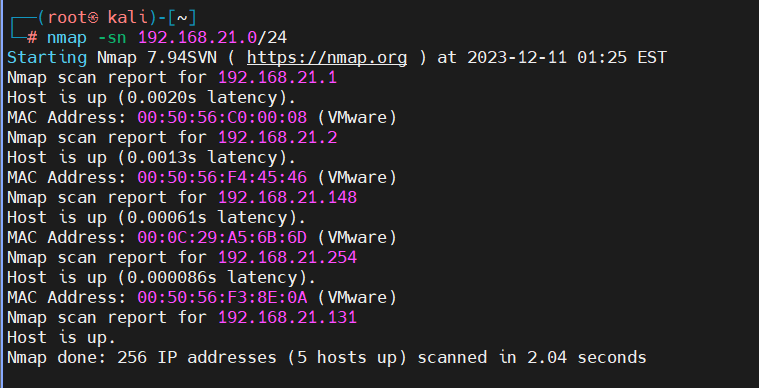
hacksudo FOG

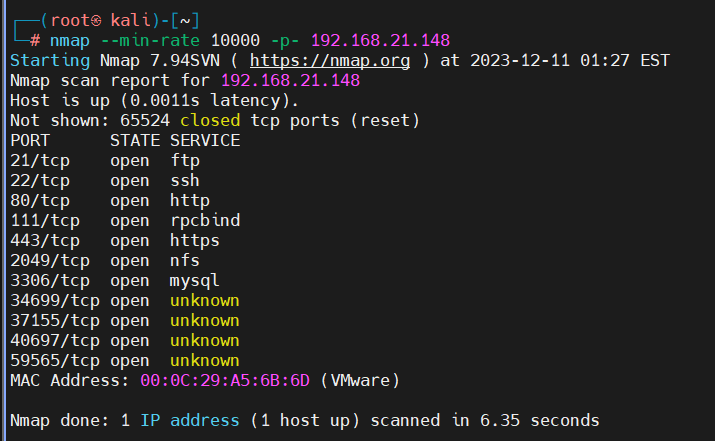
下载地址：<https://www.vulnhub.com/entry/hacksudo-fog,697/>

