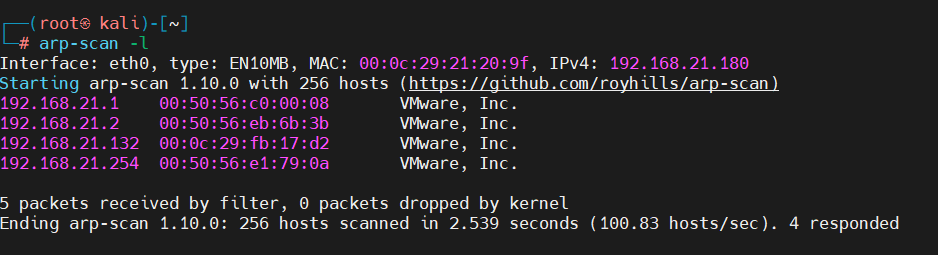
coffeeaddicts

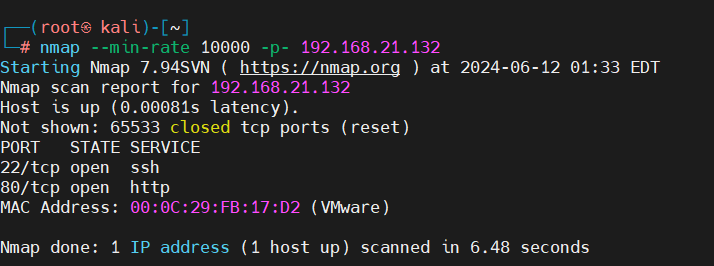
下载地址：<https://www.vulnhub.com/entry/coffee-addicts-1,699/>

