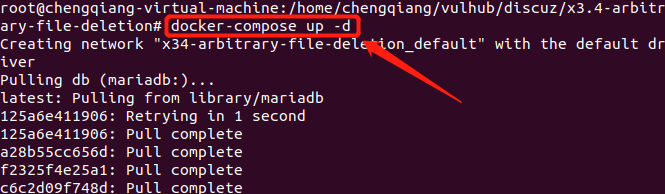
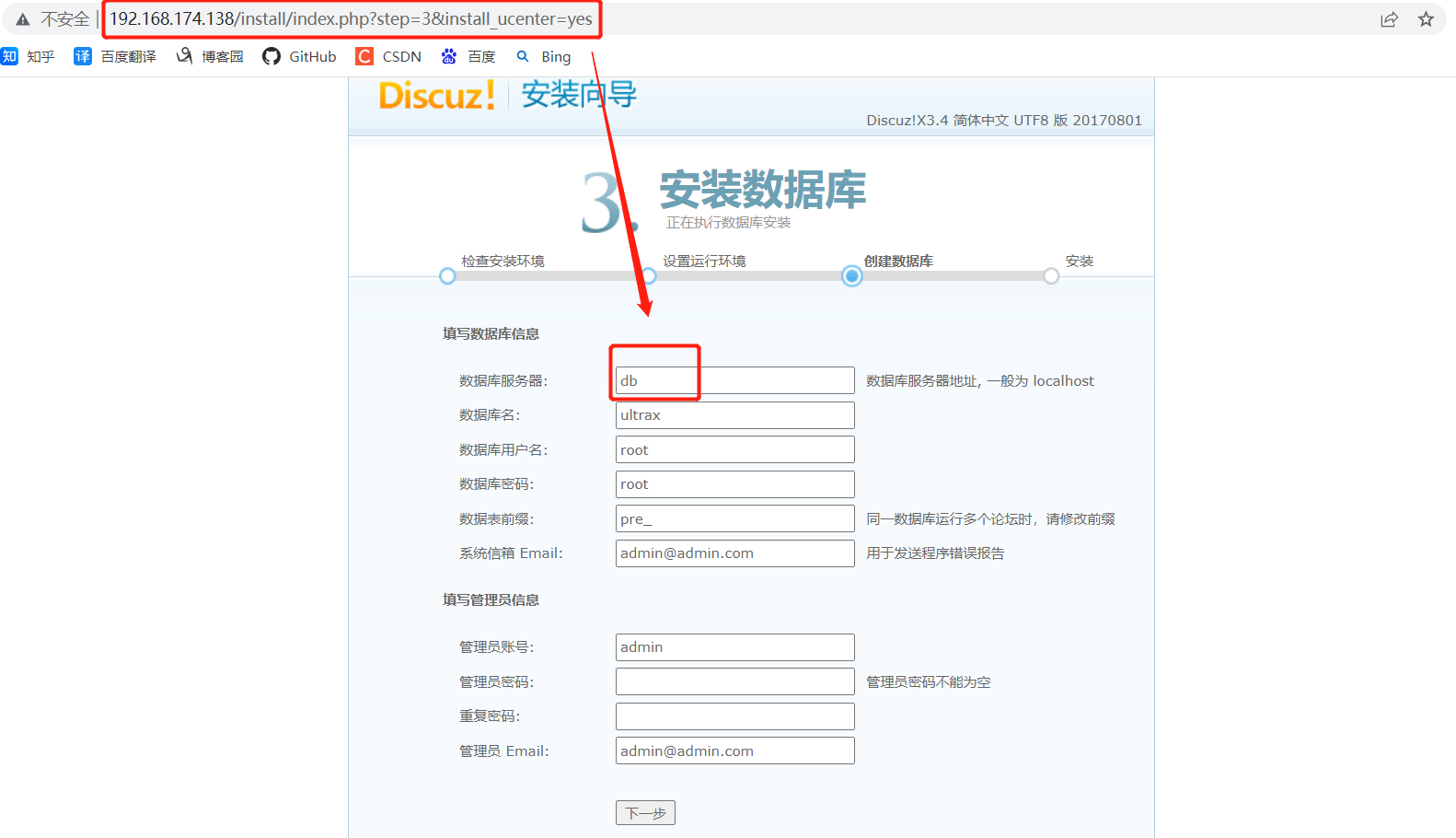
**一、靶场搭建**

