**广州大学学生实验报告**

开课学院及实验室：计算机科学与工程实验室电子楼416A室 2023年4月26日

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 学院 | 网络空间安全学院 | | 年级、专业、班 |  | 姓名 |  | 学号 |  |
| 实验课程名称 | | 操作系统及安全分析 | | | | | 成绩 |  |
| 实验项目名称 | | 常见渗透工具和思路探究及简单实践 | | | | | 指导老师 | 鲁辉 |

**一、使用仪器、器材**

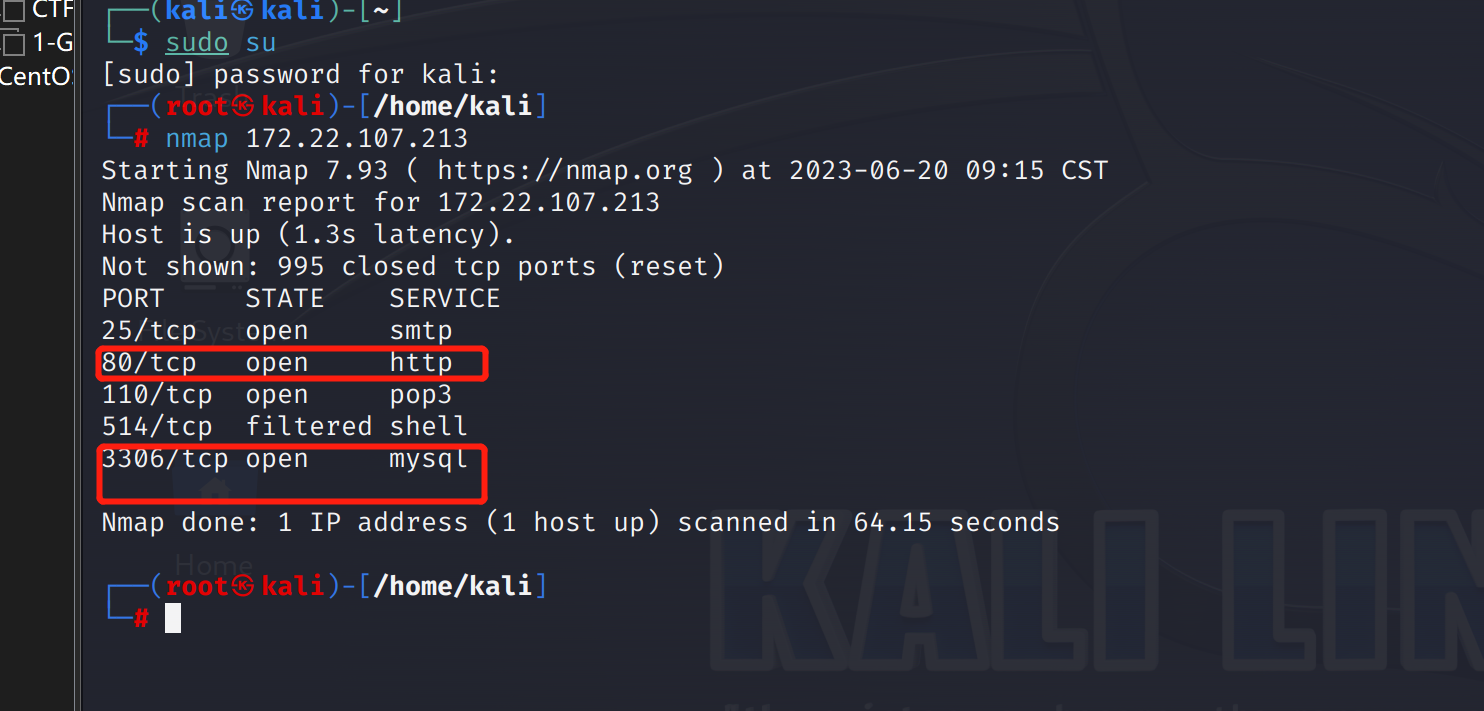
操作系统：windows 系统；kali

工具：nmap/dirsearch/antsword/yakit

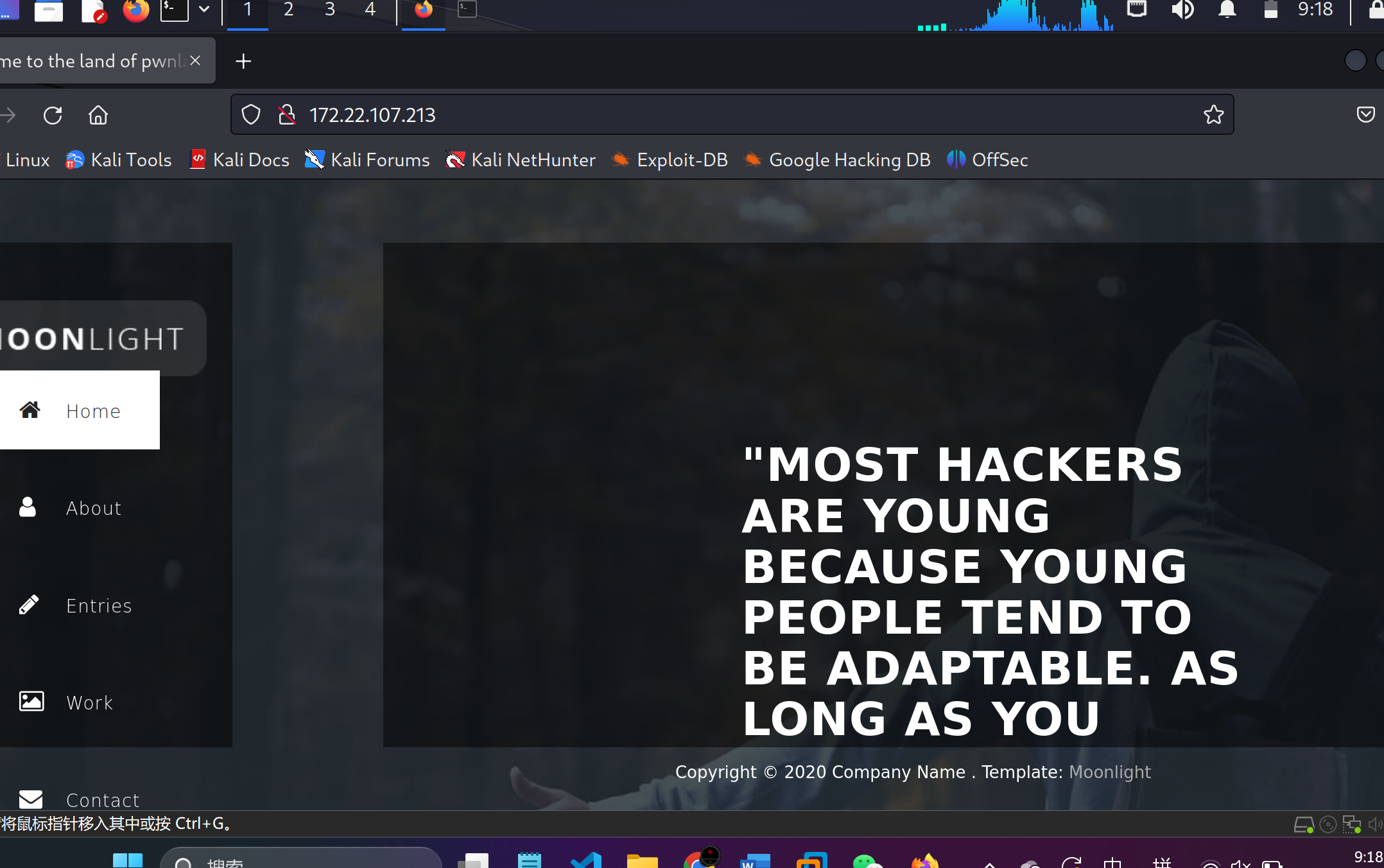