主机发现

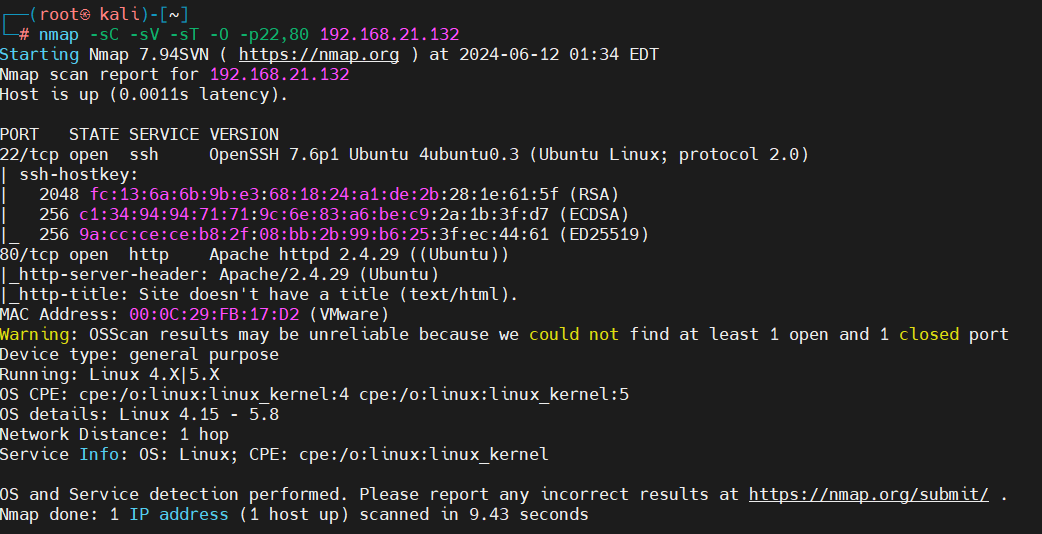


目标132

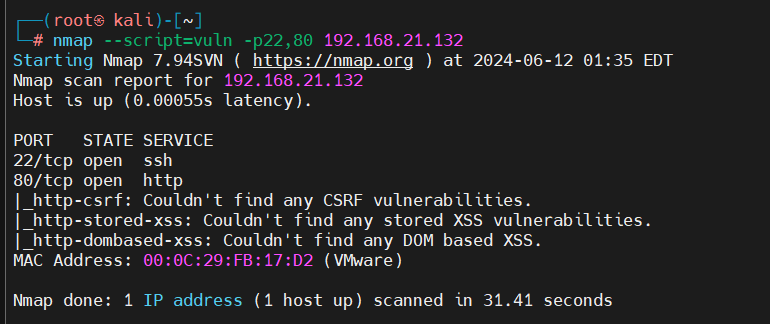
端口扫描



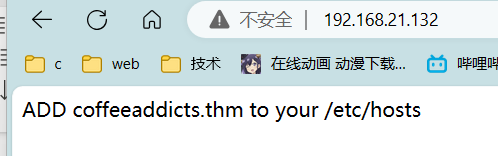
服务扫描



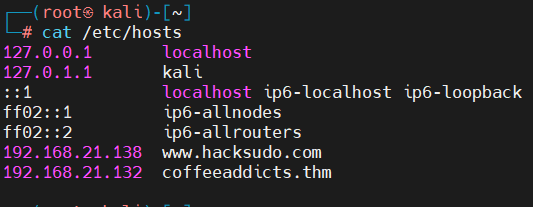
漏洞扫描



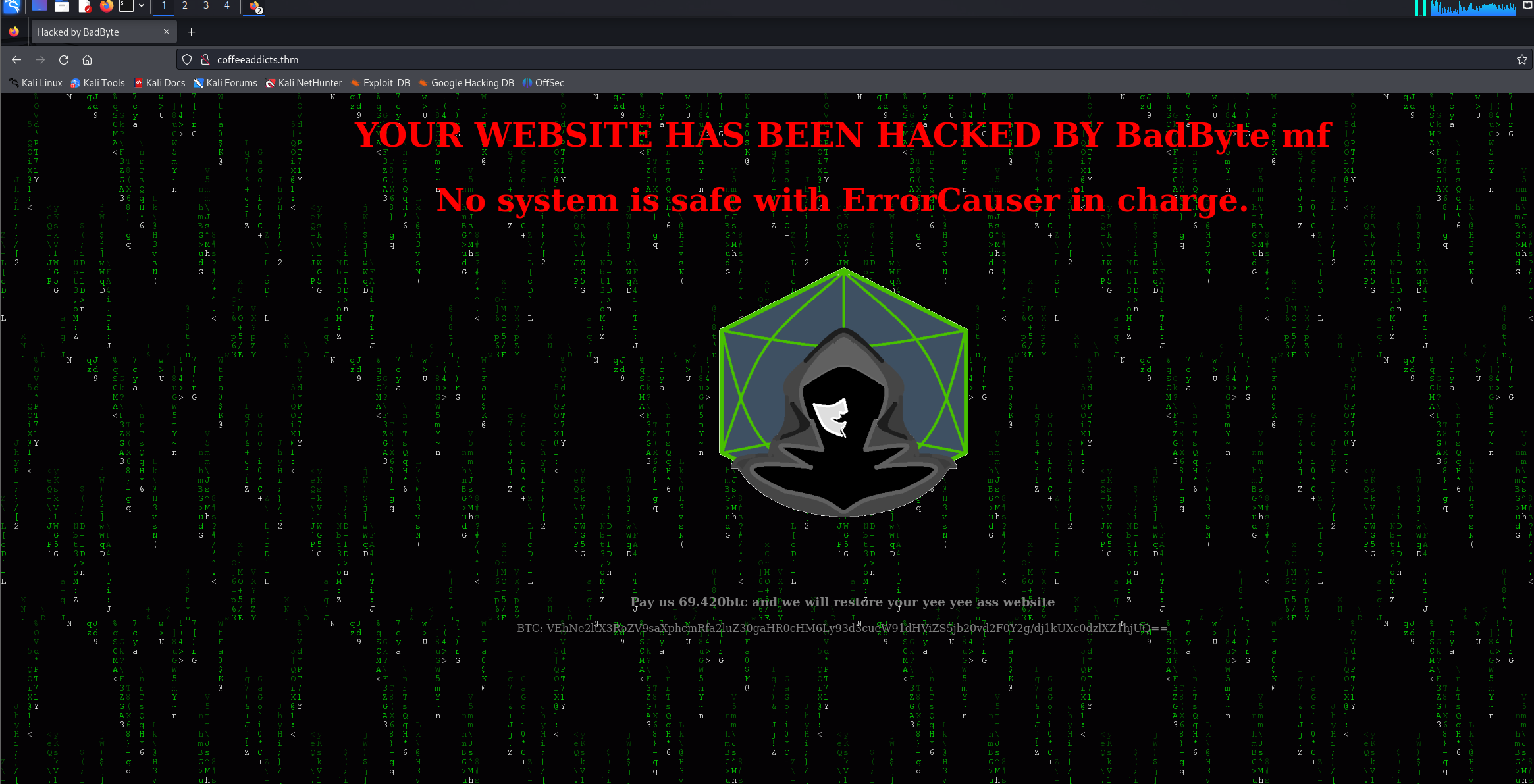
只能看web