主机发现

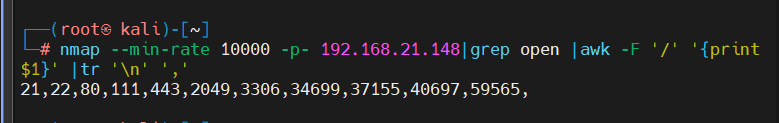


目标148

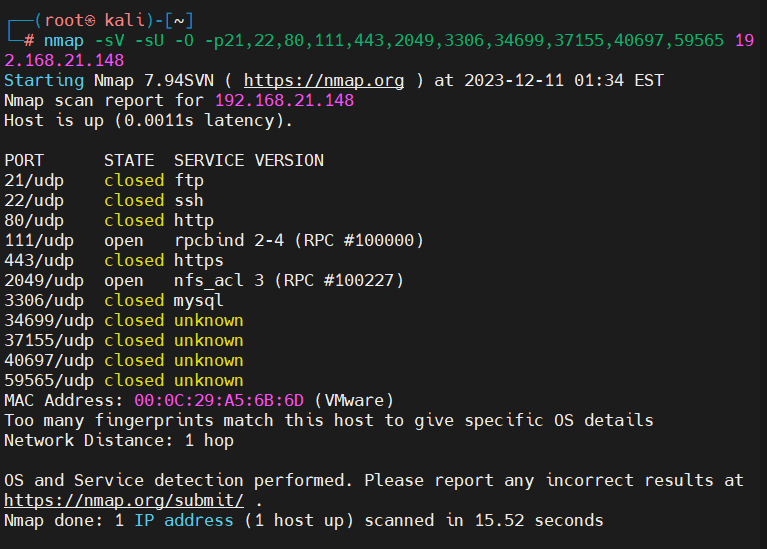
端口扫描

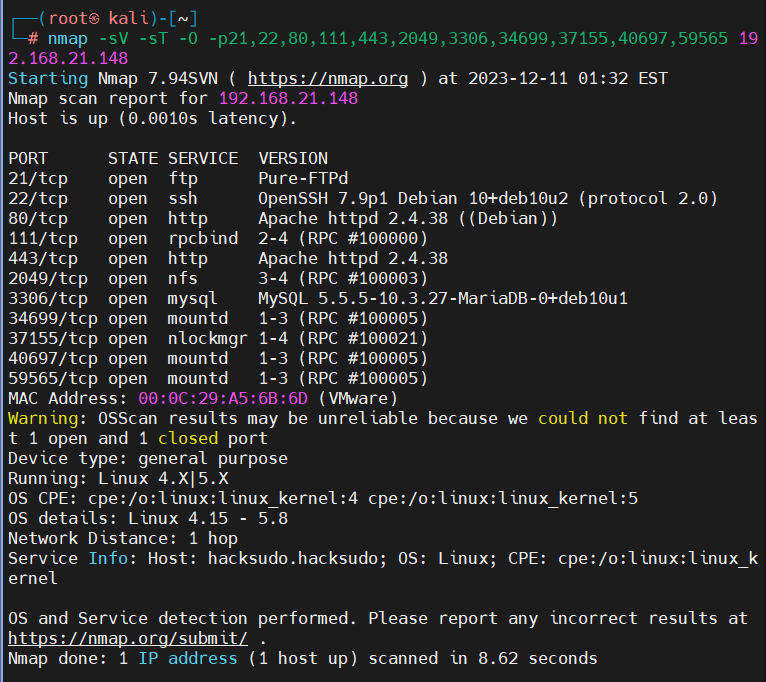


IP过多整理一下

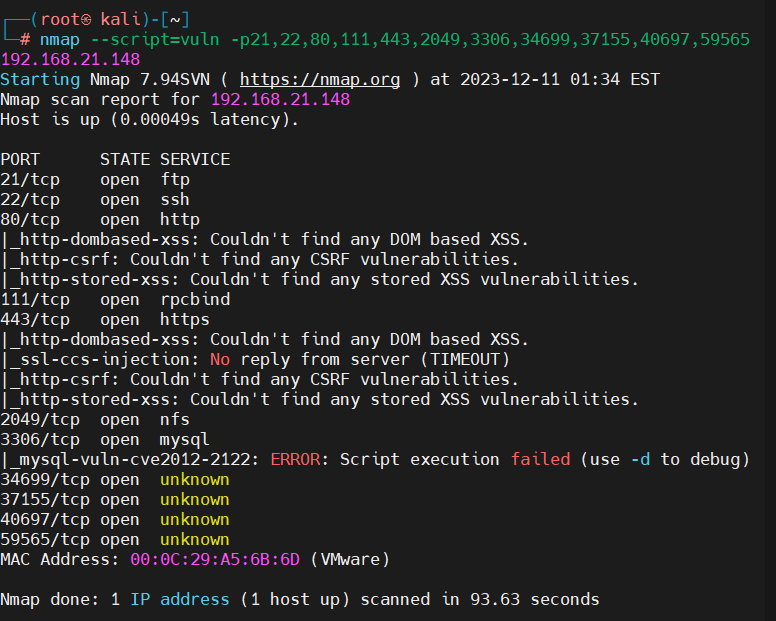


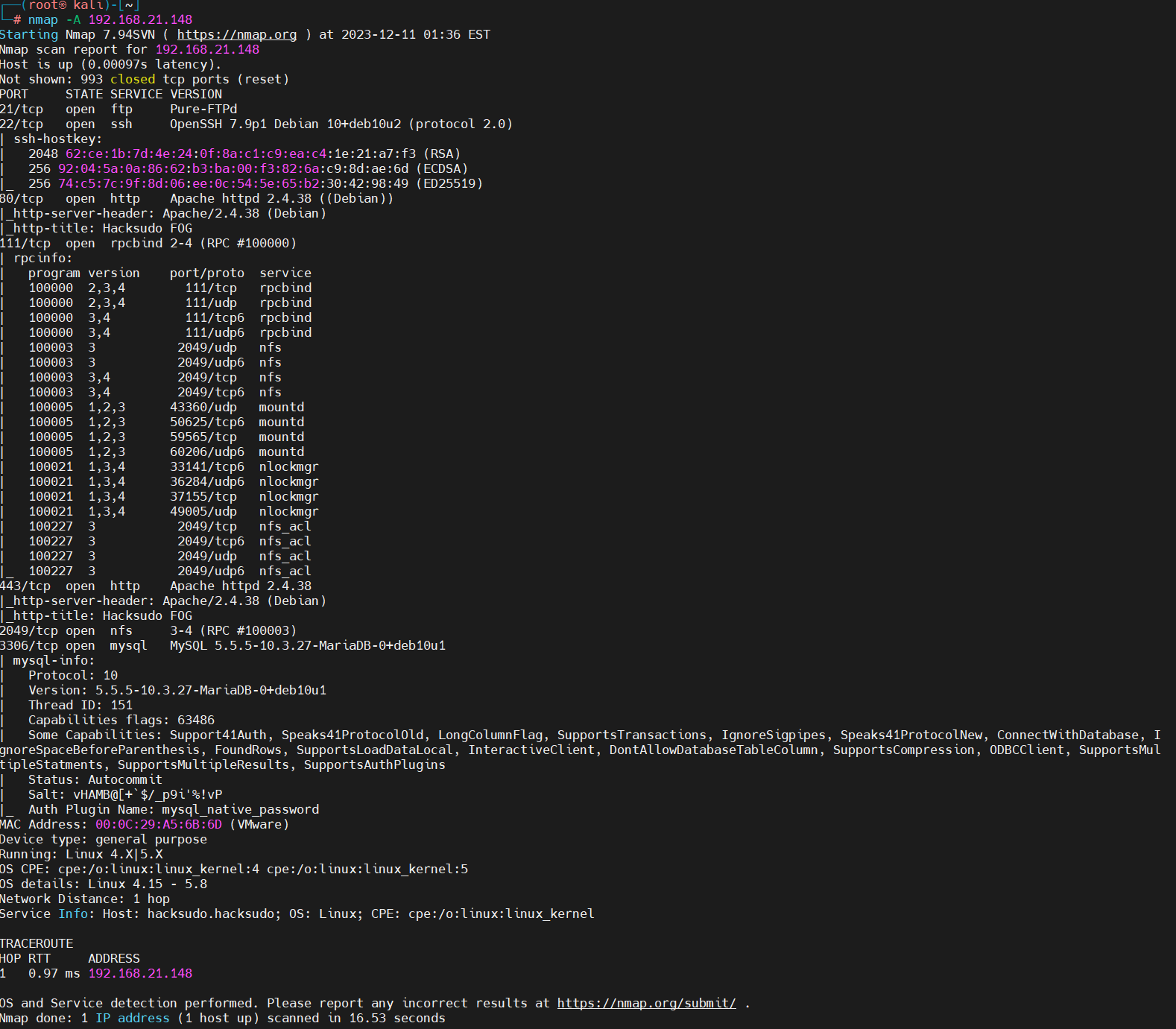
扫描服务





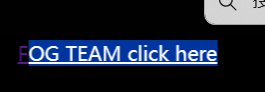
漏洞扫描

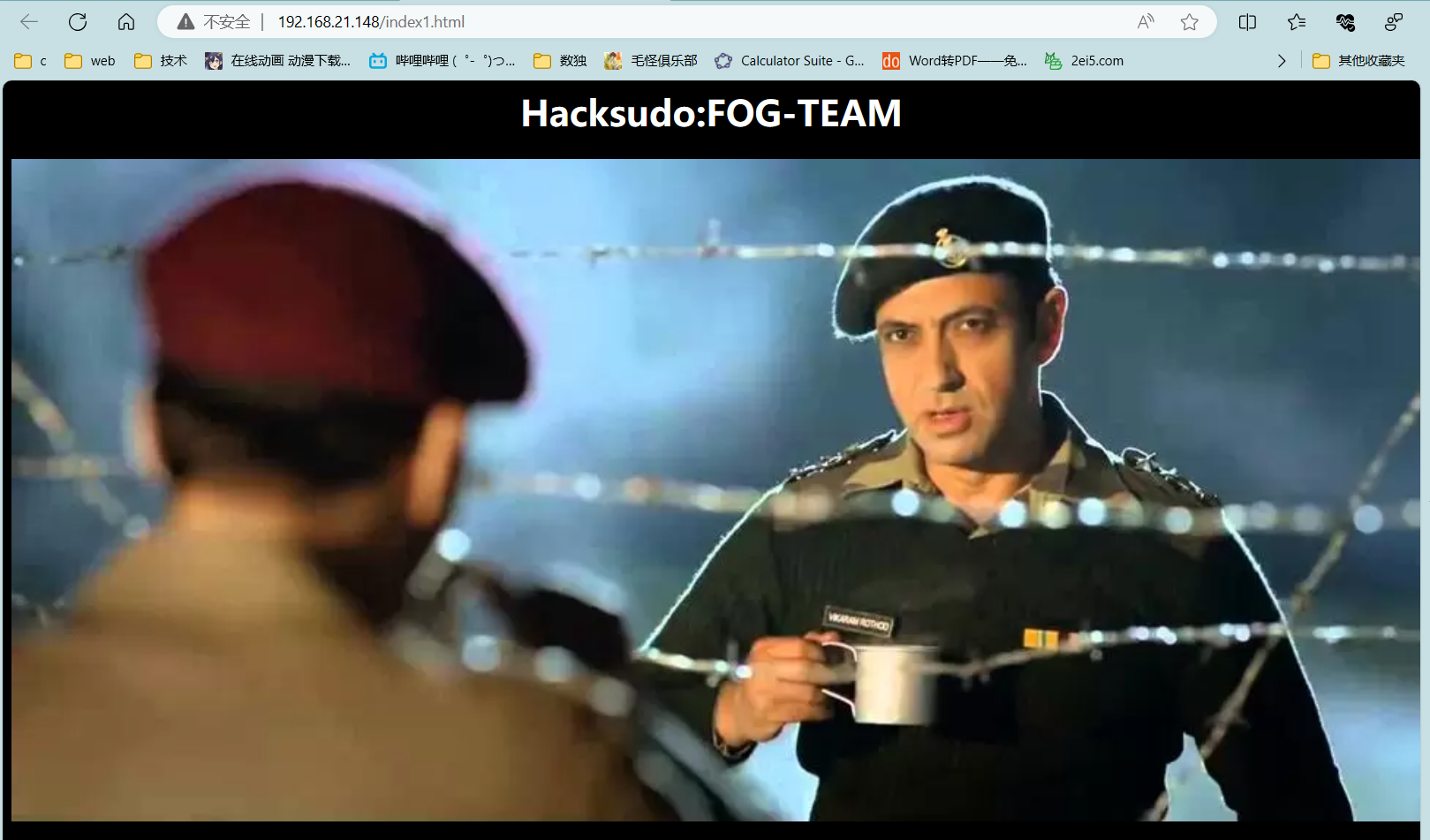




去80看看