**二、实验内容及原理**

（1）渗透测试中的信息收集

Nmap扫描：



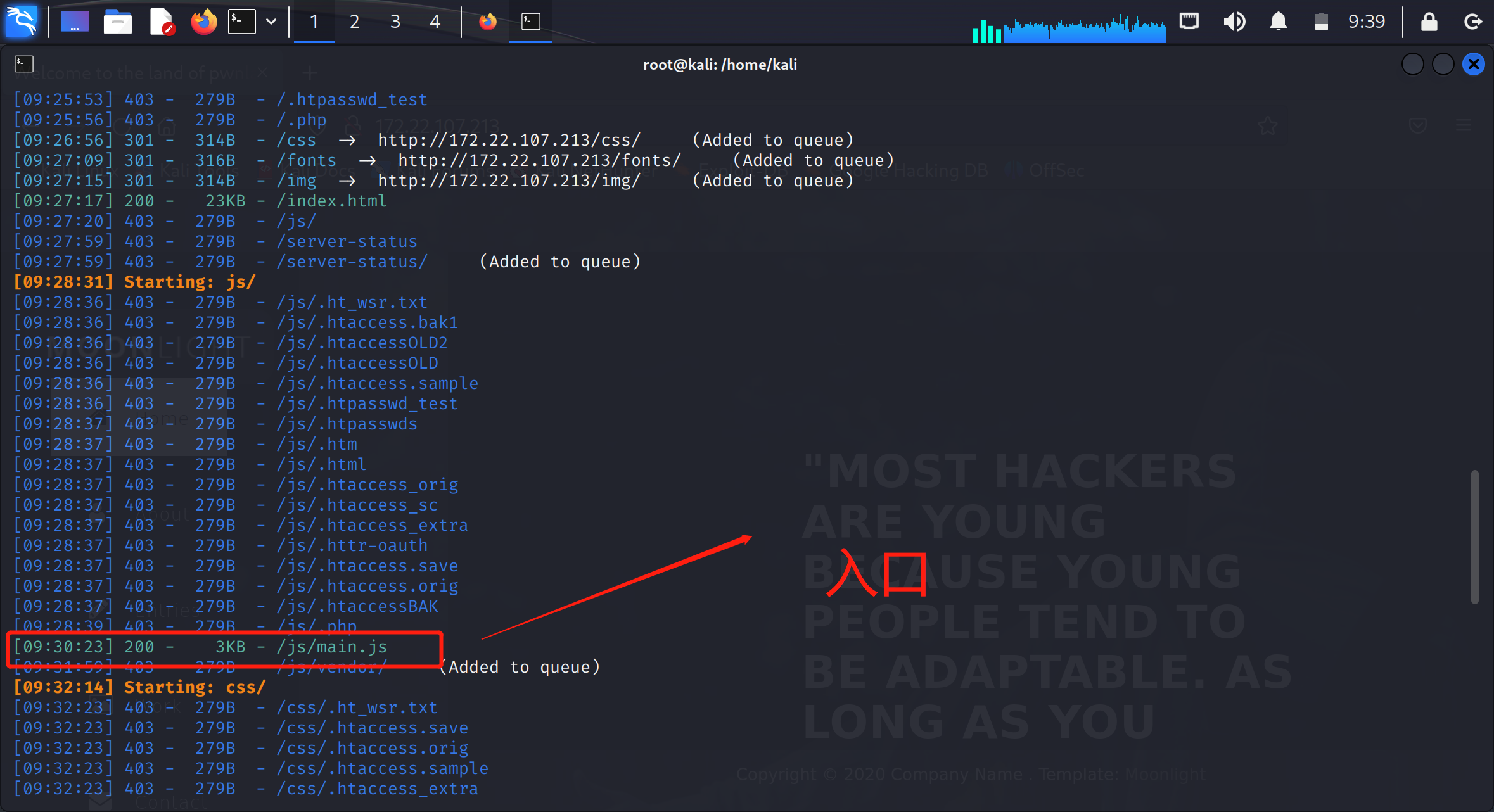
<http://172.22.107.213:80/>



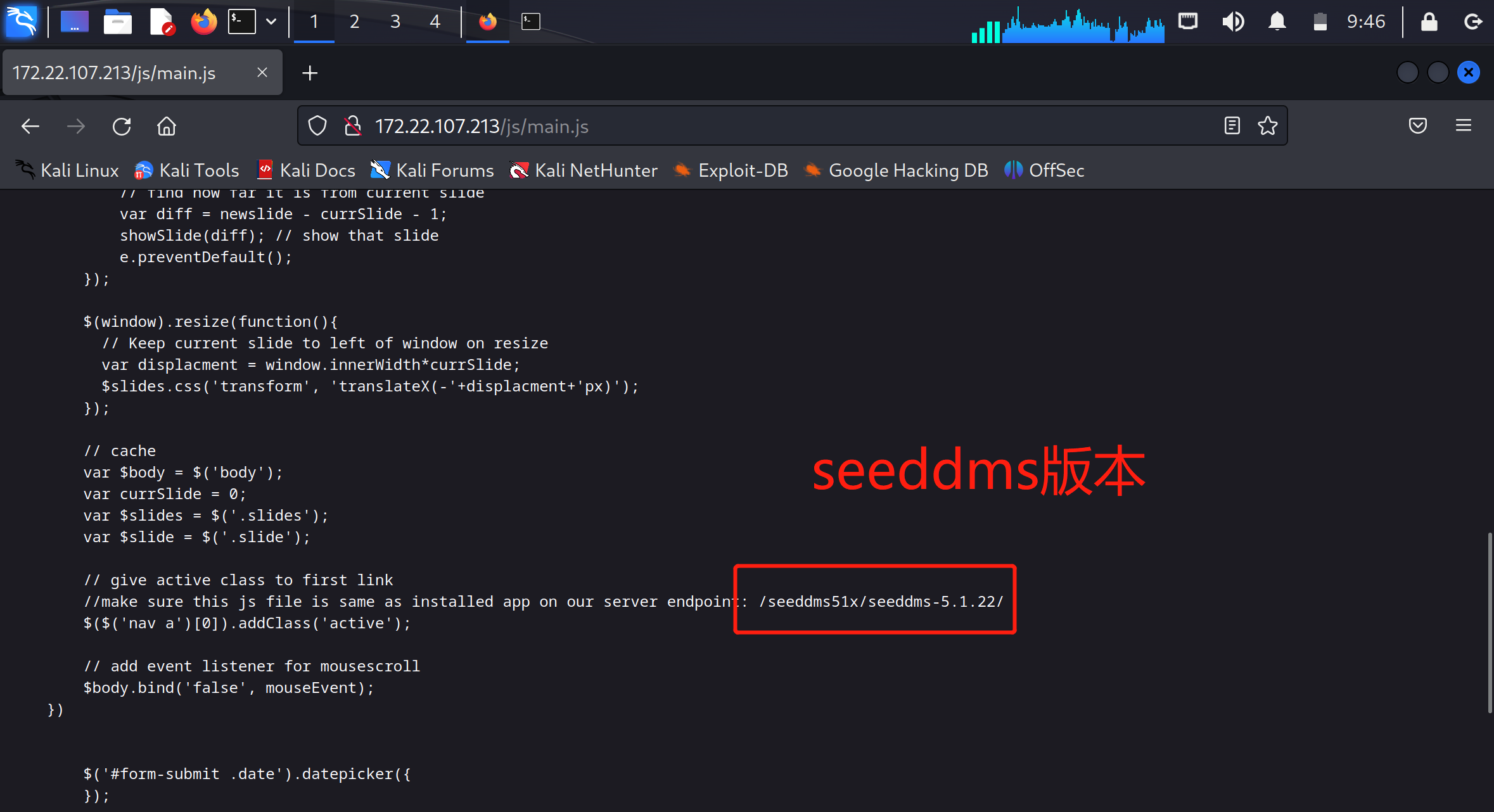
一个网站

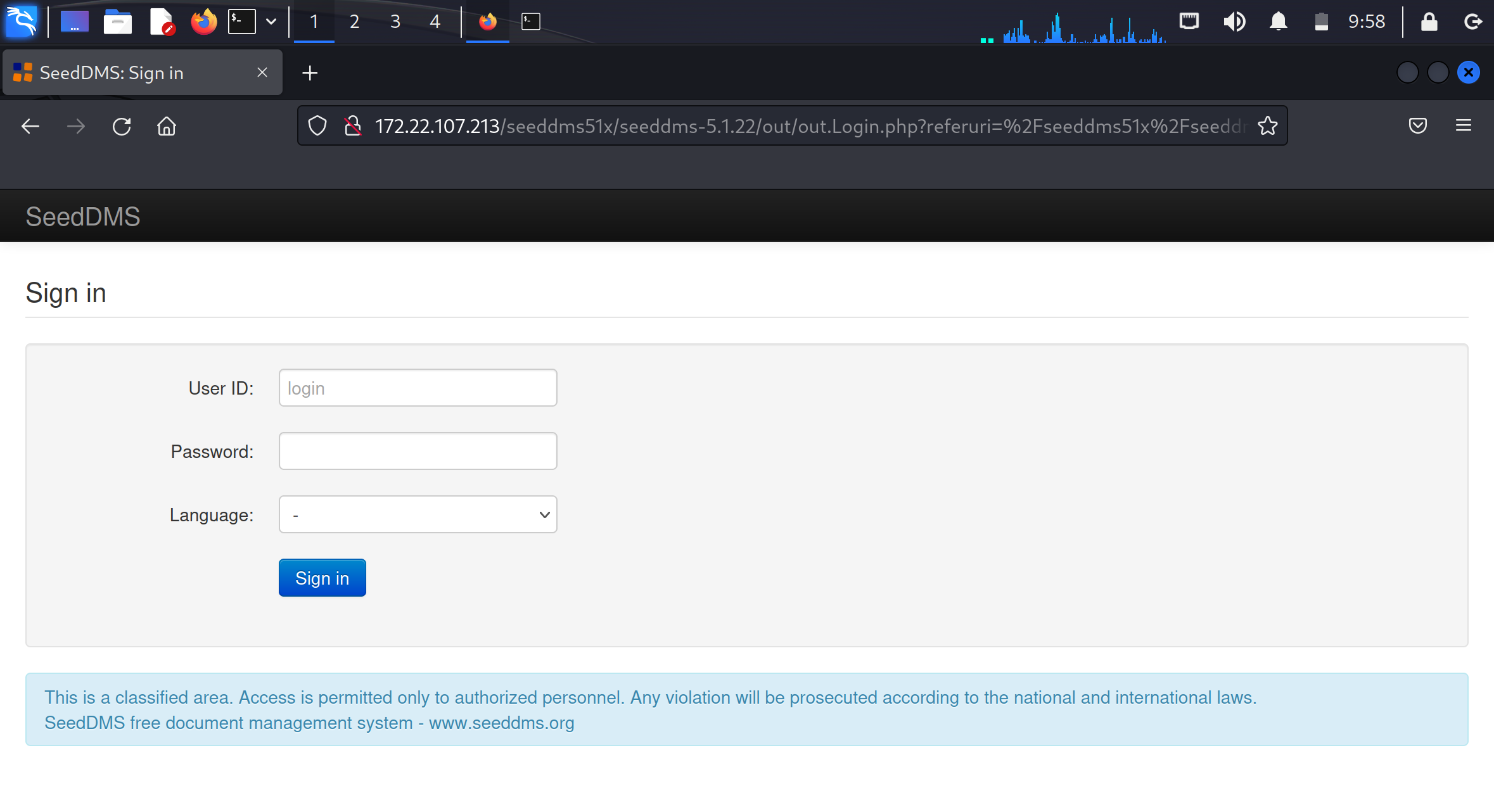
