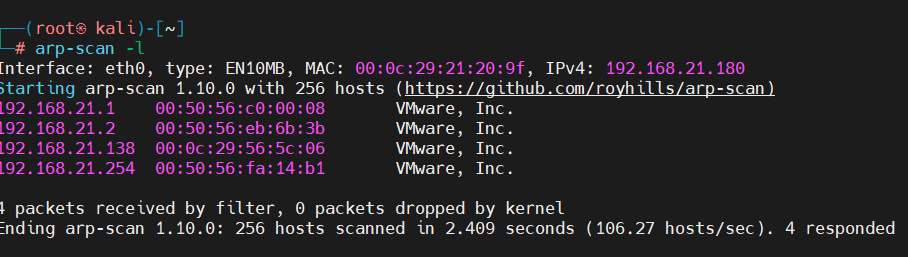
hacksudo search

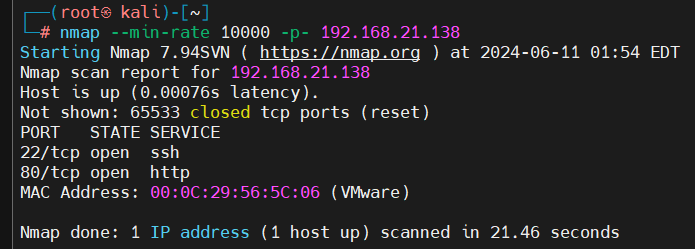
下载地址：<https://download.vulnhub.com/hacksudo/hacksudo-search.zip>

