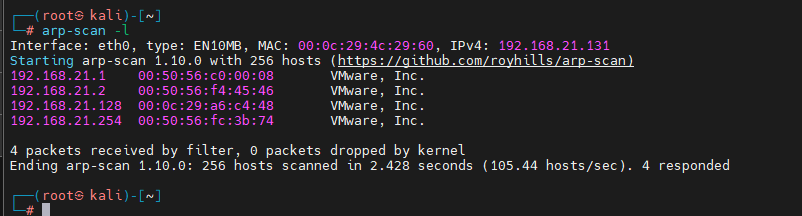
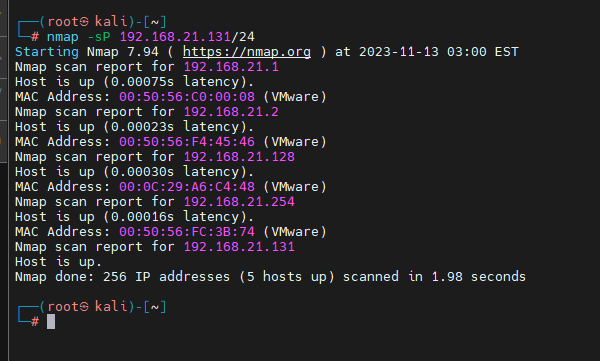
Momentum2

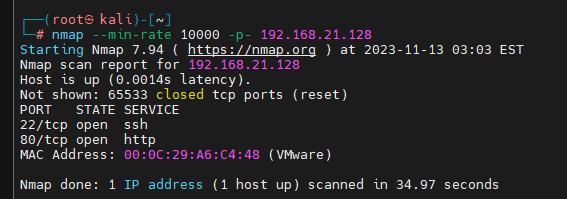
下载地址：<https://download.vulnhub.com/momentum/Momentum2.ova>

