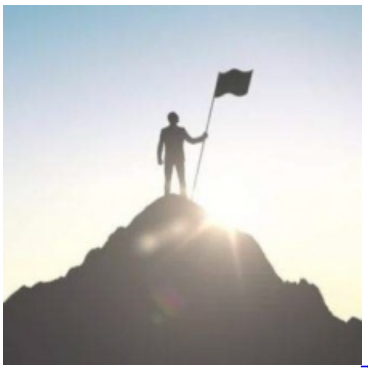
i春秋 WEB who are you?

原创

A_dmins 于 2019-06-18 13:04:10 发布 616 收藏

分类专栏： CTF题 一天一道CTF i春秋CTF

本文链接：https://blog.csdn.net/qq_42967398/article/details/92779809



CTF题 同时被 3 个专栏收录

115 篇文章 11 订阅

订阅专栏

一天一道CTF

52 篇文章 5 订阅

订阅专栏

i春秋CTF

21 篇文章 1 订阅

订阅专栏

i春秋 WEB who are you?

一天一道CTF题目，能多不能少

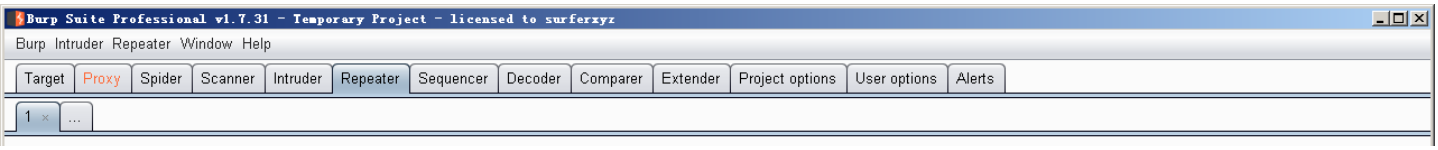
数据库实训考试结束了，做个题目压压惊~

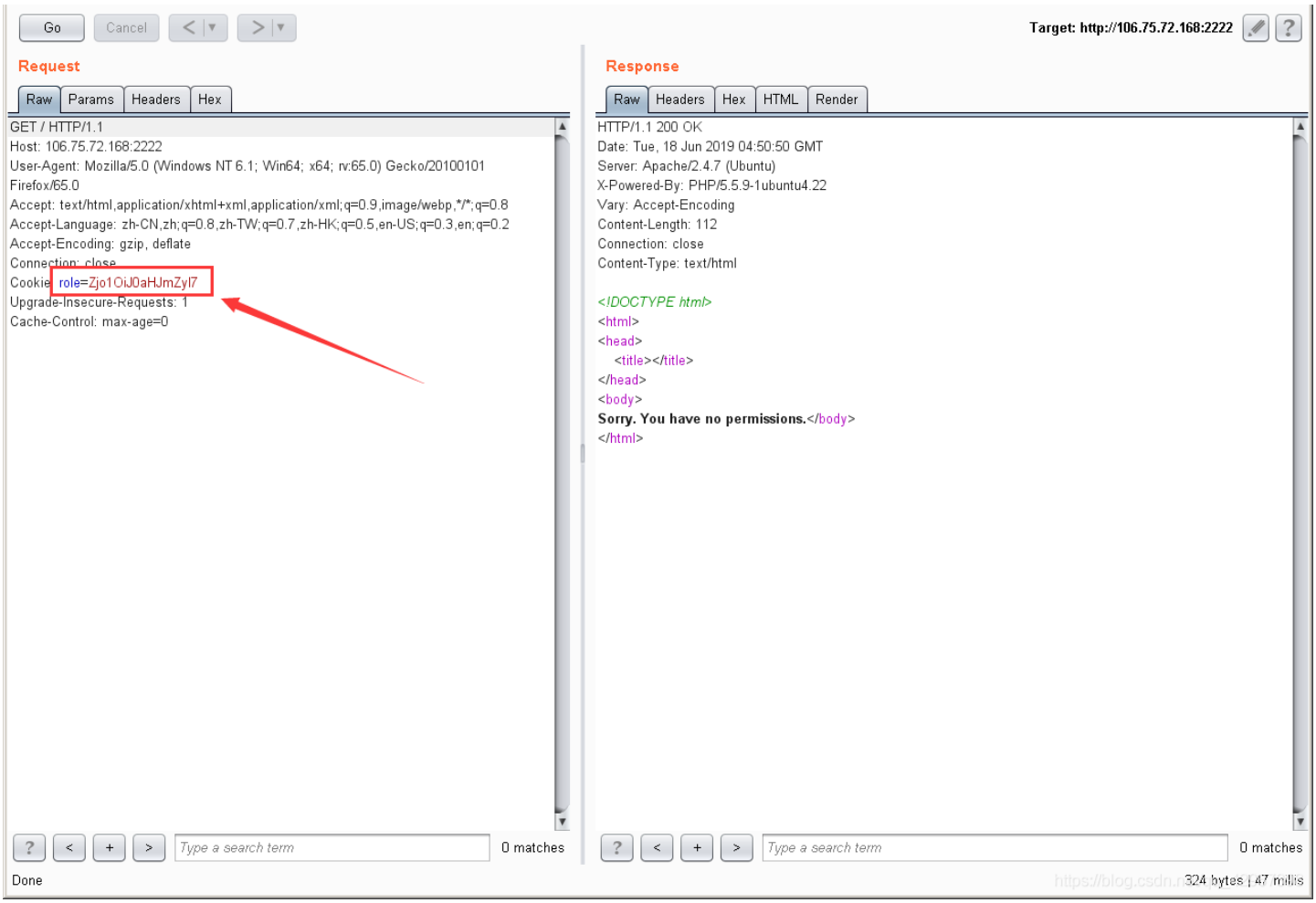
打开网页：

Sorry. You have no permissions.

