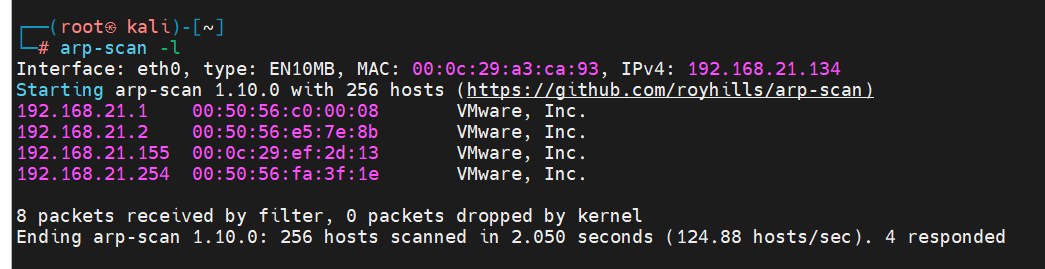
Looz

下载地址： <https://www.vulnhub.com/entry/looz-1,732/>

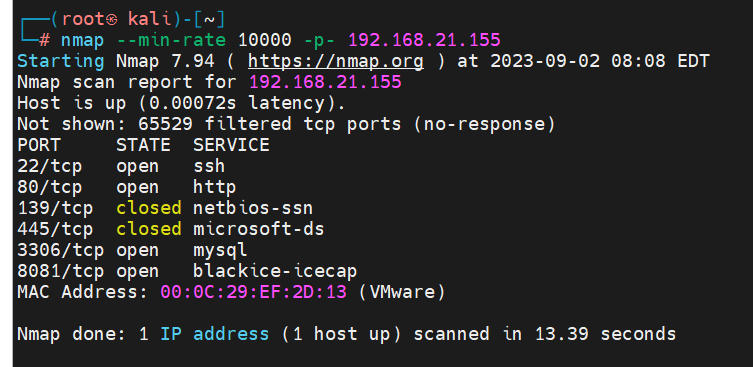
主机发现

arp-scan -l