主机发现

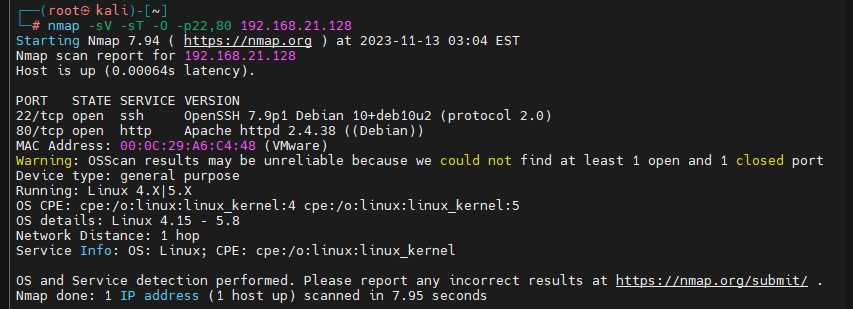




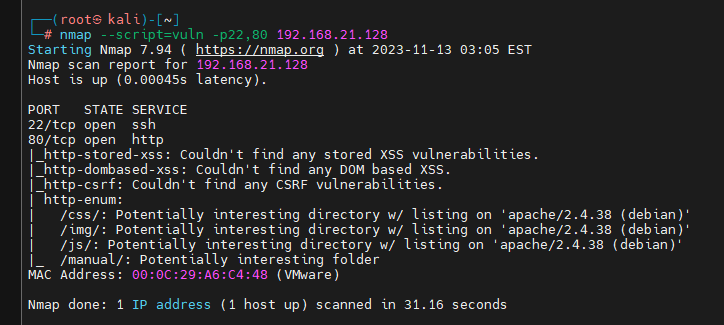
端口扫描



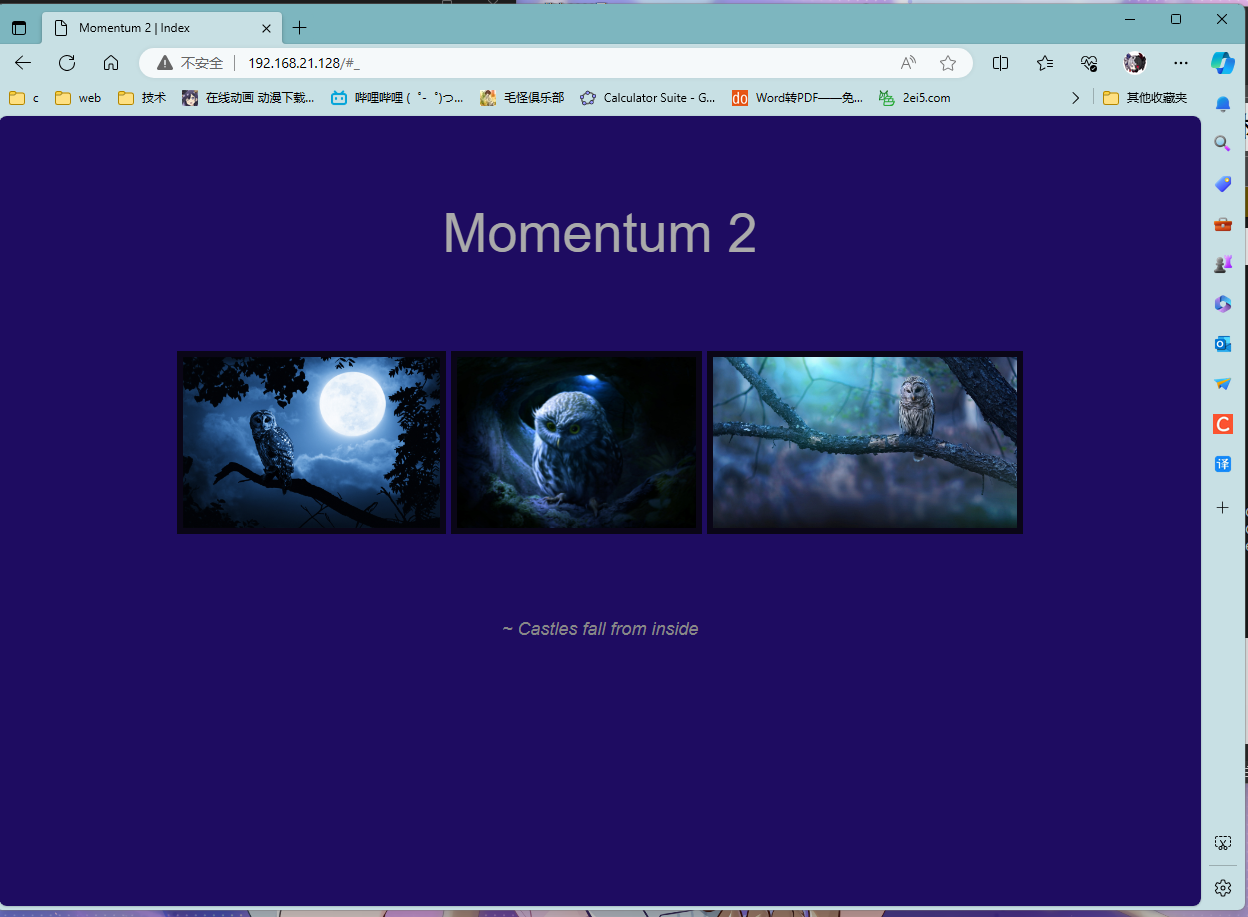
端口服务扫描



漏洞扫描

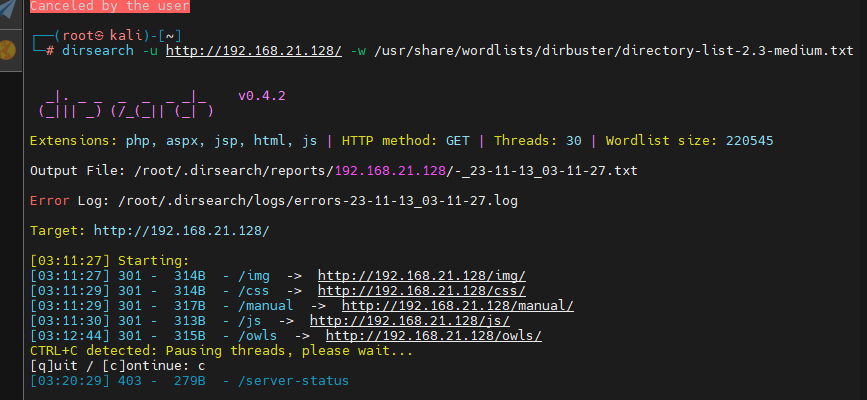