靶机发现

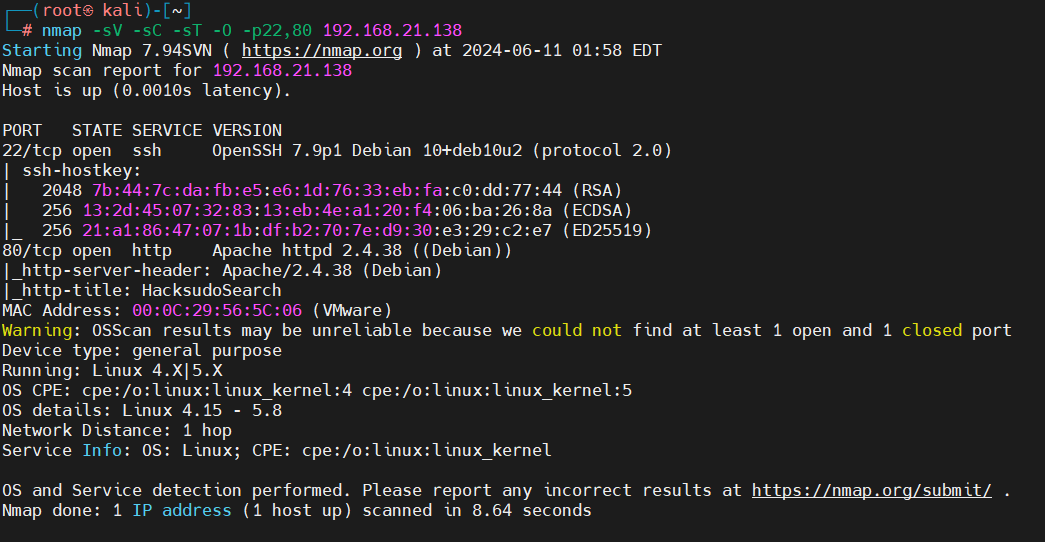


目标138

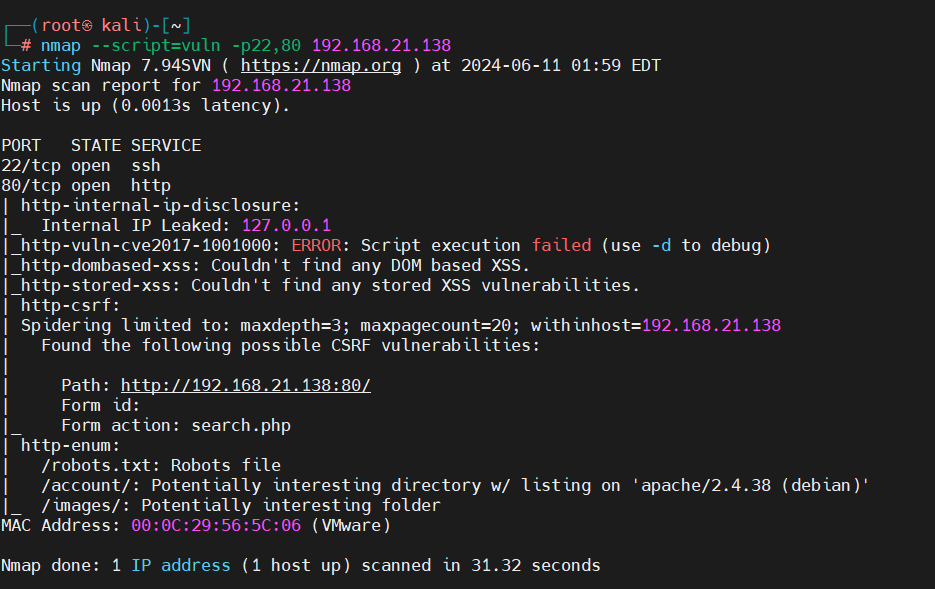
端口扫描



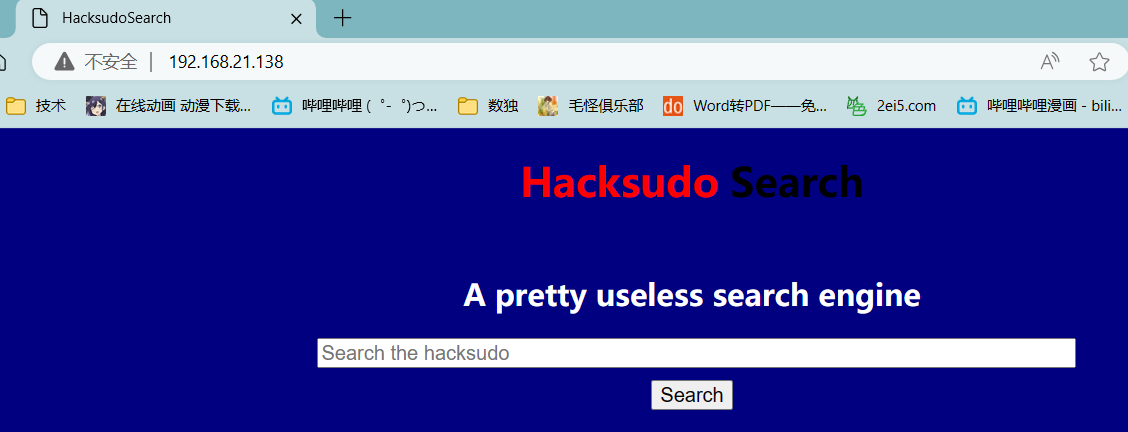
服务扫描



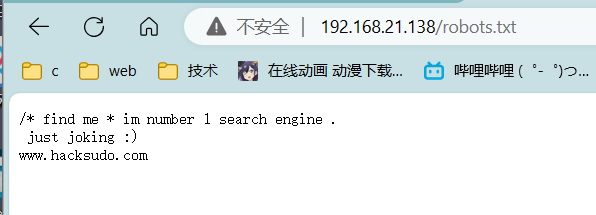
漏洞扫描



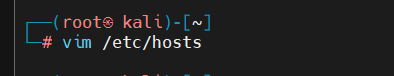
看看web

