【CTF整理】Who are you (2017强网杯web题)

原创

久违° 于 2020-04-20 10:16:02 发布 682 收藏

分类专栏： CTF 文章标签： web

本文链接：https://blog.csdn.net/weixin_42742658/article/details/105627667

【CTF整理】Who are you (2017强网杯web题)

别人思路总结：

0x01 初探

打开网页就是一句“Sorry. You have no permissions.”

按照惯例看看网页源码，发现没有提示；

0x02 初步思考

既然没有提示，也没有其他的链接，那么可能有以下几种可能：

1、敏感文件泄漏

2、跳转

3、cookie / session

第一个想法在经过扫描器扫描之后就放弃了，因为只看到index.php，还有/upload/，但是在访问的时候是403

第二个在抓包的时候也没有看到有跳转

只剩下第三个

0x03 cookie中的role

在查看cookie的时候发现了“Cookie: role=Zjo1OiJ0aHJmZyI7”，后面那串第一个想法就是base64，尝试过后得到

" f:5:“thrfg”; "。一时间没有看懂这个thrfg是什么，然后暴力猜测了一下，发现是guest，也就是rot-13。于是把它改成admin的rot13过后的值就进去了。

0x04 upload

进去之后在源码里有提示“<!-- $filename = $_POST[‘filename’]; $data = $_POST[‘data’]; -->”

这里应该是模拟一个文件上传，但是用post方法来弄的。

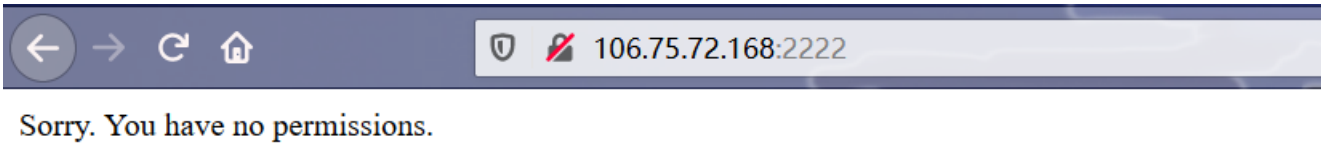
这里经过一番测试，发现在发送有<的时候会显示no no no。所以猜测源代码中有个正则表达式，用来匹配

这里我用data[]=的方法，把data从字符串变成数组，导致绕过正则匹配。

上传之后能够发现它返回了文件的地址，访问它就得到flag

自己复现

访问：http://106.75.72.168:2222
得到：Sorry. You have no permissions.