递归地扫描目标网站的目录和文件

dirsearch -u http://172.22.107.213/ -r 1



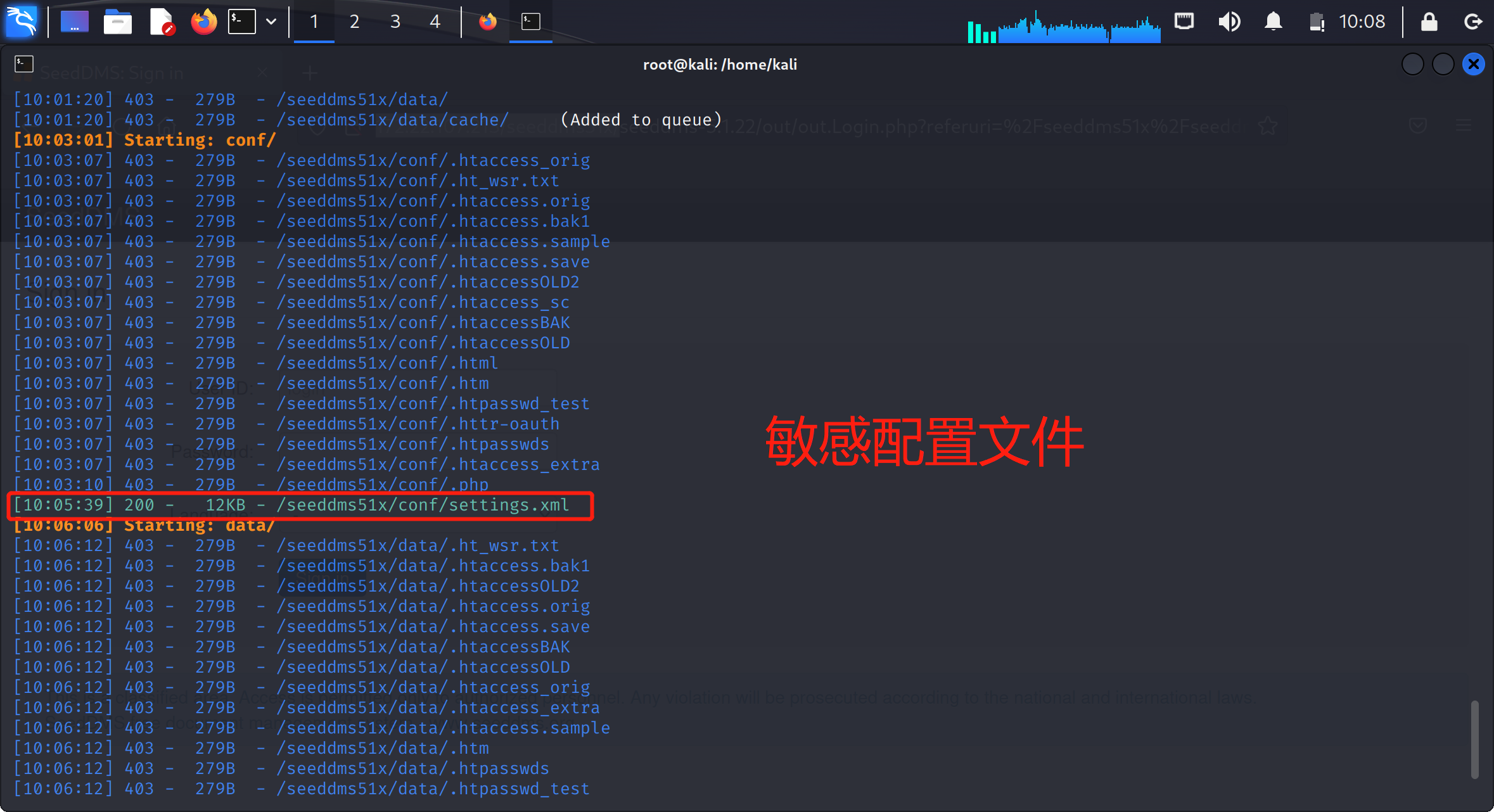
进去看看



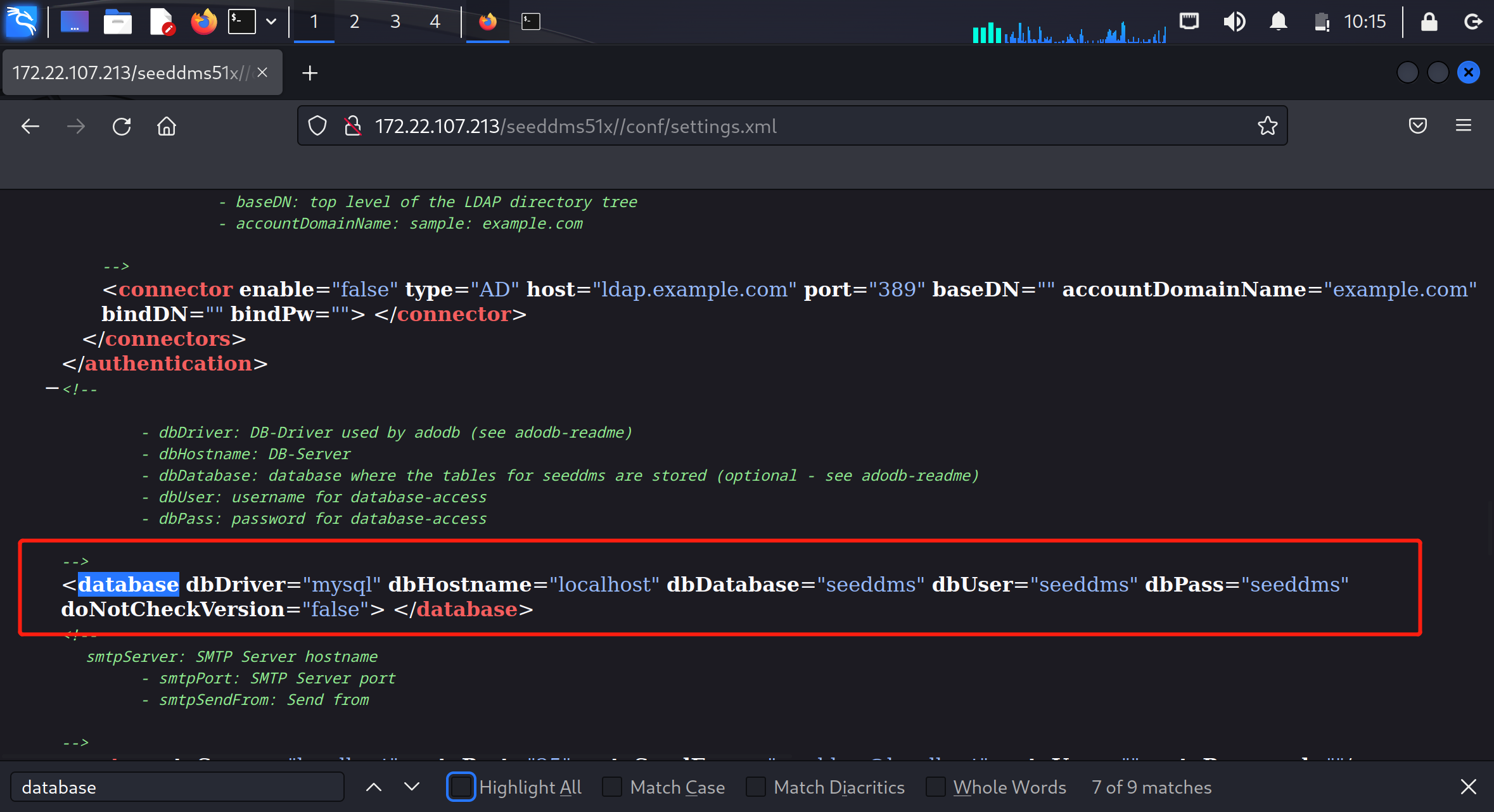


再往下扫一层：

dirsearch -u http://172.22.107.213/seeddms51x/ -r 1