先去看看web



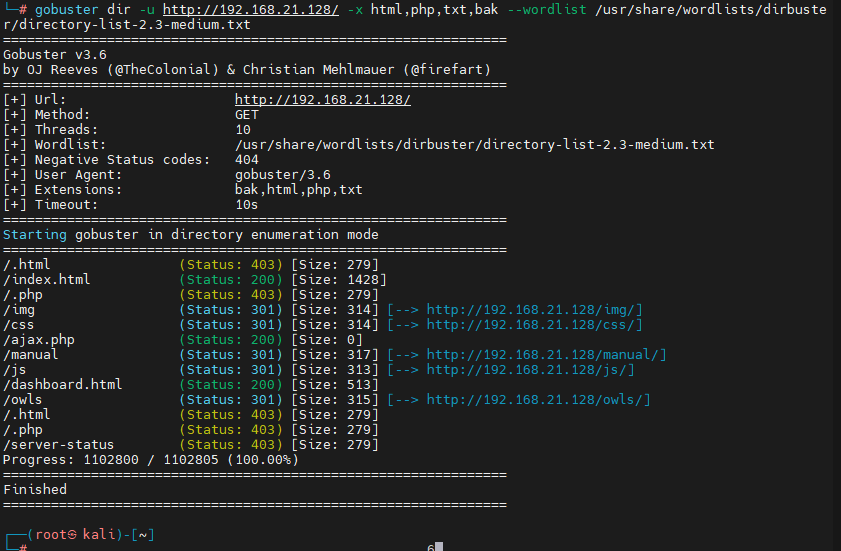
这里面没有什么，就顺手扫一下目录

发现一些可疑的目录

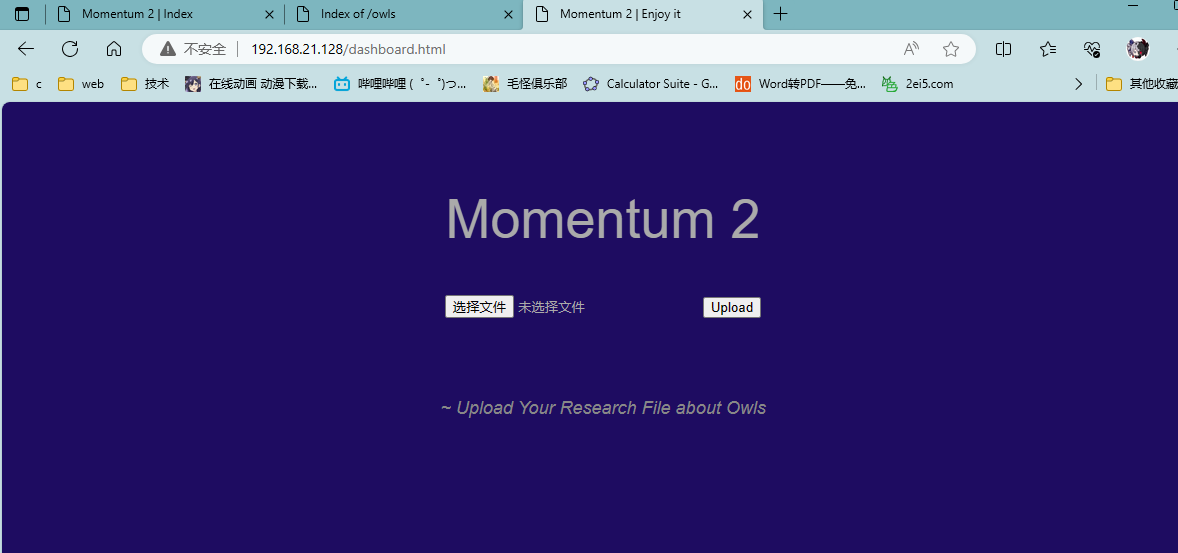


比较正常

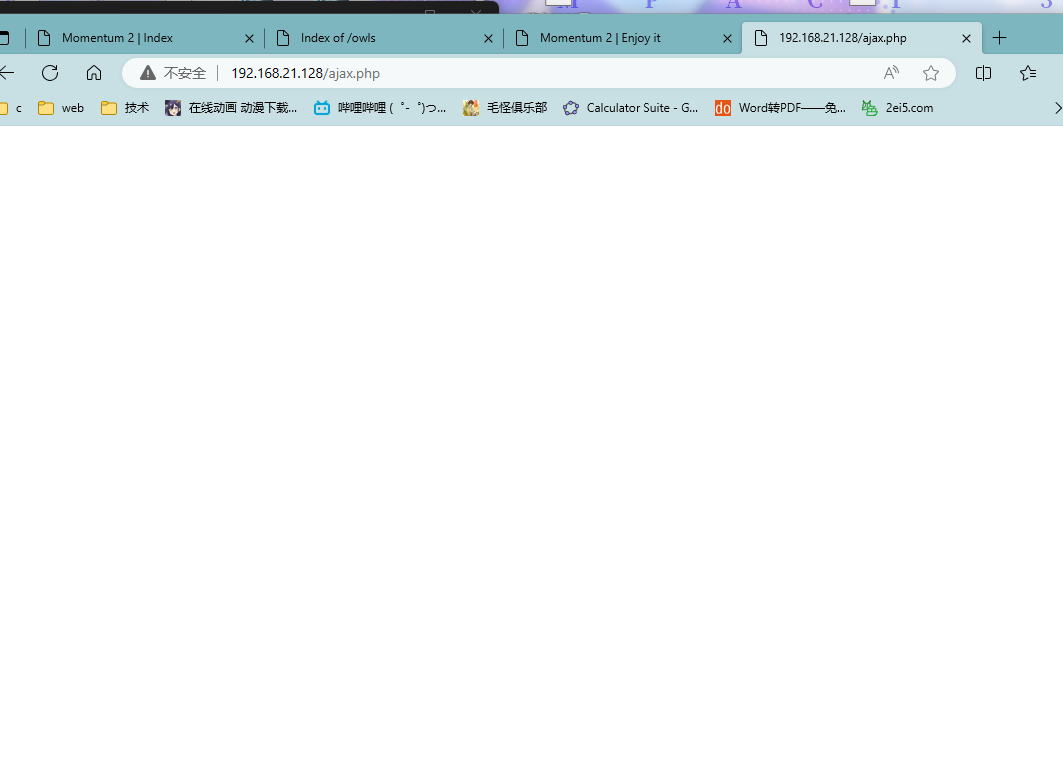