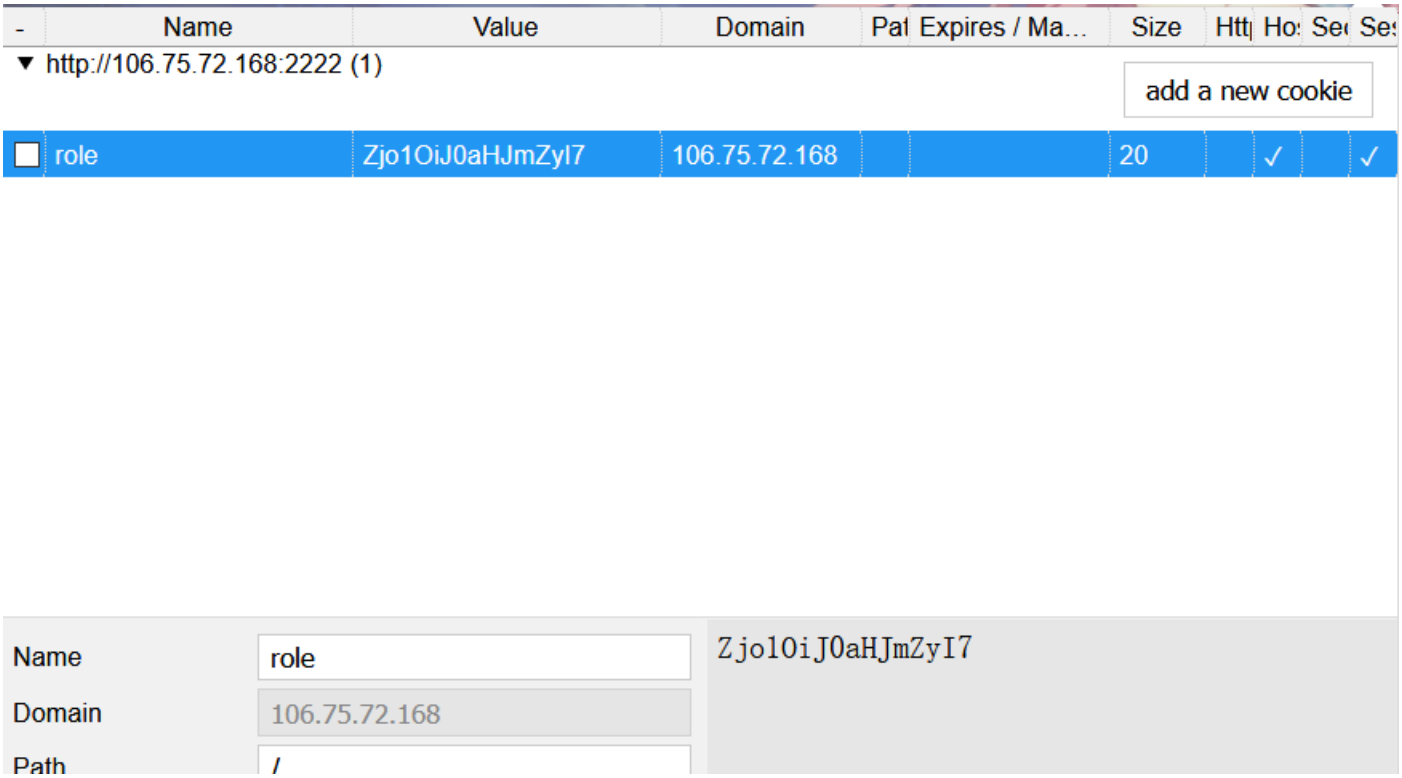


Sorry. You have no permissions.