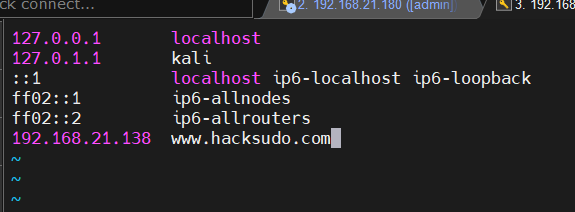


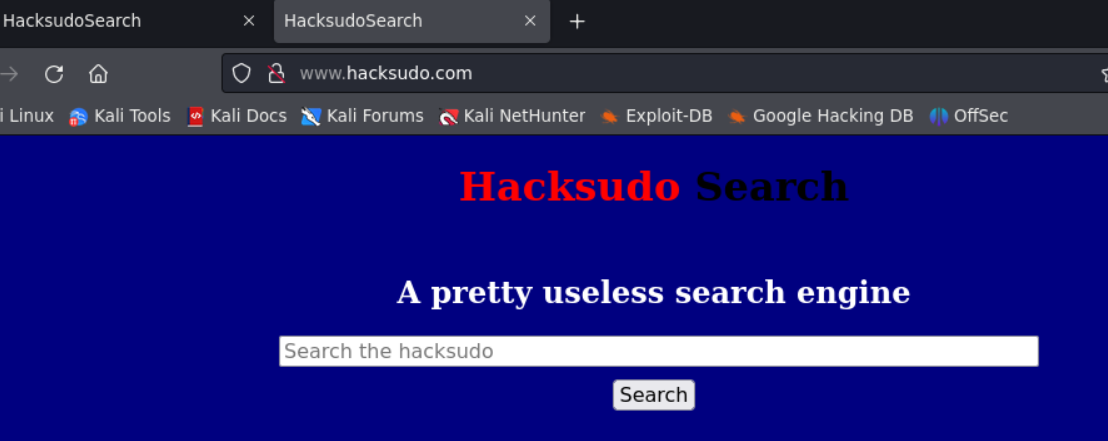
先看robots

****

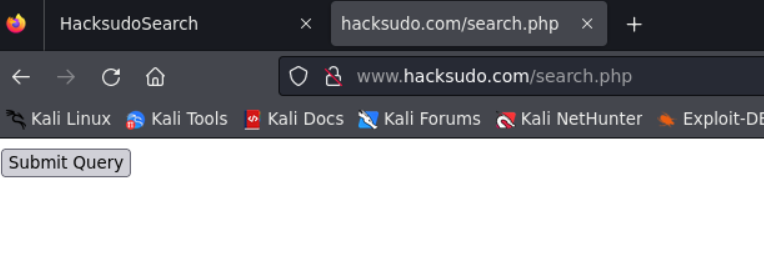
emmm又要改hots



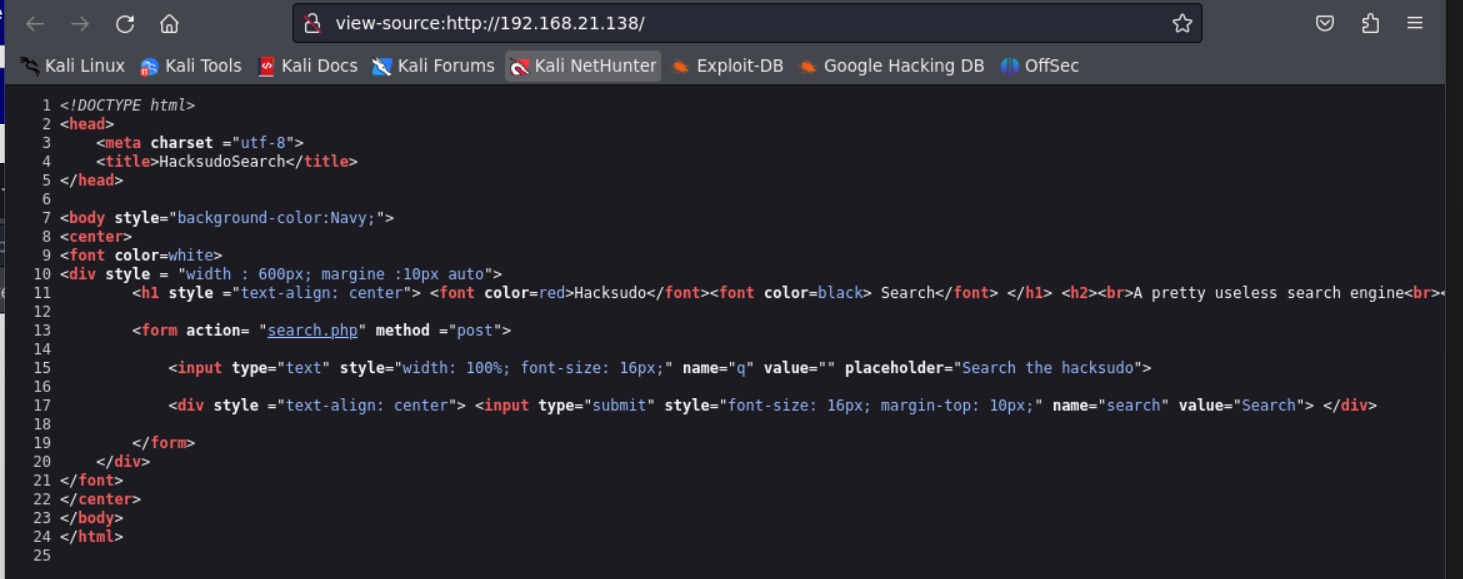


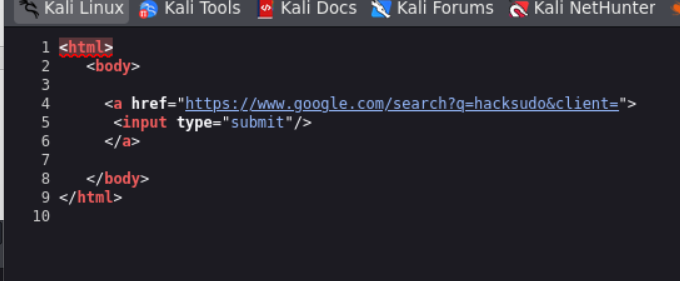


随便输入字符之后发现