1、Vulhub启动



2、访问/install/目录并安装，只需修改数据库地址为db，其他默认

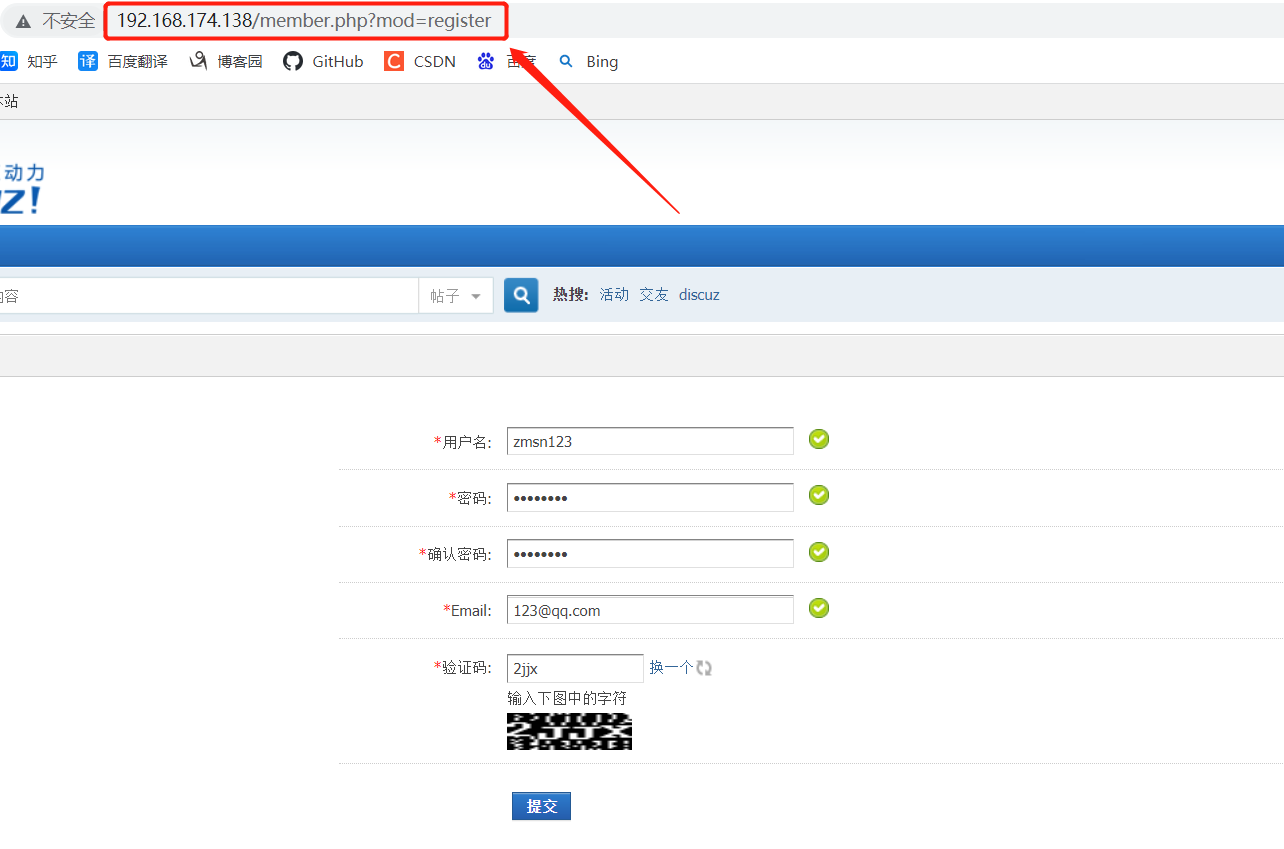


**二、漏洞复现**

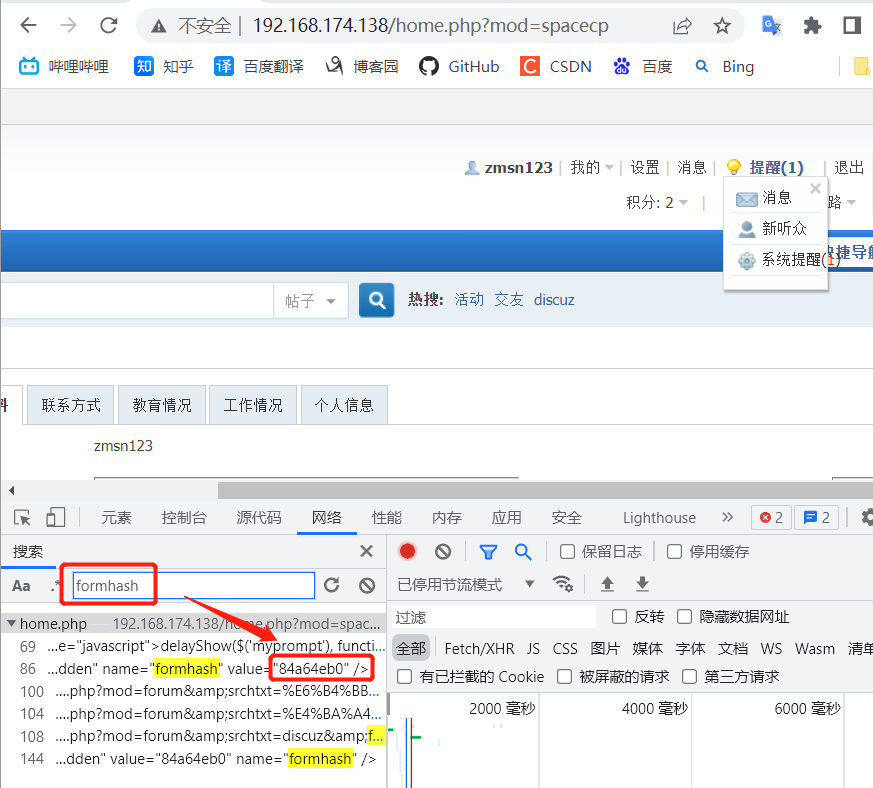