御剑扫描，无法访问

ID	地址
1	http://106.75.72.168:2222/uploads/
2	http://106.75.72.168:2222/index.php

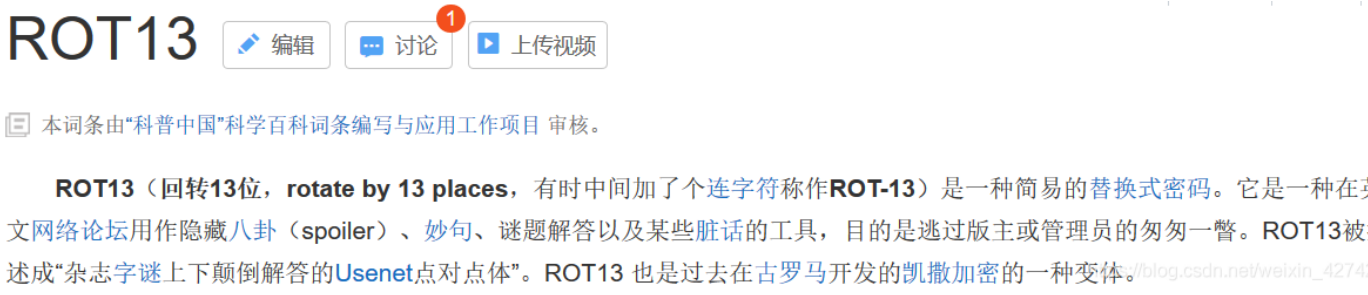
查看cookie：



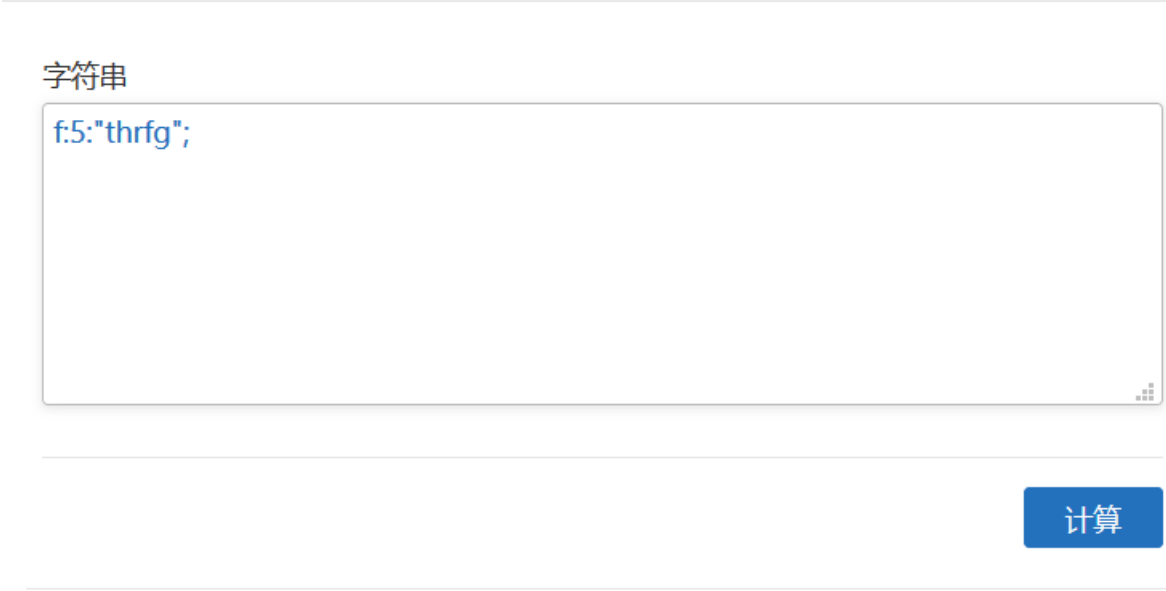
base64解码cookie：

经过百度得知这玩意叫

ROT13编码：



然后在线ROT-13解码：

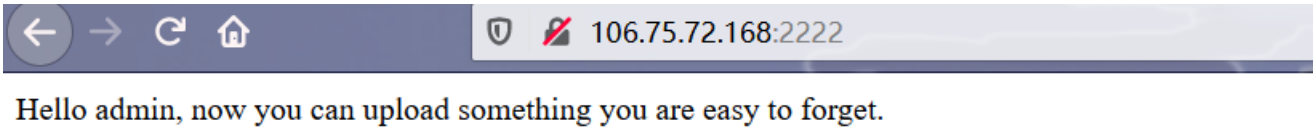


看到guest改成admin

尝试：

对f:5:“nqzva”;进行base64编码得到Zjo1OiJucXp2YSI7，用于替换原来的cookie

用新的cookie访问，进入管理员界面