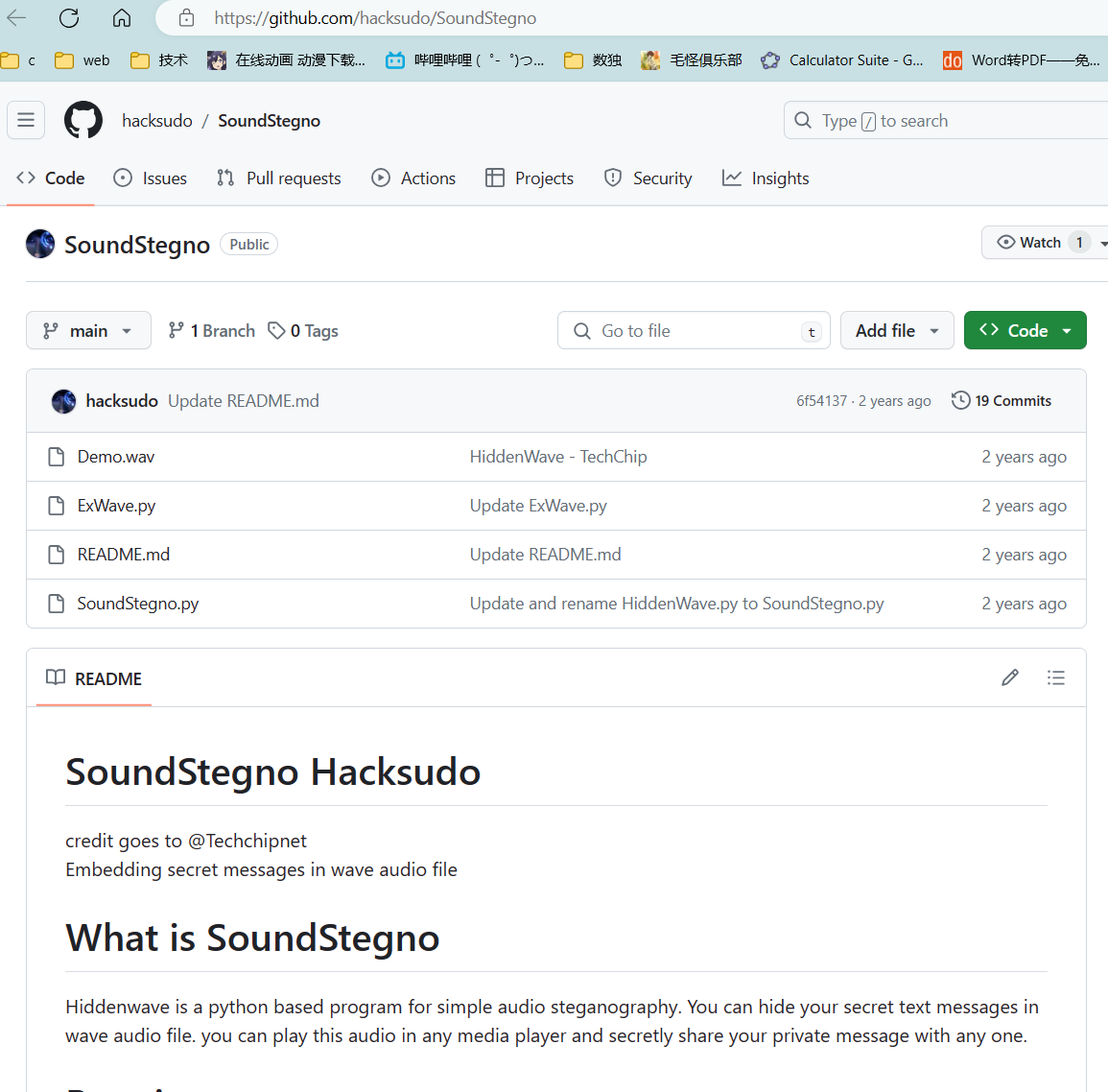


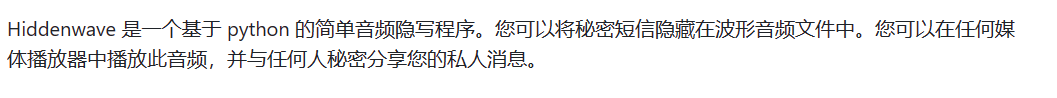


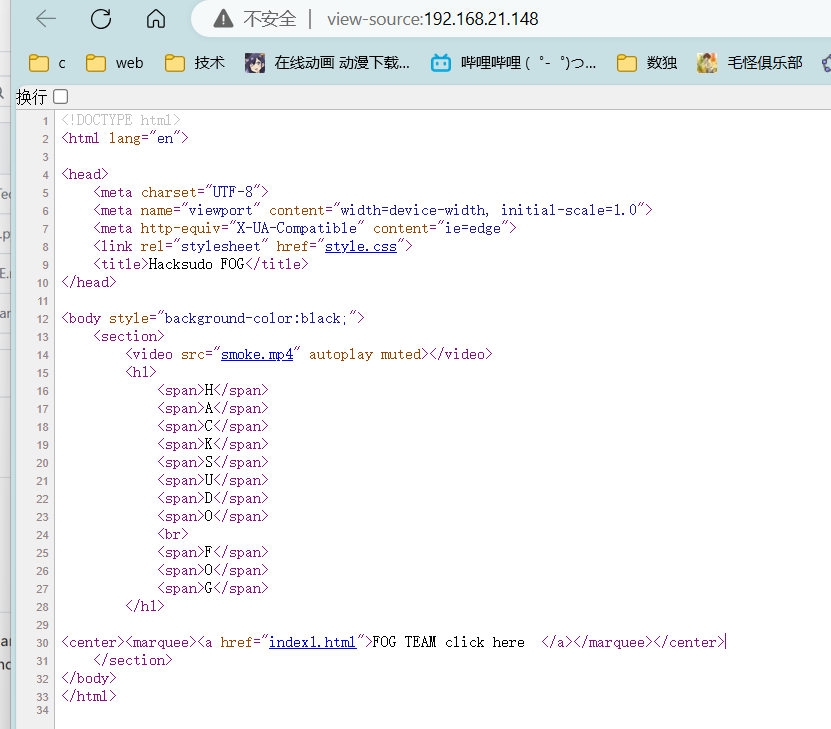




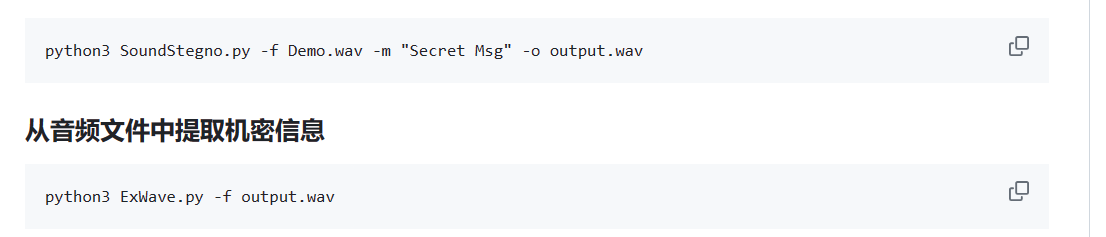
经典凯撒，后面还是一个github



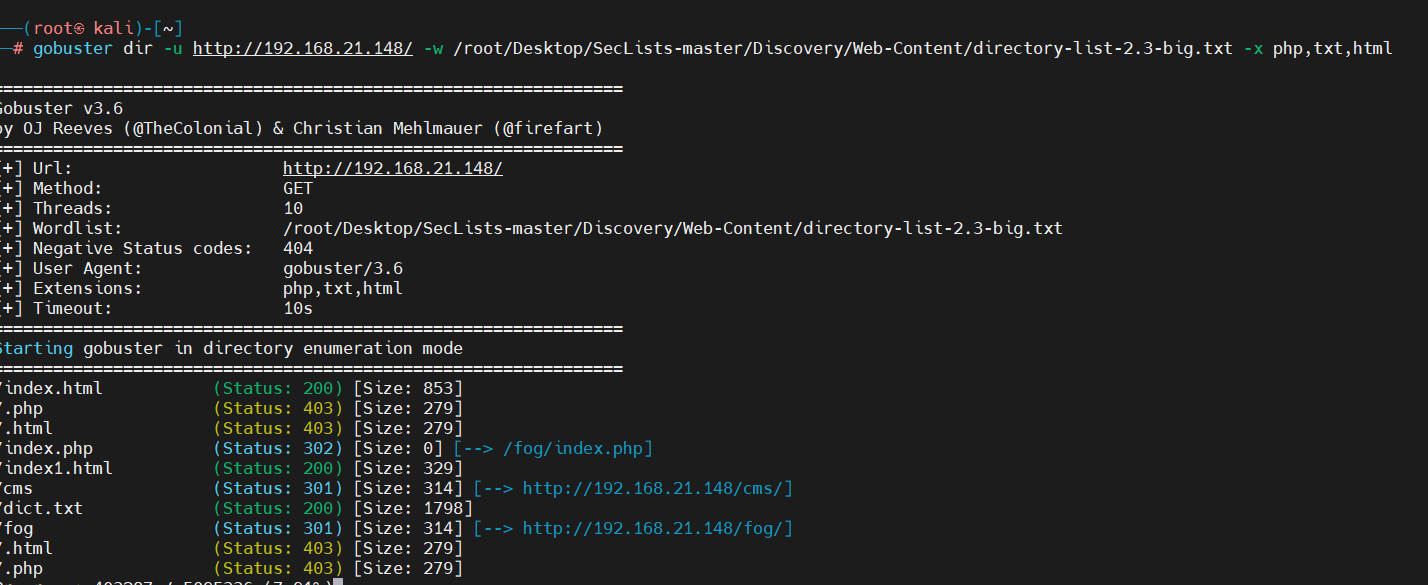




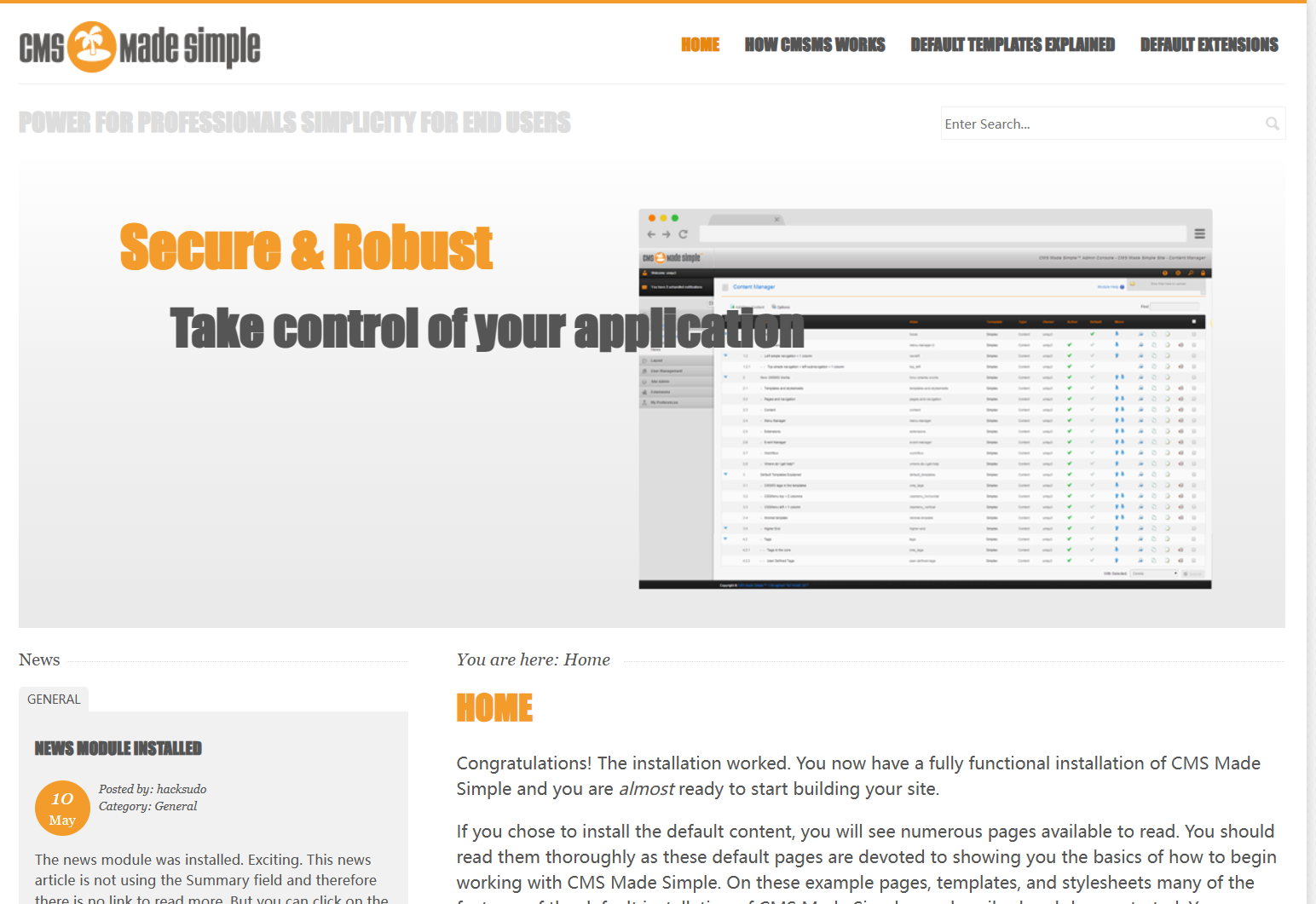
好好好，mp4

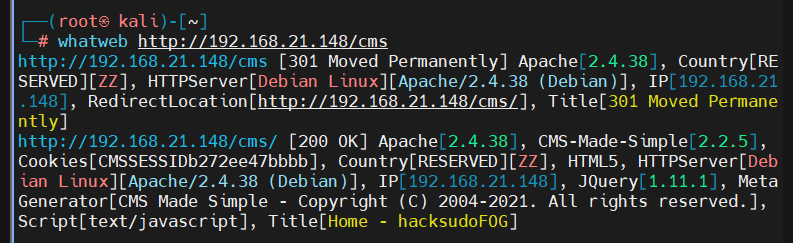


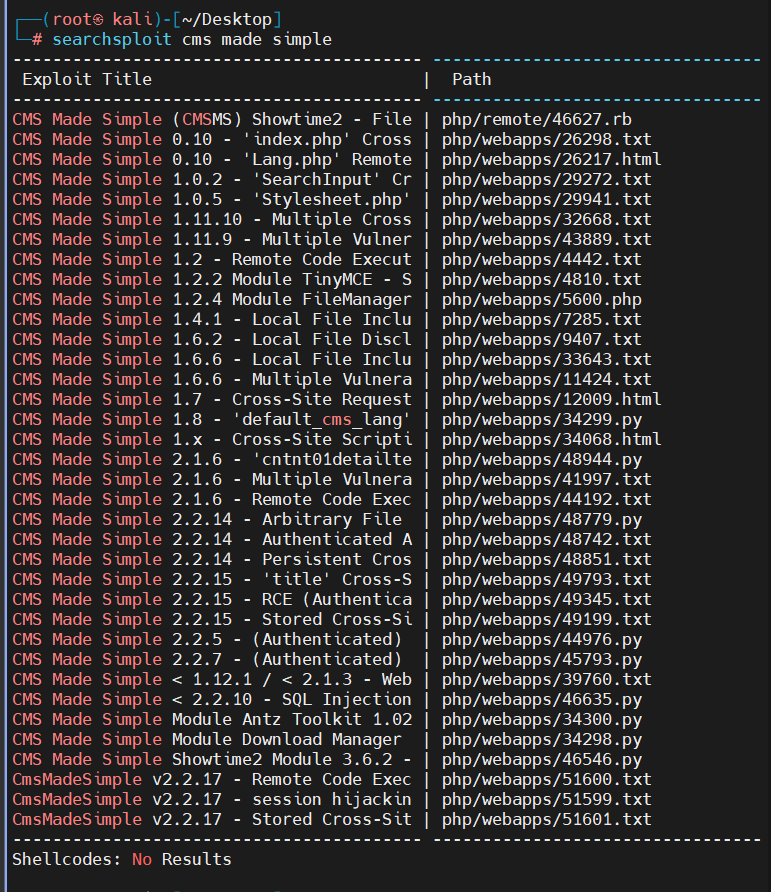