1、访问/robots.txt文件，查看是否存在



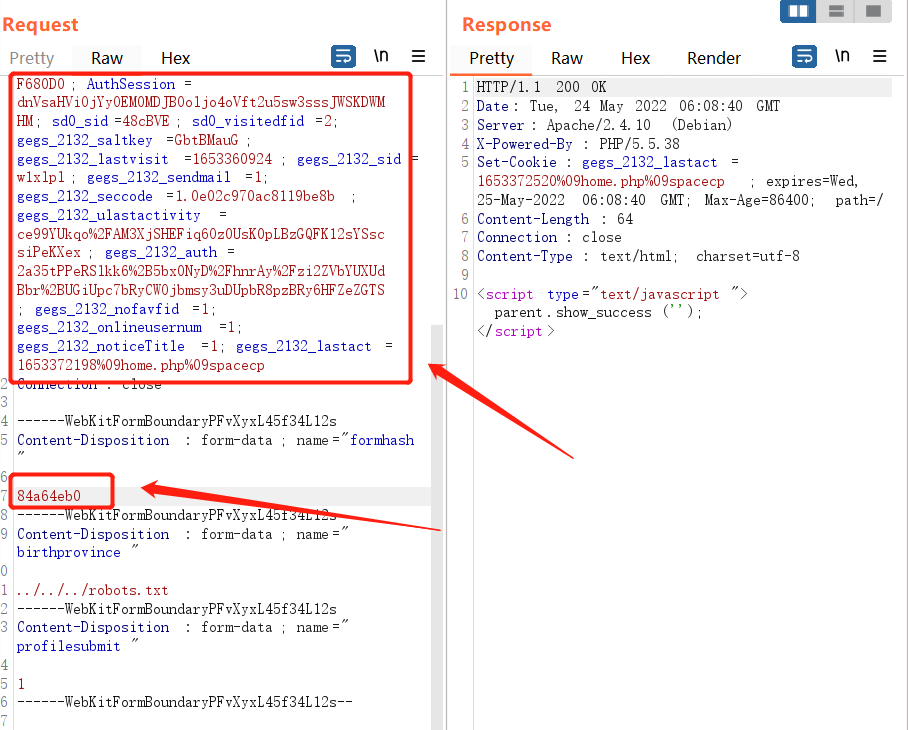
2、注册用户



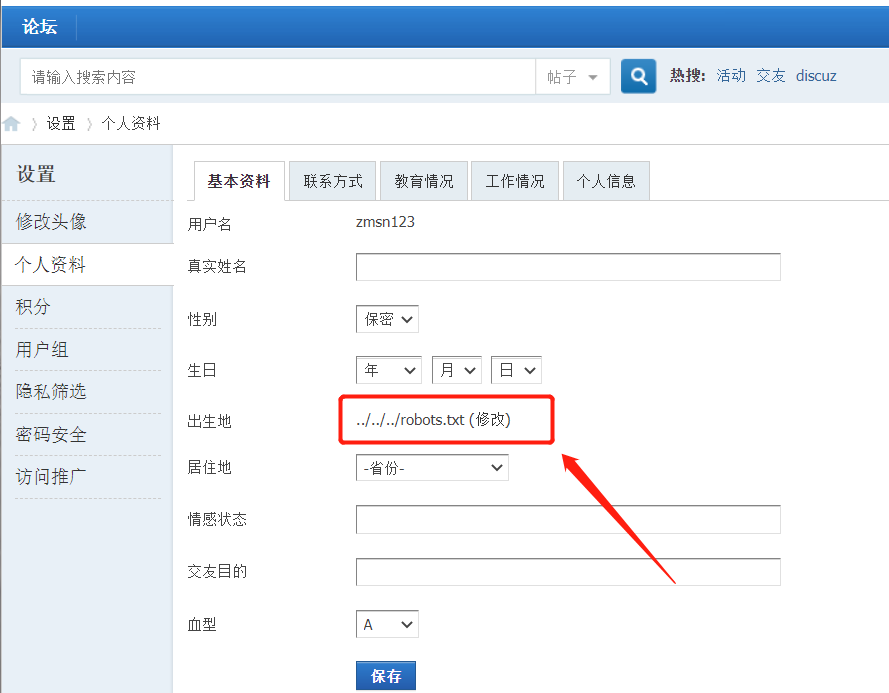
3、在设置中找到formhash值