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

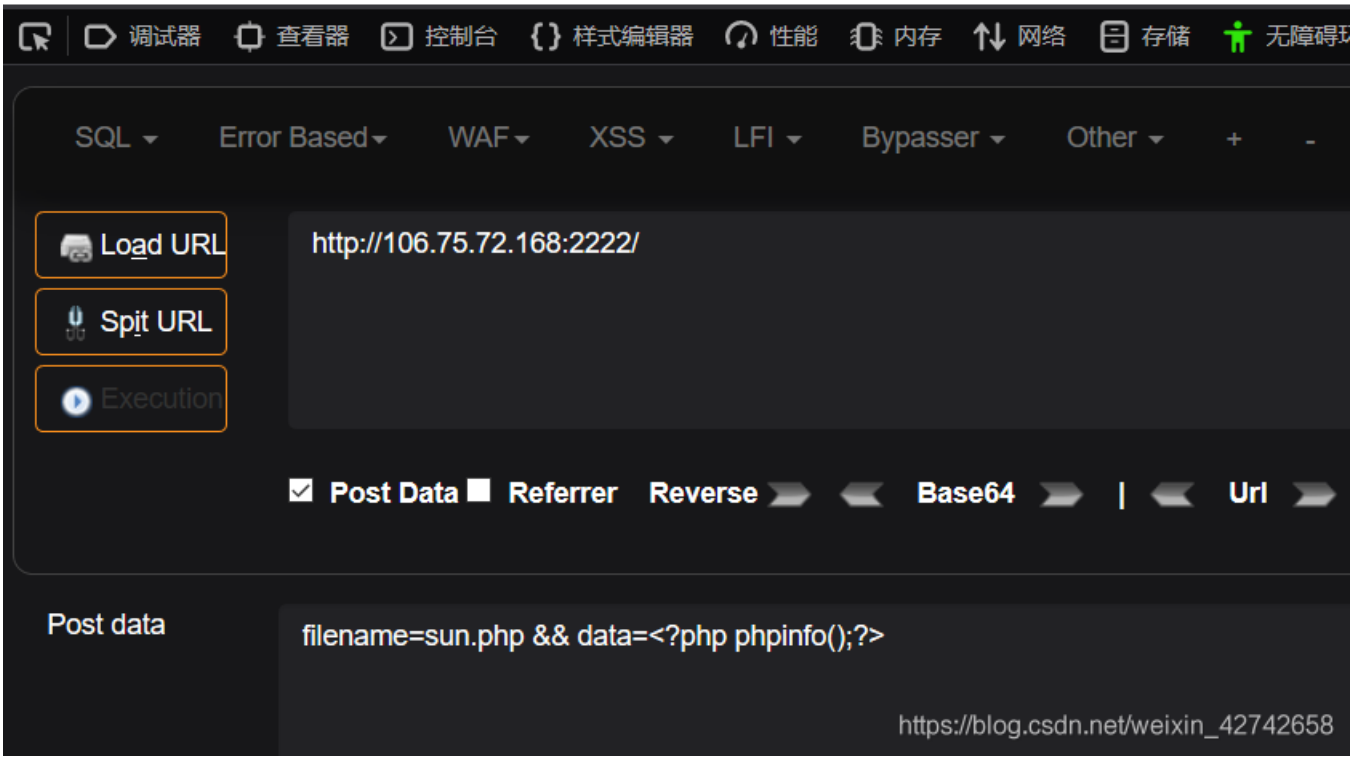
查看源码：


```
<!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>

```

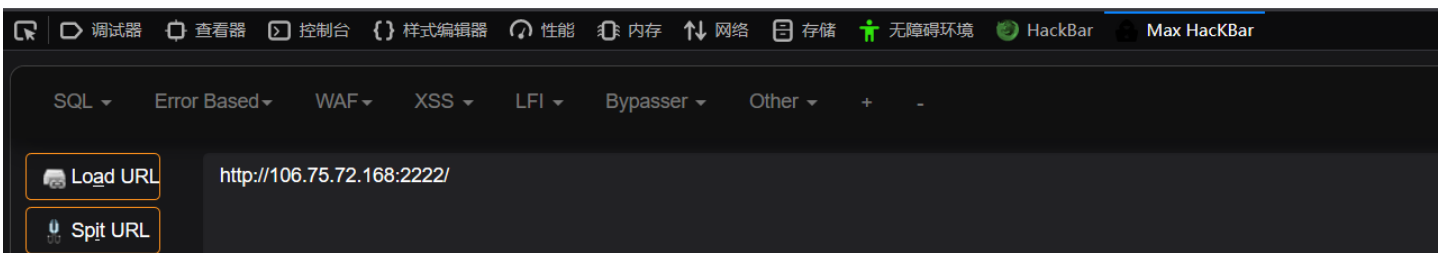

构造post提交：

No No No!



需要绕过：

your file is in ./uploads/42a430a5f79d46be10e92ed9efd987besun.php



访问返回的网址得到flag：

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

可能太久了，我加上返回的网址访问不到结果，光保留uploads可以访问。

by 久违 2020.4.19