i-春秋-2017第二届广东省强网杯线上赛who are you?

原创

Kvein Fisher 于 2020-05-06 10:26:12 发布 250 收藏

分类专栏： i 春秋 文章标签： 信息安全 加密解密

本文链接：https://blog.csdn.net/qq_36438489/article/details/105944533

2017第二届广东省强网杯线上赛who are you?

WEB赛题

拿到之后提示说没有权限 于是用火狐看cookie ， 写的 **role：Zjo1OiJ0aHJmZyI7**

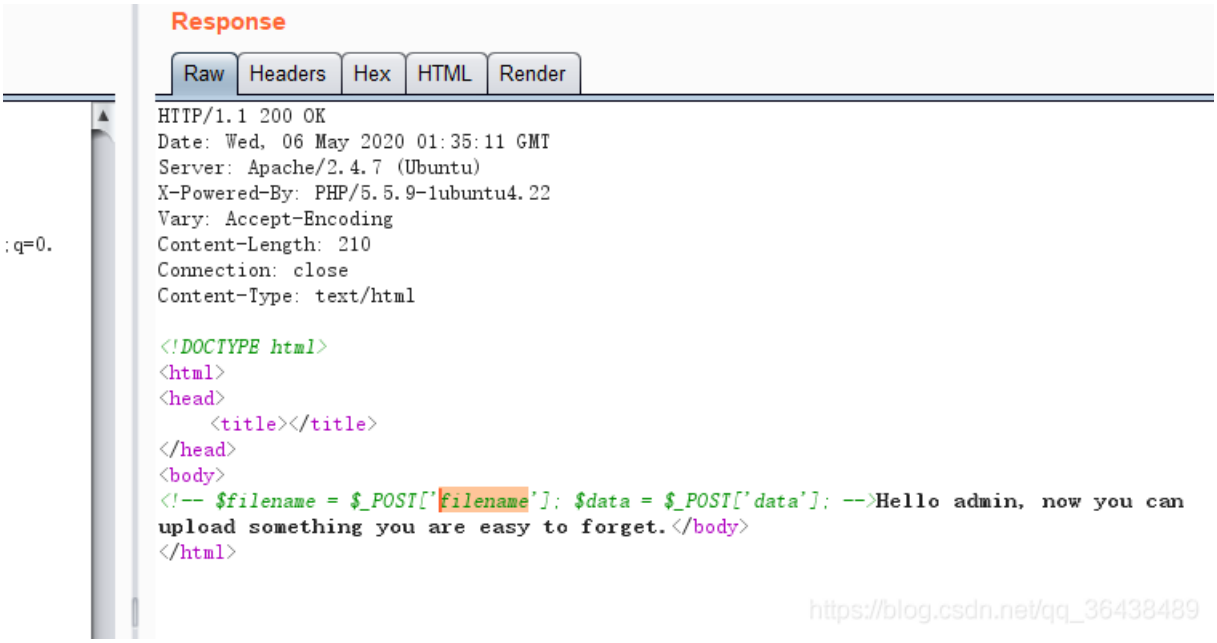
将Zjo1OiJ0aHJmZyI7解密base64 **f:5:"thrfg"**

扔到凯撒密码里看到 ***f:5:"thrfg"*** *根据大佬说是rot13，*

*解码得到s:5:“guest”**

之后将guest换成admin，在**s:5:“admin”**，之后在rot13加密，

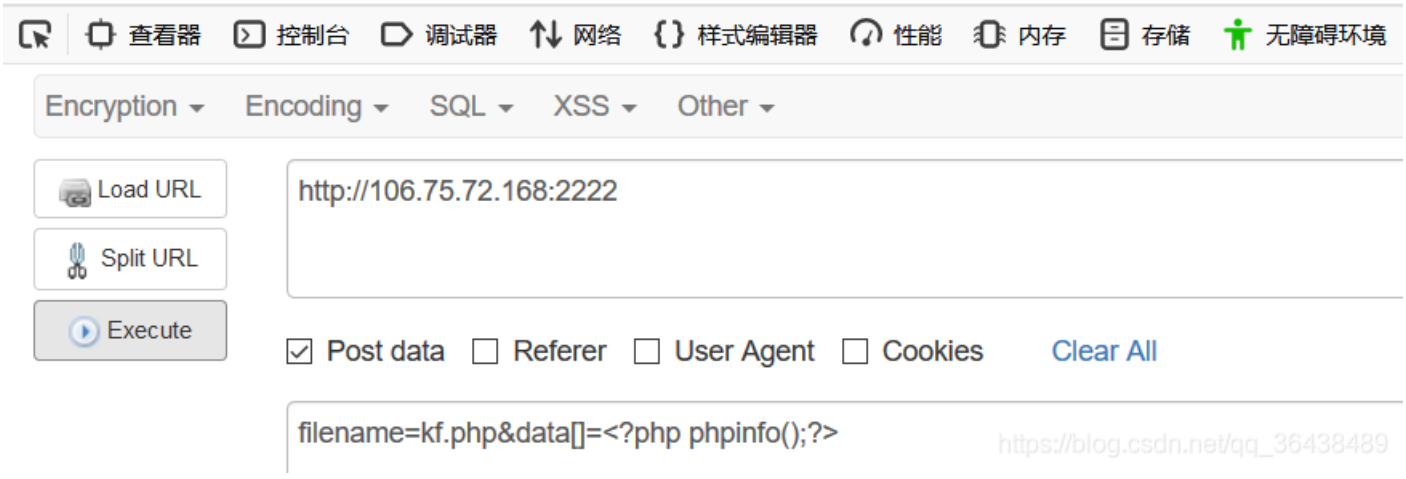
得到**f:5:“nqzva”** ，在base64加密Zjo1OiJucXp2YSI7,用burp repeater



看见有权限，有提示 filename=kf.php&data=<?php phpinfo();?>，但是好像被过滤掉了，提示NONONO

看见大佬payload: filename=kf.php&data[]=<?php phpinfo();?>
这里用数组进行绕过

your file is in ./uploads/6f8ad6b2c694d1807c625433a9299de1kf.php



之后访问http://106.75.72.168:2222/uploads/得到flag

这里说一下data[]也就是数组绕过，php中存在一些函数对传入数组无法处理，进而返回false，进而绕过，这道ctf赛题对<>进行过滤，我们在这里可以用数组进行绕过。详见下面这位大佬的博客：
https://www.jianshu.com/p/5fd1b624fd7a