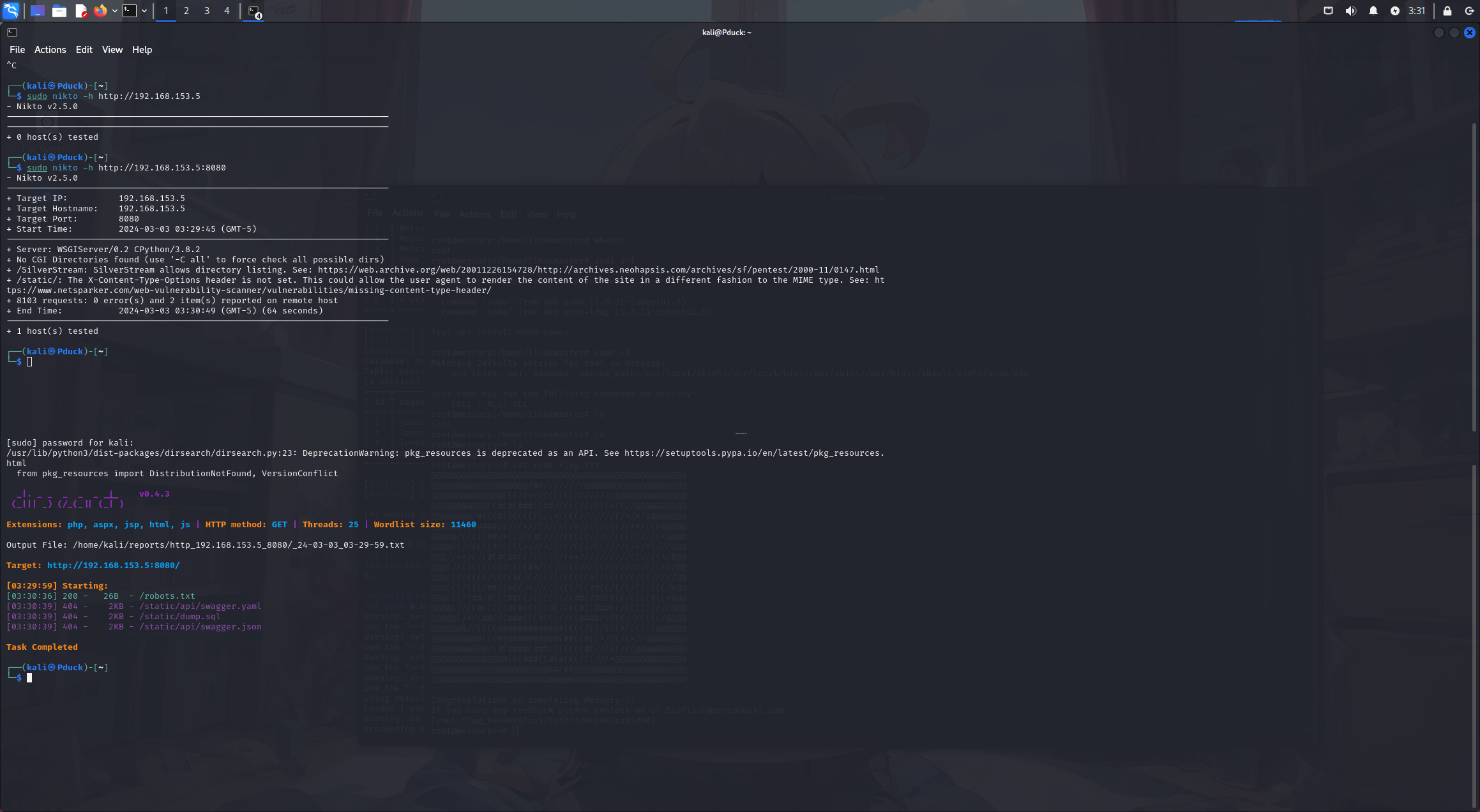
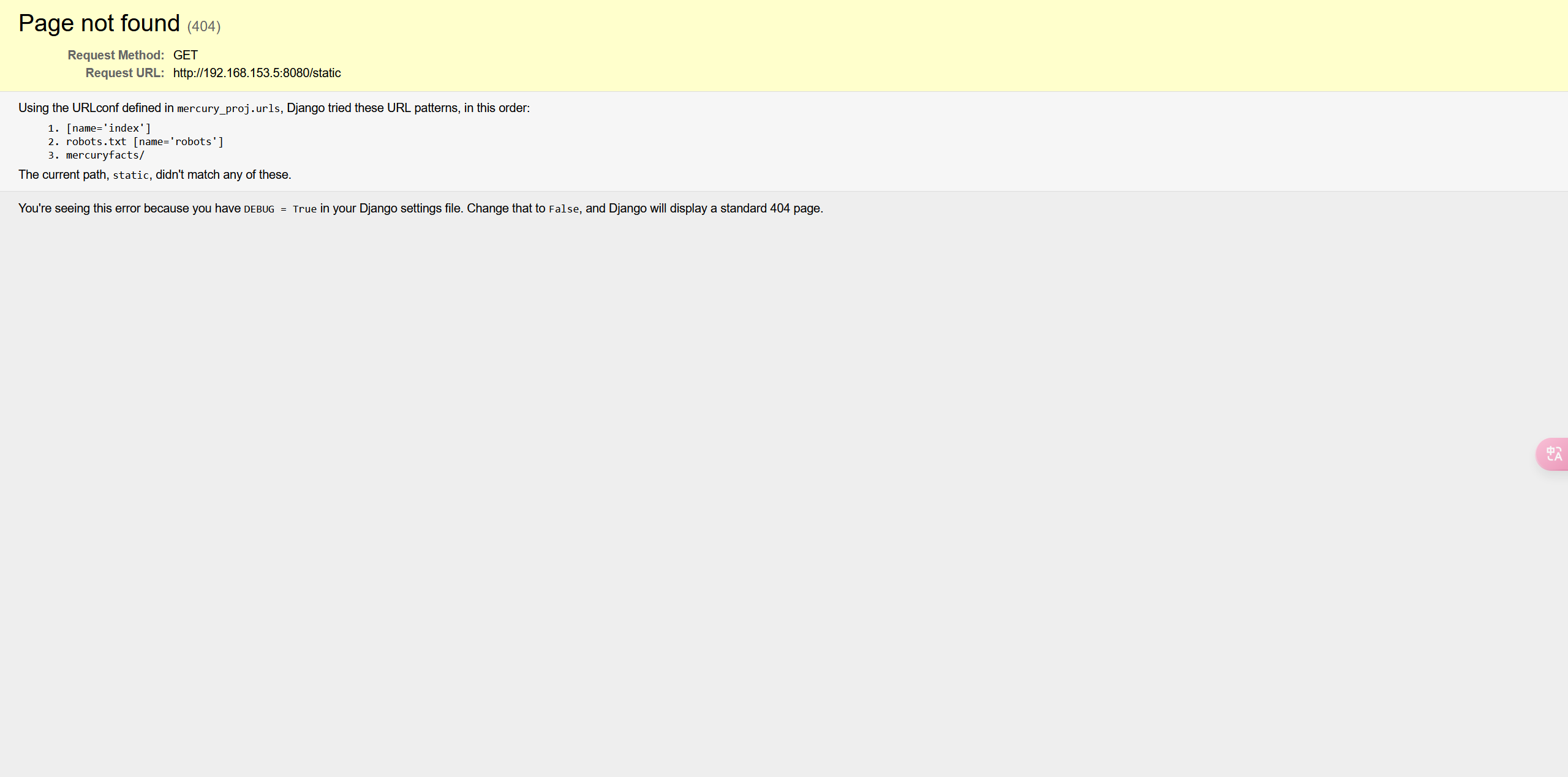
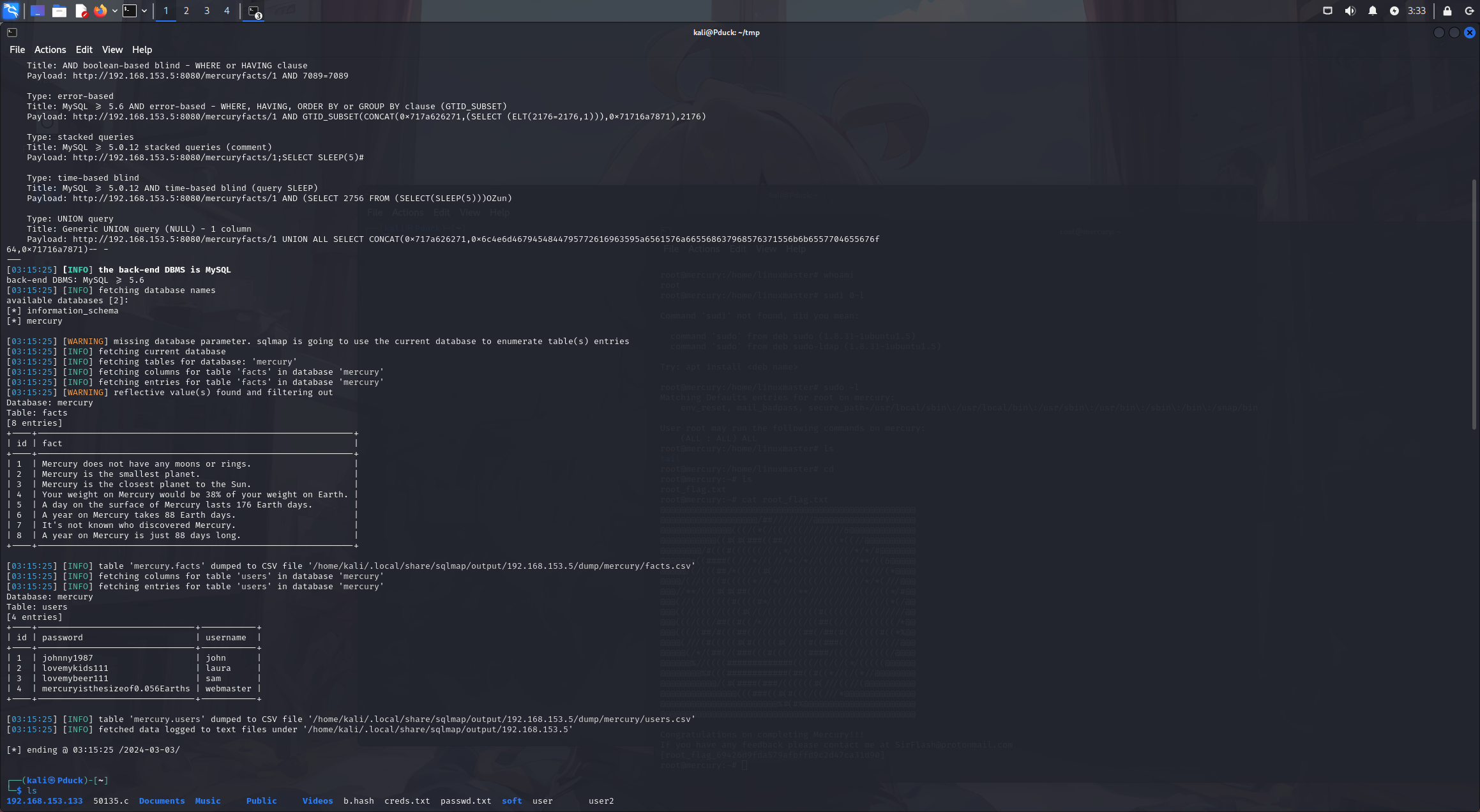
# Mercury

## 信息收集

* Nmap扫描目标开放22和8080端口
* 详细扫描和漏洞扫描并无发现
* robots.txt有不允许的目录

## Web渗透

* Gobuster目录爆破没有扫描到任何信息
* Static路径，发现错误，但是暴露出了另一个目录
* 
* <http://192.168.153.5:8080/mercuryfacts/1/路径发现1-8>都可反馈内容，存在sql注入，sqlmap注出用户密码
* 
* Webmaster可登录成功，在目录下有notes.txt文件存在linuxmaster的密码，base64解码，切换用户发现权限
* Sudo -l 发现有文件执行权限，执行tail 一个文件
* 尝试把tail 软链接到vi
* Ln -s /bin/vi tail 并且把当前环境路径导入环境变量
* Export PATH=.:$PATH
* sudo --preserve-env=PATH /usr/bin/check\_syslog.sh
* !bash提权成功
* 