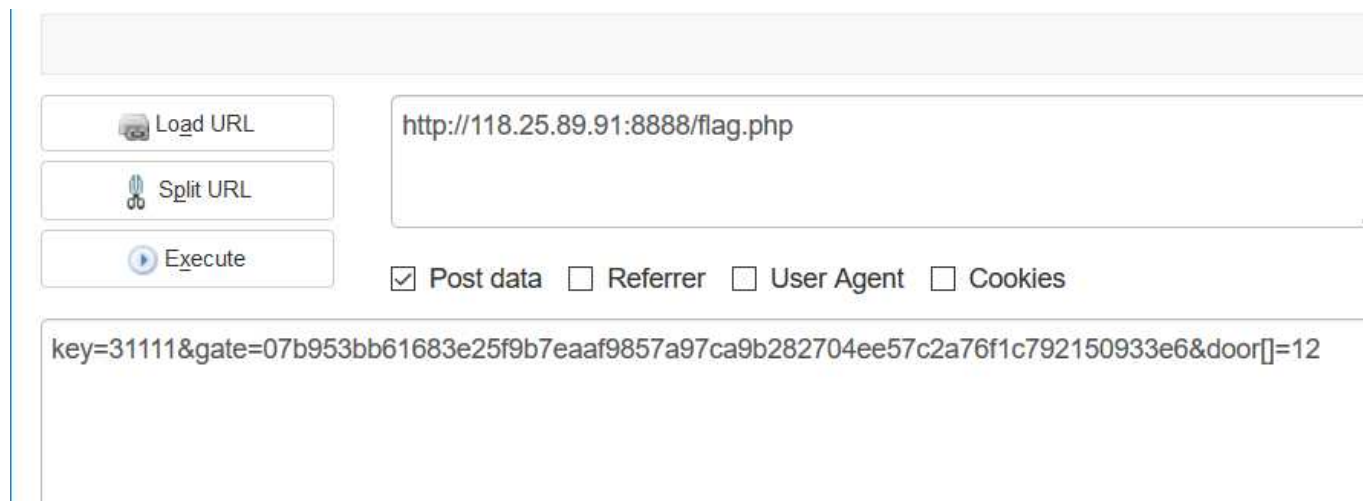
## php trick

```
http://118.24.3.214:3001/?str1=s1091221200a&str2=s1836677006a&str3[]=1&str4[]=21&H.game[]=%209.1e12q&url=http://www.baidu.com@127.0.0.1:80@www.baidu.com/admin.php?filename=php://filter/read=convert.base64-encode/resource=flag.php
```

前

面大抵是一些弱类型比较，一些函数不能处理数组返回0或者null的问题，我记一些新学到吧，找不到在哪看的了，貌似是php处理参数时会把一些变量不能出现的字符转成，然后\$SERVER['QUERY\_STRING']读取的是用户输入，所以成功绕过，然后curl和parseurl关于@的解析差异，curl读取第一个@后的内容，parseurl最后一个@后的内容，开始到这里卡住了，直接用ip访问还是提示本地才行，后来改127.0.0.1返回空，后来把端口改了80才好，可是感觉没道理啊，这种vps一般不都是独立ip，因该没有把内网端口映射到外网的需要吧，难道因为用了docker 后面伪协议文件读取，没什么

# PHP Is The Best Language



The screenshot shows a web tool interface for sending HTTP requests. It has a sidebar with three buttons: 'Load URL' (with a document icon), 'Split URL' (with a scissors icon), and 'Execute' (with a play button icon). The main area contains a text input field with the URL 'http://118.25.89.91:8888/flag.php'. Below the input field, there are four checkboxes: 'Post data' (checked), 'Referrer' (unchecked), 'User Agent' (unchecked), and 'Cookies' (unchecked). At the bottom, there is a large text area containing the POST data: 'key=31111&gate=07b953bb61683e25f9b7eaaf9857a97ca9b282704ee57c2a76f1c792150933e6&door[]=12'.

这道题还好，没卡住，gate传数组，就知道secret是null，然后key的传值就可以控制了，只要传一个加密一次和两次开头都是字母的就行，然后算出gate，拿到flag

## 后面两个没做出来，记记思路吧

### Baby\_Spider

开始以为python3没requests库，用request各种难受，爬虫写好后，发现每次到第十次的样子就会出错，然后把cookies消掉，试过把之前的存下来，再去访问，或者带着cookis访问根目录，会更新cookies，但这时会出现俩个cookies，可能是requests的bug吧，虽然用哪个cookies访问question都是禁止，然后试着传token更新cookies，不禁止了，但是一直答40多次也没出flag，卡住了

### Math有趣

看题目要爆破的样子，然后事比较多，还要在阿大上课，写作业，周五下午才开始爆破，爆到几万的样子，没结果，新题出来了，遂放弃，可能思路有问题吧