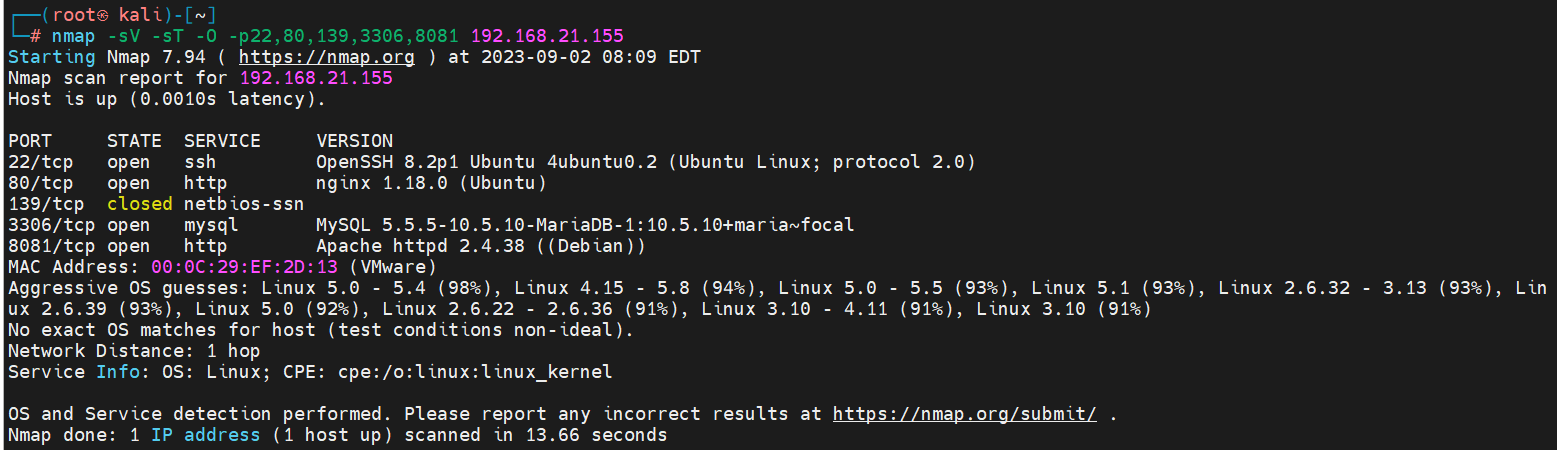
端口扫描

nmap --min-rate 10000 -p- 192.168.21.155



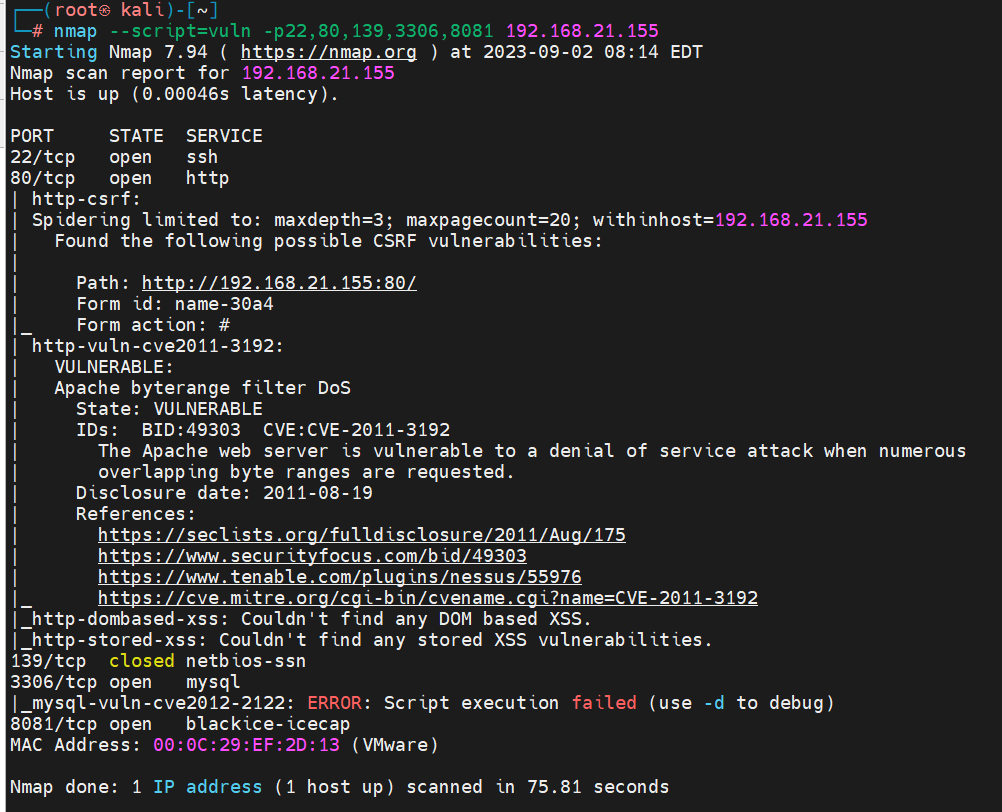
扫描端口信息

nmap -sV -sT -O -p22,80,139,3306,8081 192.168.21.155

