i春秋web题学习记录

原创

柒柒不是染染 于 2019-04-25 16:08:51 发布 393 收藏 1

分类专栏： CTF练习

本文链接：https://blog.csdn.net/weixin_38659379/article/details/89518239


CTF练习 专栏收录该内容

2 篇文章 0 订阅

订阅专栏

**

1、2017强网杯web题who are you

**

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

看网页源码，发现没有提示；

（2）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

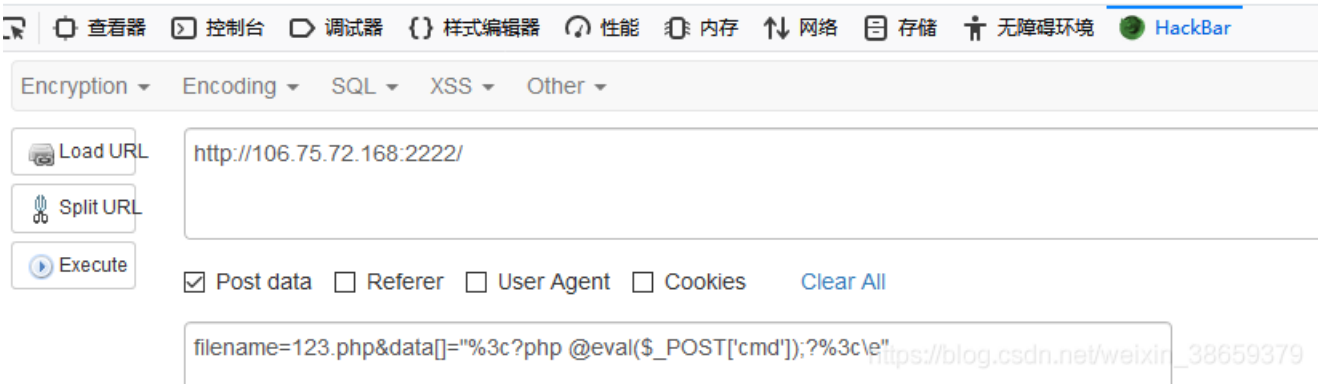
（3）cookie中的role

F12的时候发现了“Cookie: role=Zjo1OiJ0aHJmZyl7”，后面那串第一个想法就是base64，尝试过后得到

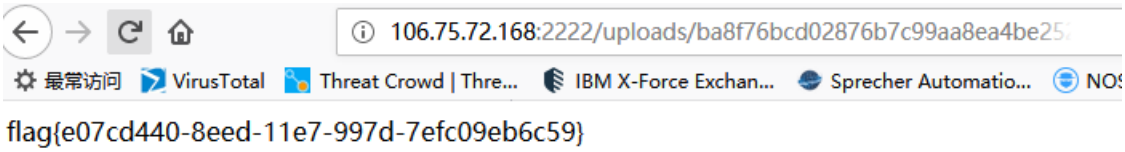
" f:5:“thrfg”; "。一时间没有看懂这个thrfg是什么，然后暴力猜测了一下，发现是guest，也就是rot-13。于是把它改成admin的rot13过后的值就进去了。

（4）upload

查看源码发现源码里有提示，这是利用了post上传方法。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。



直接访问这个路径，即可得到flag



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