什么都没有，源码也没看见什么东西，按照惯例，抓包！！！

发现一个奇怪的东西：





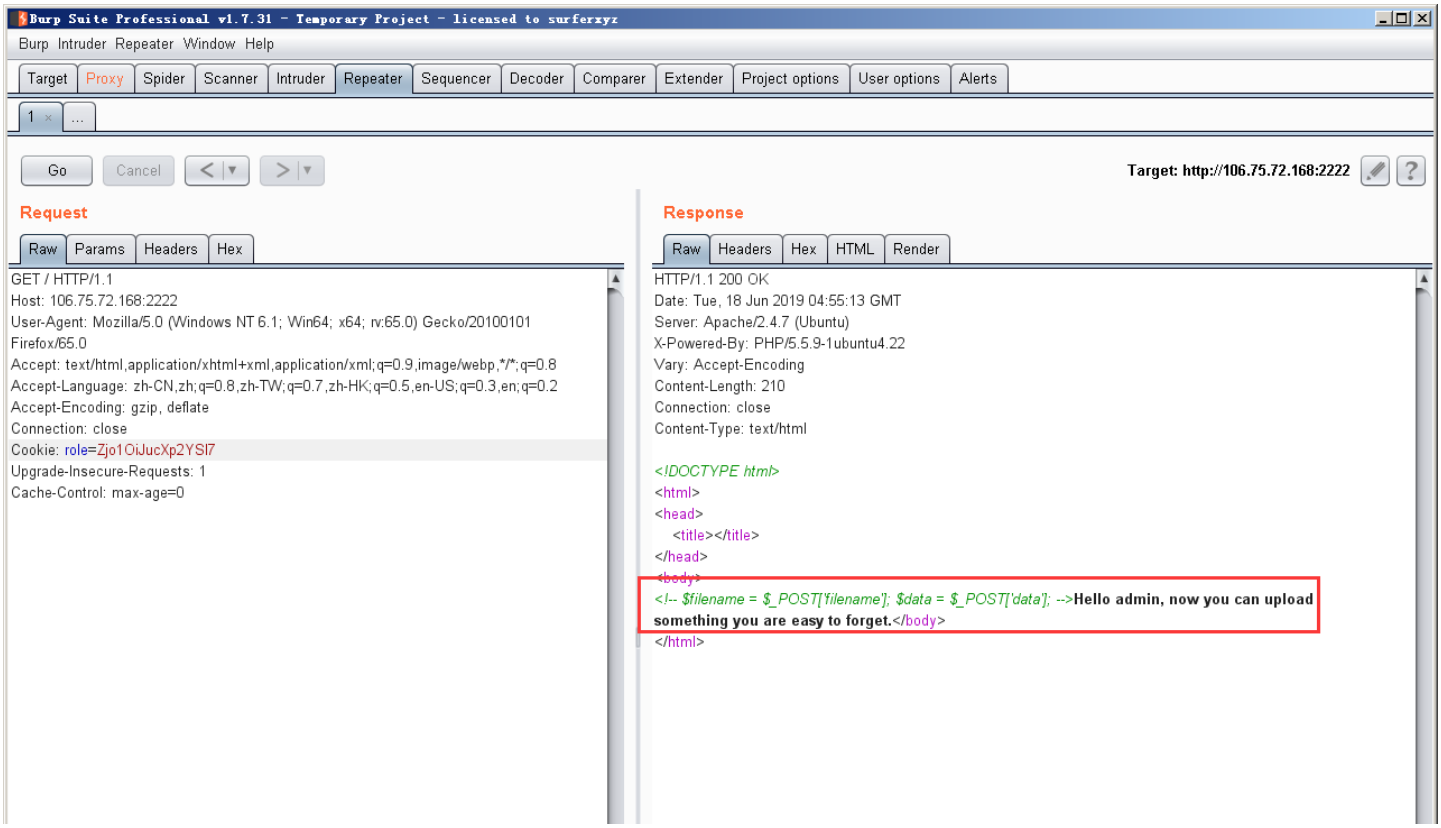
base64解码得到：`f:5:"thrfg";`

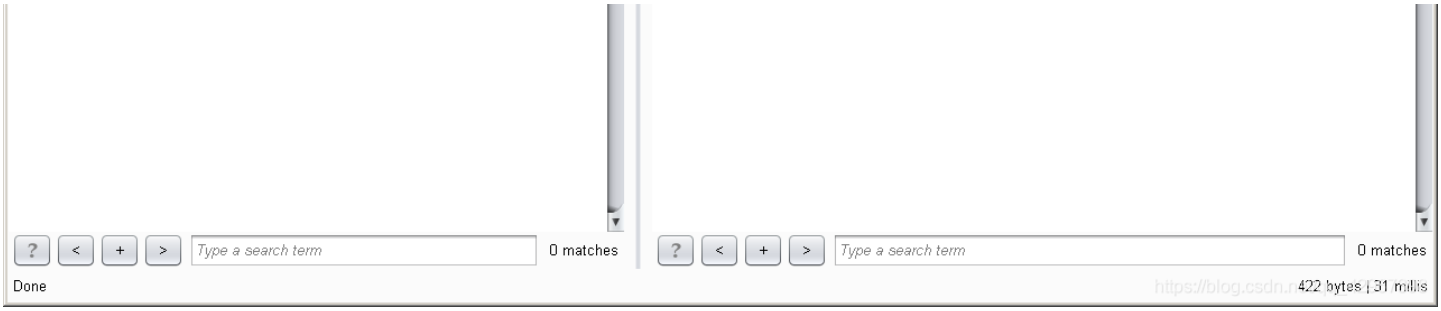