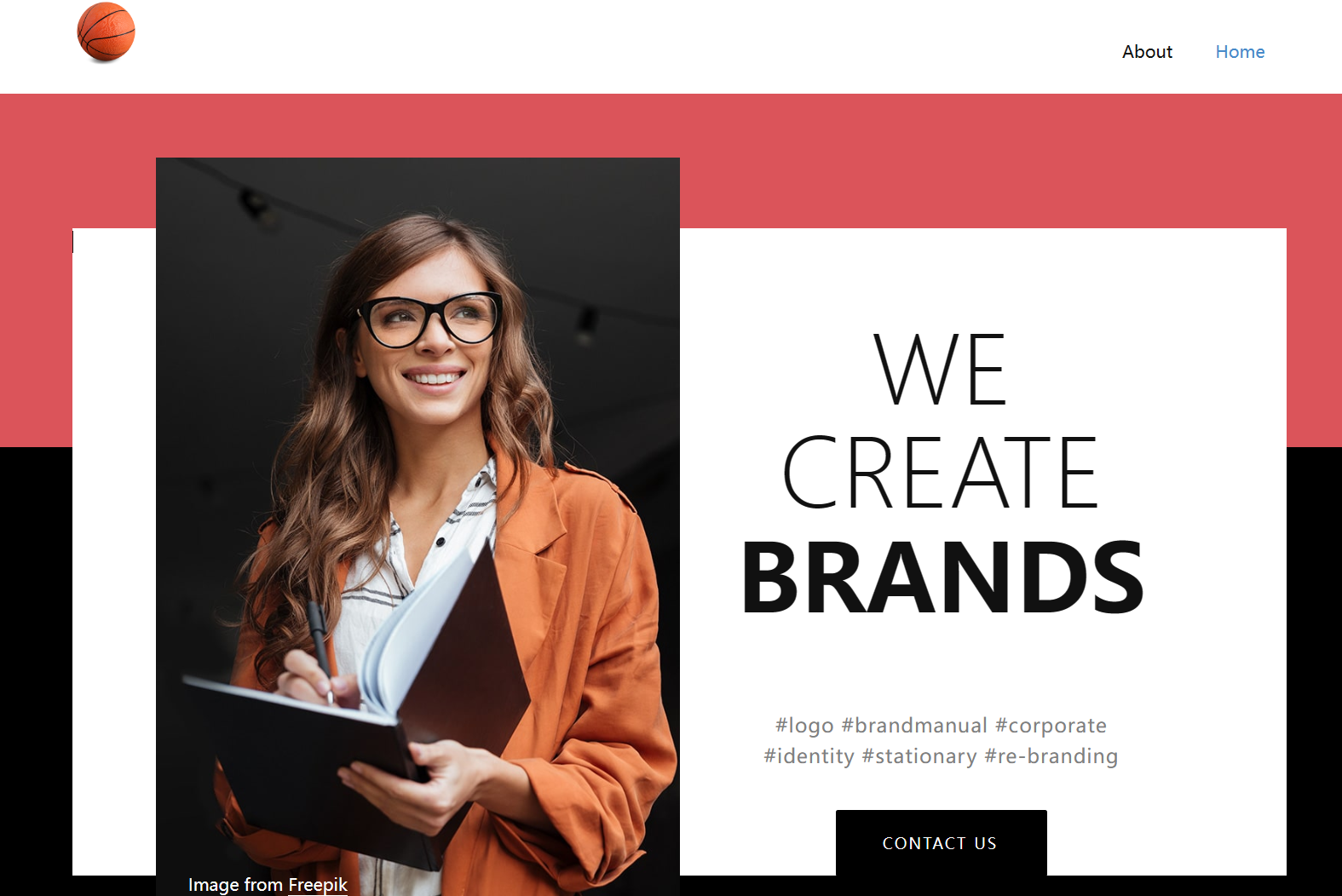


漏洞扫描

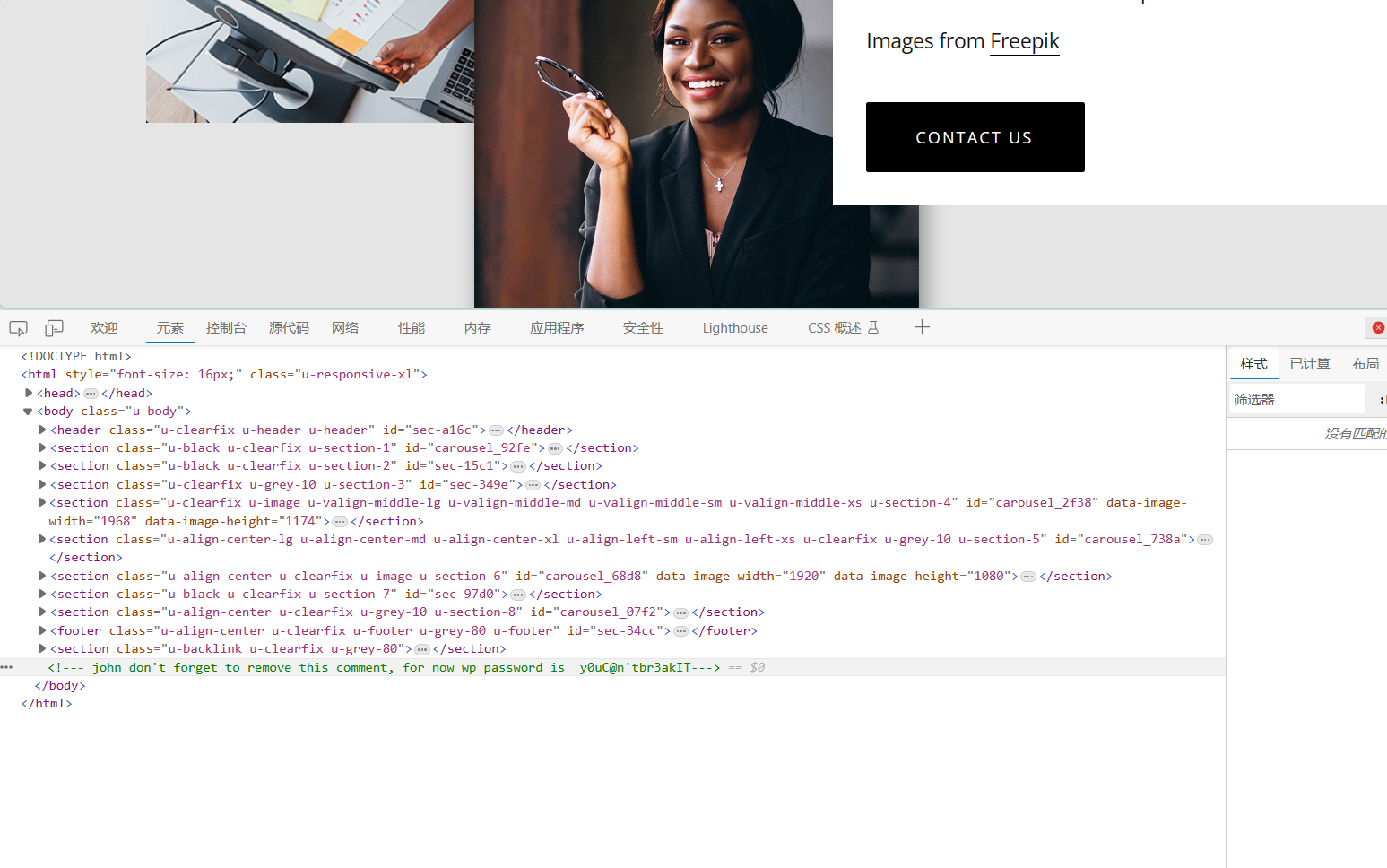
nmap --script=vuln -p22,80,139,3306,8081 192.168.21.155