泄露配置文件

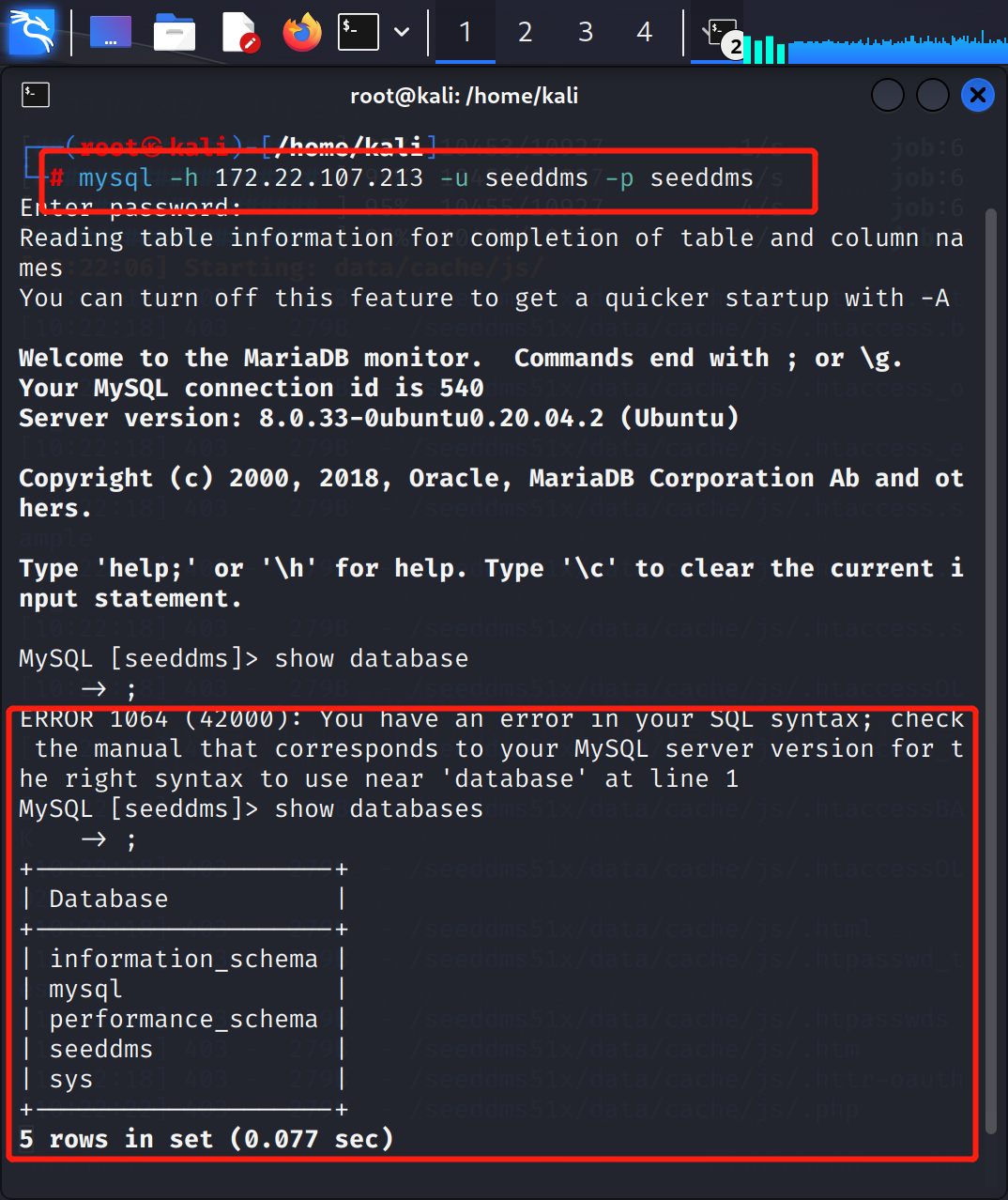


**<database dbDriver="mysql" dbHostname="localhost" dbDatabase="seeddms" dbUser="seeddms" dbPass="seeddms" doNotCheckVersion="false"> </database>**