这是个啥？？？？单词不像单词的，不应该啊

后来才知道是rot13加密的，解码得到guest

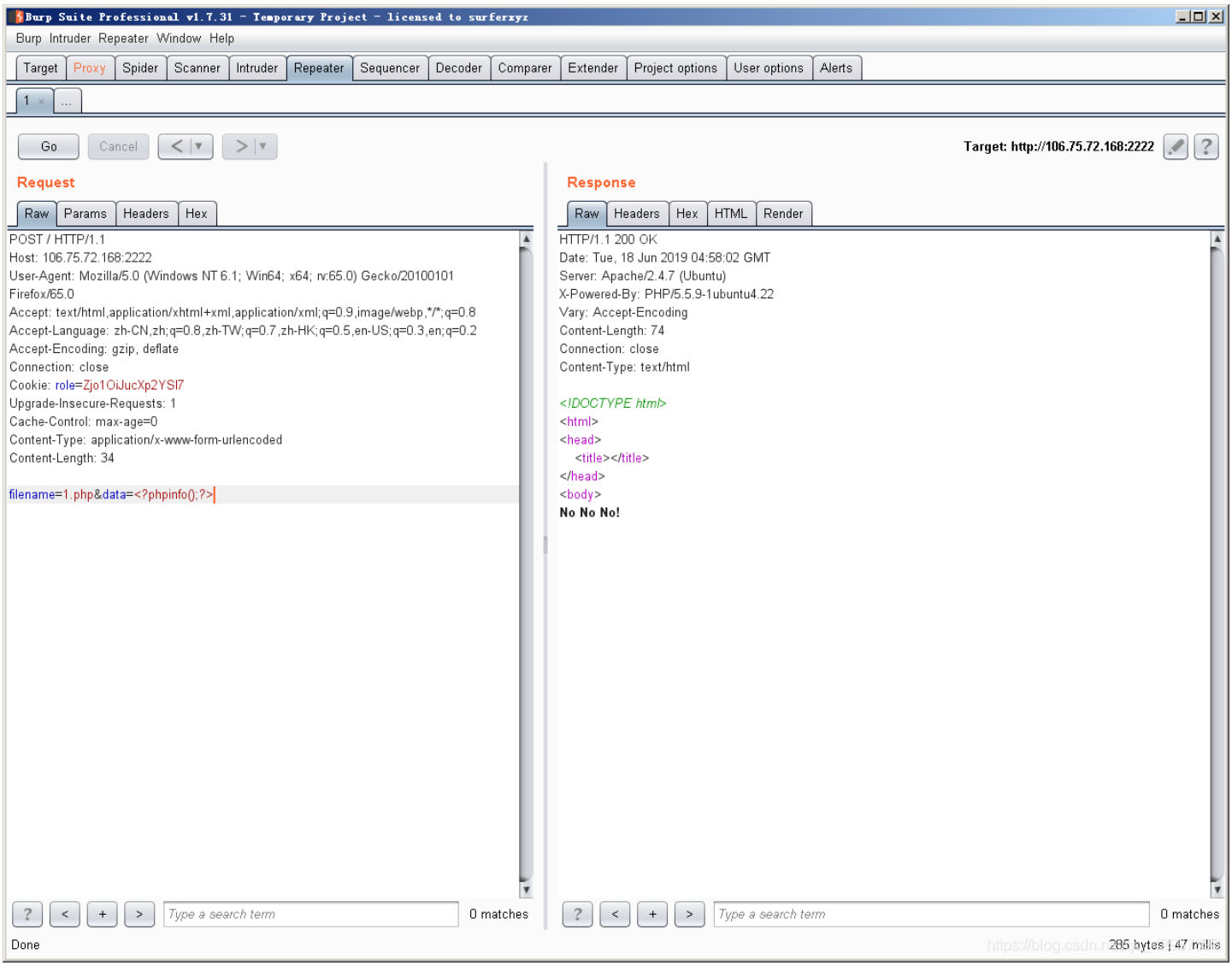
那我们就猜，我们把admin进行rot13加密，在进行base64加密传入：`Zjo1OiJucXp2YSI7`