再看一下有没有别的web



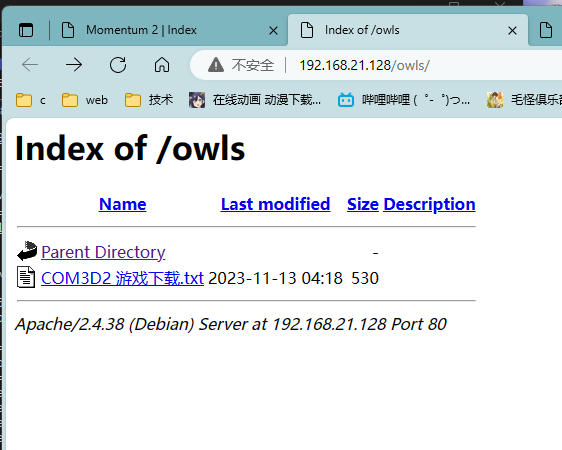
看到几个新的东西去看看



文件上传



啥都没有



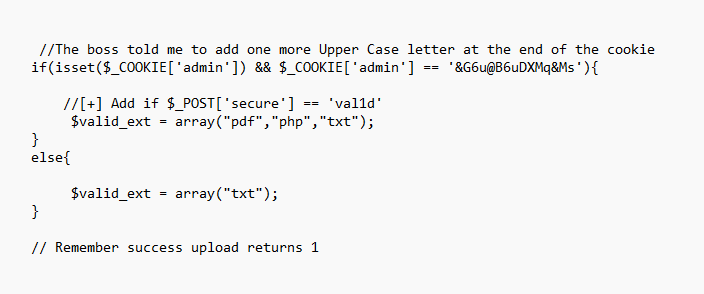
此处是上传文件的地址，而且发现只能上传txt文件

但是html要将文件传给php处理无论如何不应该大小是0