接下来目录爆破

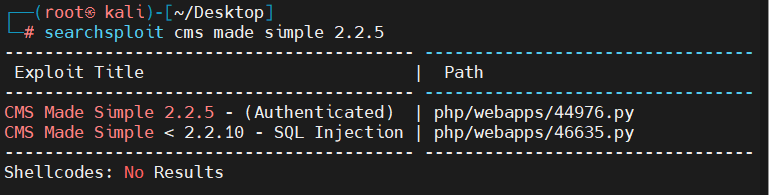


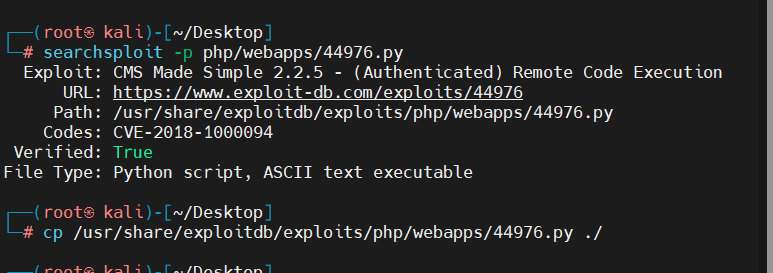
一个一个去看

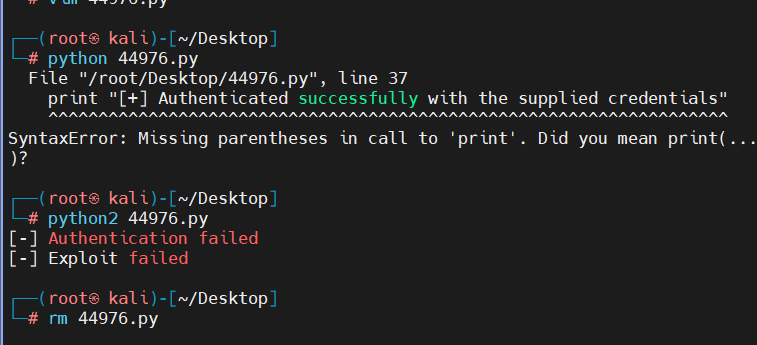


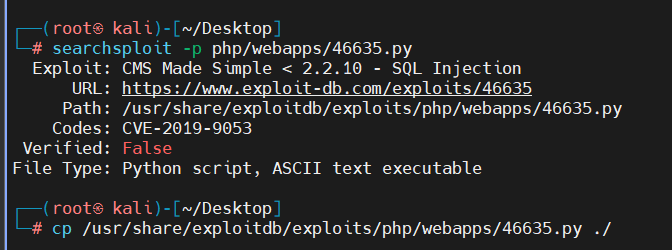


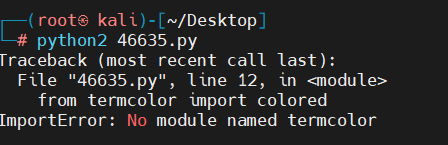




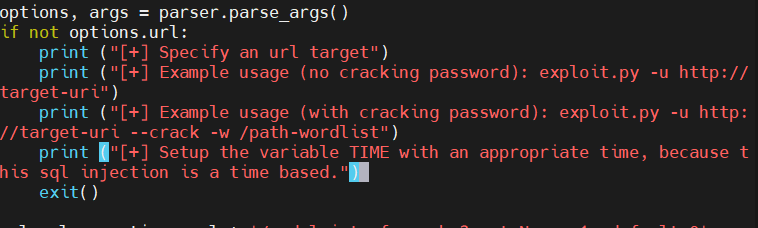


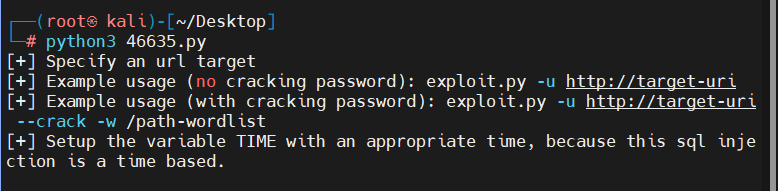
失败了换一个

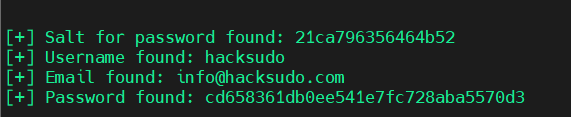