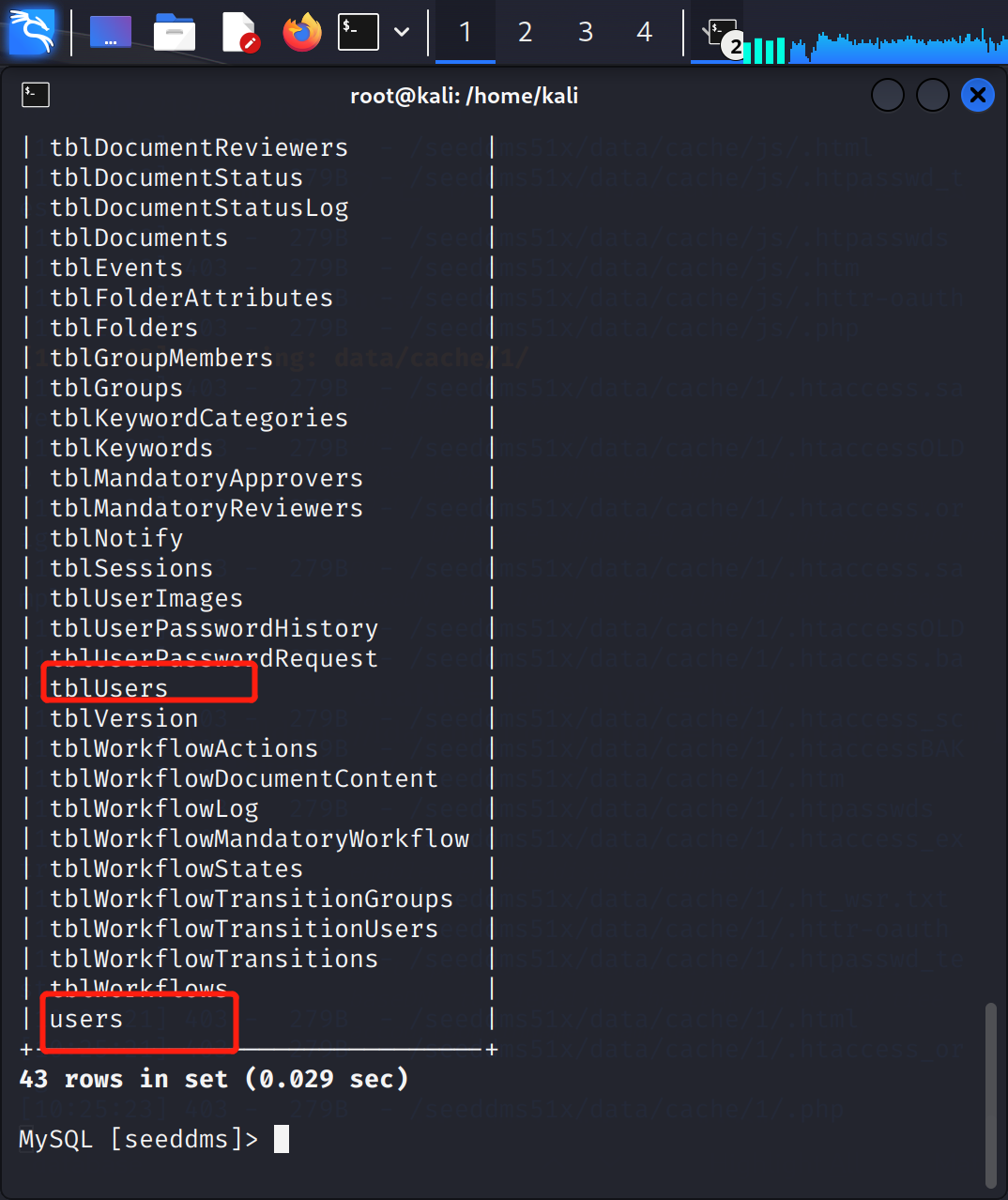
**又因为开放了3306端口，这个应该是数据库账号**

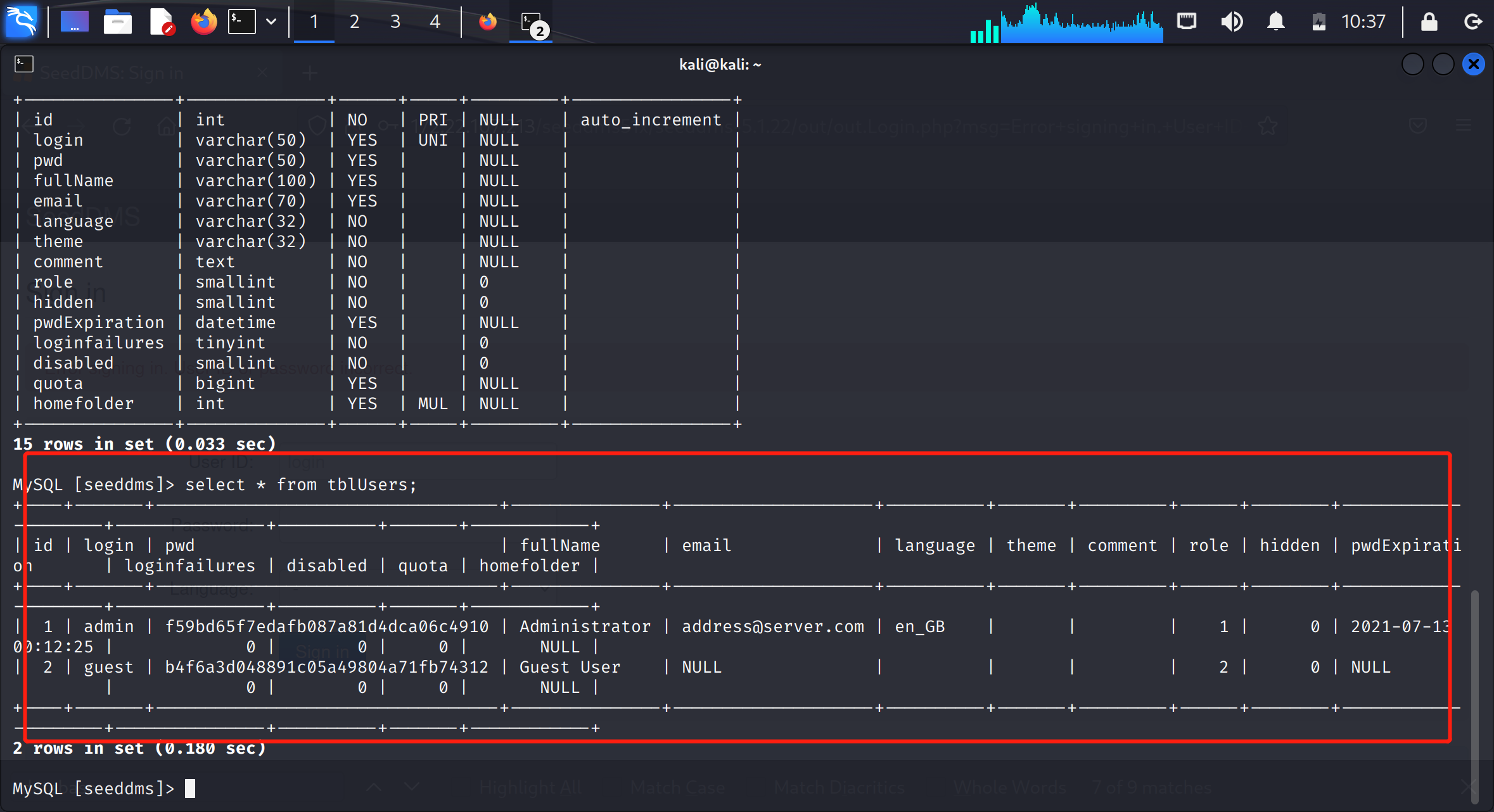
1. 数据库利用

