# Cookie 攻防世界

原创

今天不学习，明天变腊鸡 已于 2022-04-14 17:02:10 修改 2189 收藏
分类专栏： 笔记 CTF 文章标签： web安全 安全
于 2022-04-07 11:23:04 首次发布


 笔记 同时被 2 个专栏收录
29 篇文章 0 订阅
订阅专栏

 CTF
3 篇文章 0 订阅
订阅专栏

1.第一步还是看题：


由题目信息我们可以知道，这次题目和Cookie有关

2. 进入题目进行分析：

你知道什么是cookie吗?



题目问我们知道什么是Cookie，Cookie:（比如说你进入一个网站，输入你的密码和用户名，客户端就会把你的信息传递给服务器，传递信息（用户名，密码）的载体就是Cookie，request就是一串数据，其中就会包括Cookie等信息，服务器接收request信息后，就会给客户端发送response应答（密码正确还是错误））

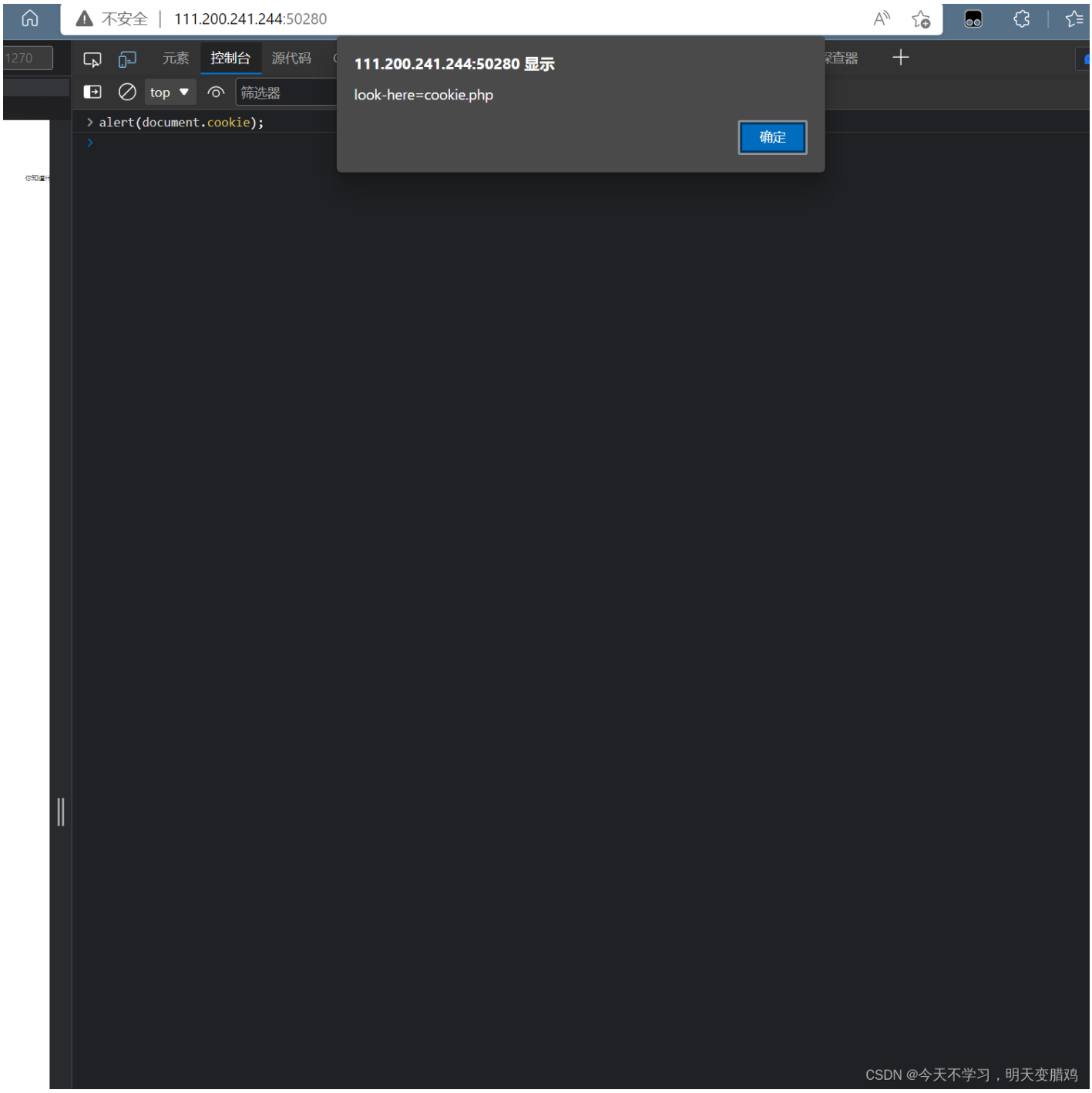
```
Request 和 Response 对象起到了服务器与客户机之间的信息传递作用。
Request 对象用于接收客户端浏览器提交的数据，
Response 对象的功能则是将服务器端的数据发送到客户端浏览器。
比如说你进入一个网站，输入你的密码和用户名，客户端就会把你的信息传递给服务器，传递信息（用户名，密码）的载体就是Cookie，r

response：（一般有服务器名称）
Connection: Keep-Alive
Content-Encoding: gzip
Content-Length: 253
Content-Type: text/html
Date: Thu, 07 Apr 2022 03:06:36 GMT
flag: cyberpeace{b96c80999a82b4f8eb5b2241cabde6b8}
Keep-Alive: timeout=5, max=99
Server: Apache/2.4.7 (Ubuntu)
Vary: Accept-Encoding
X-Powered-By: PHP/5.5.9-1ubuntu4.26

request：
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8,application/s
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9,en;q=0.8,en-GB;q=0.7,en-US;q=0.6
Cache-Control: max-age=0
Connection: keep-alive
Cookie: look-here=cookie.php
Host: 111.200.241.244:50280
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Linux; Android 6.0; Nexus 5 Build/MRA58N) AppleWebKit/537.36 (KHTML, like Gecko) C
```