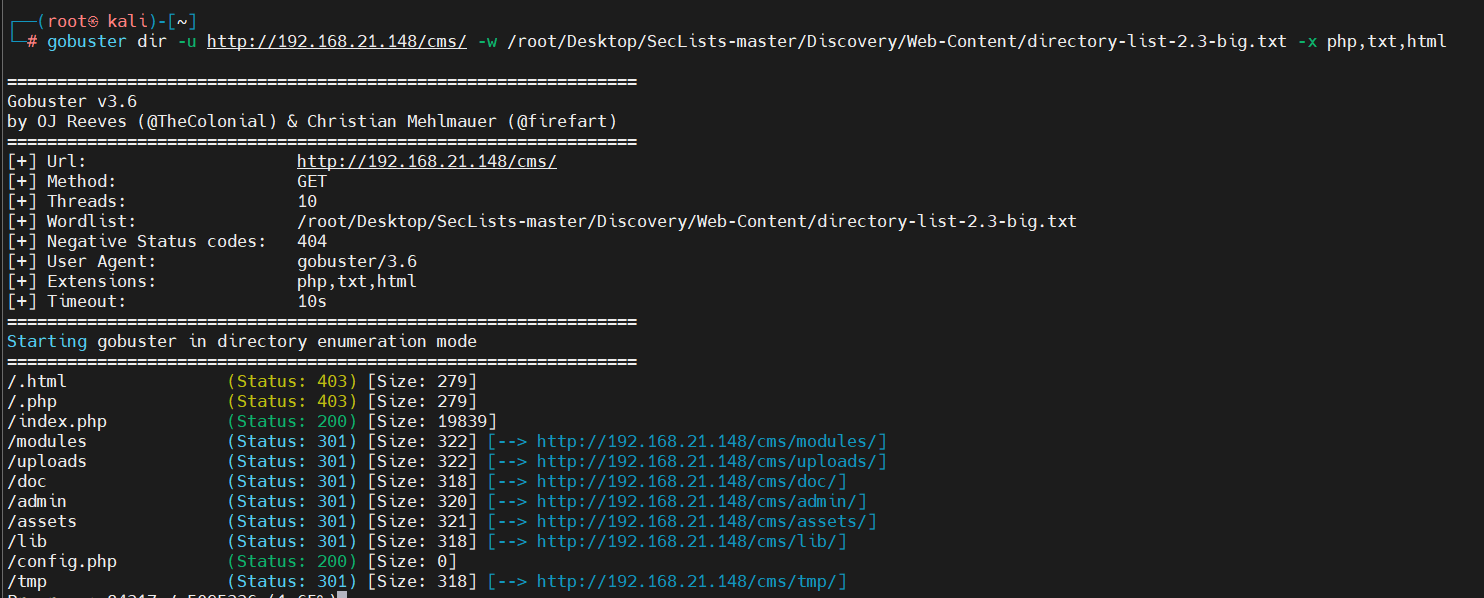
少模块，有点麻烦，直接改成python3

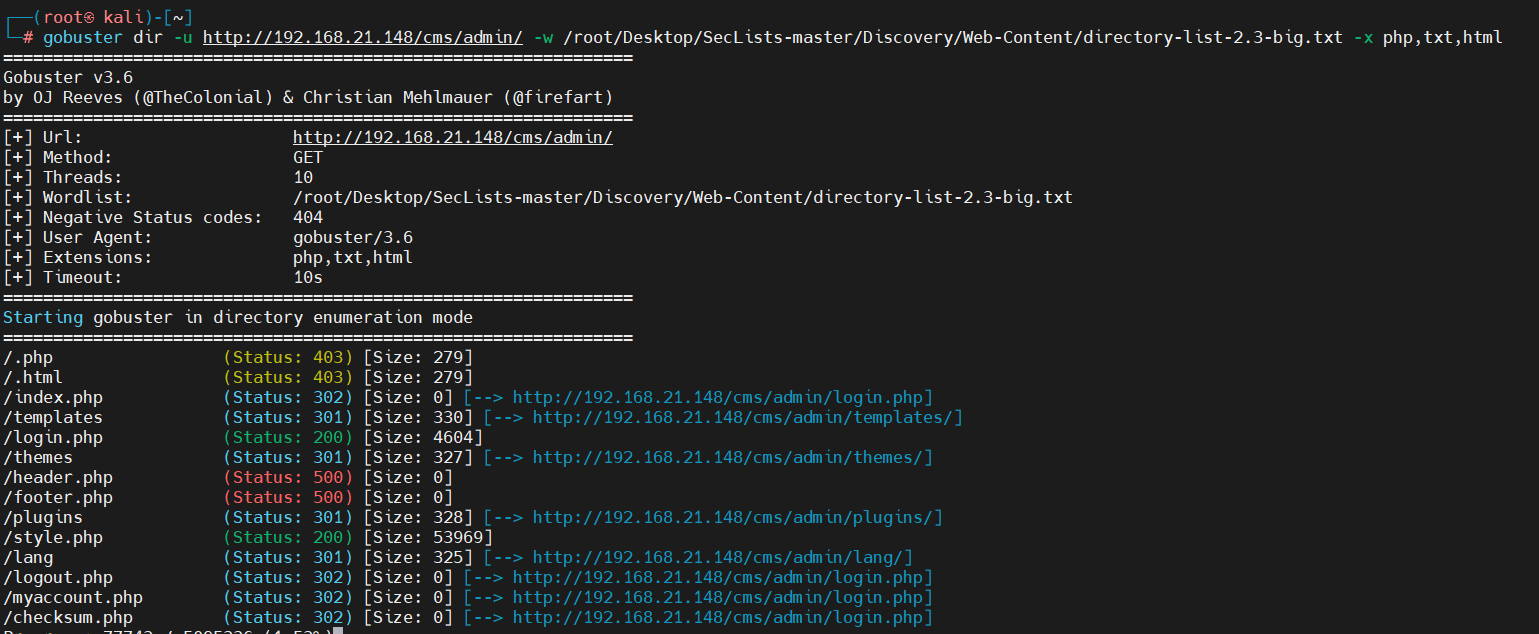






出来咯

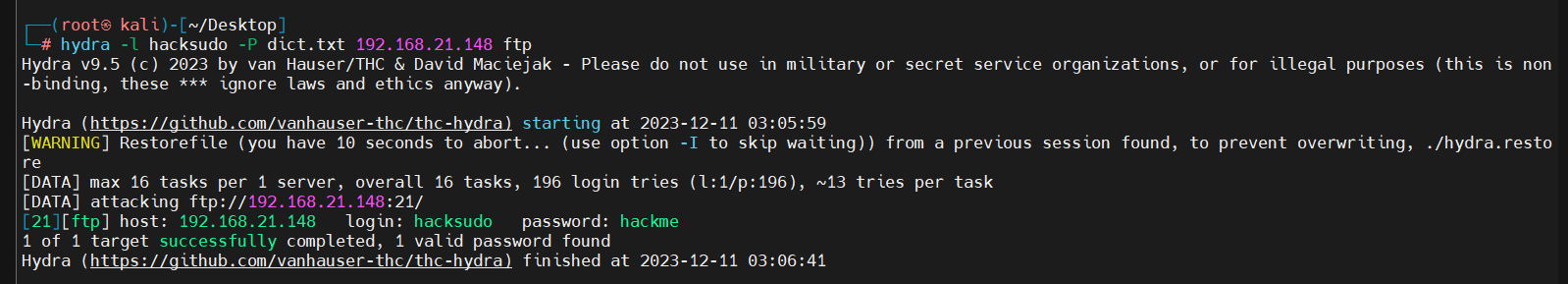




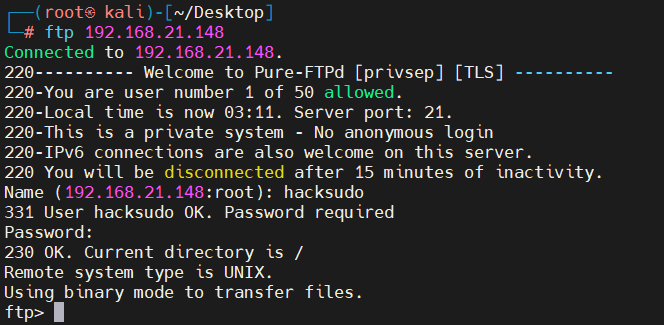
看到login

进不去，换一个突破口了

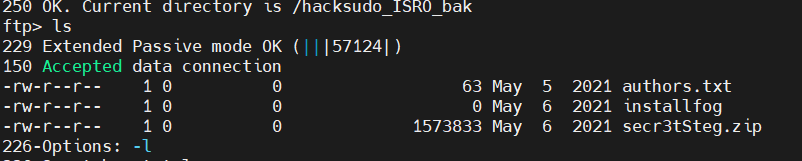
用其实是出来了

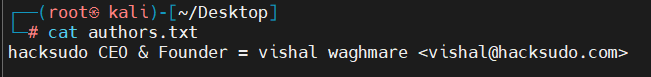


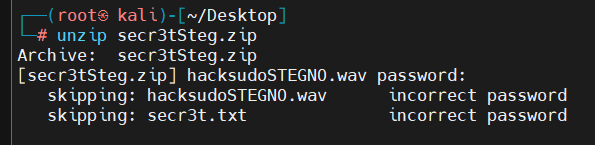