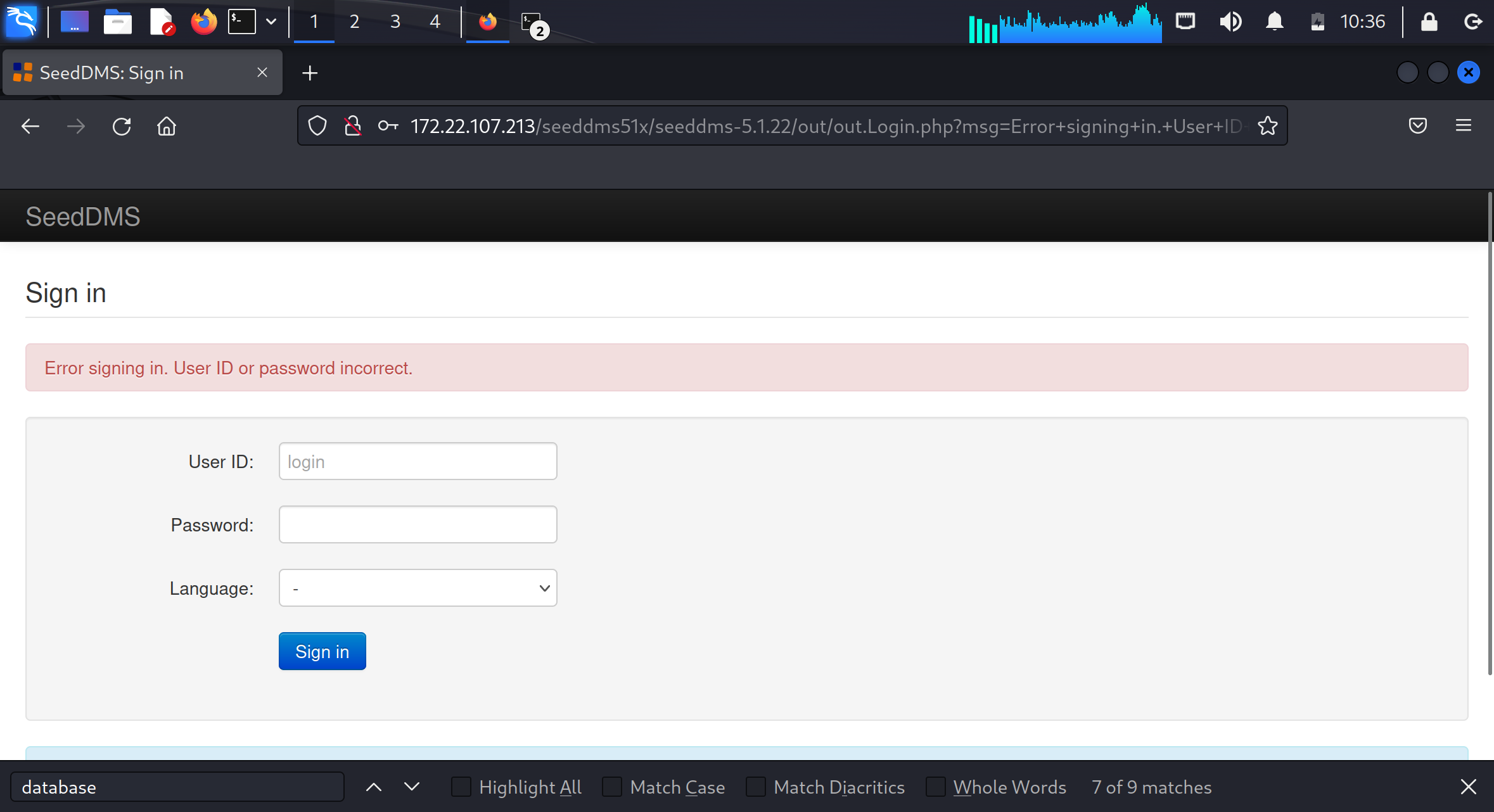
登录查看数据库：



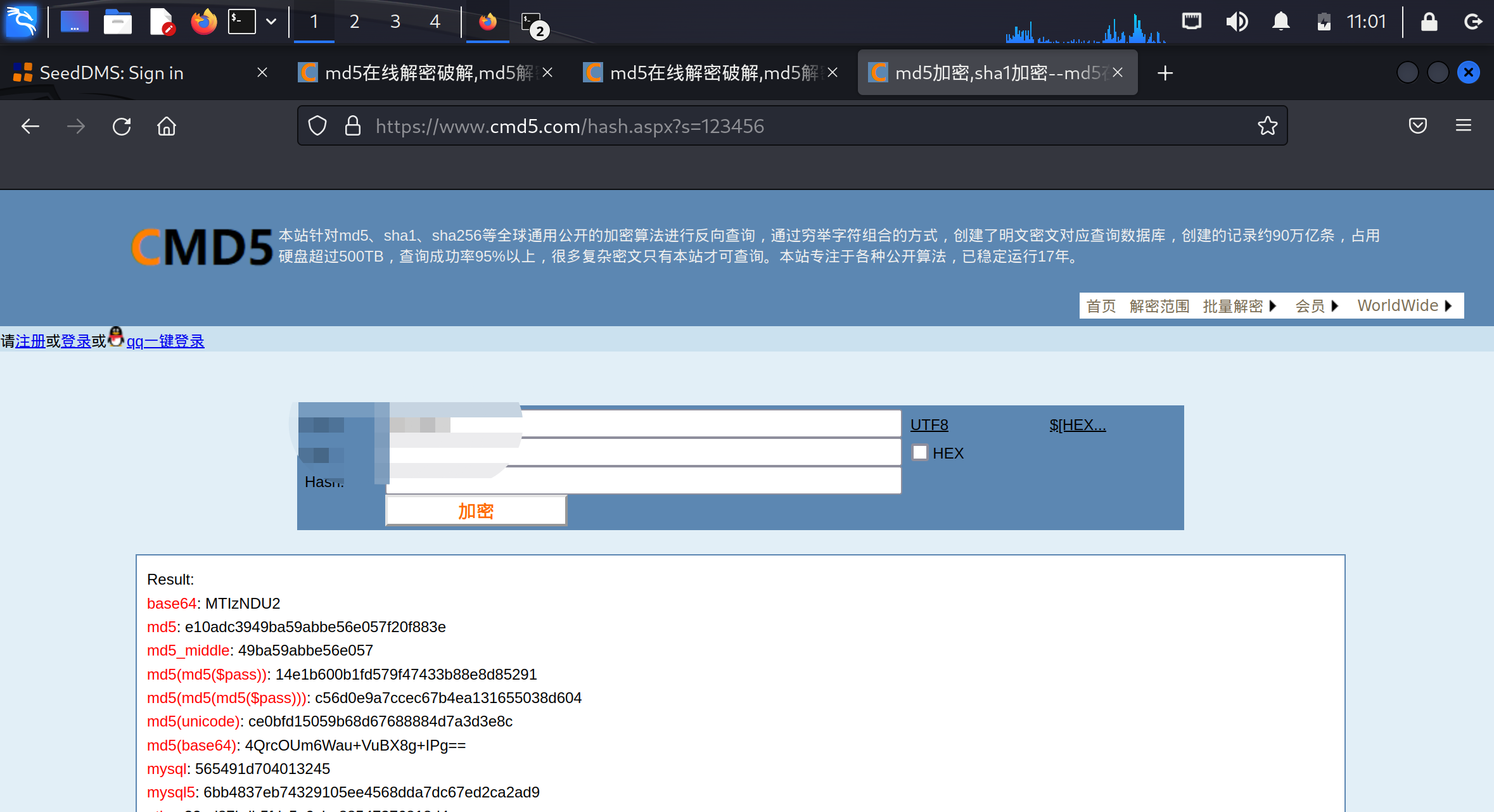
查看表：