看看有没有bak（备份）



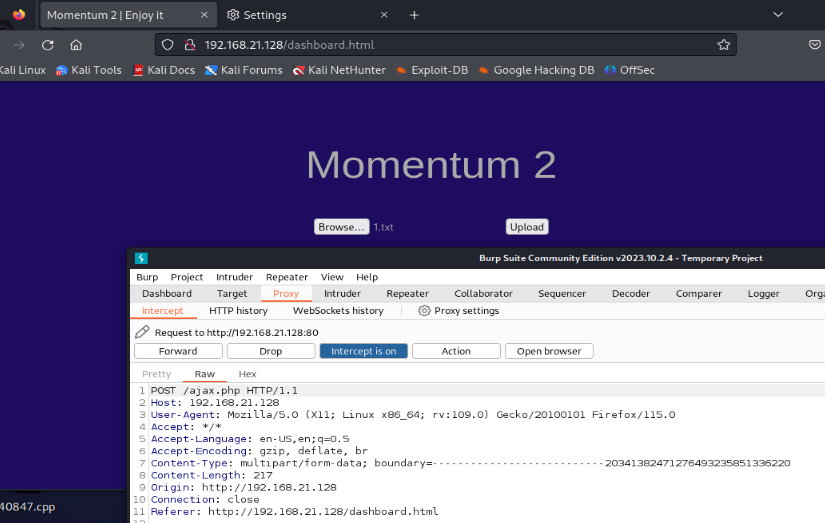
还是有的用txt打开看看

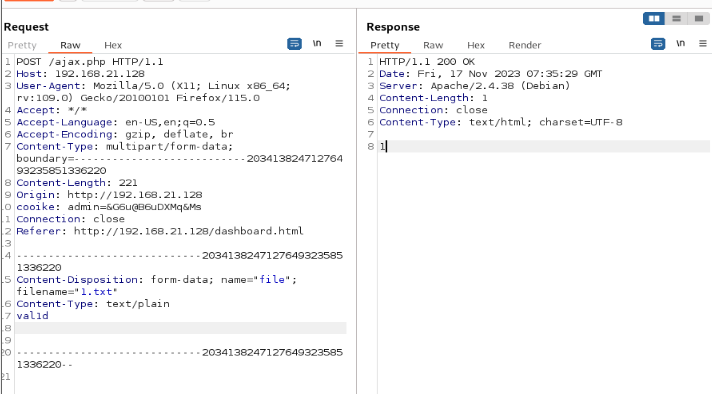


发现admin的cookie并且后面还有一个大写字母，这里需要抓包了

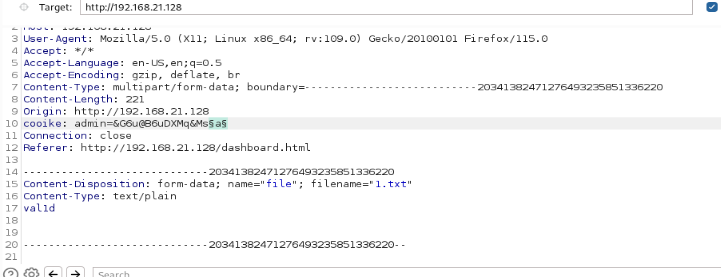