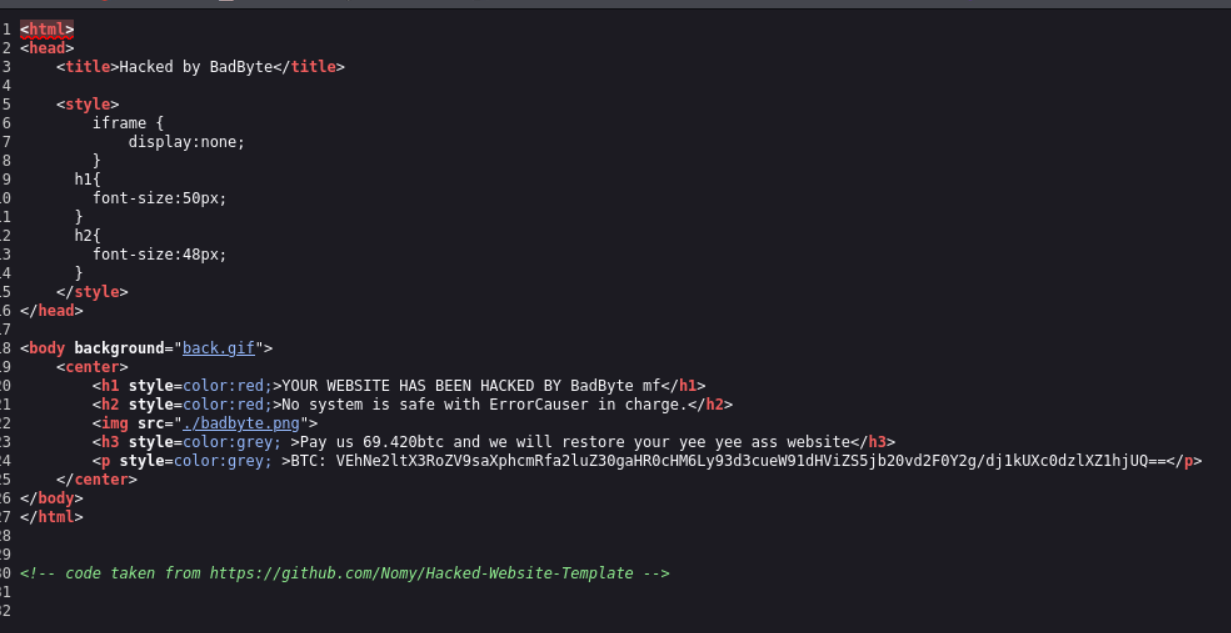
改hosts

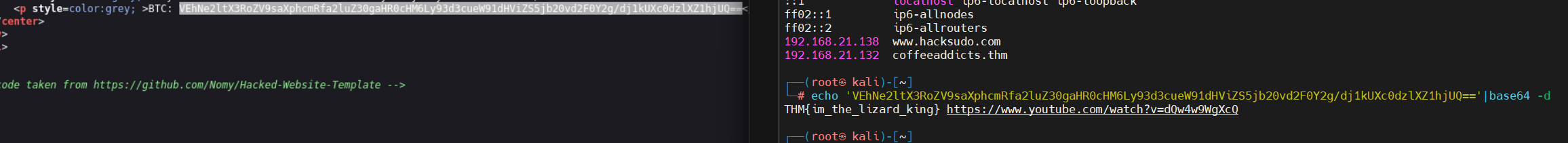


再次访问web



经典被黑

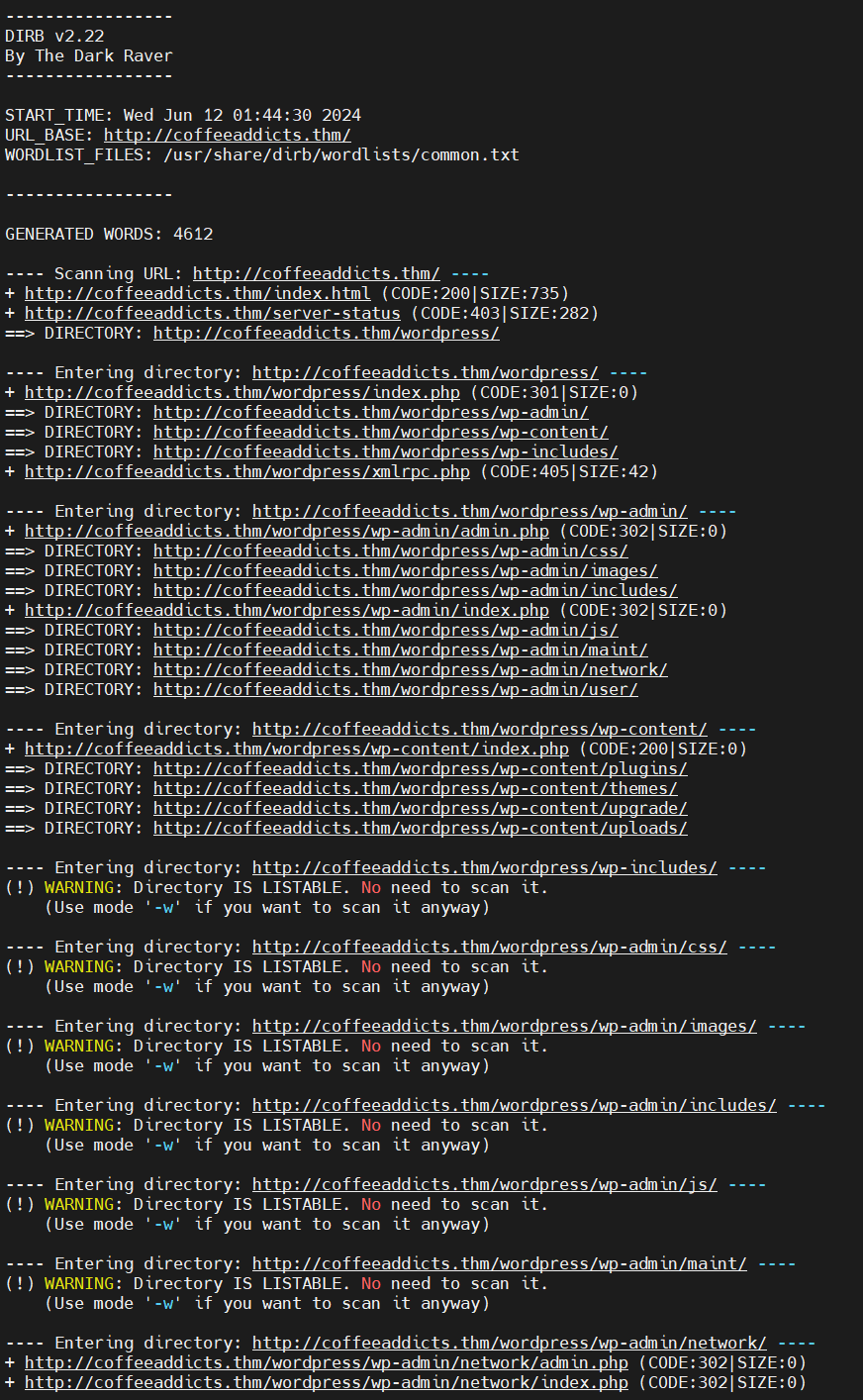




？这算彩蛋吗

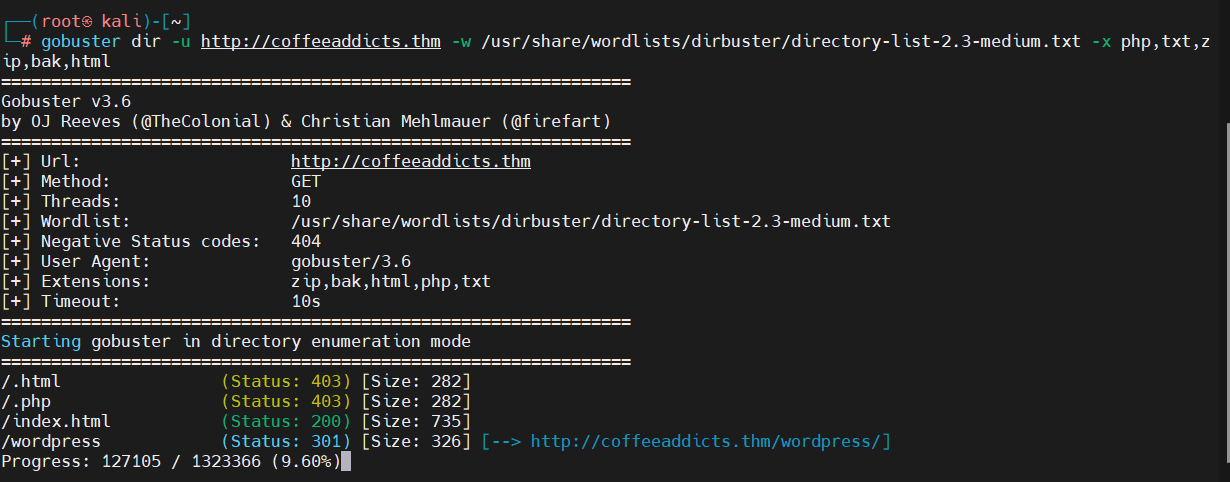
还是扫描一下web

dirb的结果

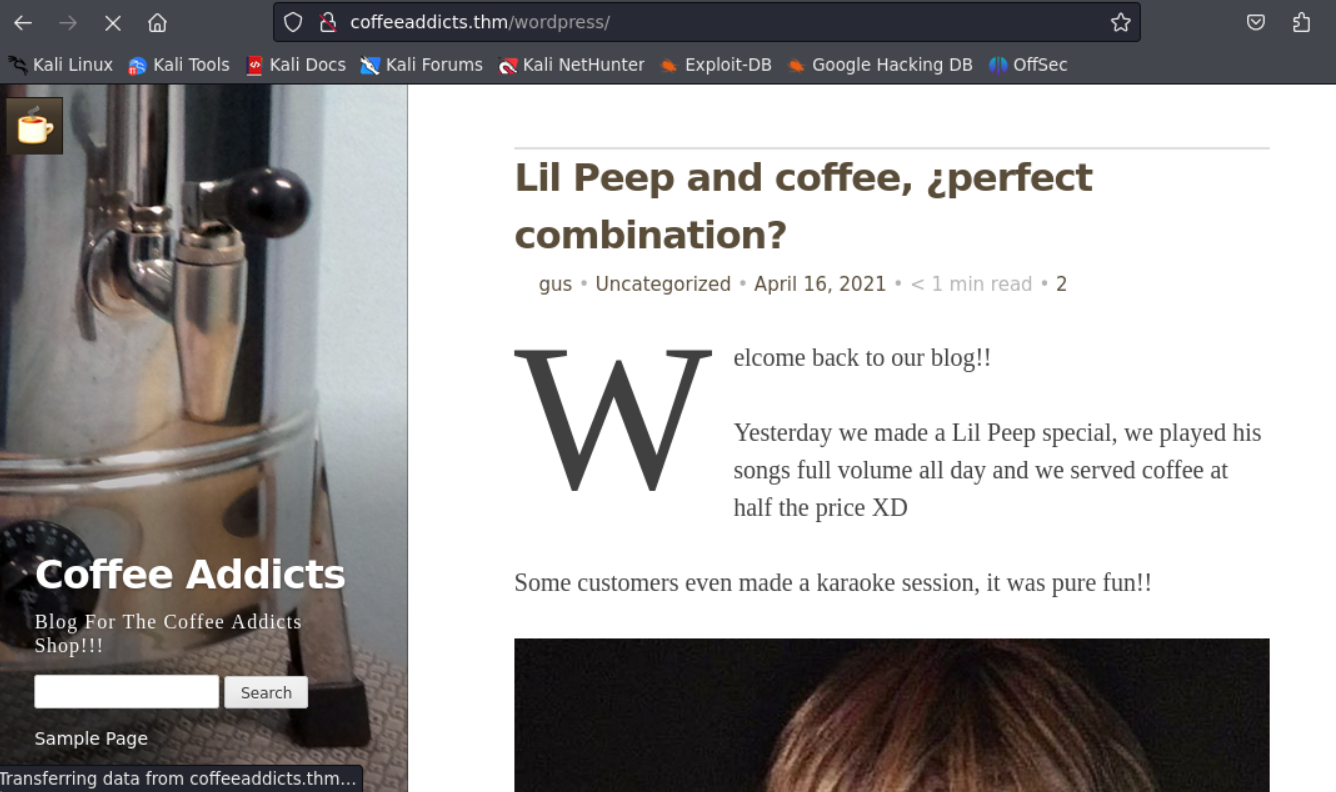