出来了



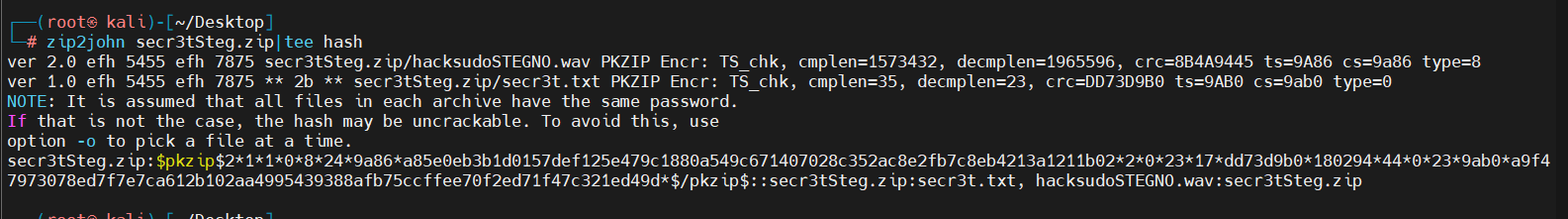


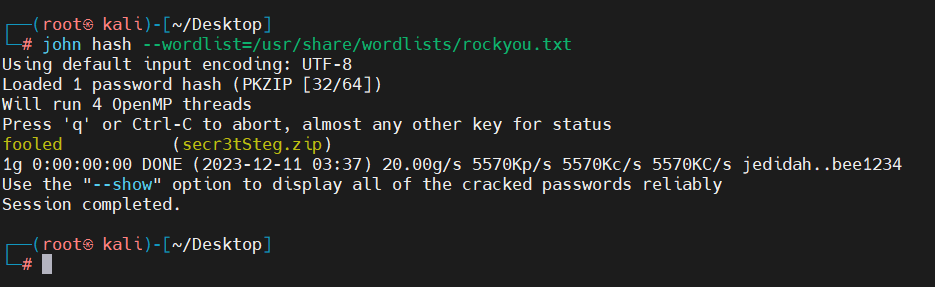






这个要密码



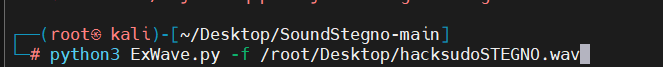


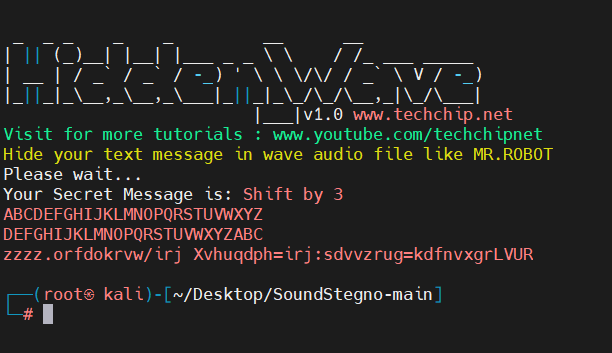
搞定



还有一个音频文件

正好有工具



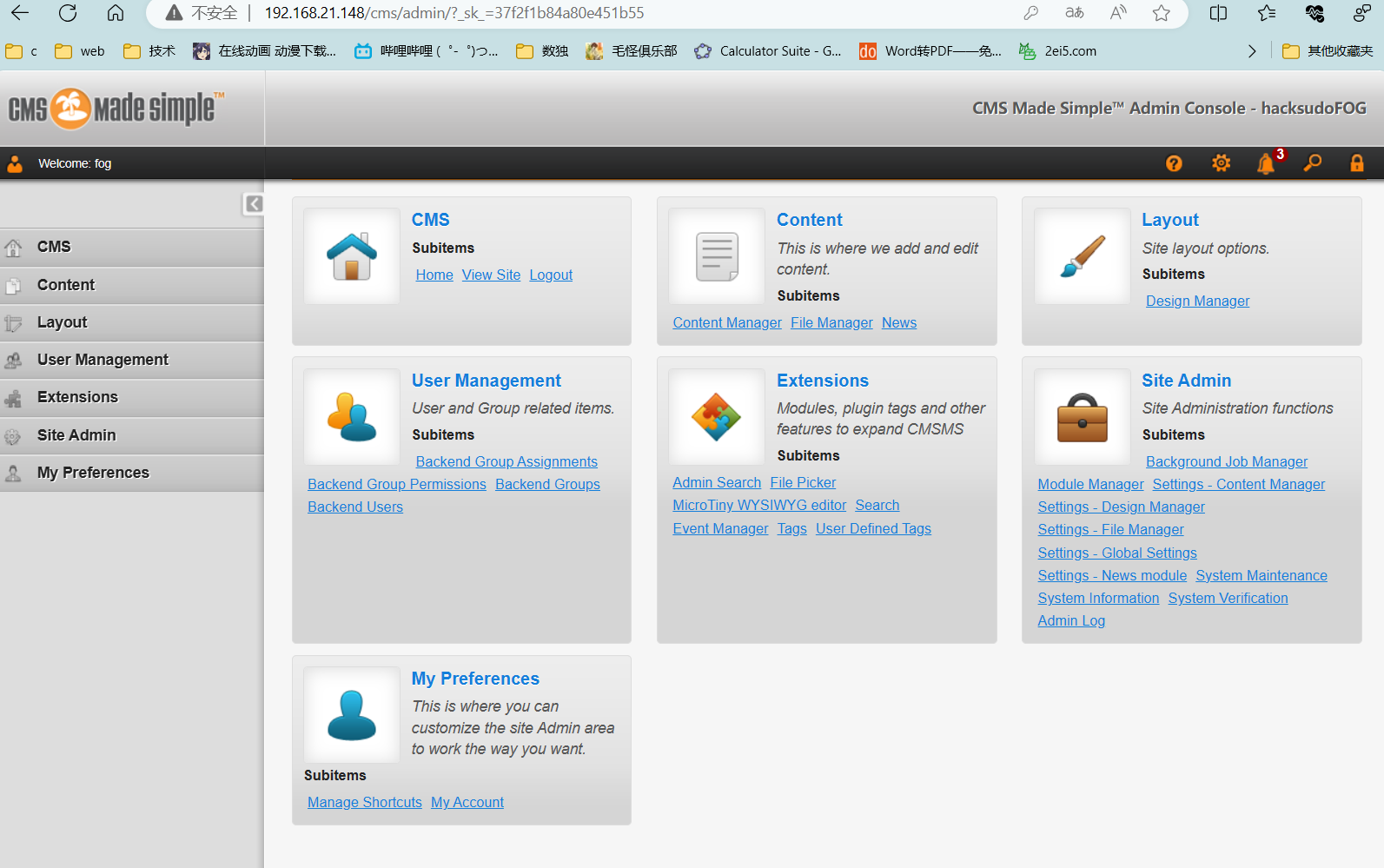


那就是凯撒加密位数应该是3

[在线凯撒密码加密解密 (lddgo.net)](https://www.lddgo.net/encrypt/caesar-cipher)