而且secure的值必须是val1d

在上传的地方抓包

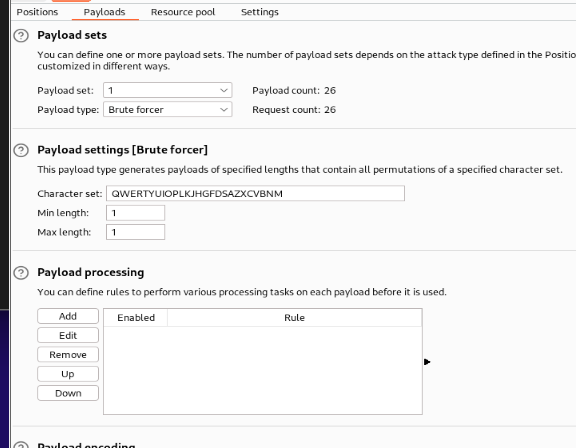


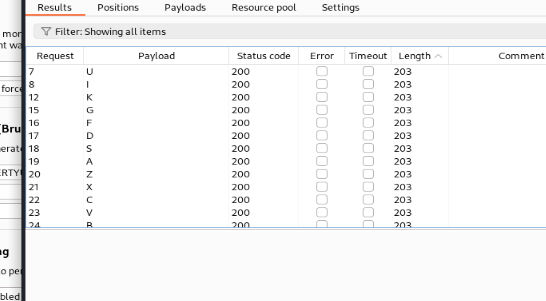


此处返回1，表示上传成功

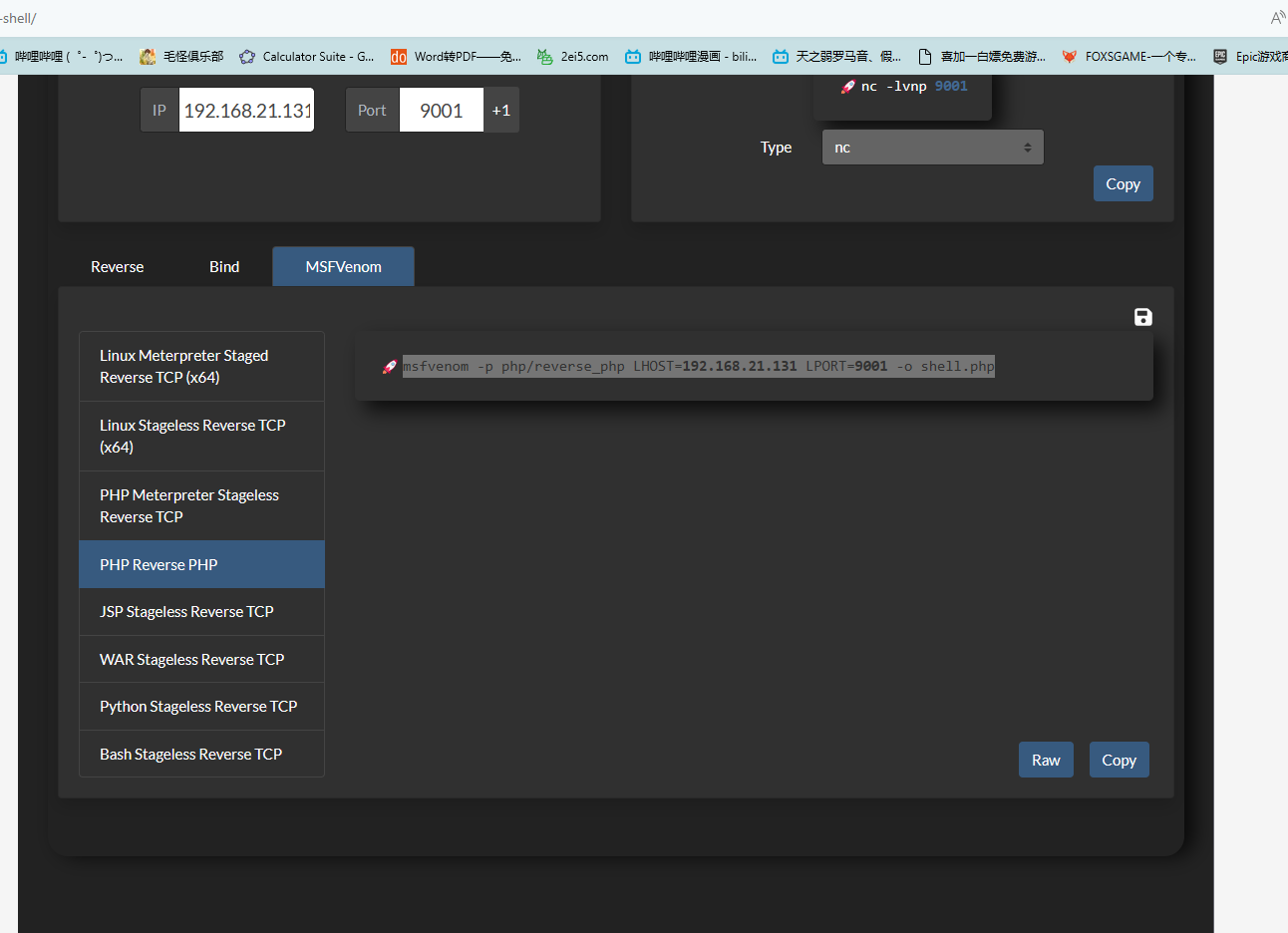