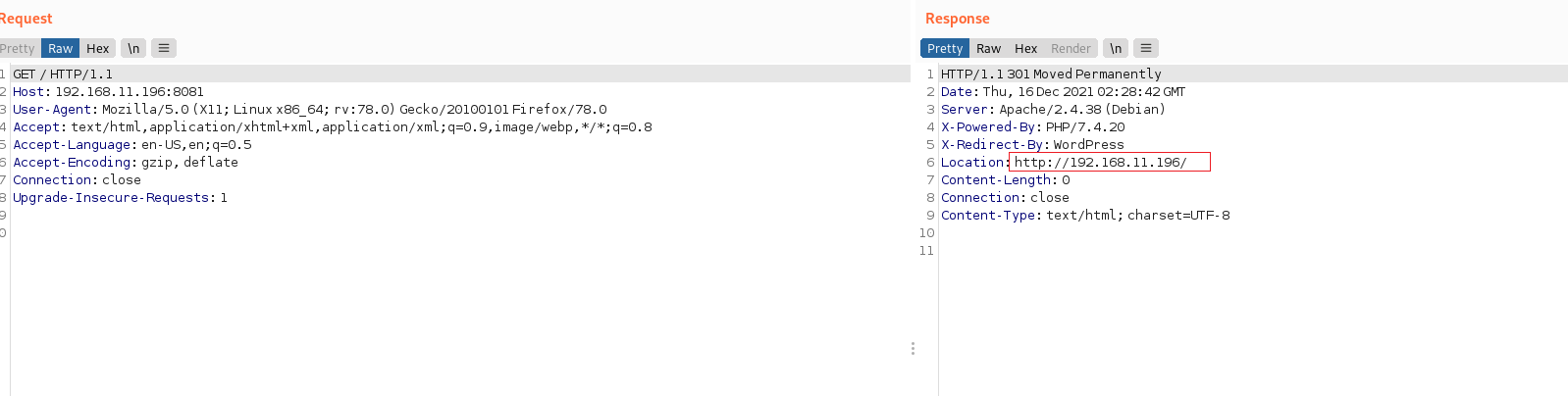
去web网站上看看



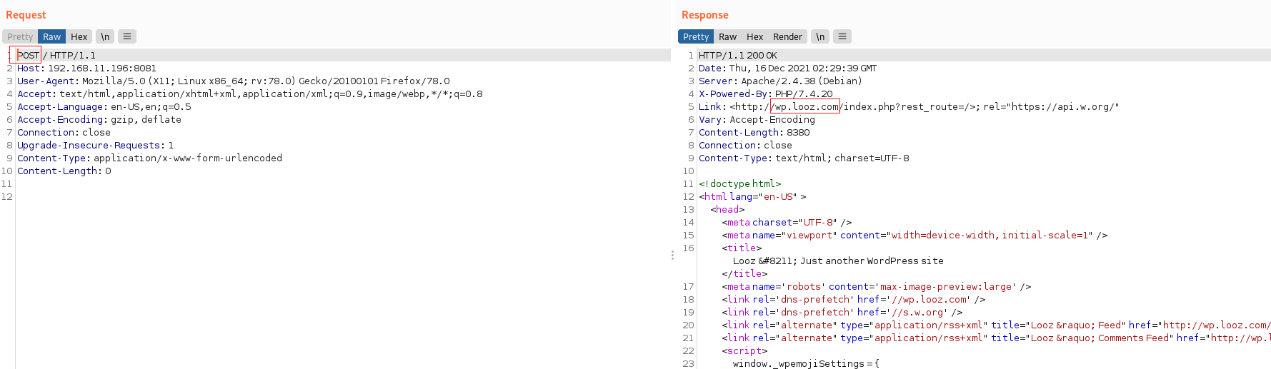
在f12看到的



没什么了再去看8081



这里发现他转跳到了80端口，改一下请求方式

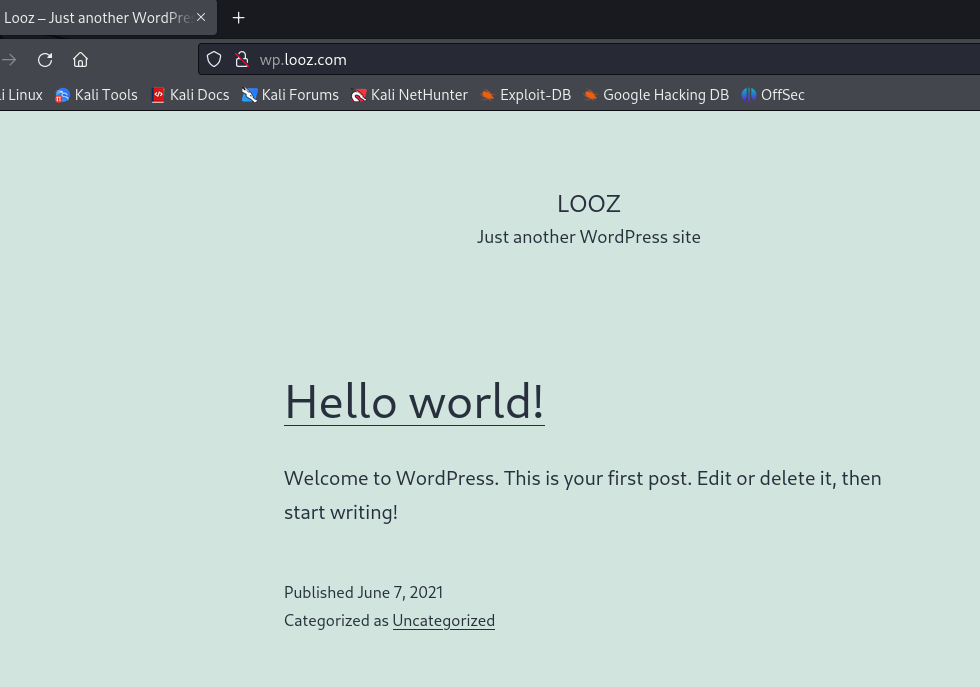


发现会转跳到80端口这里抓包就能发现域名

修改域名配置文件

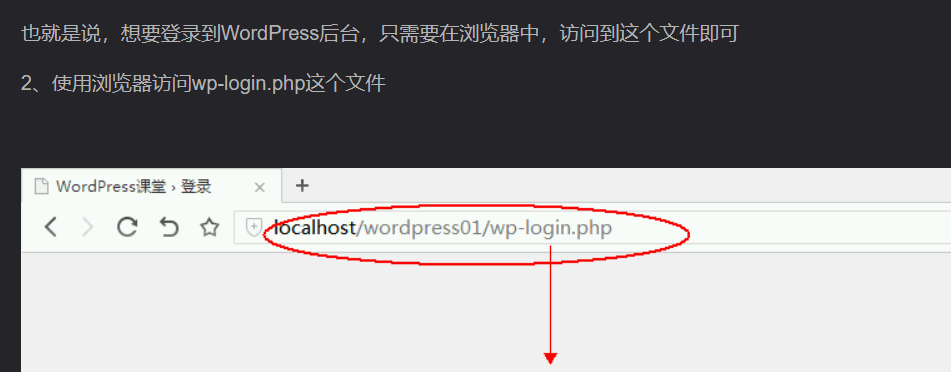


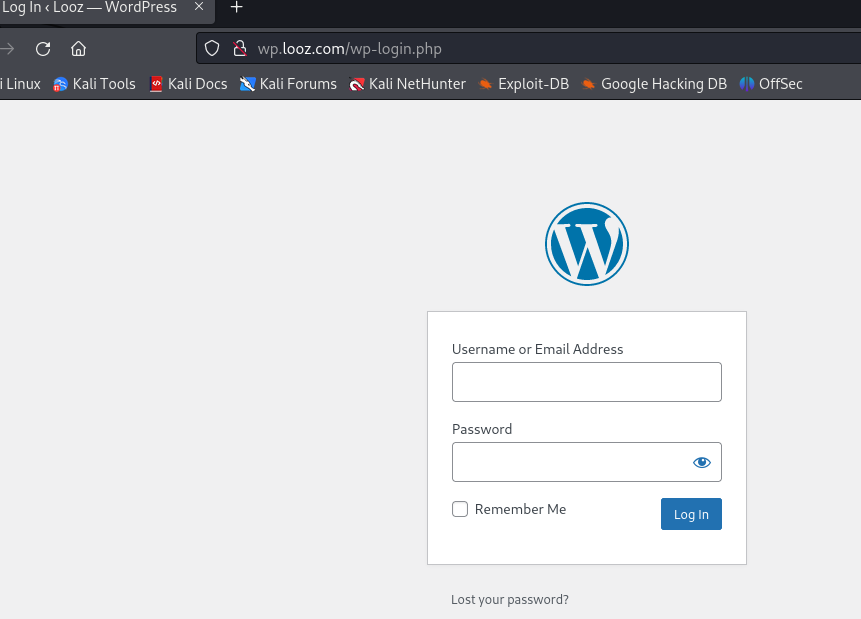