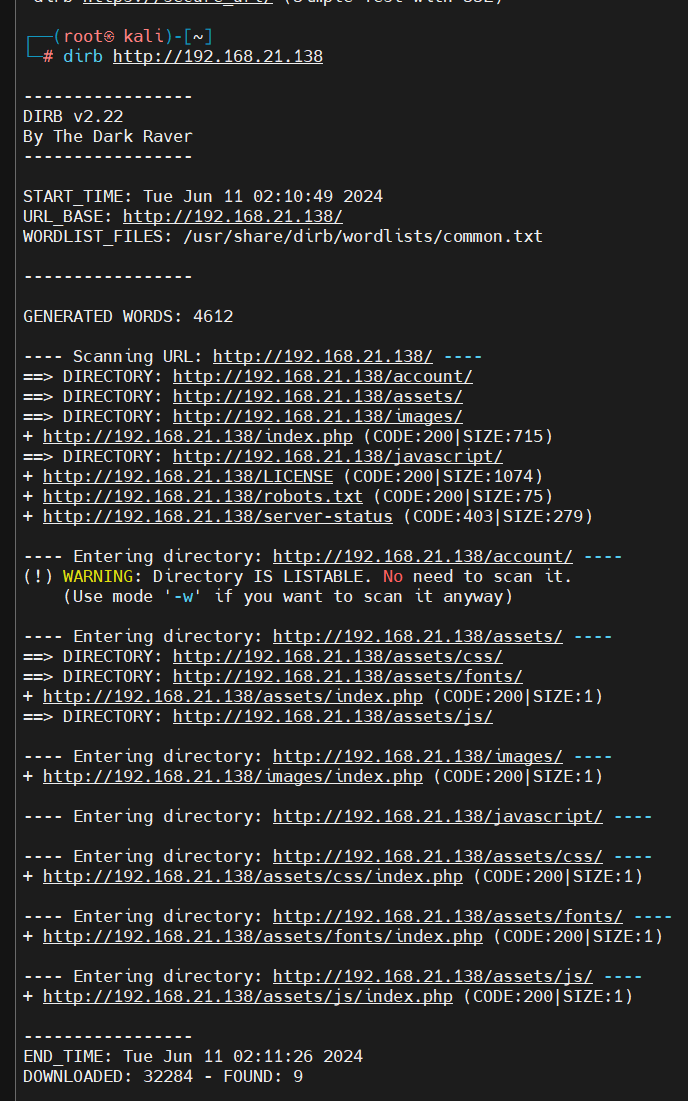


线索断了看一下源代码

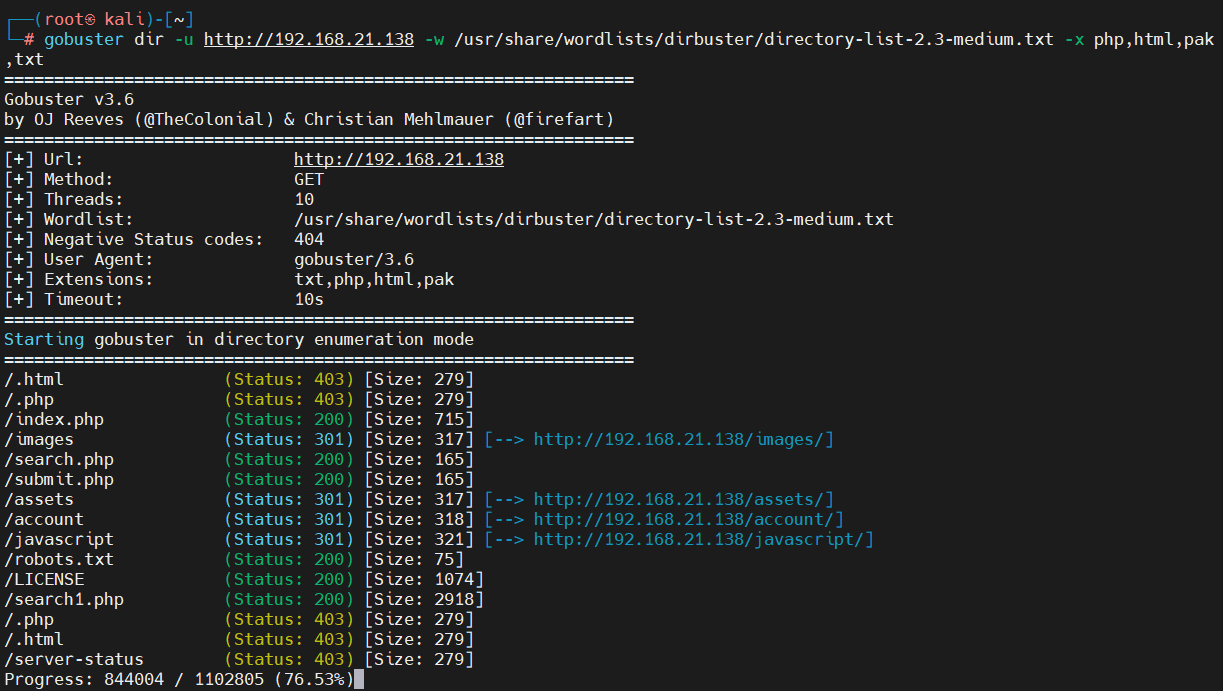




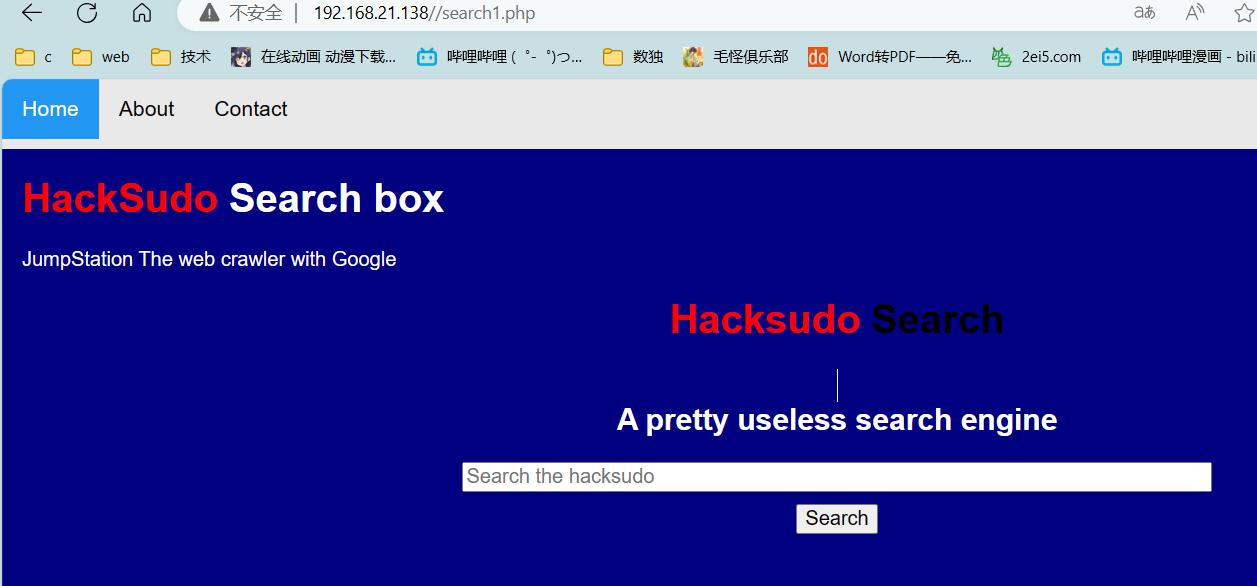
只能去目录爆破

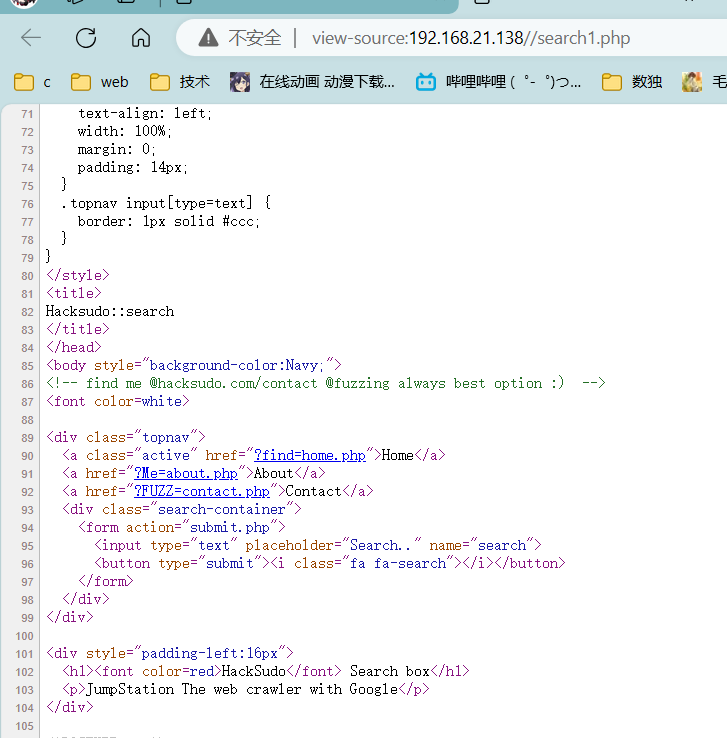


扫出来的没什么用



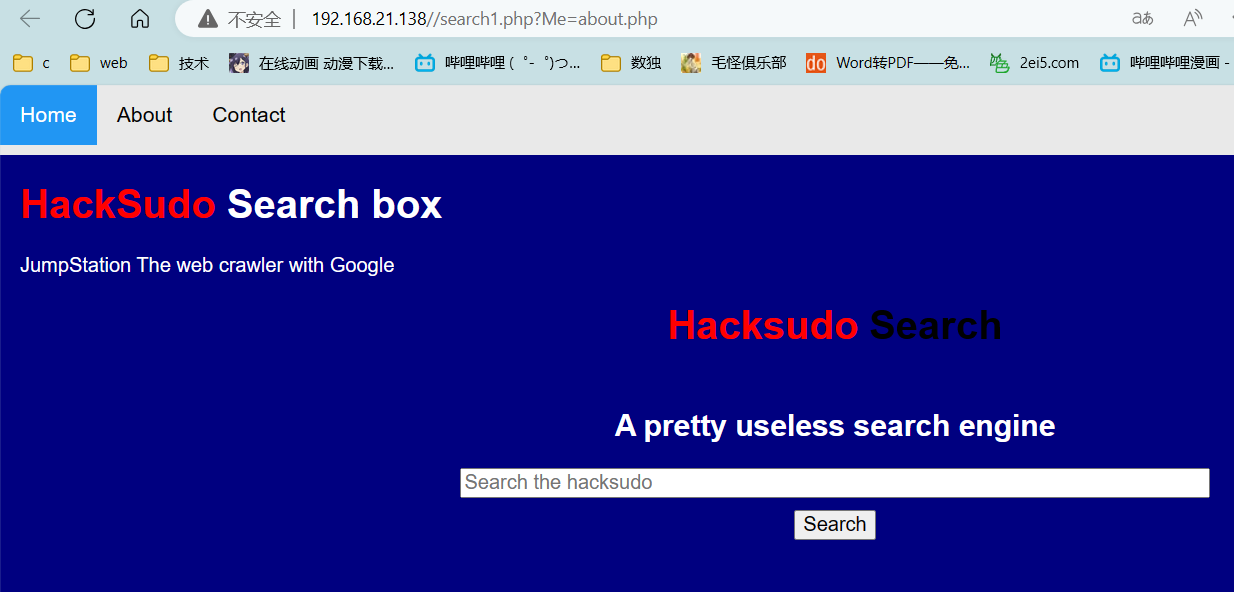
边扫边看