得到一个新的提示：

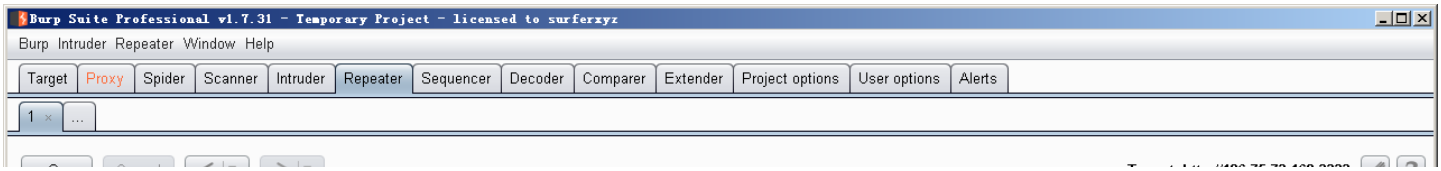


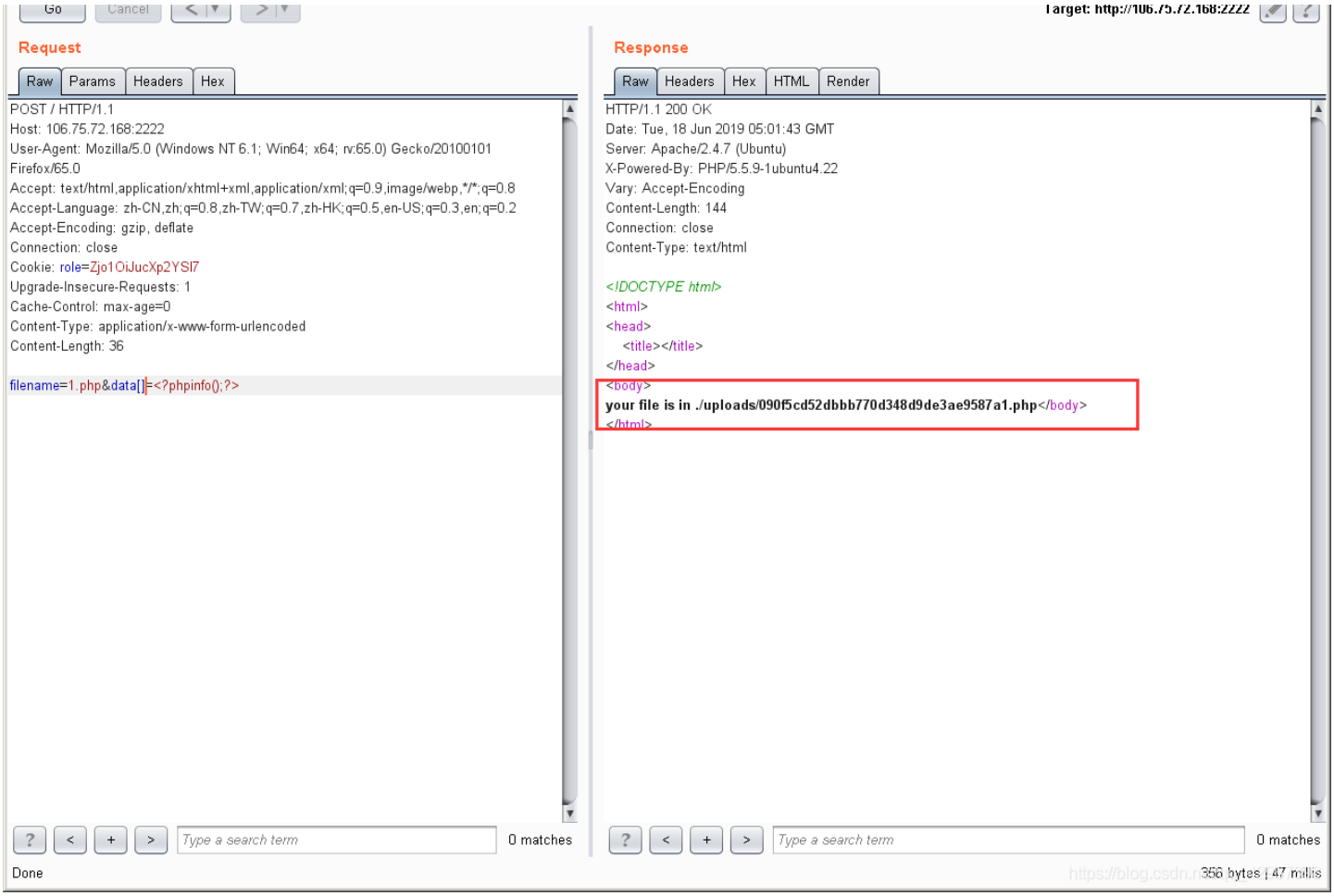


提示上传文件~~
给了两个变量，看名字好像是一个是文件名，一个是数据？
先构造一下变量：`filename=1.php&data=<?phpinfo();?>`
得到说NO NO NO，怀疑是不是有正则匹配，后来证实有`<`的时候会出现NO NO NO



既然正则了，那就不代表没有办法，要知道php的函数一般都无法执行数组的
用数组来当参数，一般都能绕过，
再次执行`filename=1.php&data[]=<?phpinfo();?>`
果然，得到：





访问这个文件，get flag：`flag{e07cd440-8eed-11e7-997d-7efc09eb6c59}`：

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