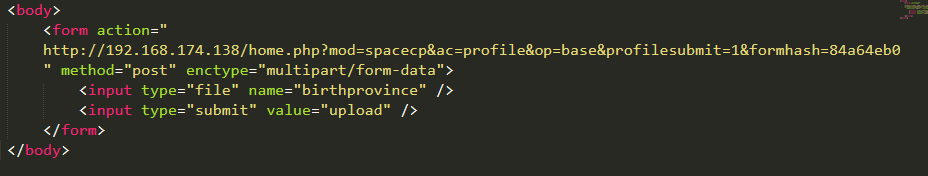
4、带着Cookie、formhash发送数据包



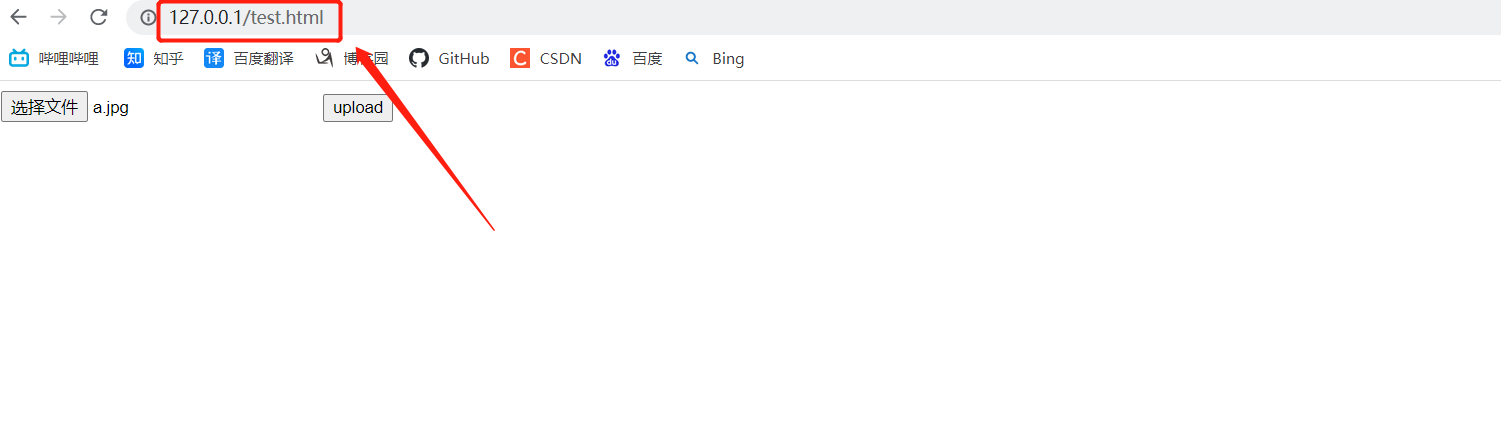
5、此时个人页面中数据已被篡改