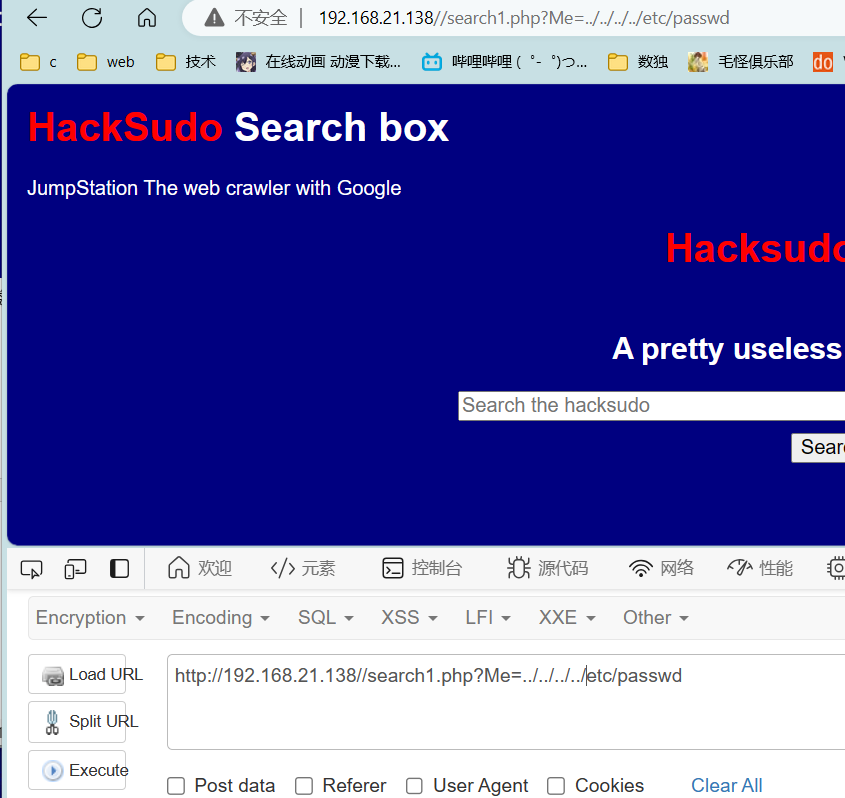


看到点fuzz

不是吧又要扫

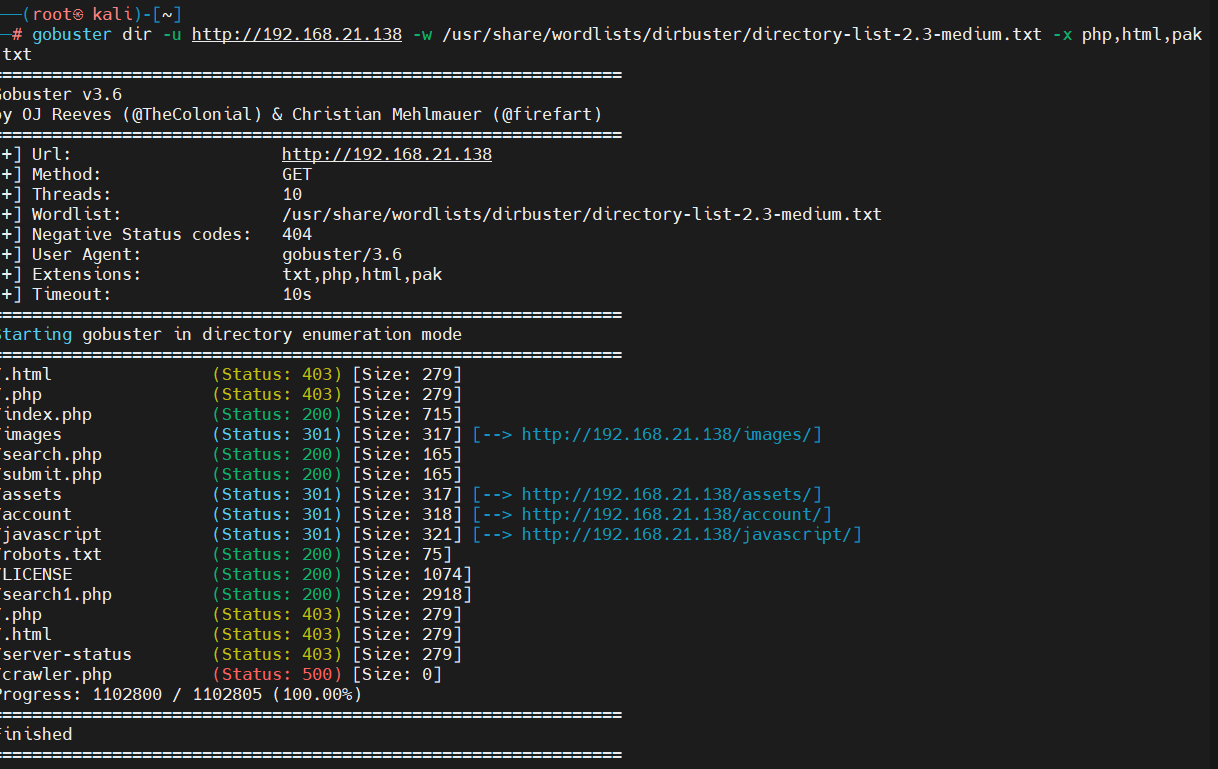


应该没事先试试这个参数

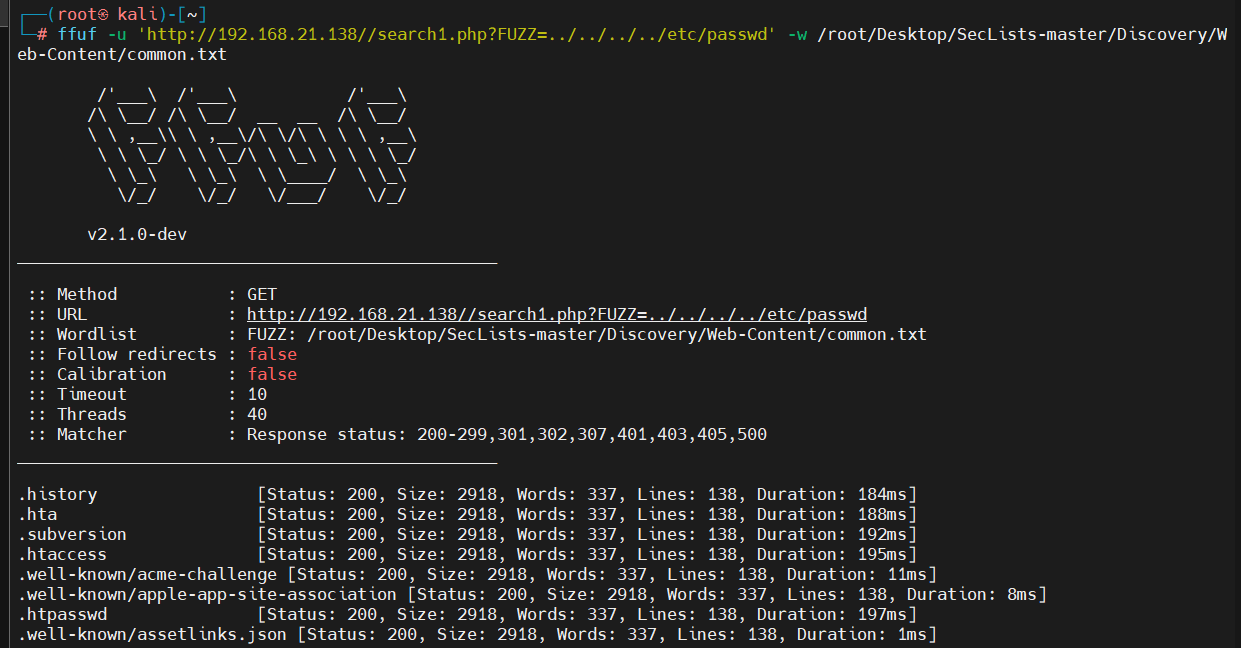


失败了因该是要爆破参数了

这时候目录扫描完了



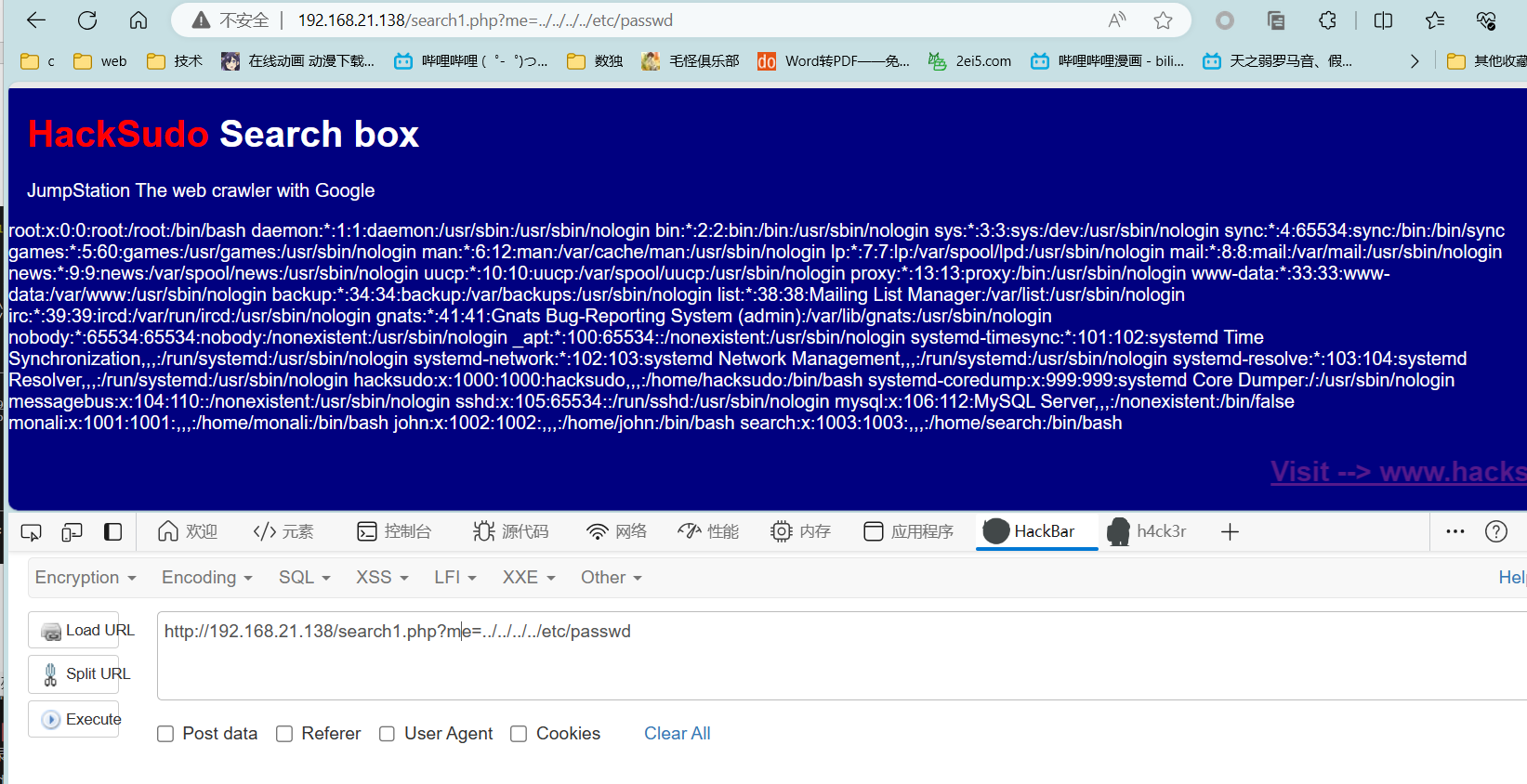
由于参数是开发自己写的并没有利用框架只能用comm试试