不需要看完就知道这个是wp搭建的

gobuster的结果

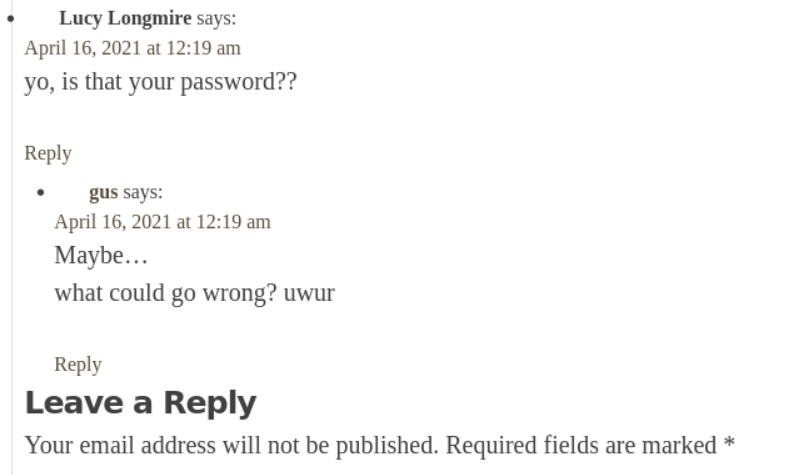


扫不扫完问题已经不大了



典型的挂黑页

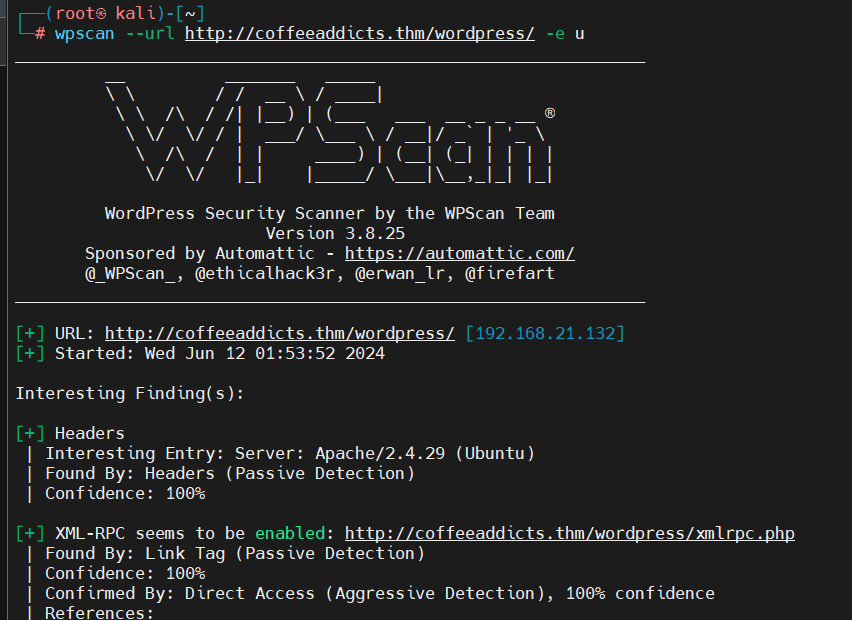
翻一下看看有没有什么东西顺便拿wpscan看看

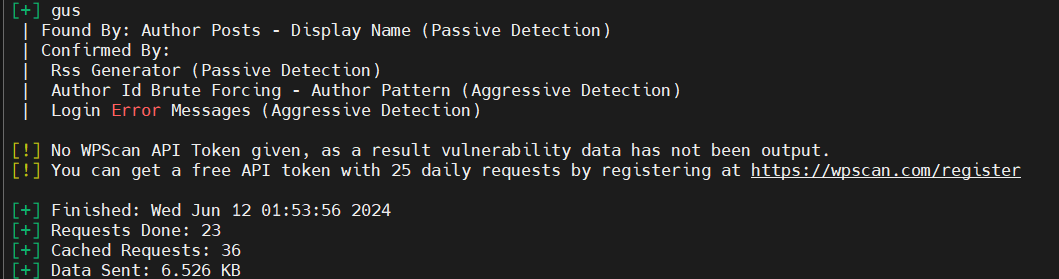


注意对话

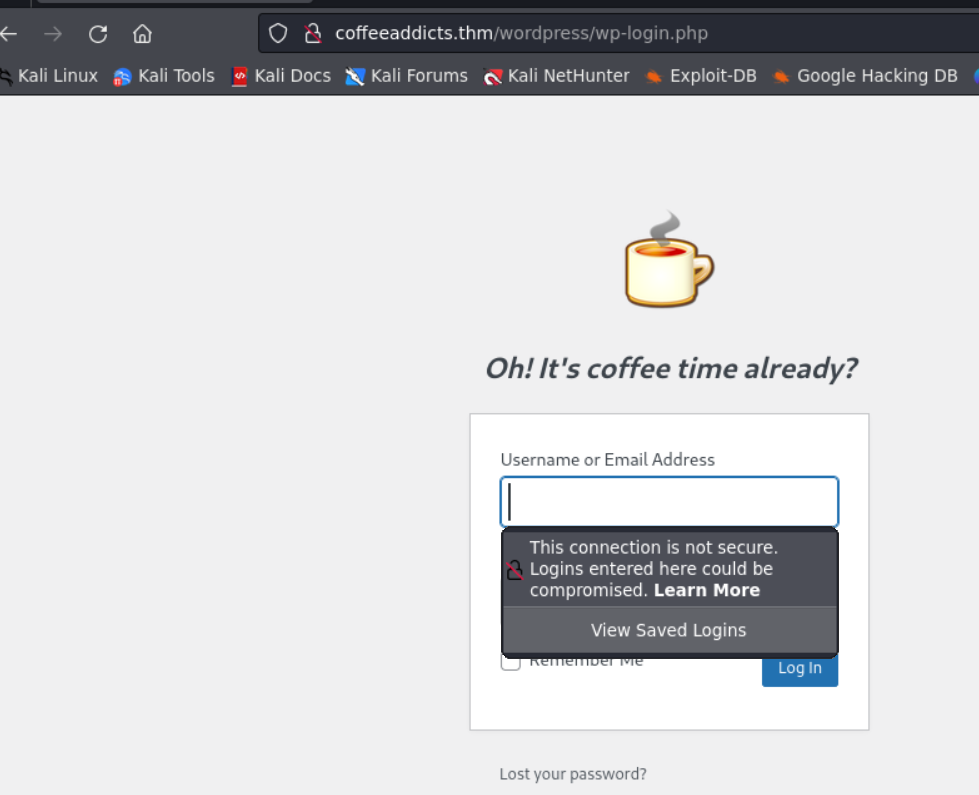