直接访问



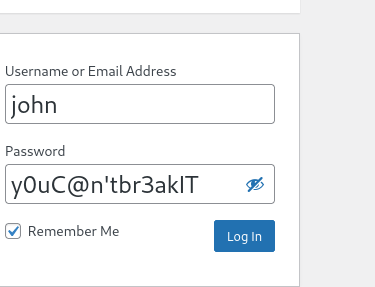
这个用的是wordpress的框架

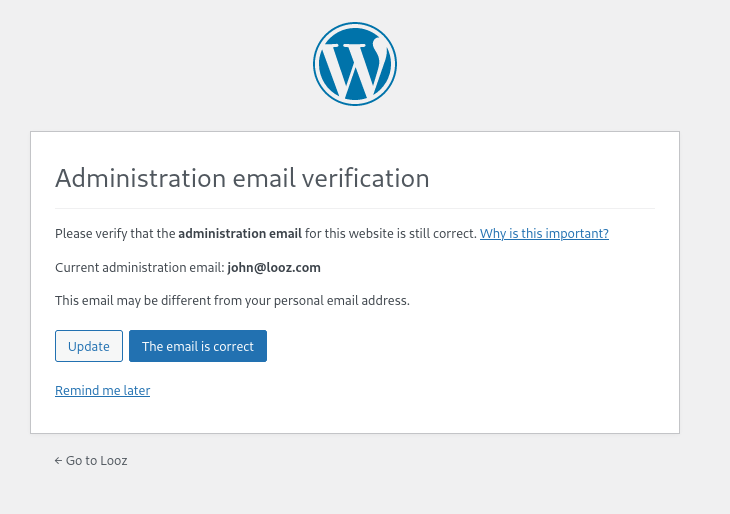
第一件事就是直接找这个的后台，随手一查就行



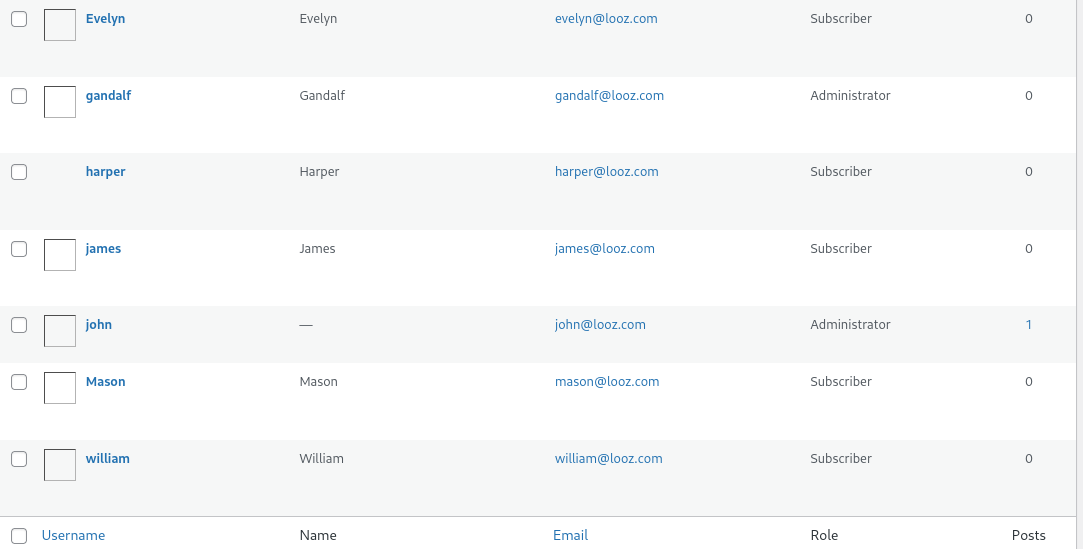


密码和账号是之前找到的





翻一下后台的用户当然要看看管理员

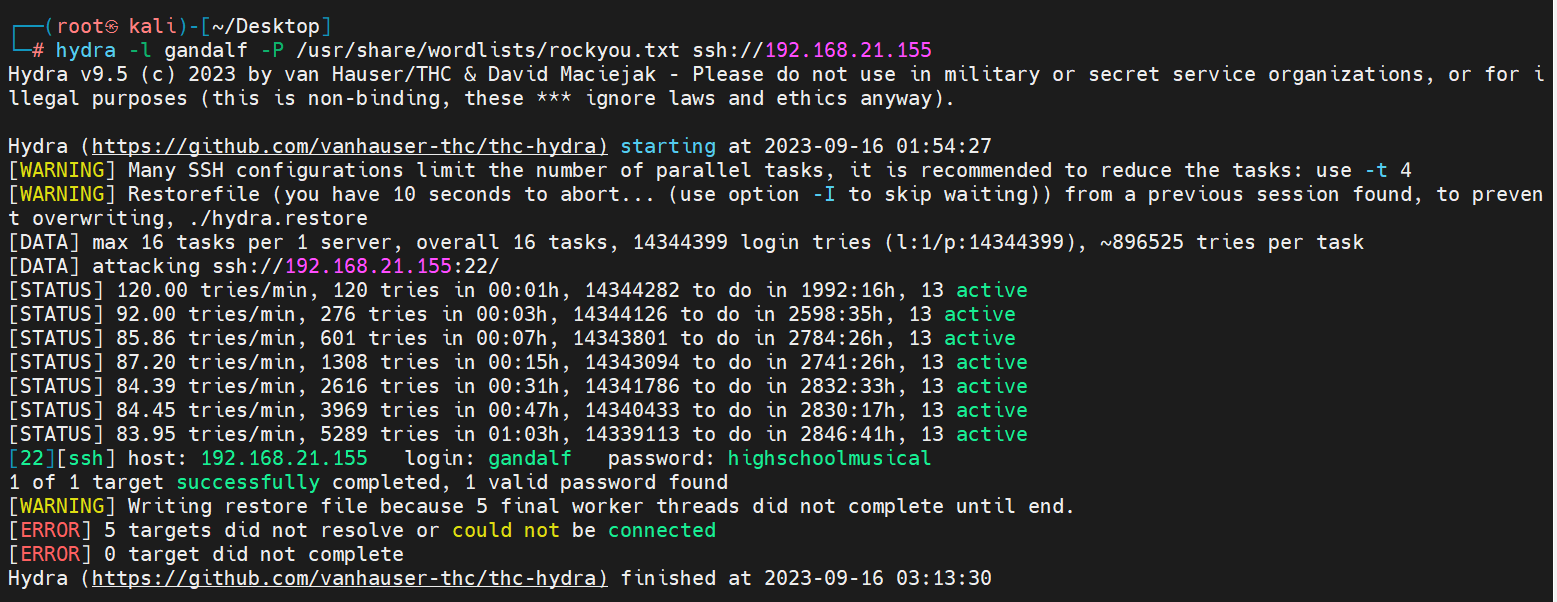


找到一个

这个因该是ssh的账号了