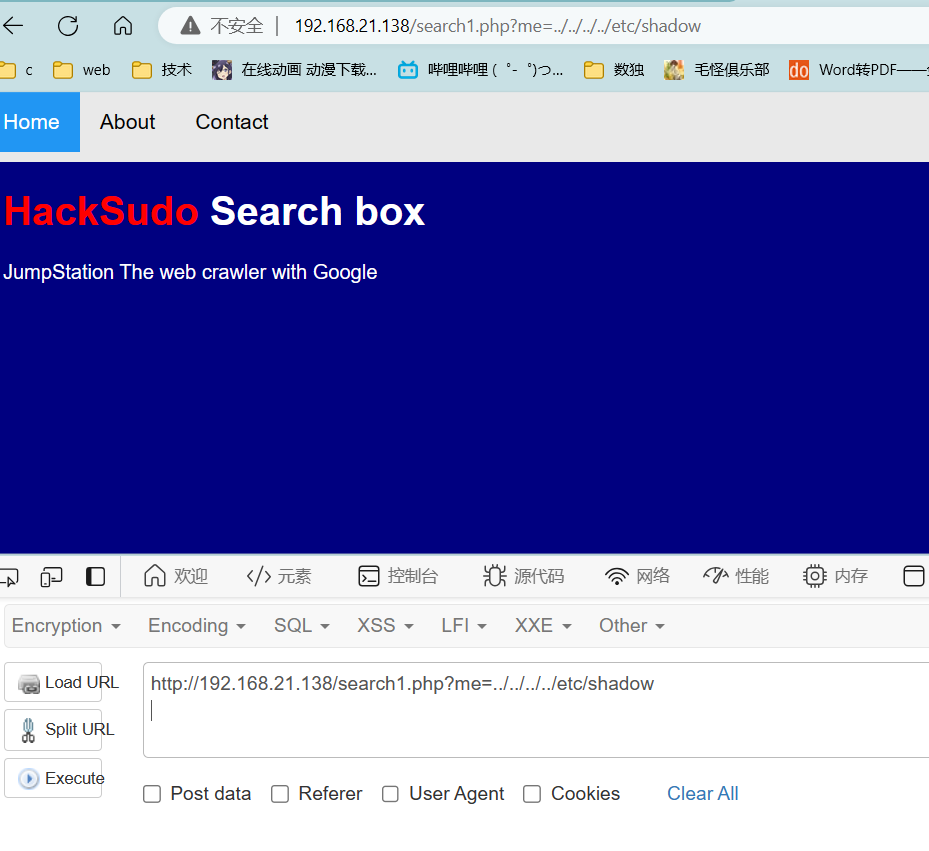
回显太多改一下参数



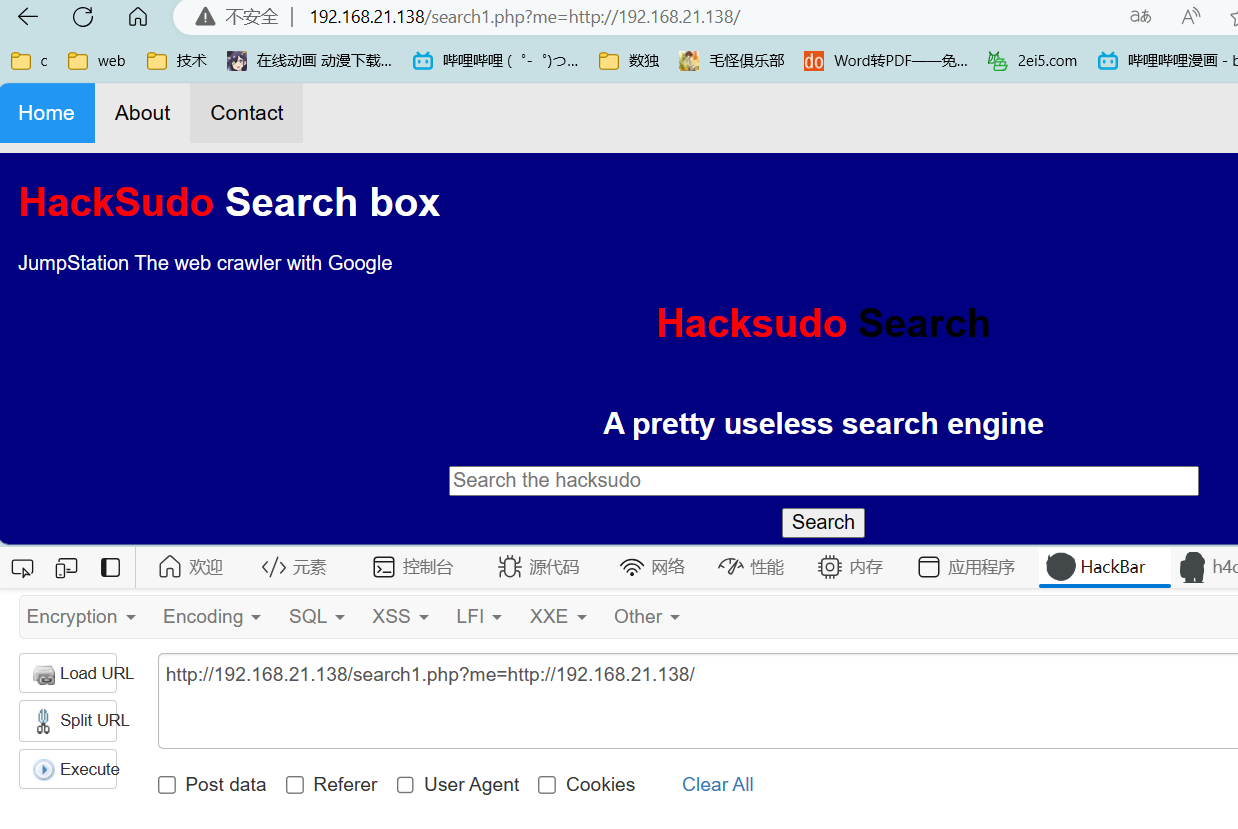
访问看看



小提示看看shadow行不行，不行的话再看远程请求



远程试试

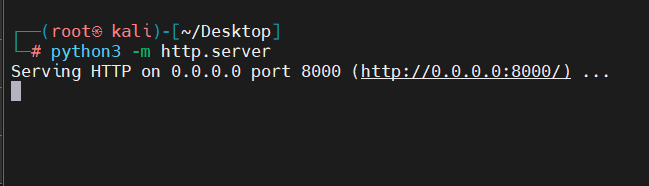


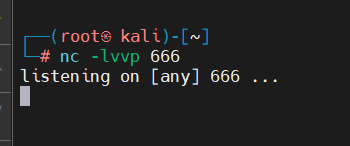
成功了

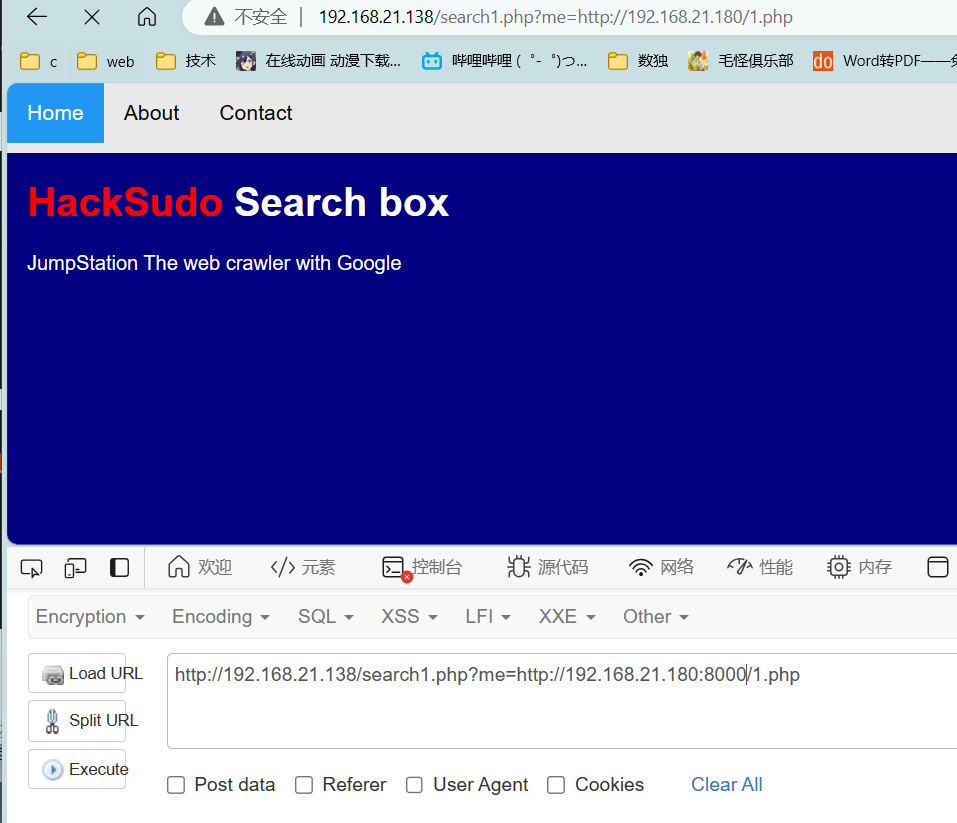