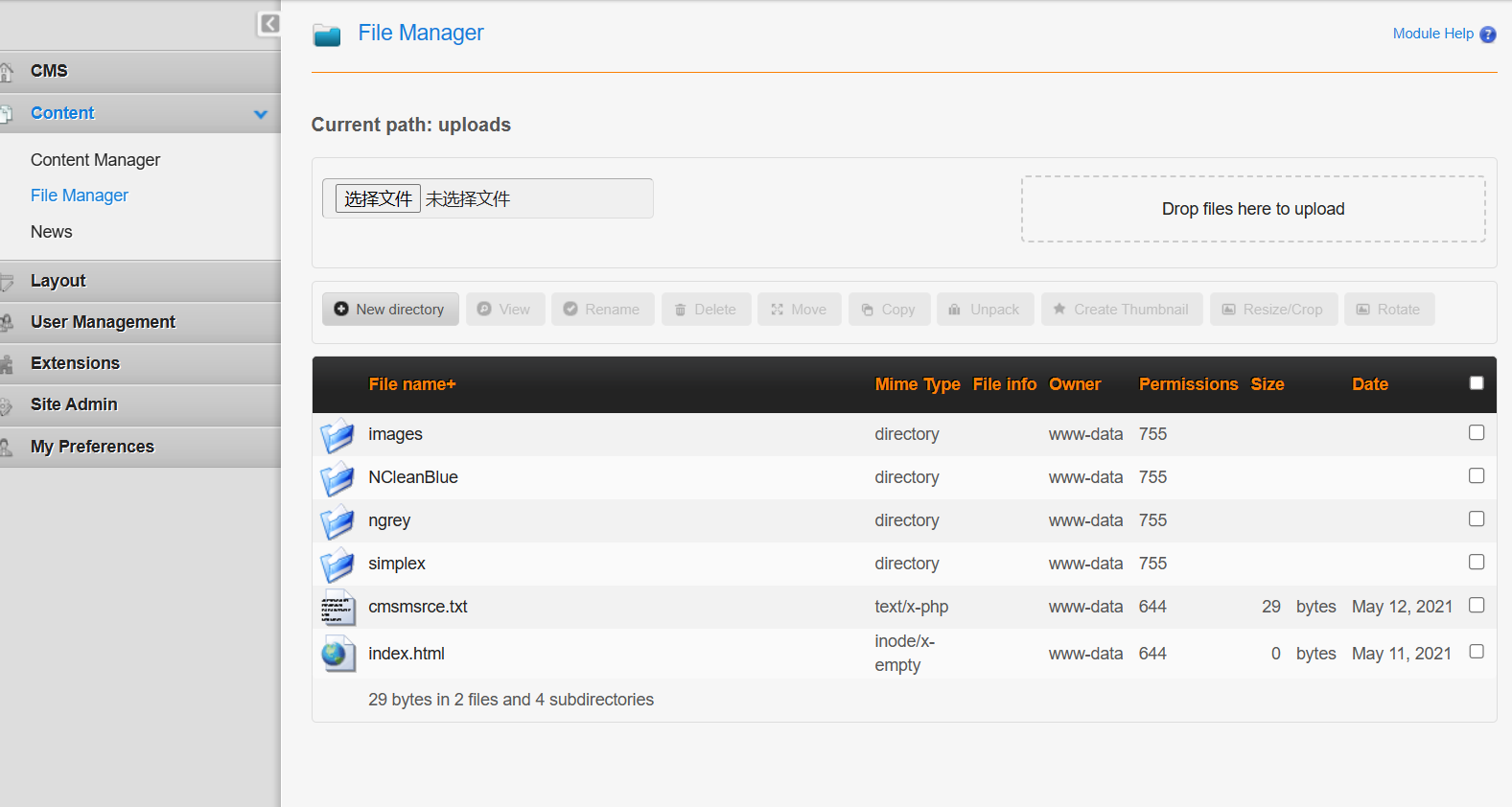


这个是账号密码去试一下web

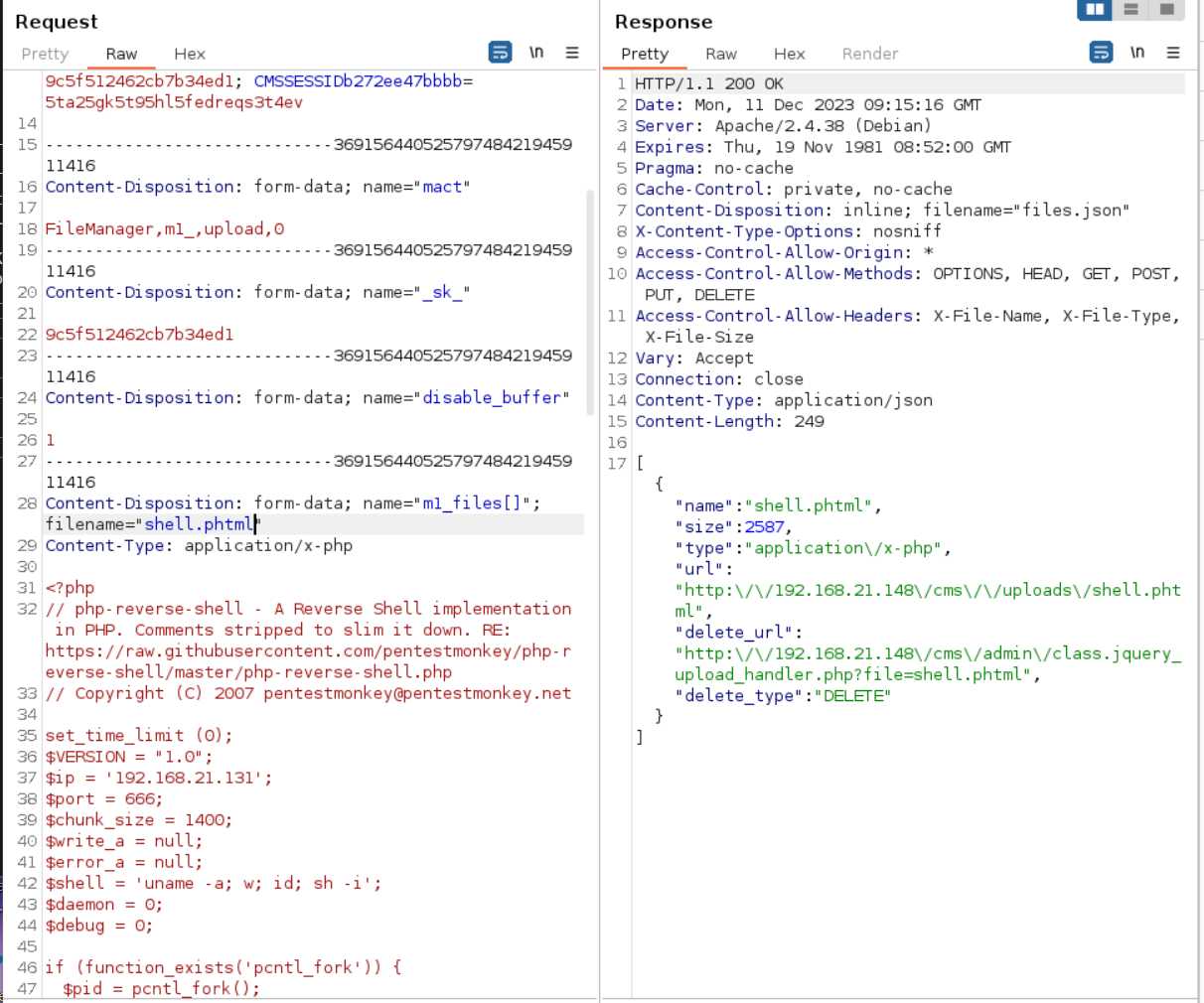


成功了

拿到后台那就是反弹shell

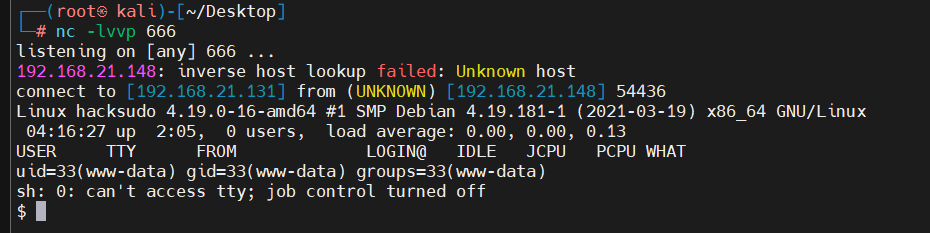


上传反弹shell

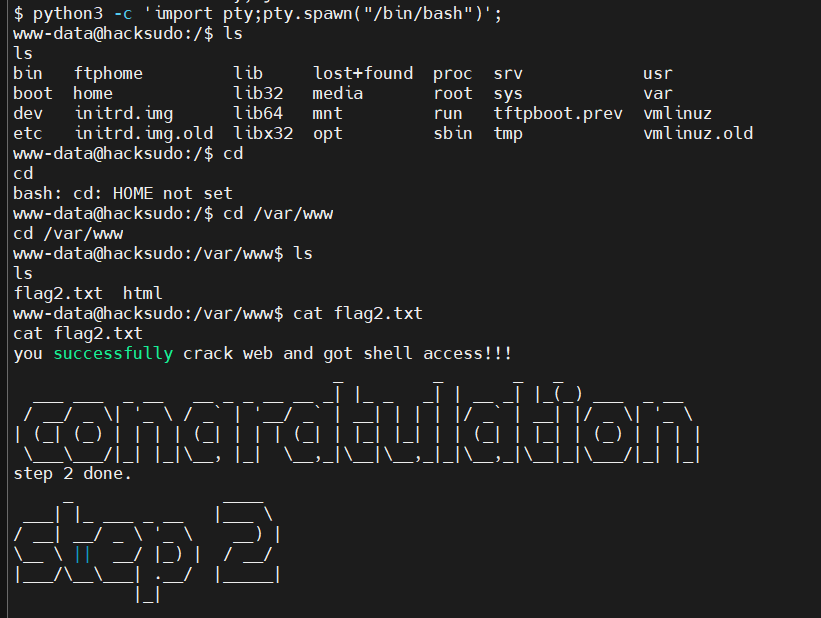


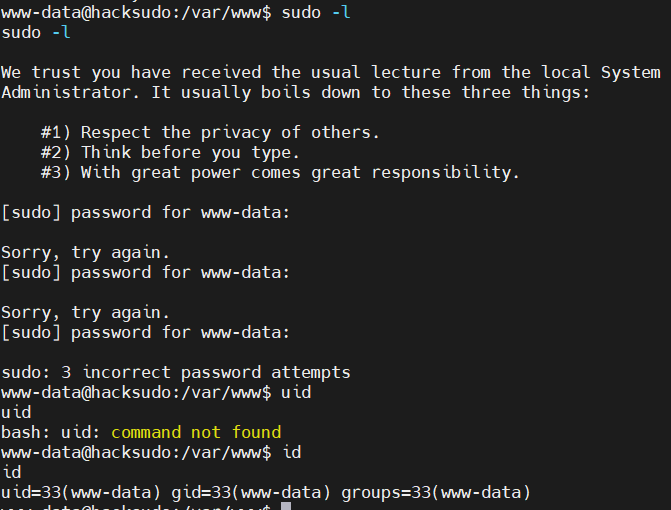
Phtml能上传

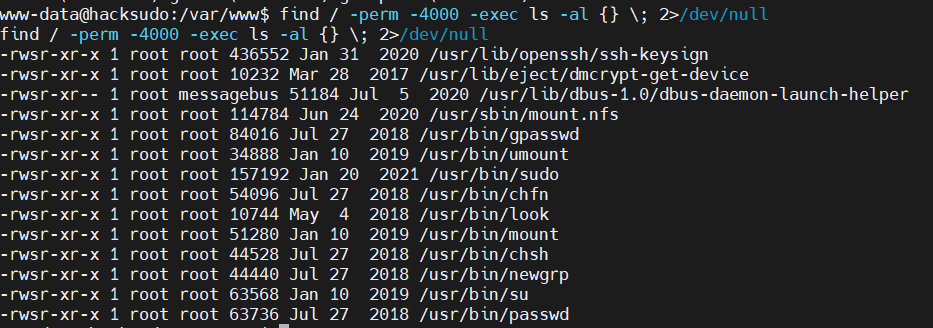
访问监听就可以

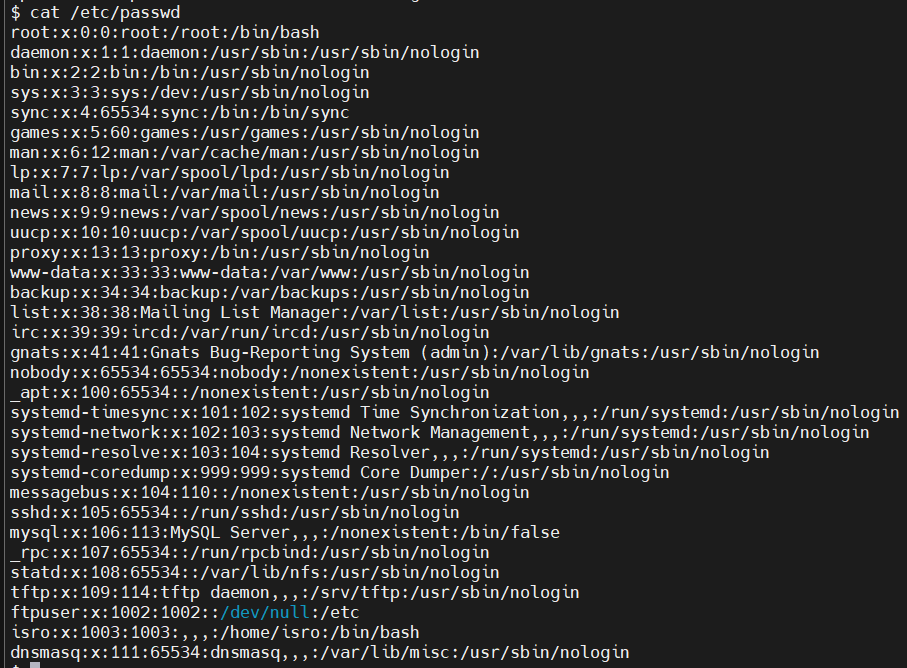


成功

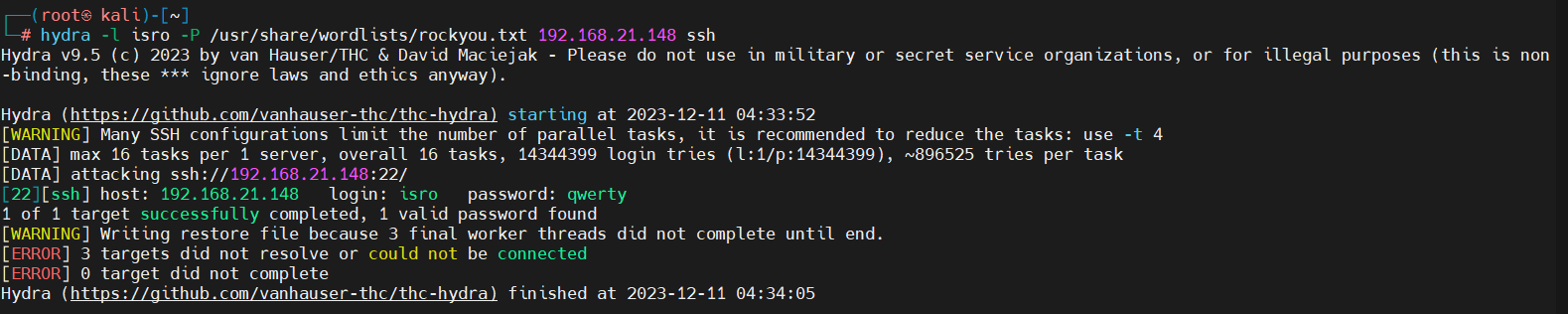


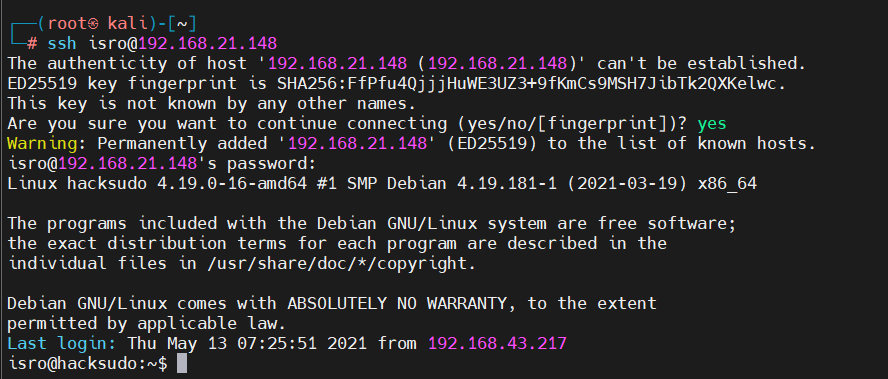




