CTF-2017第二届广东省强网杯线上赛：who are you?

原创

Flutter&Python&Test 于 2018-07-24 16:21:35 发布 80 收藏
文章标签： web php vim wordpress java

本文链接：https://blog.csdn.net/MidSummer411/article/details/111957224

题目：

> 分值：100分 类型：Web题目名称：who are you?
> 题目内容: 我是谁，我在哪，我要做什么？

解题过程：

1. 开启burpsuite,打开页面,显示"Sorry. You have no permissions."
2. 查询报文,没有发现跳转之类,只有`Cookie: role=Zjo1OiJ0aHJmZyI7`有点价值
3. Base64解密`Zjo1OiJ0aHJmZyI7`,得到内容是`f:5:"thrfg";`
4. `thrfg`猜测是使用了rot-13加密,解密得到`guest`
5. 顺其自然推论把`admin`用`rot-13`加密,得到`nqzva`
6. 使用Base64加密`f:5:"nqzva";`,得到`Zjo1OiJucXp2YSI7`
7. 修改`Cookie: role=Zjo1OiJucXp2YSI7`后提交,页面显示:`Hello admin, now you can upload something you are easy to forget.` 查看源码:

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

</body></html>
```

8. 根据页面源码提示,打开firefox插件hackbar,Post内容为`filename=1.php&data[]=<?php phpinfo();?>`

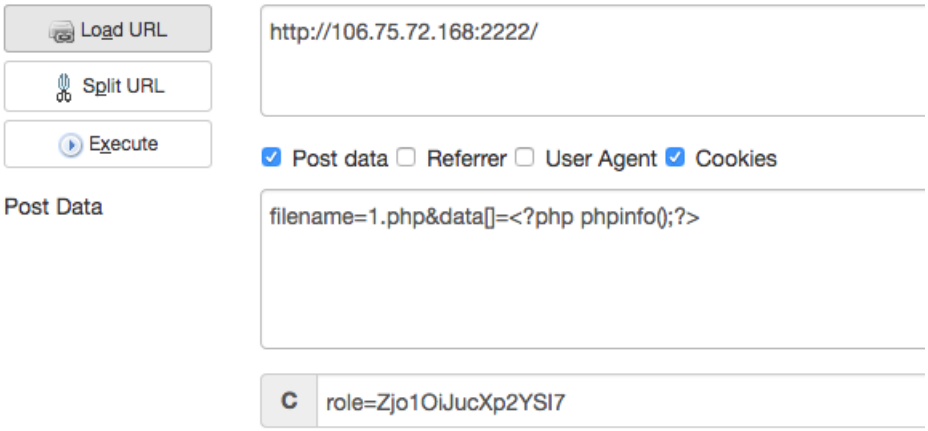

image.png

> 如果直接输入`filename=1.php&data =<?php phpinfo();?>`页面会报错"No No No!", 因为网页做了正则匹配过滤. 而用data[]=的方法，把data从字符串变成数组，可以绕过正则匹配的过滤。

9. 提交后页面显示`your file is in ./uploads/7b2fe94f4cec09a7c9818c48f4ef62471.php`
10. 打开页面即可拿到flag.