写一个反弹shell

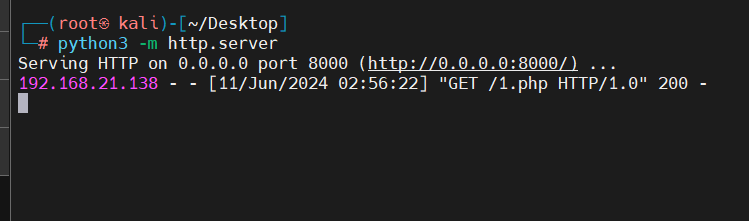


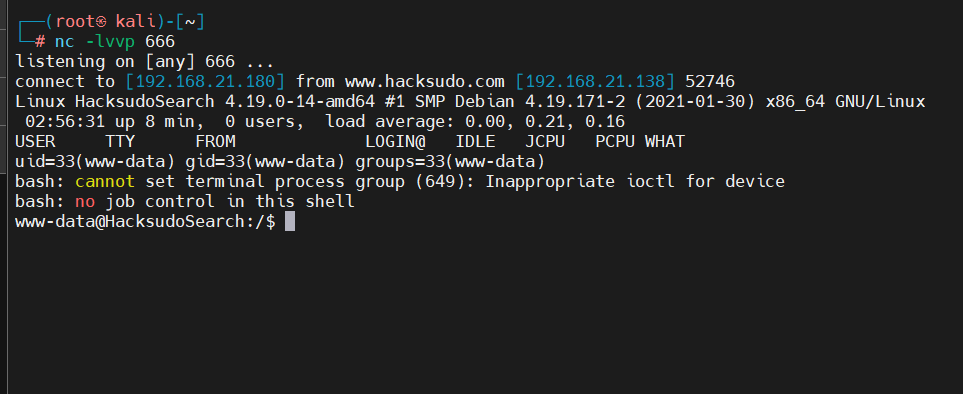
（在线生成就可以）











搞定

提权了

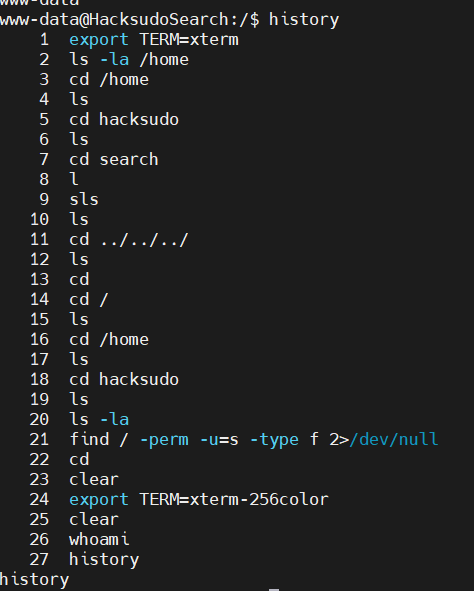
如果出现clear的时候报错

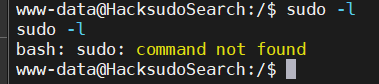
TERM environment variable not set.