然后我们查看Cookie：

按f12,再按照如下图所示：（在控制台输入alert(document.cookie)）



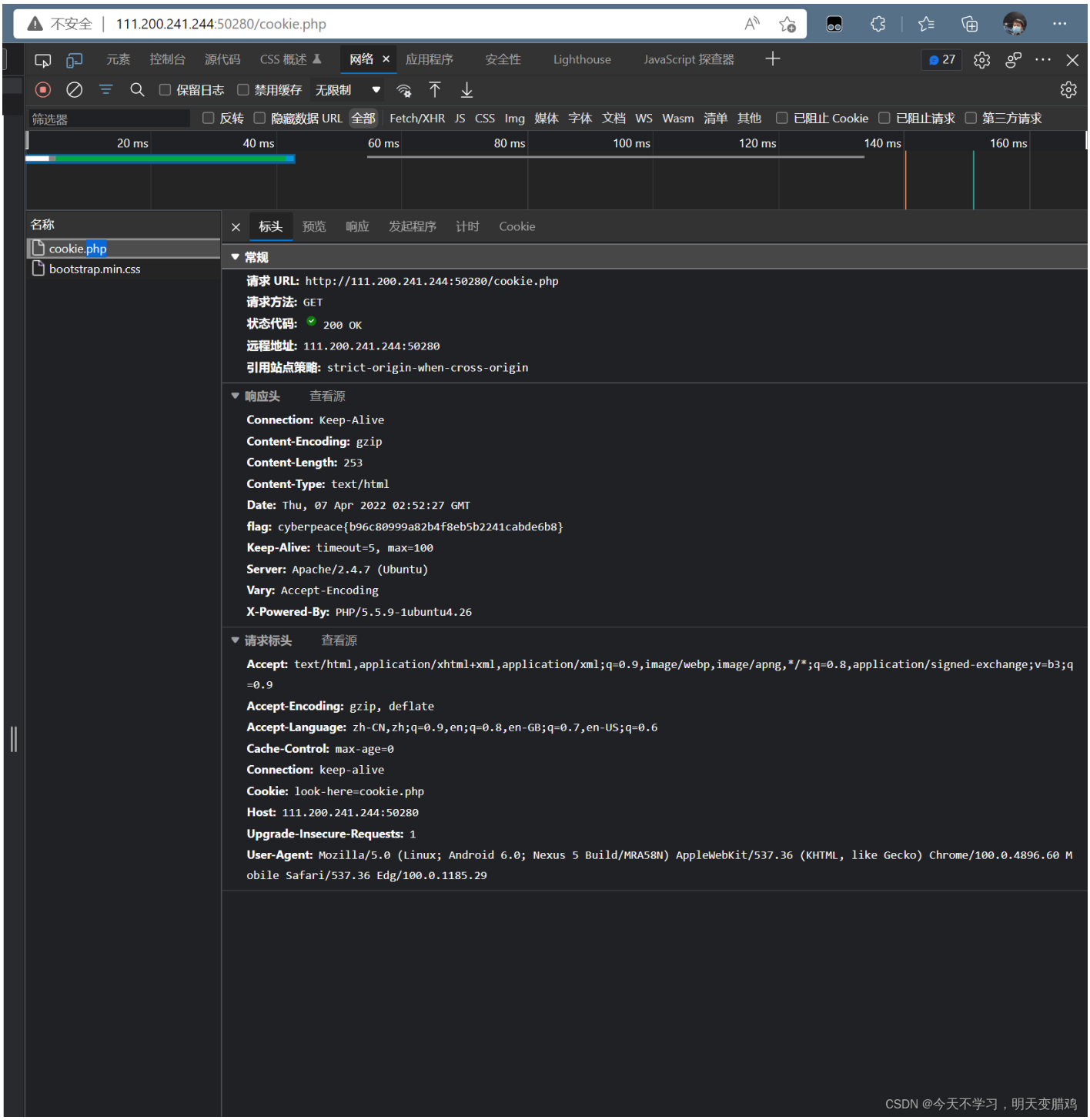

cookie放在cookie.php文件中：（进入文件：网址加\cookie）


See the http response



题目要我们看http response：

按如下图所示进行操作：




最后看到flag