密码应该是gusineedyouback

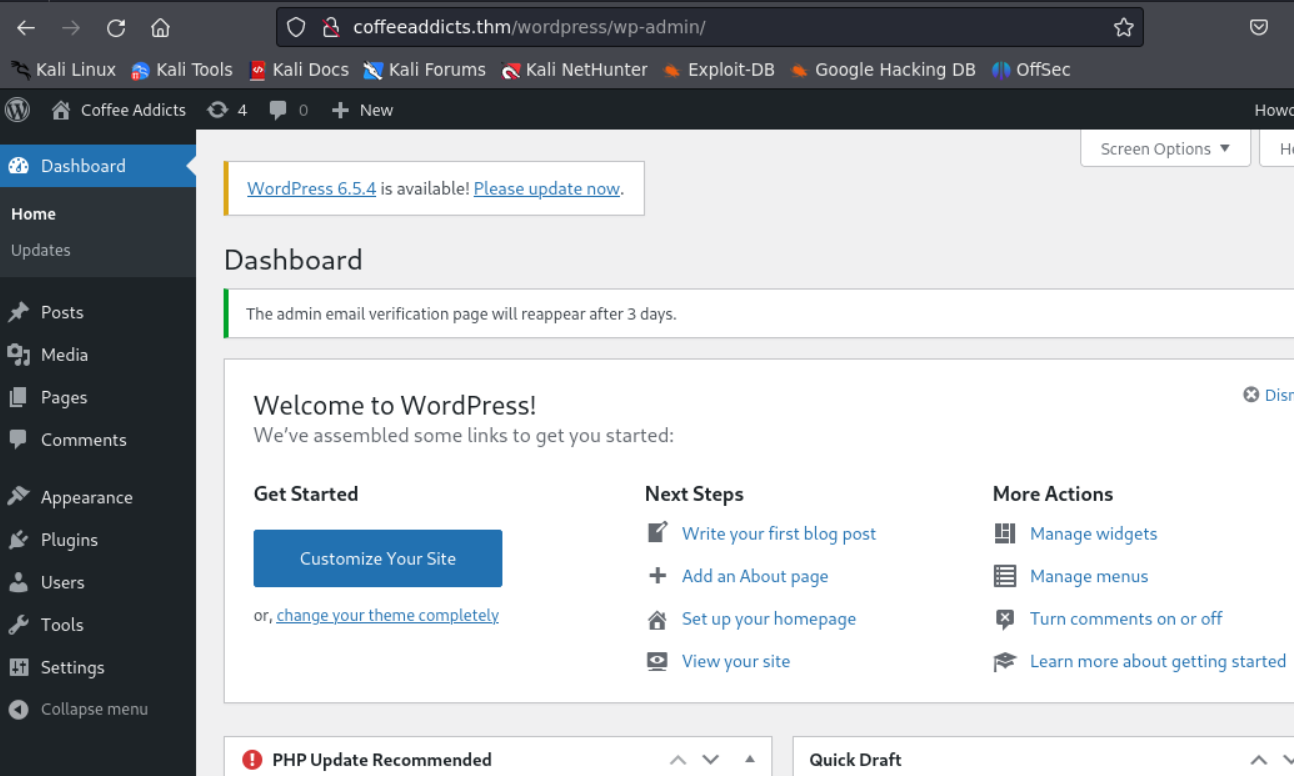
少一个用户名（其实也能猜到）



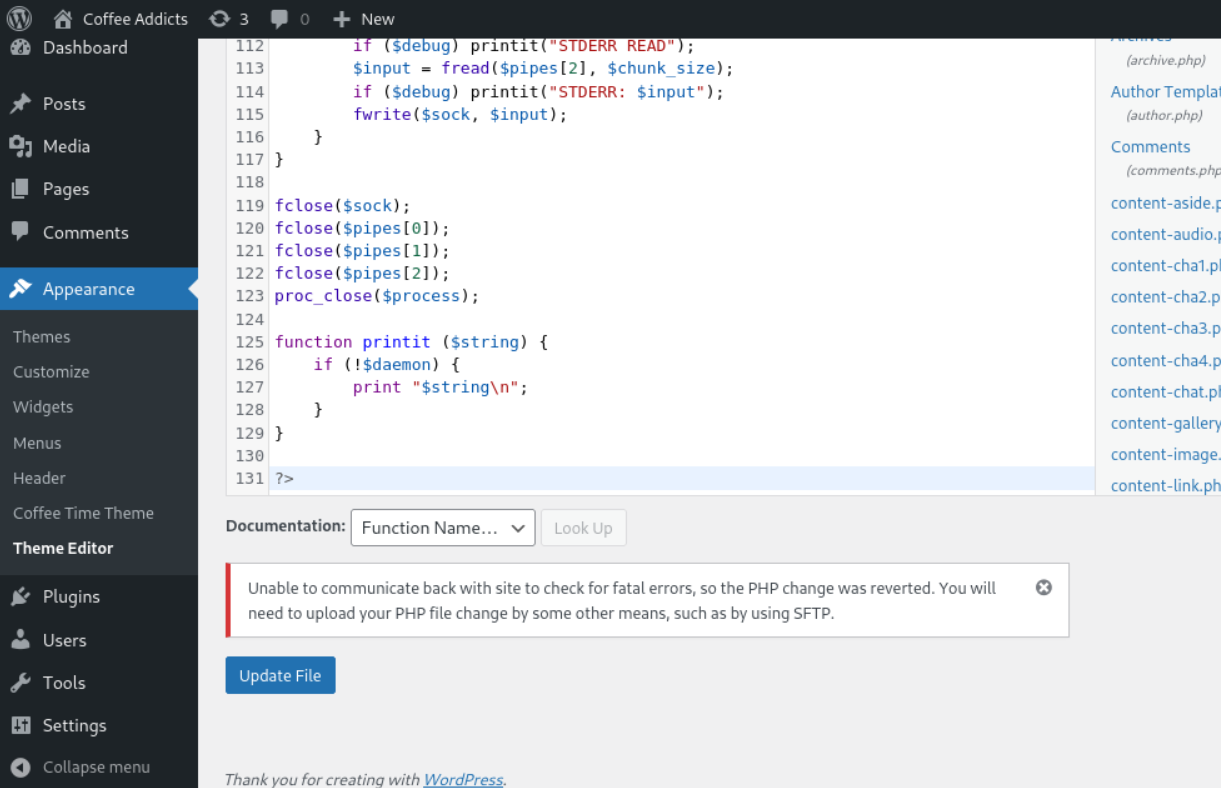


这个说白了就是wp做的比较多直接进后台

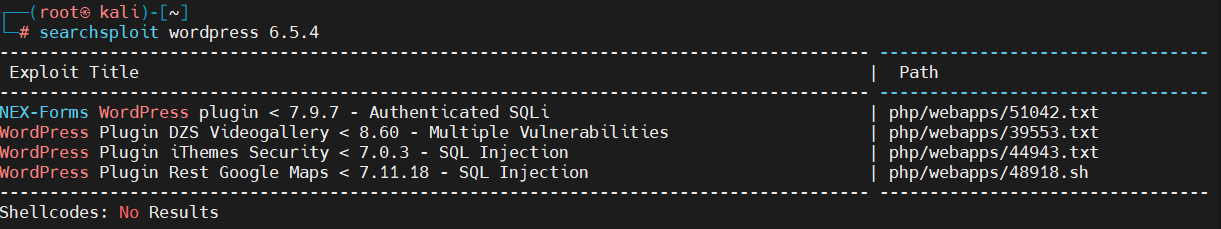




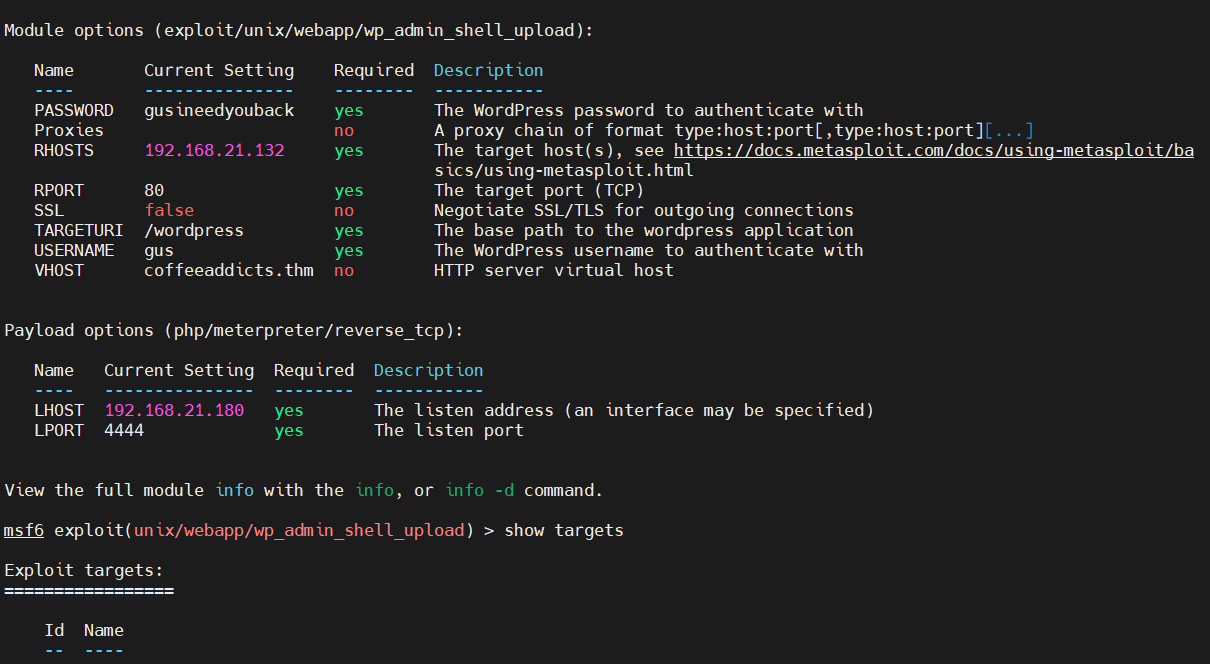