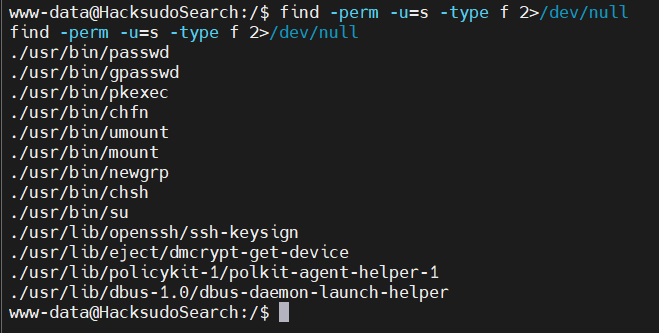
用export TERM=xterm-256color可以解决



信息收集

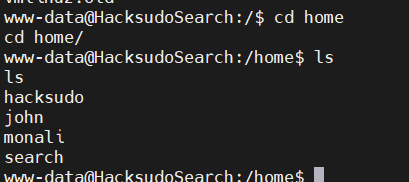




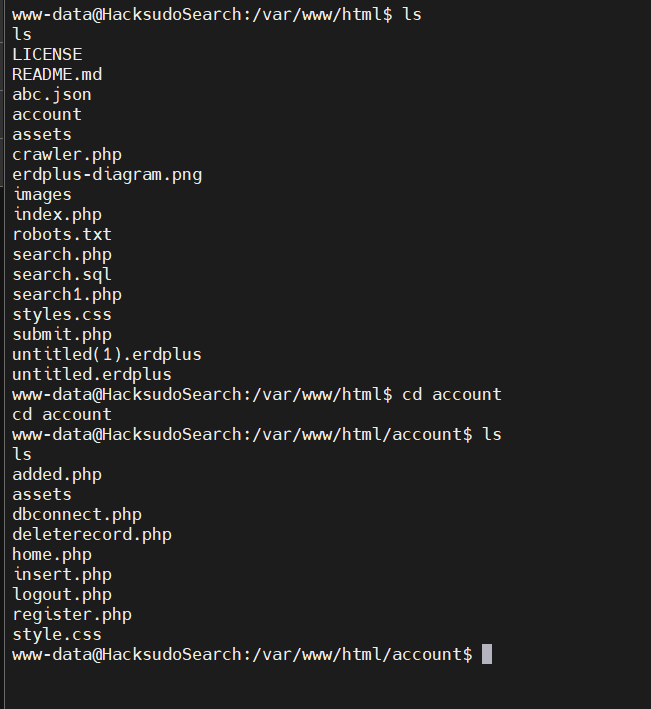


没用

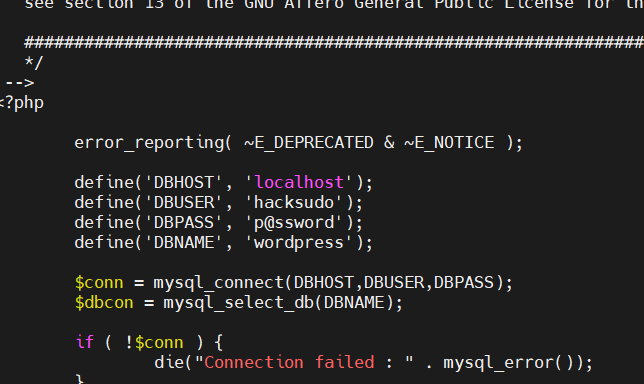
用户信息



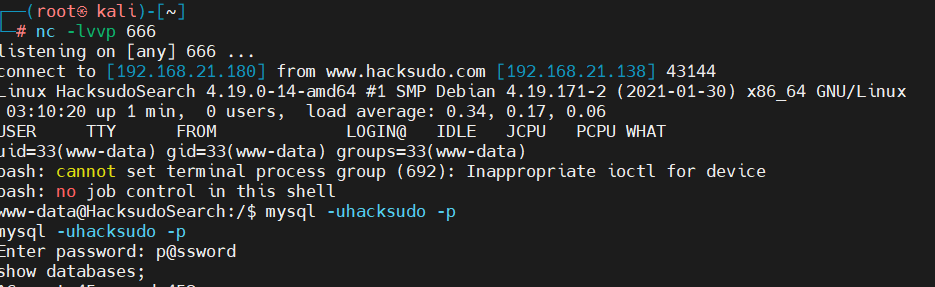
看看web的源码吧



发现其实是有数据库的

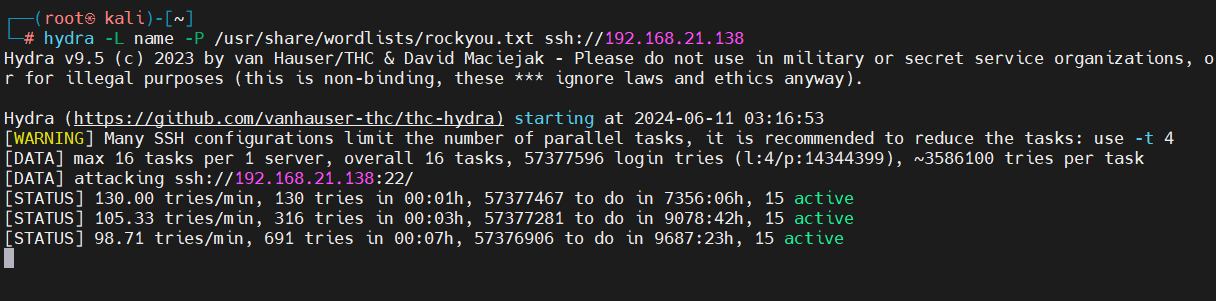


因该只能本地连接了



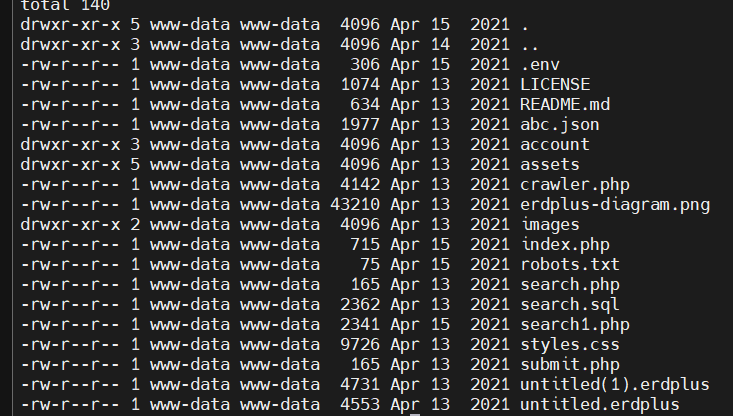
重启多此不回显只能转ssh去看了

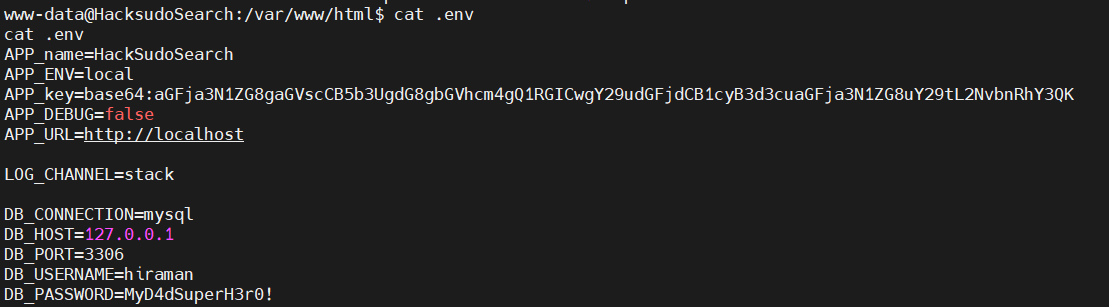
只能进行爆破



太慢了，应该是信息收集不到位

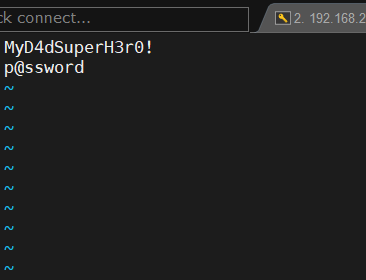
再web这发现点东西

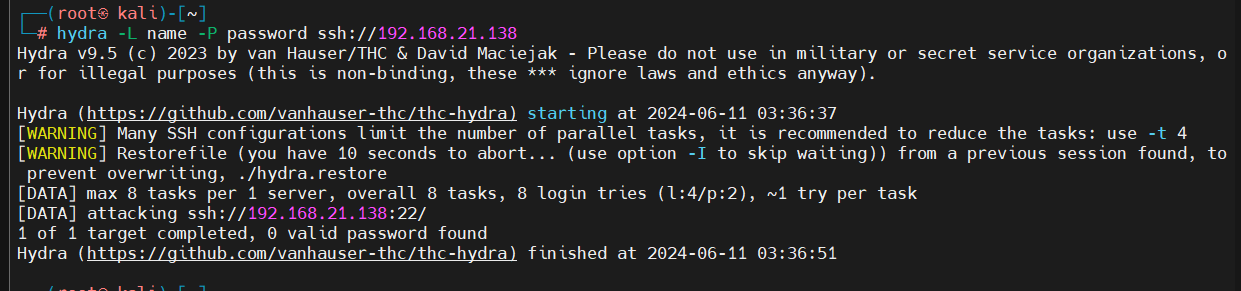




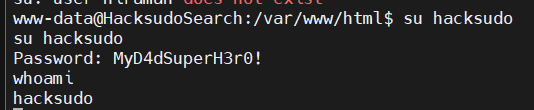
密码出来了

试试撞库



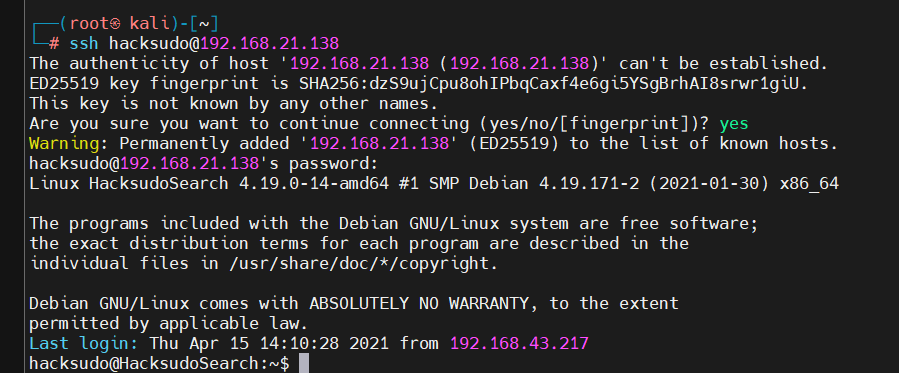


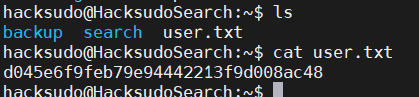
就是爆破不出来



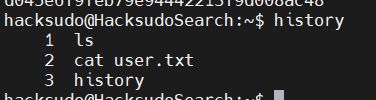
但是一个个试的时候密码确实没有问题

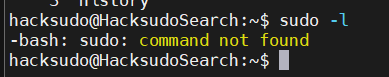
连接ssh

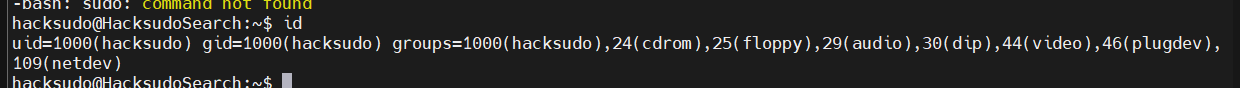


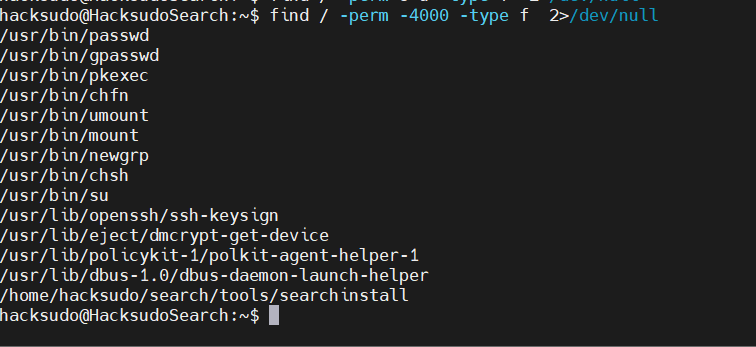


信息收集

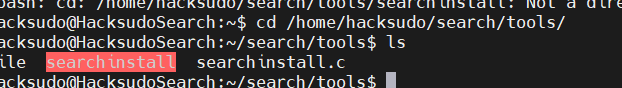




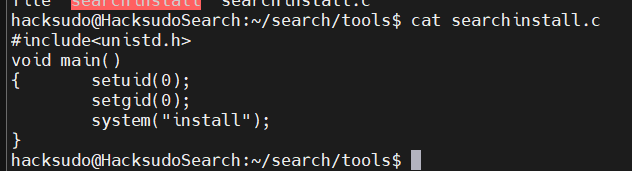




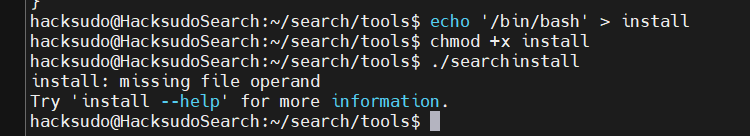
不正常的是home这个



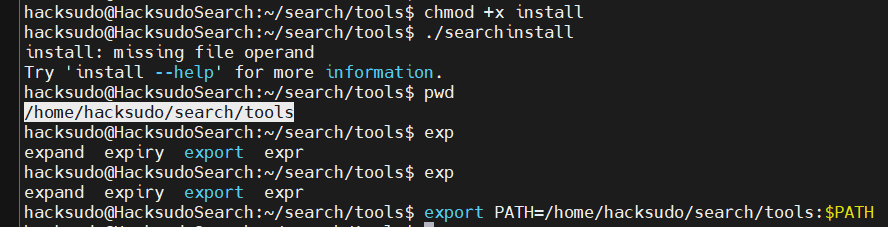
看看源码



这个是将install改成root权限，那么加上bash就可以提权



要把install加入环境变量





结束

