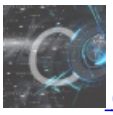
CTF writeup -who are you?

原创

一个潜心学习的小白 于 2018-07-29 10:28:54 发布 2266 收藏

分类专栏： CTF 渗透测试平台笔记 文章标签： who are you? i春秋 ctf writeup

本文链接：https://blog.csdn.net/dragon_18/article/details/81268582


CTF 同时被 2 个专栏收录

2 篇文章 0 订阅

订阅专栏


渗透测试平台笔记

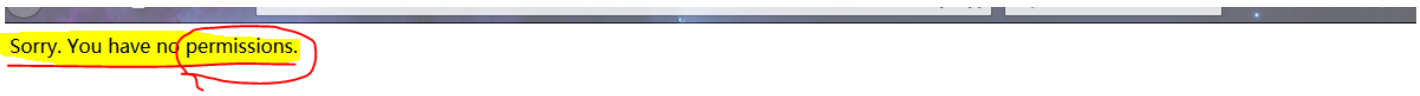
4 篇文章 0 订阅

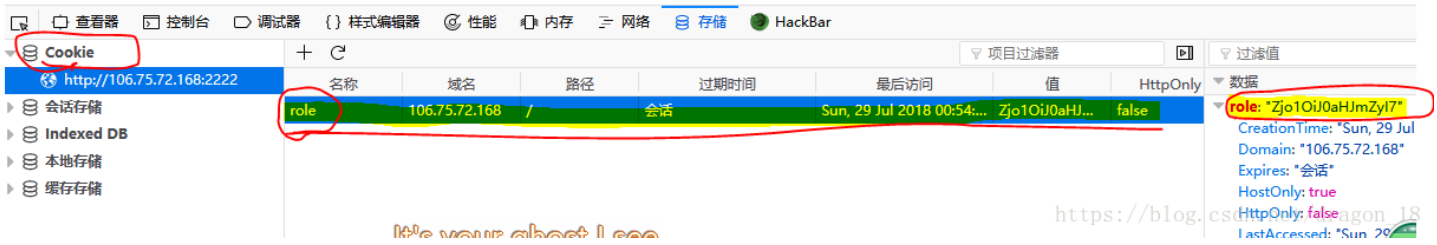
订阅专栏

题目为：who are you?

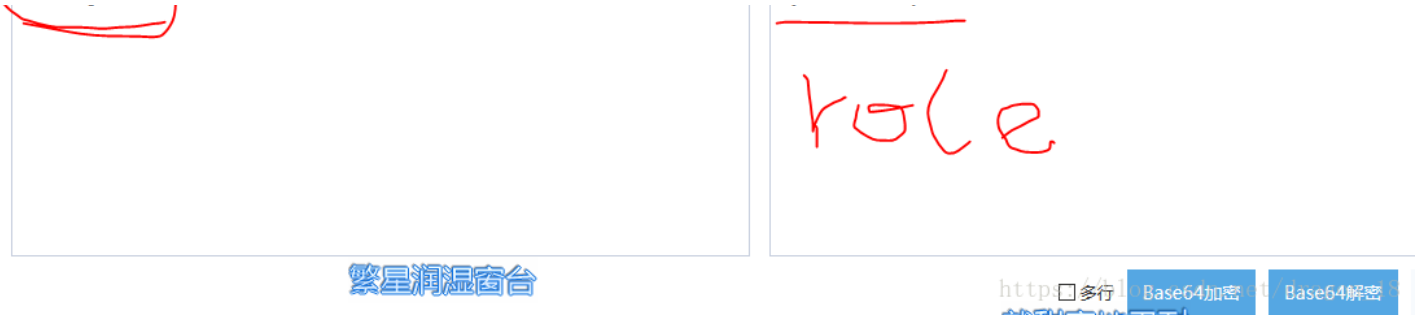
描述为：我是谁，我在哪，我要做什么？

首页内容为：Sorry. You have no permissions.此时推断本题与cookie有关（50%的可能性）。查看cookie，发现cookie中有一个名为role的数据（此时可以推断此题有90%的可能性与此有关）。