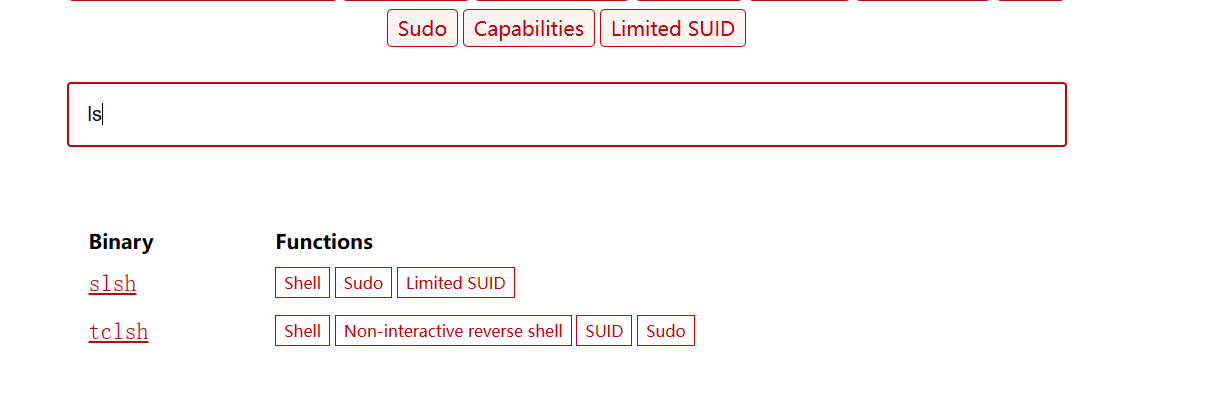
可以利用shadow文件，爆破密码，但是用不了

爆破一下别的账号的密码

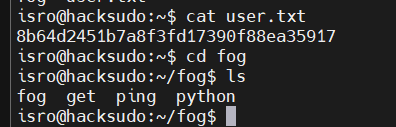




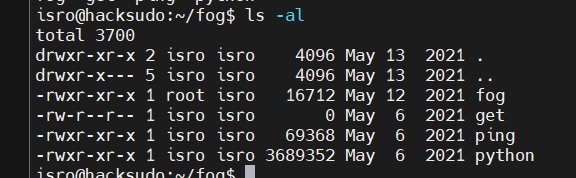




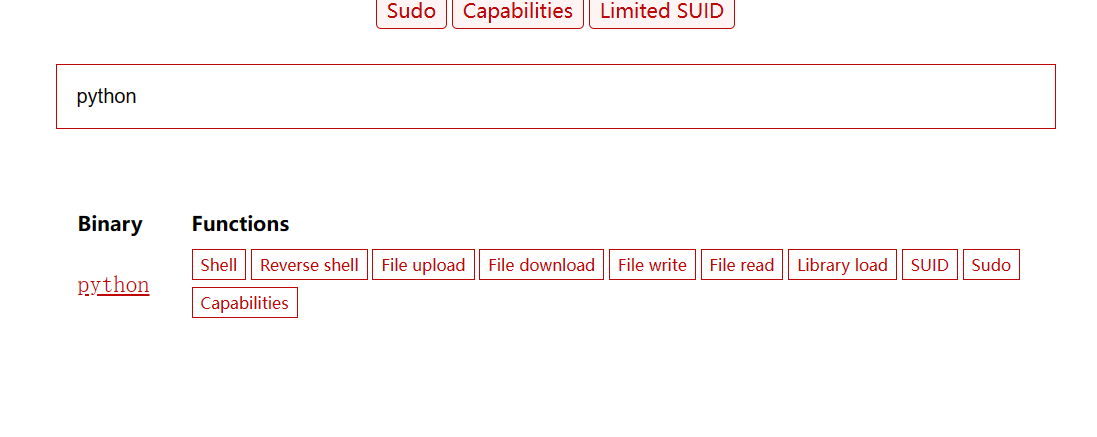
Ls能用但是ls提不了权



翻文件发现好东西



那就是python或者是ping了



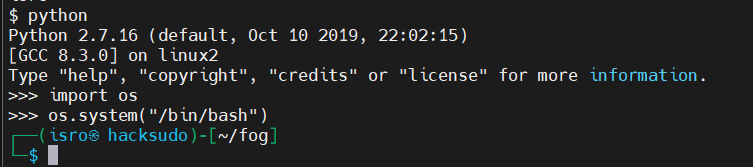
查到了python就不用说了吧

直接找payload



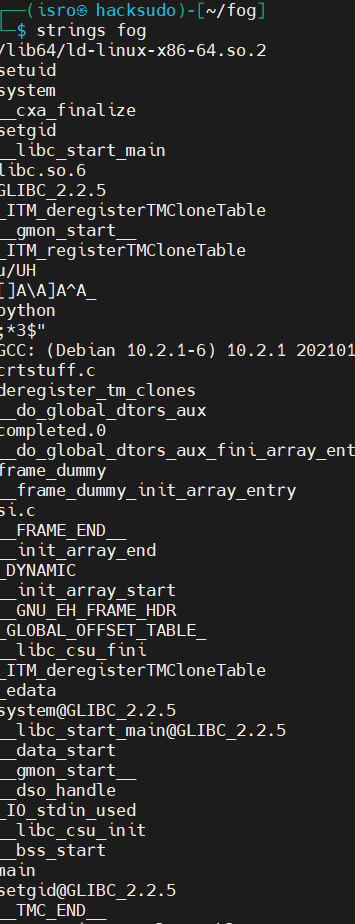
失败了

看看python运行能不能上去

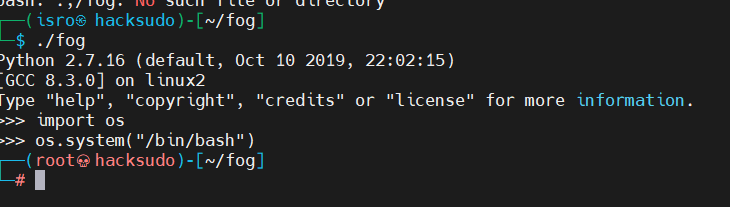


有点尴尬

看一下别的



正好有python，应该是直接执行



搞定