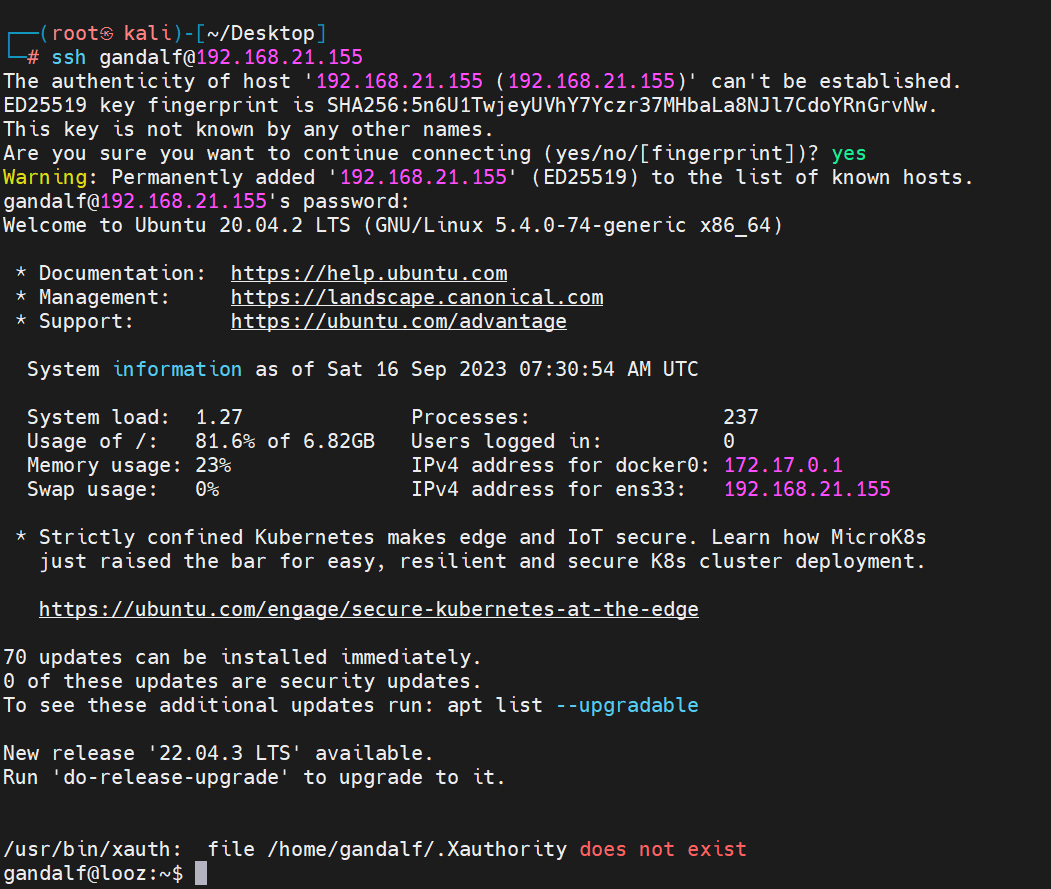
先爆破试试（这个很慢）

hydra -l gandalf -P /usr/share/wordlists/rockyou.txt ssh://192.168.21.155

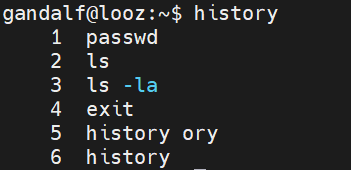


ssh登入

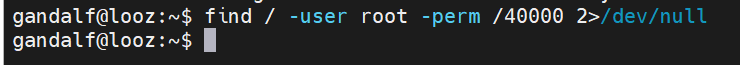
ssh [gandalf@192.168.21.155](mailto:gandalf@192.168.21.155)