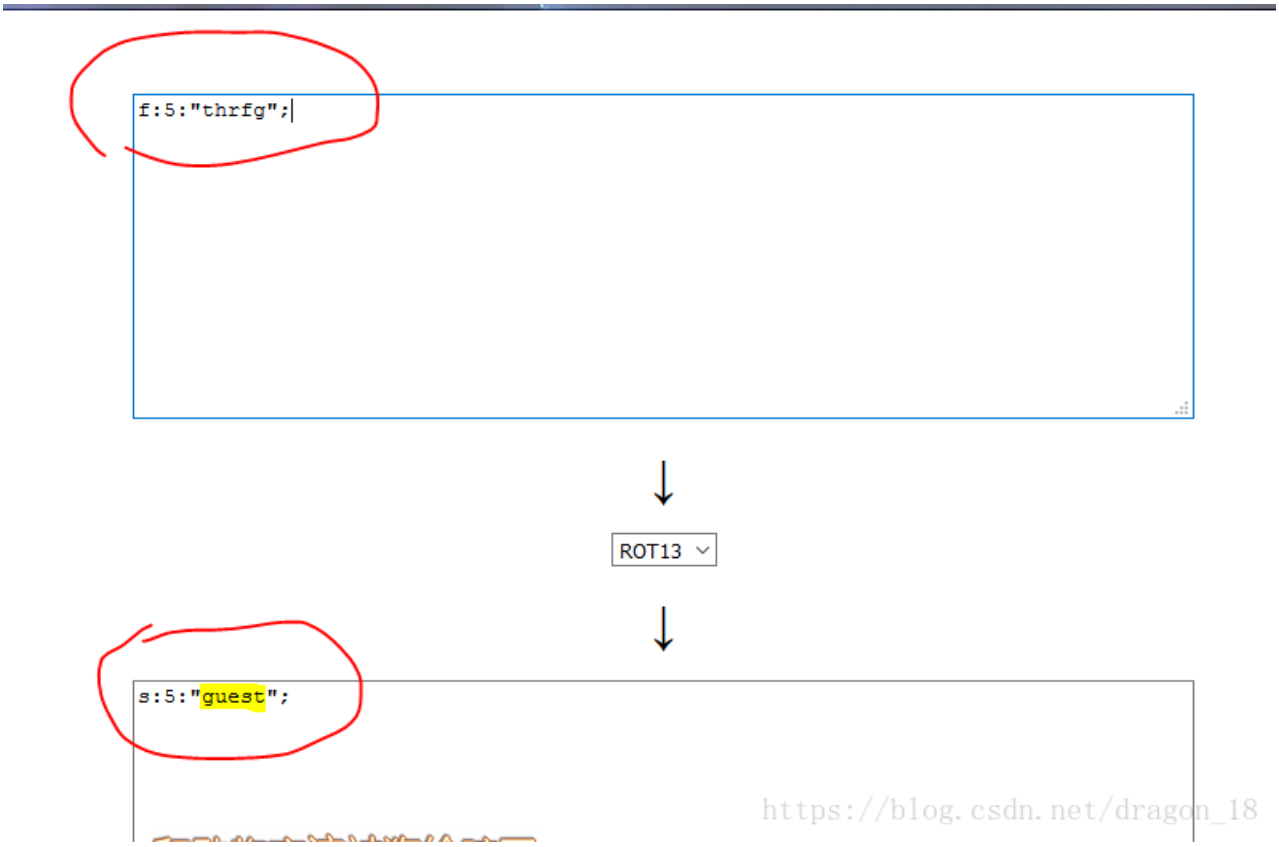




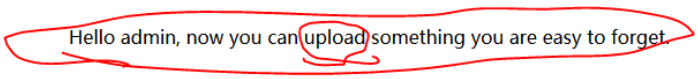
此时看role的值一定是明文加密后生成的。这时就Google或百度在线解码，首先试试看是不是比较主流的base64加密方法（通常web常用的加密方法为base64 MD5 rot13）。发现经base64解码后值为 f:5:"thrfg";