接下来传反弹shell



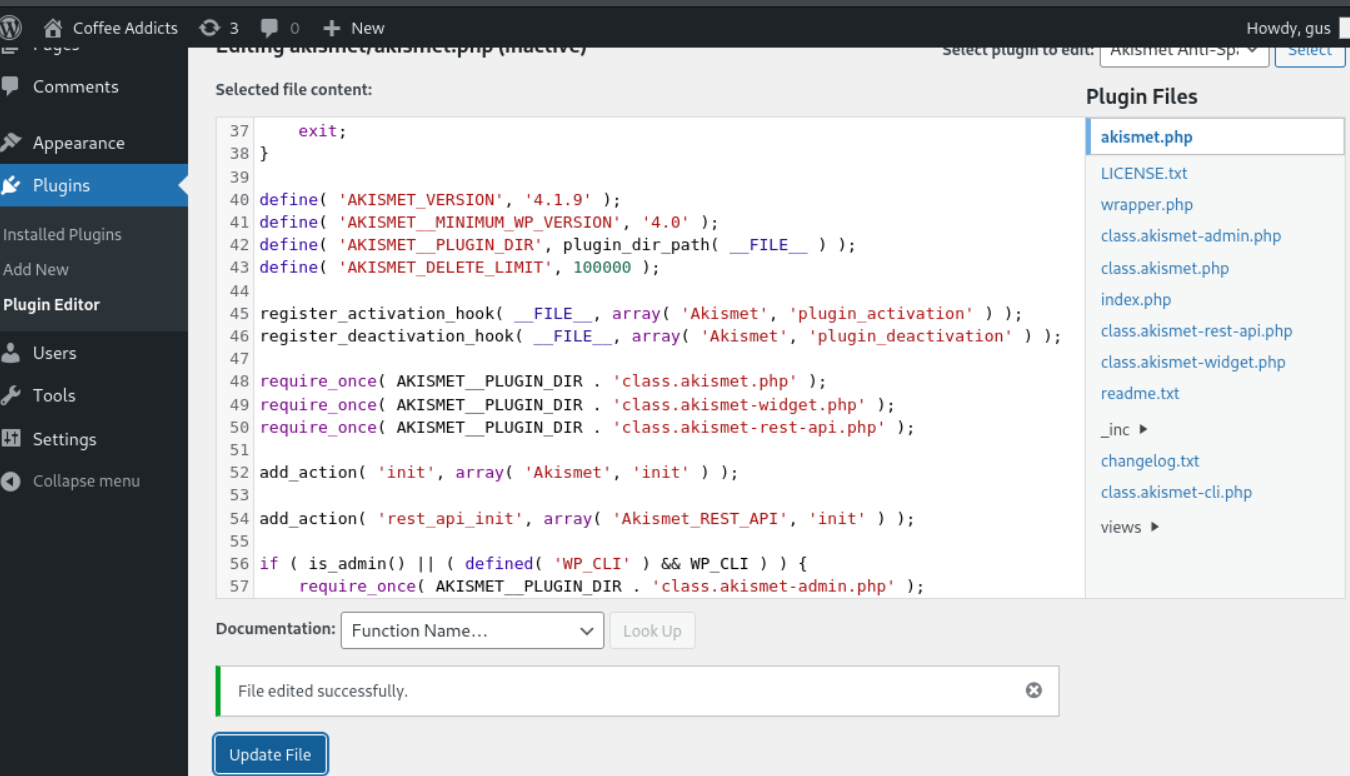
传不上去



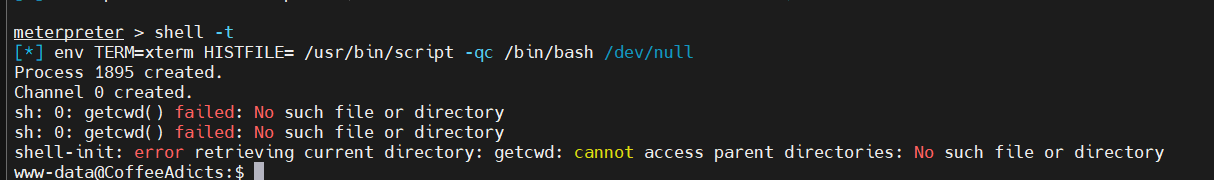
msf



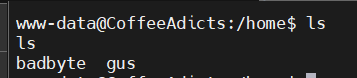
上传插件也可以

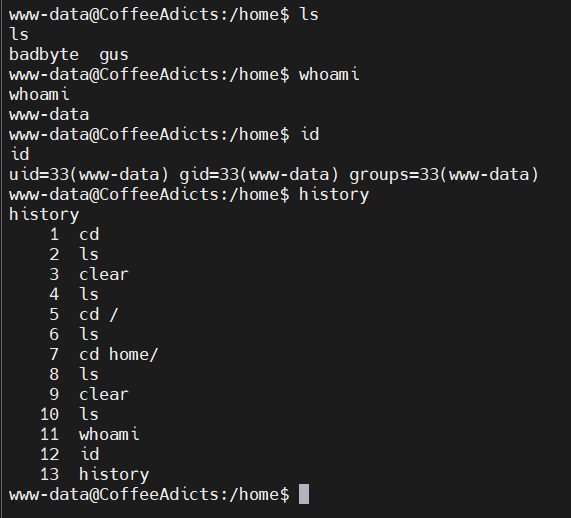


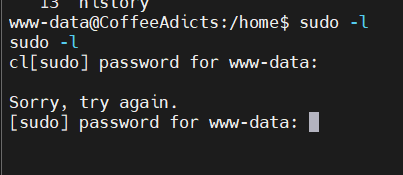
直接改成反弹shell就可以