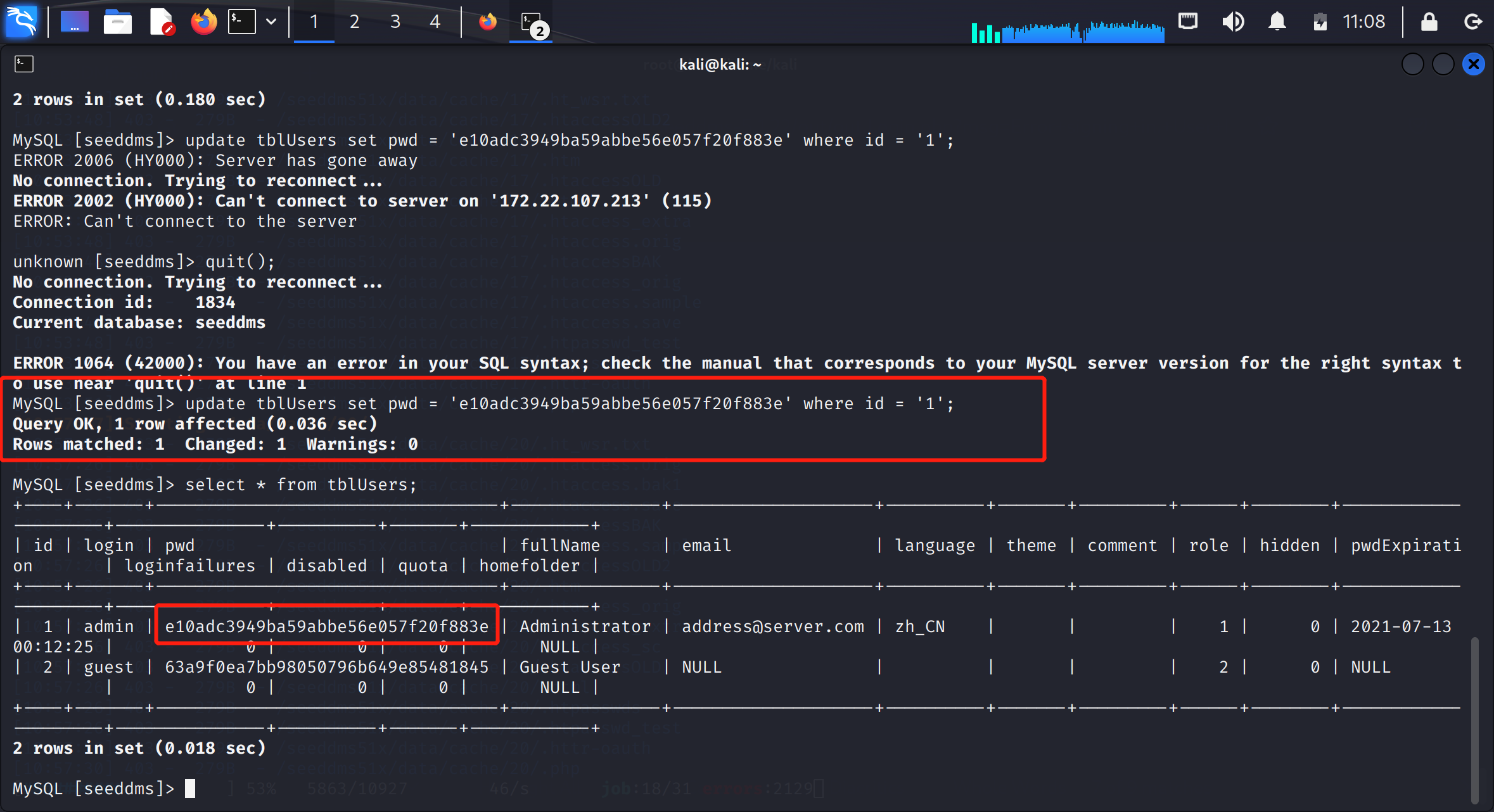




没登成功，可能加密了



直接换密码



进入后台：



1. 漏洞发现和利用



（4）权限提升

**三、实验过程原始数据记录**

1. **实验总结**