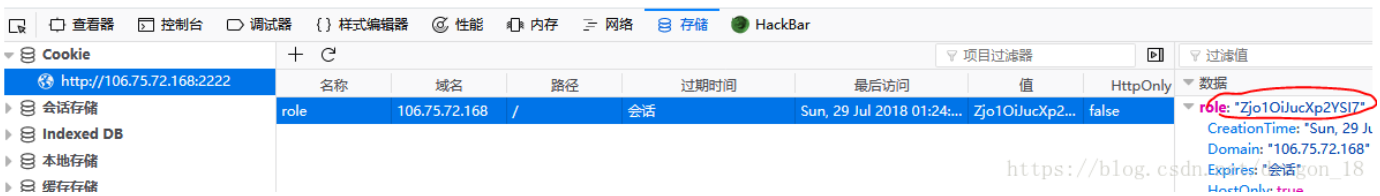


发现这个字符串非常像rot13加密的值，经rot13解码后值为 s:5:"guest";



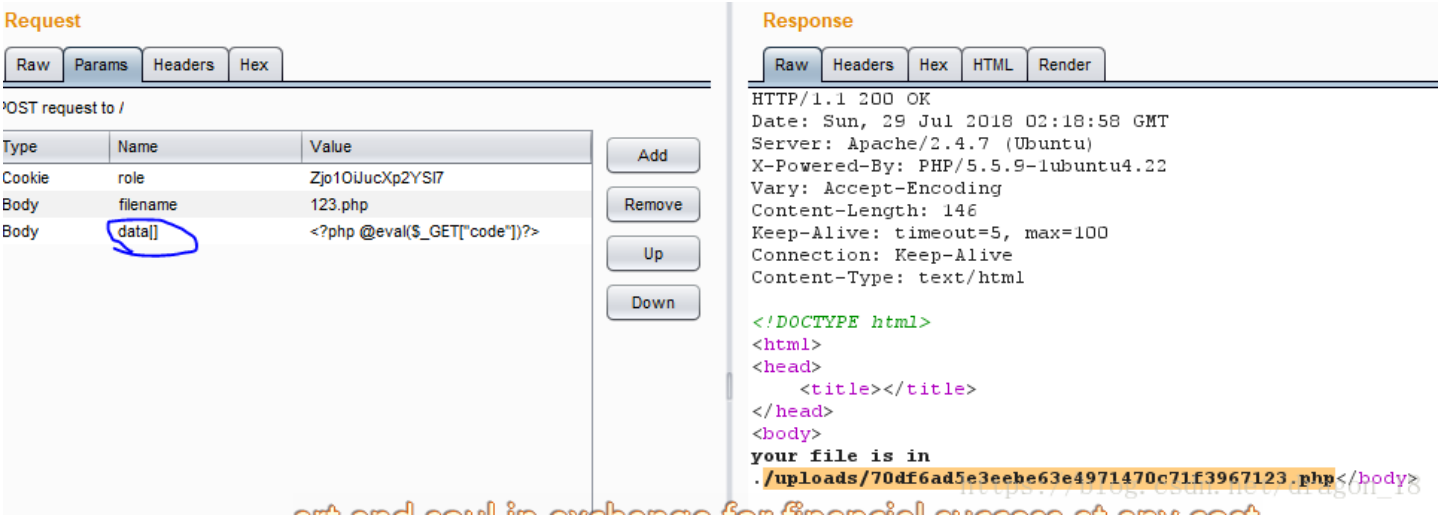
这时就很明了了，role的值是经base64加密后又经rot1加密处理。发现“guest”！！此时将guest改为admin，并经rot13加密base64加密后得到的值填入cookie的role中刷新页面。网页跳转并提示：Hello admin, now you can upload something you are easy to forget.

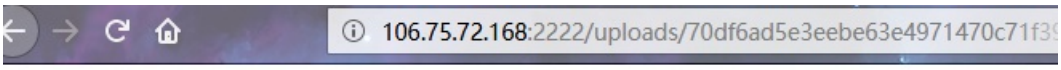




upload很重要，虽然提示要upload但并不知道要上传什么东西。查看网页源代码发现有一句很重要的提示：filename = _POST['filename']; data = _POST['data']; 提示要构造post方式上传filename和data。（有很多工具可以使用，如Firefox的hackbar插件和burpsuit）利用burpsuit抓包并修改为POST上传，添加 filename项和data项。

发现回显为no no no,想到data可能是用一个数组存取的内容,抱着试试的想法将data改为data[]其他内容不变(filename和data的值不重要)。回显一个文件地址，将地址打开出现答案：flag{}





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