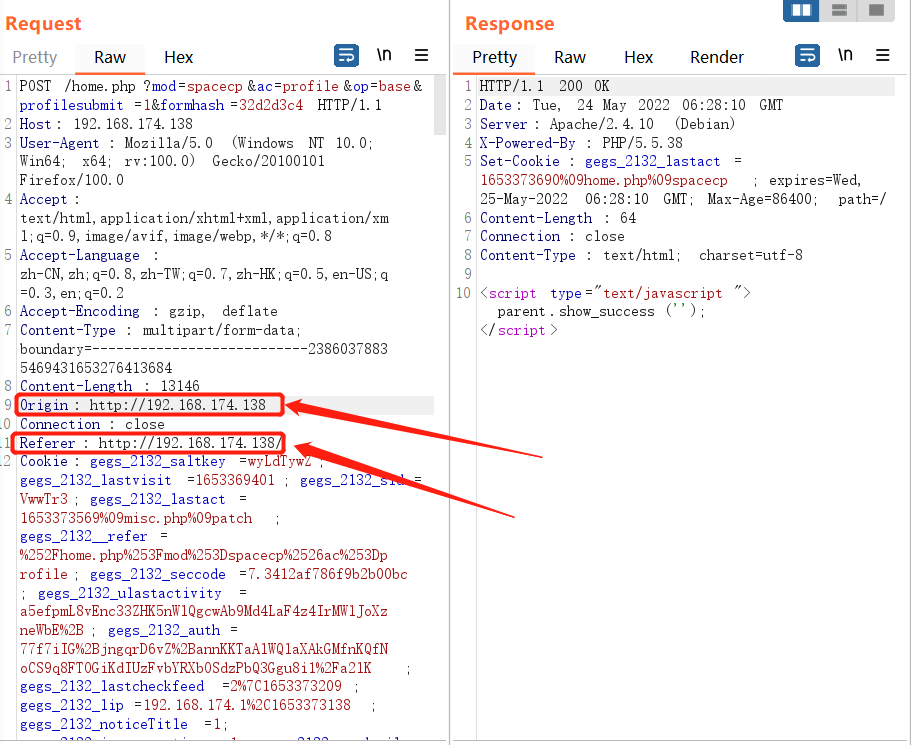
6、本地新建一个test.html



7、访问test.html并上传任意图片



8、提交时抓包并修改数据包中的Referer和Origin为目标地址



9、再次访问/robots.txt，发现文件成功被删除