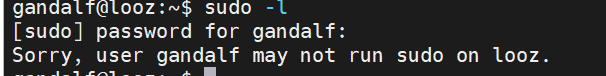


信息收集



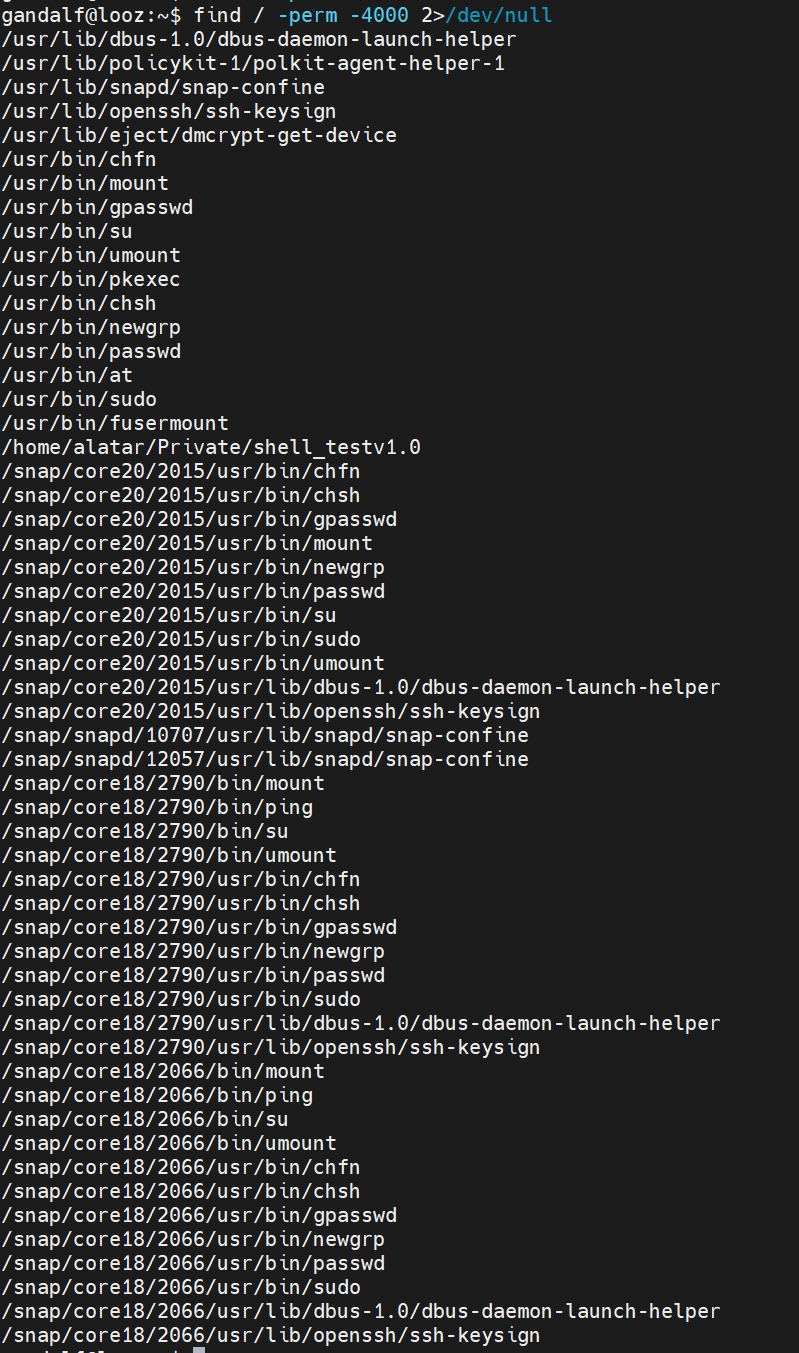






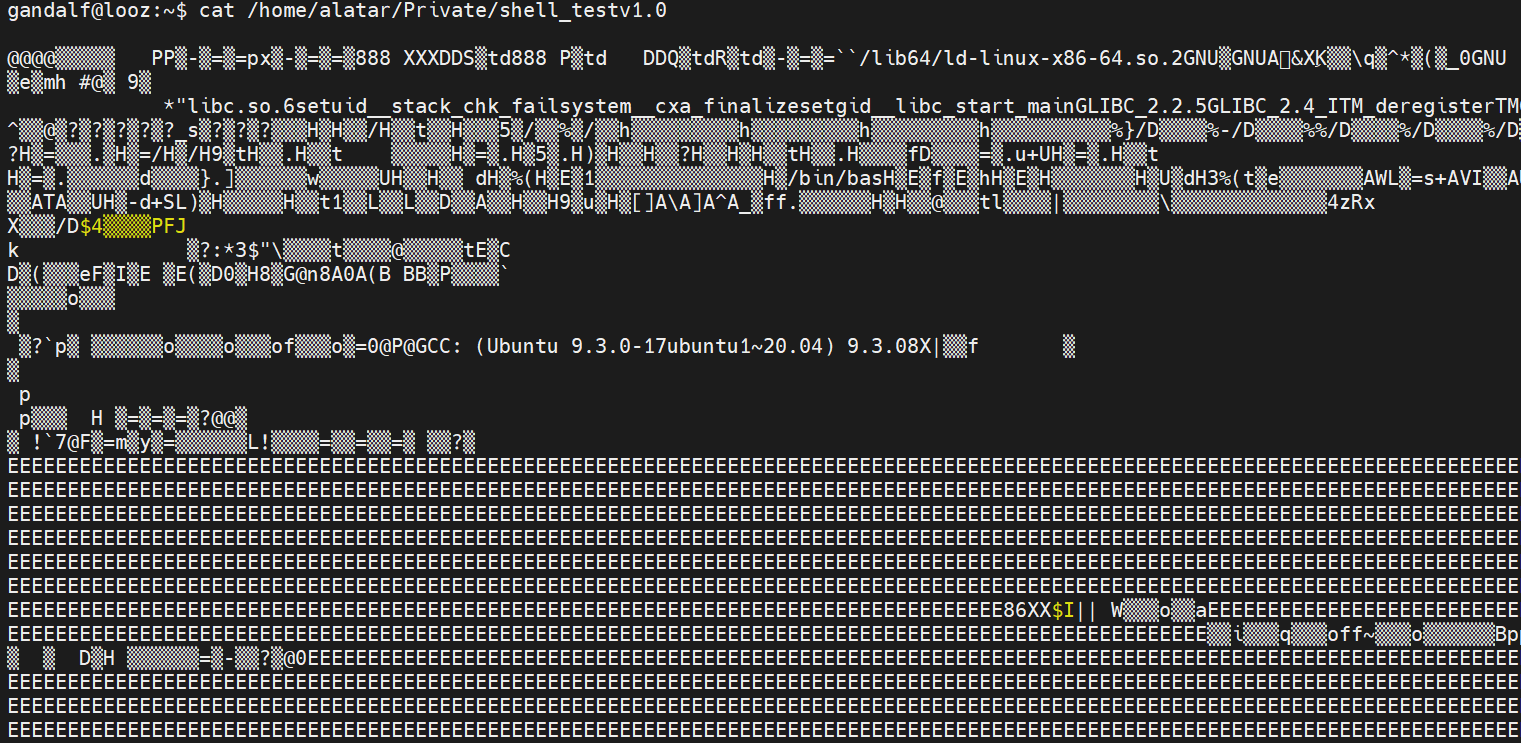
重新找一下可执行文件

