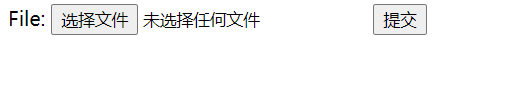
**一、靶场搭建**

1、Vulhub启动

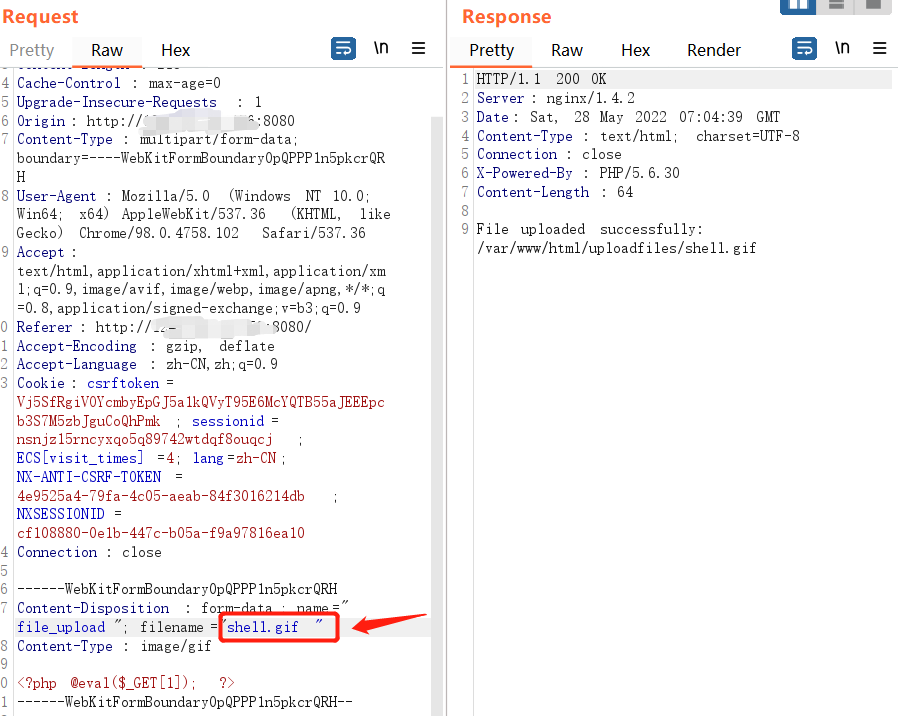
docker-compose up -d

2、访问8080端口可看到一个上传页面

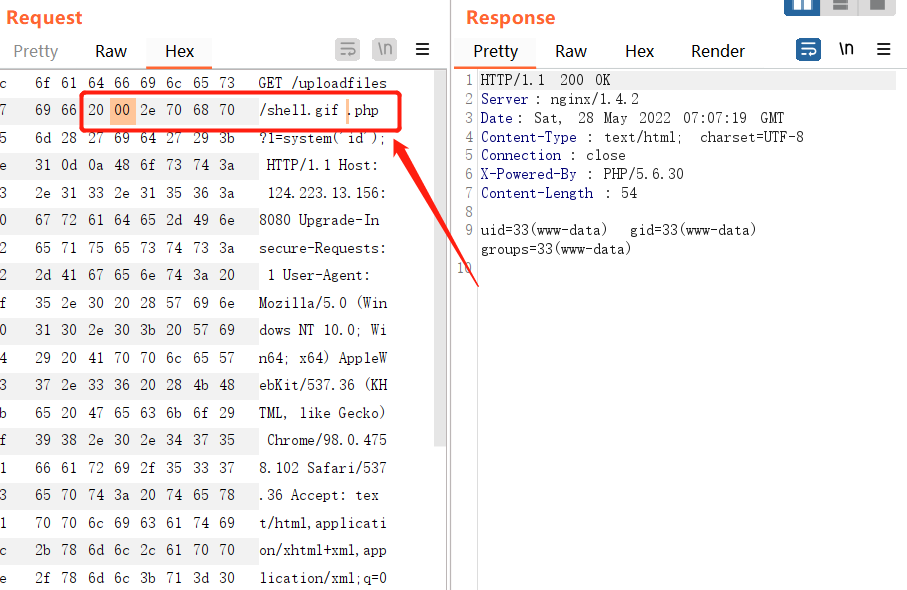


**二、漏洞复现**

1、上传一个1.gif，内容为一句话木马，抓包并在gif后面留一个空格



2、抓包访问/uploadfiles/1.gif .php?1=system(‘id’);， 通过二进制修改第二个空格的值为00



3、成功执行id命令