爆破cookie



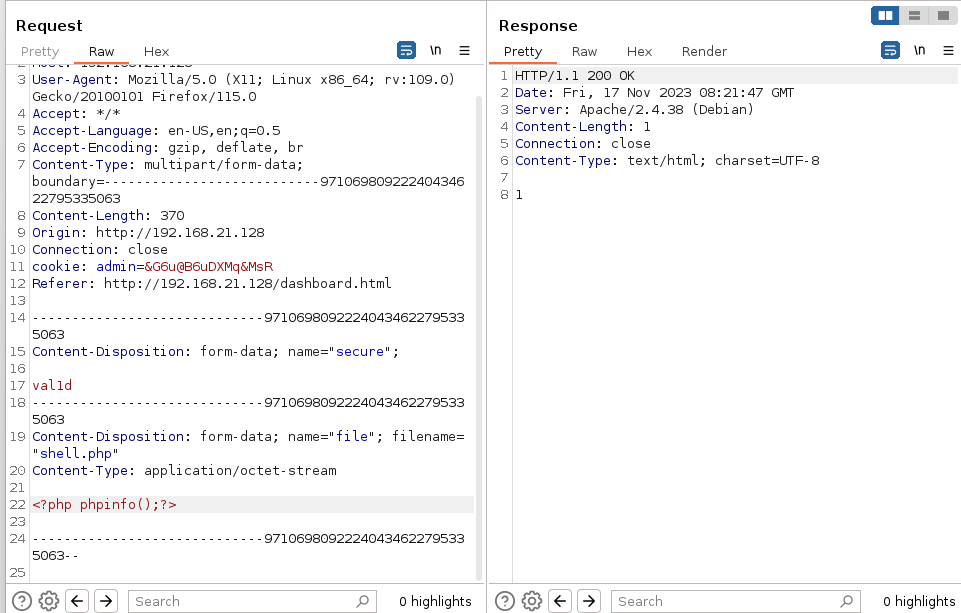


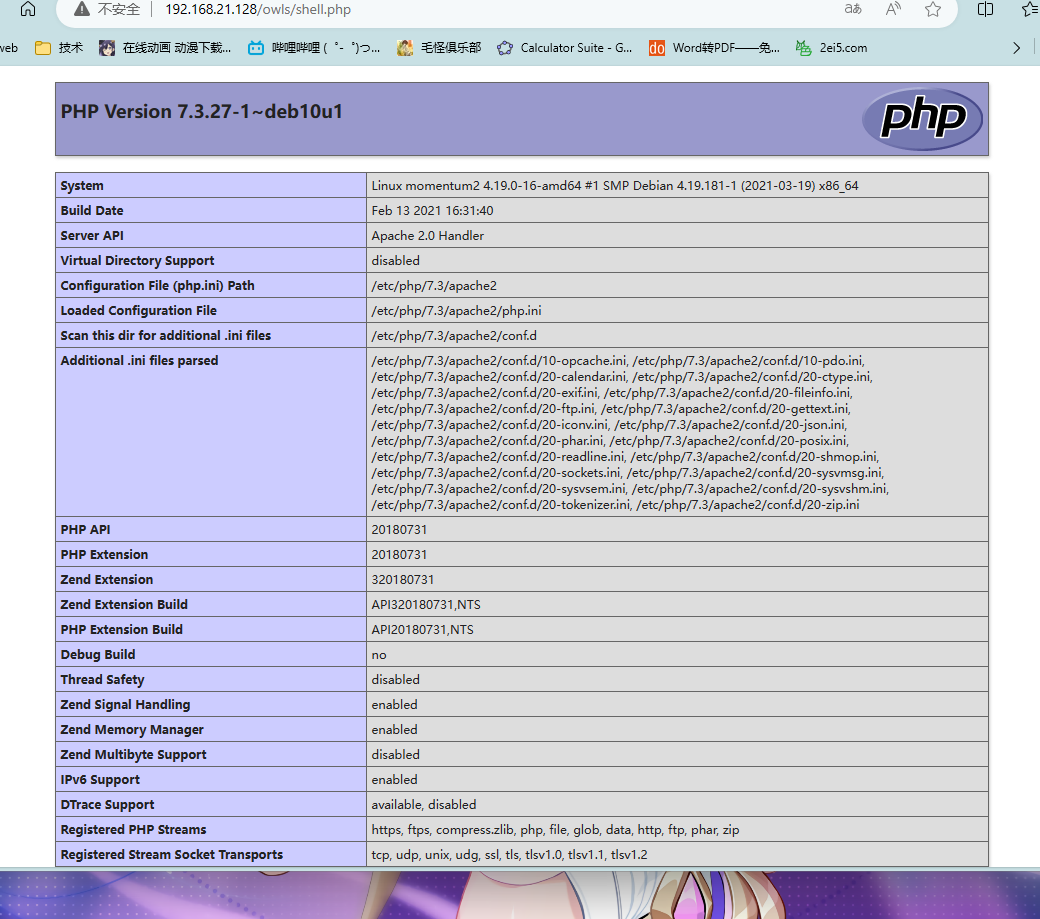
测试成功，看看上传文件是什么情况（直接上反弹shell[在线反弹shell生成工具 – Zgao's blog](https://zgao.top/reverse-shell/)）