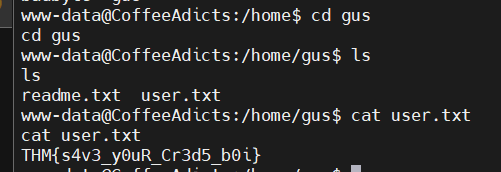


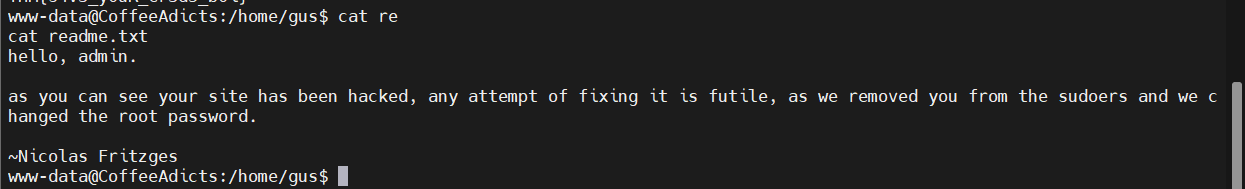
信息收集



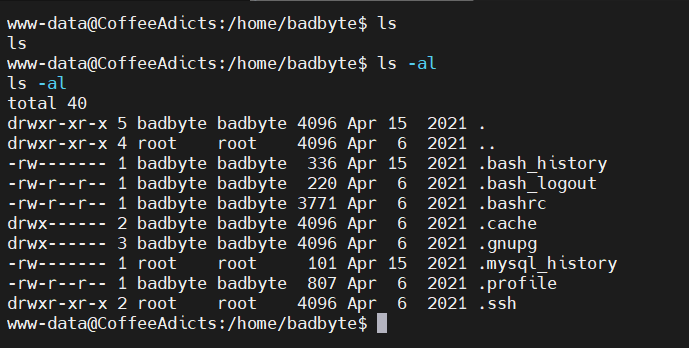




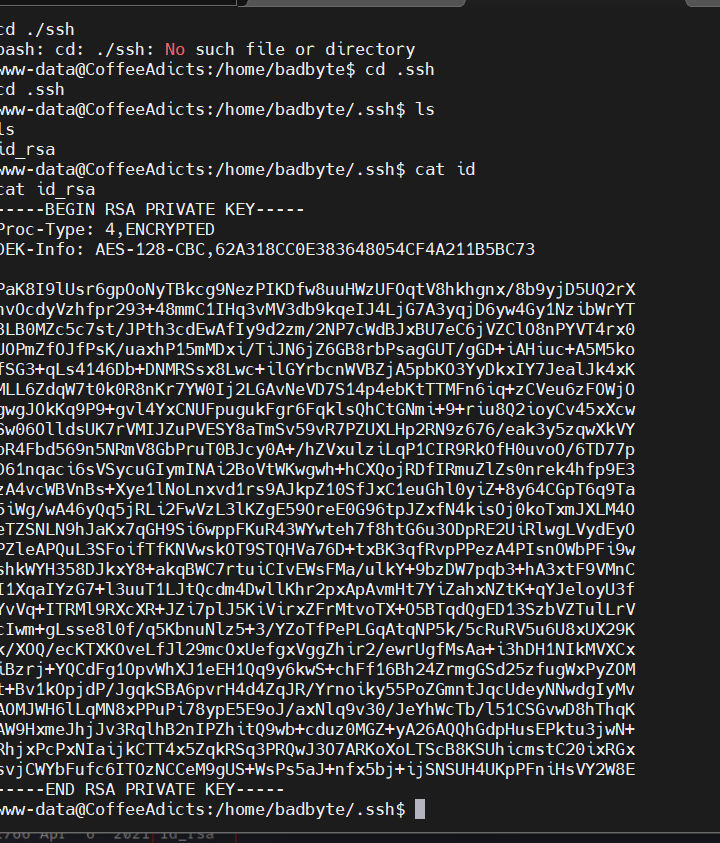


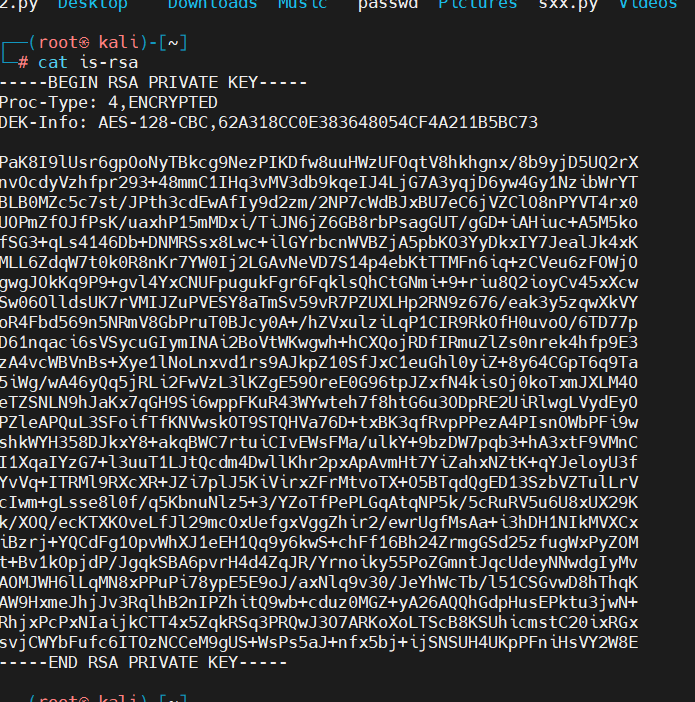


看看另外一个用户的东西