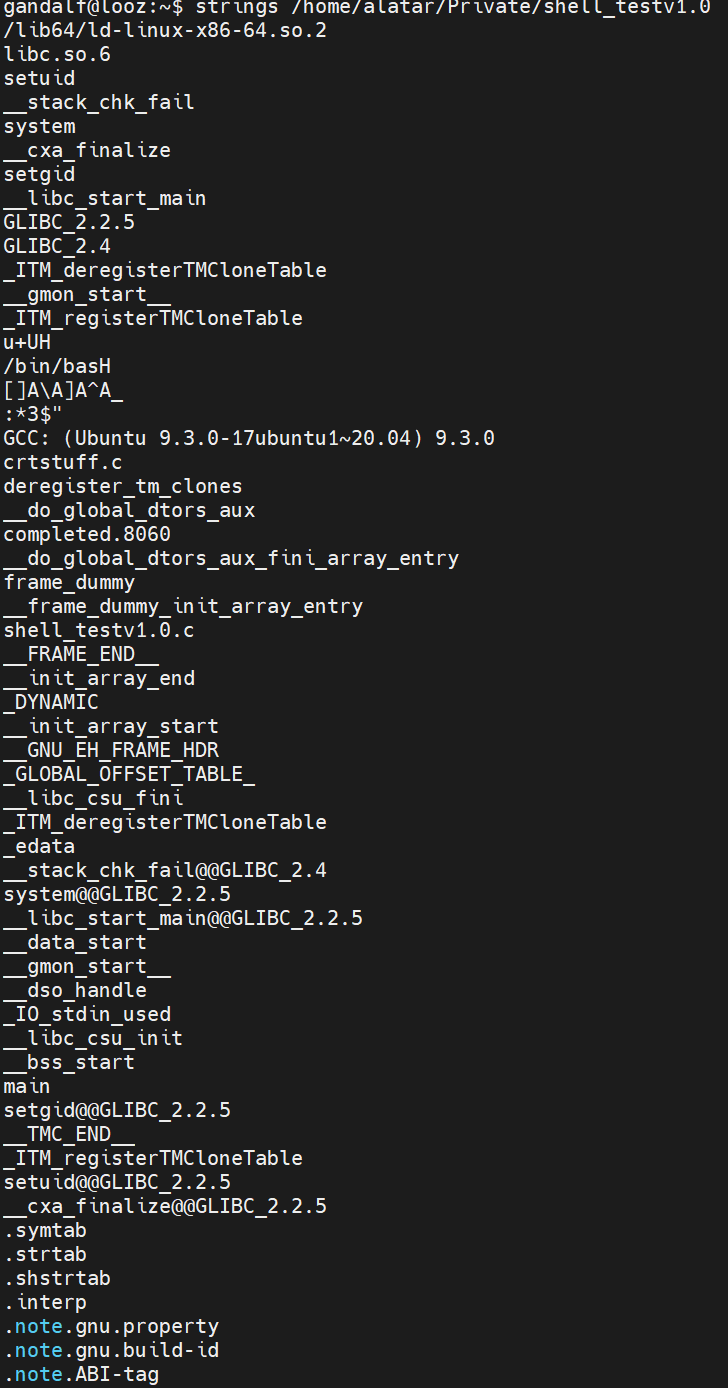
find / -perm -4000 2>/dev/null



主要看home目录

去看一下

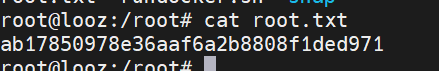




直接执行

/home/alatar/Private/shell\_testv1.0





结束