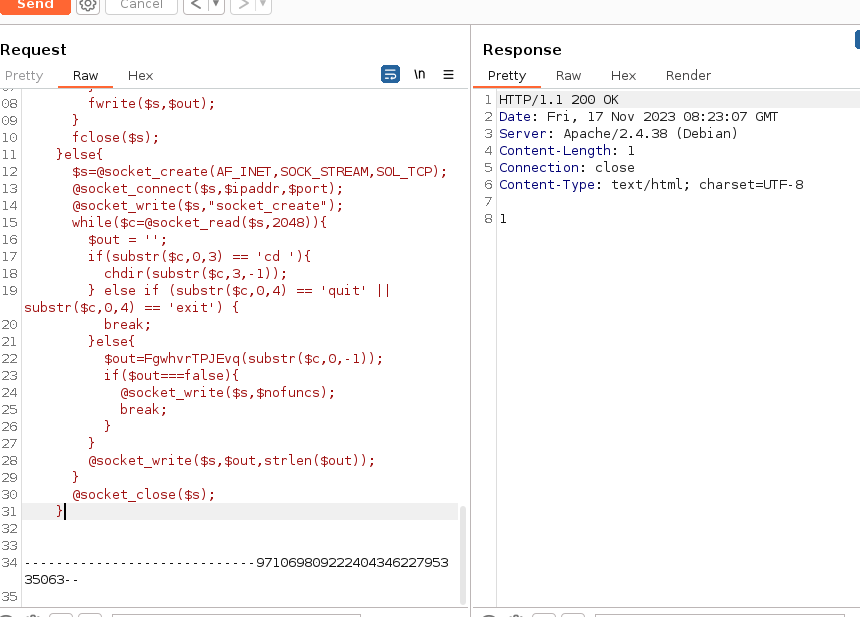
生成的shell放到数据包





成功

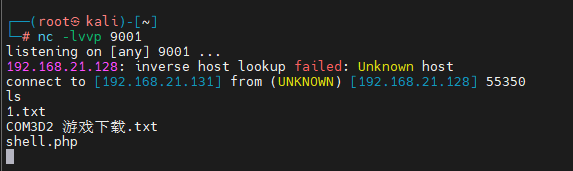
来吧反弹shell

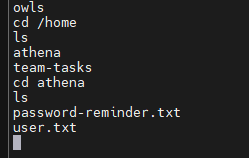


监听端口

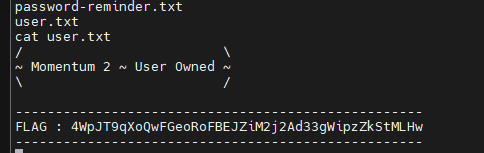


点击shell

搞定



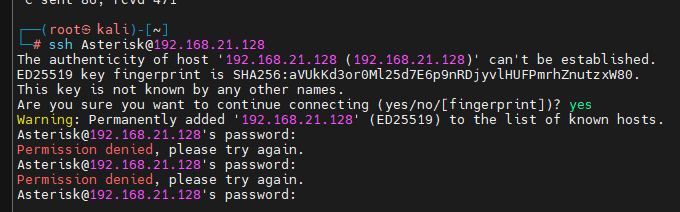
在home文件发现密码



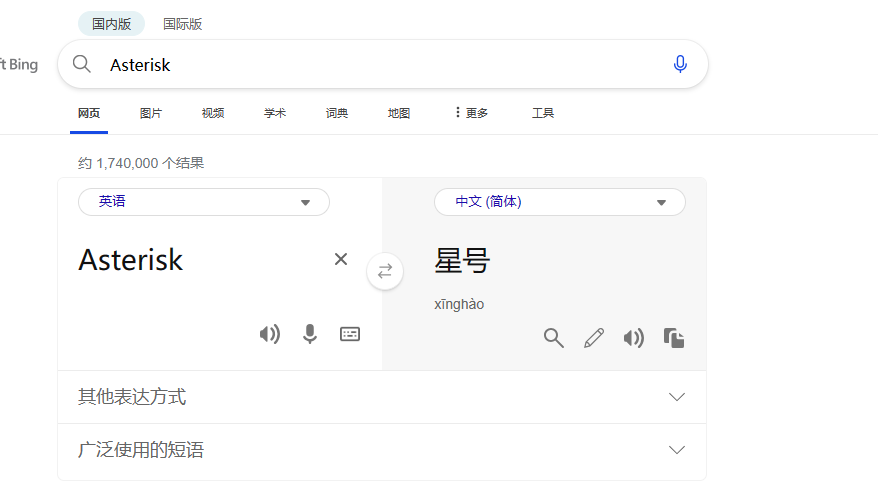


拿到

直接ssh

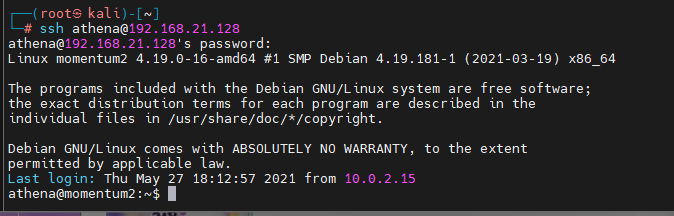


发现密码不对，同时发现了不对劲



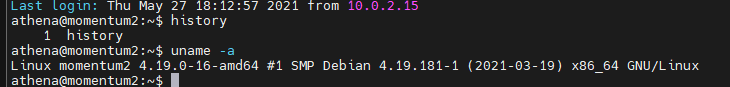
感觉我的用户登入不是我输入的用户名

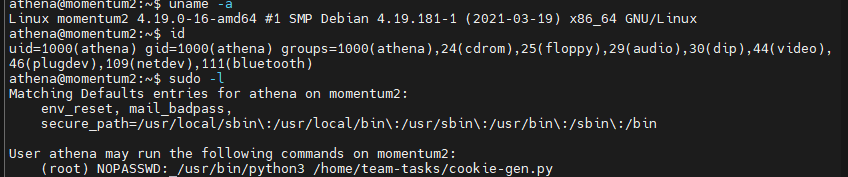
想起来了这里文件夹是用户的名字，密码应该是要在后面加一个\*



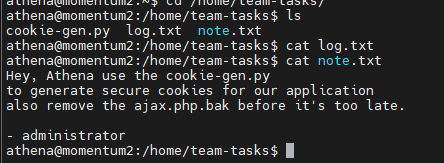
Ok登入成功

信息收集

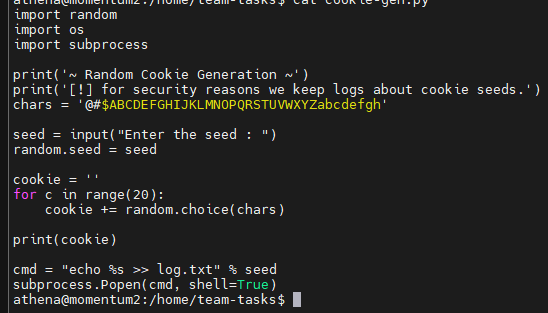


发现有root权限运行的python脚本

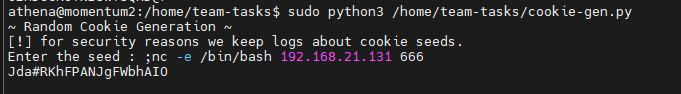
去看看

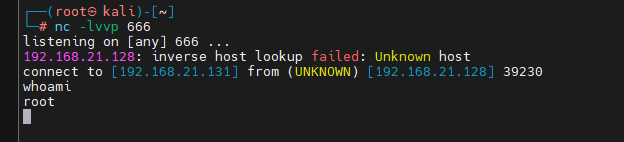


发现note去看看，去看看源文件



这里是直接执行输入的seed，所以我们直接反弹shell





结束