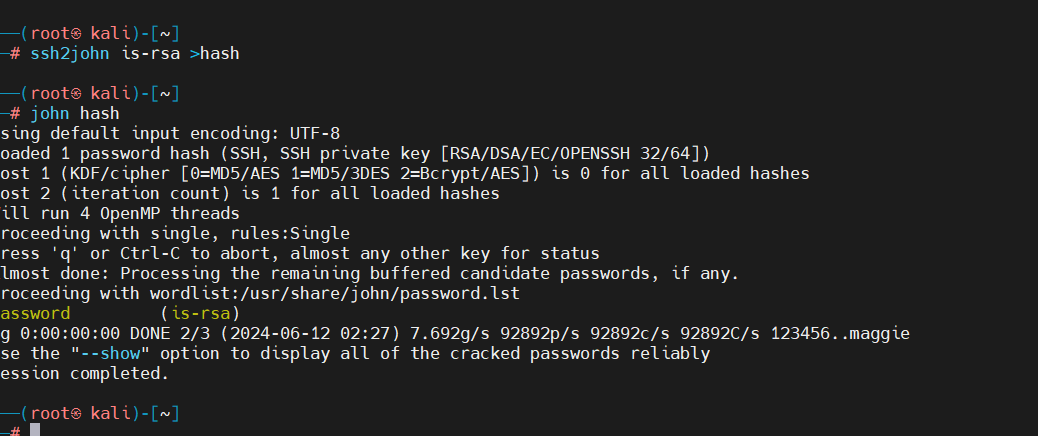


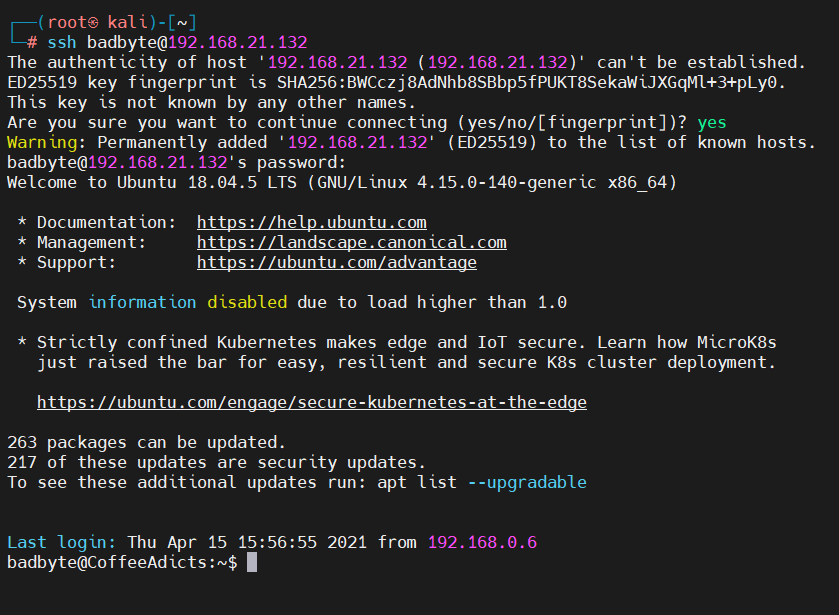
下载时肯定的





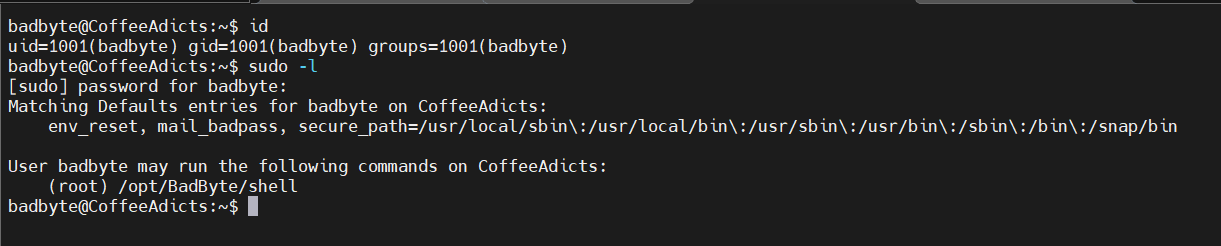
破解

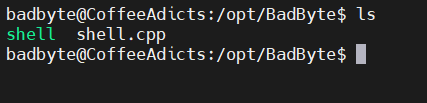




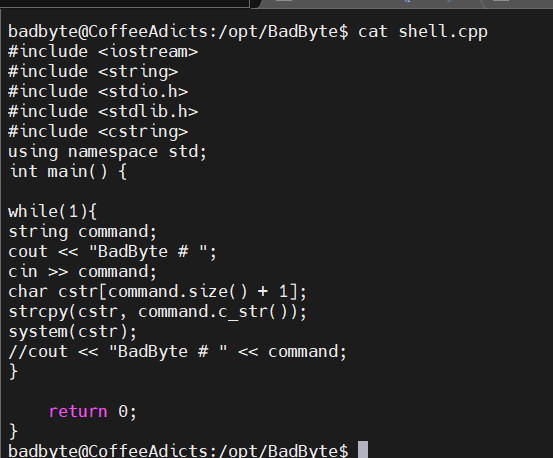
提取

信息收集





进来之后



让cstr执行bin/bash

