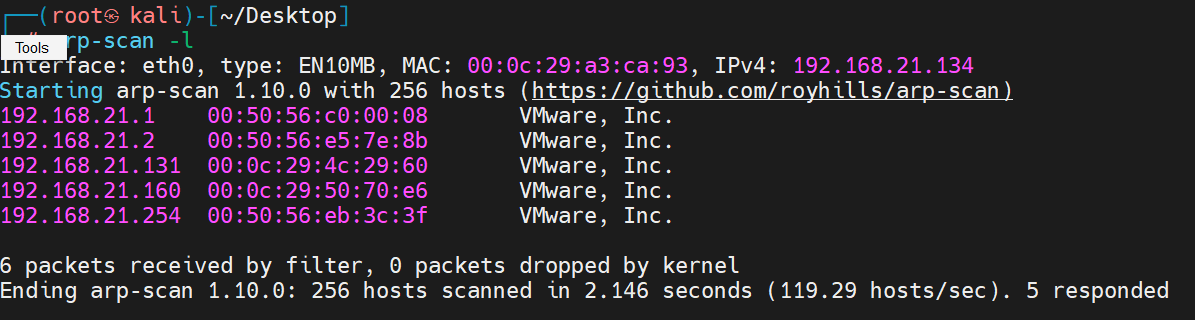
Hack\_Me\_Please

下载地址：<https://download.vulnhub.com/hackmeplease/Hack_Me_Please.rar>

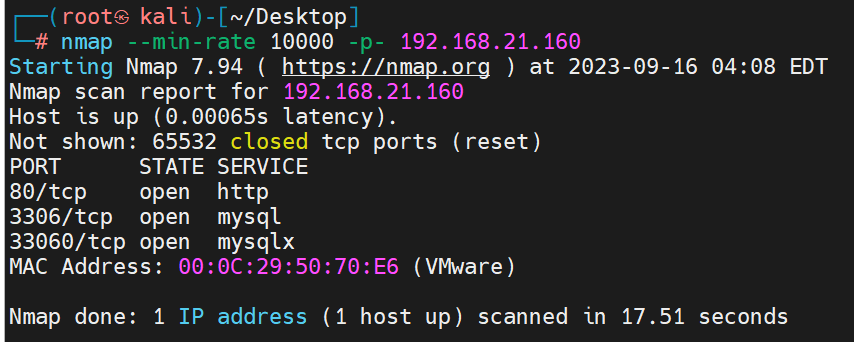
主机发现



目标192.168.21.160

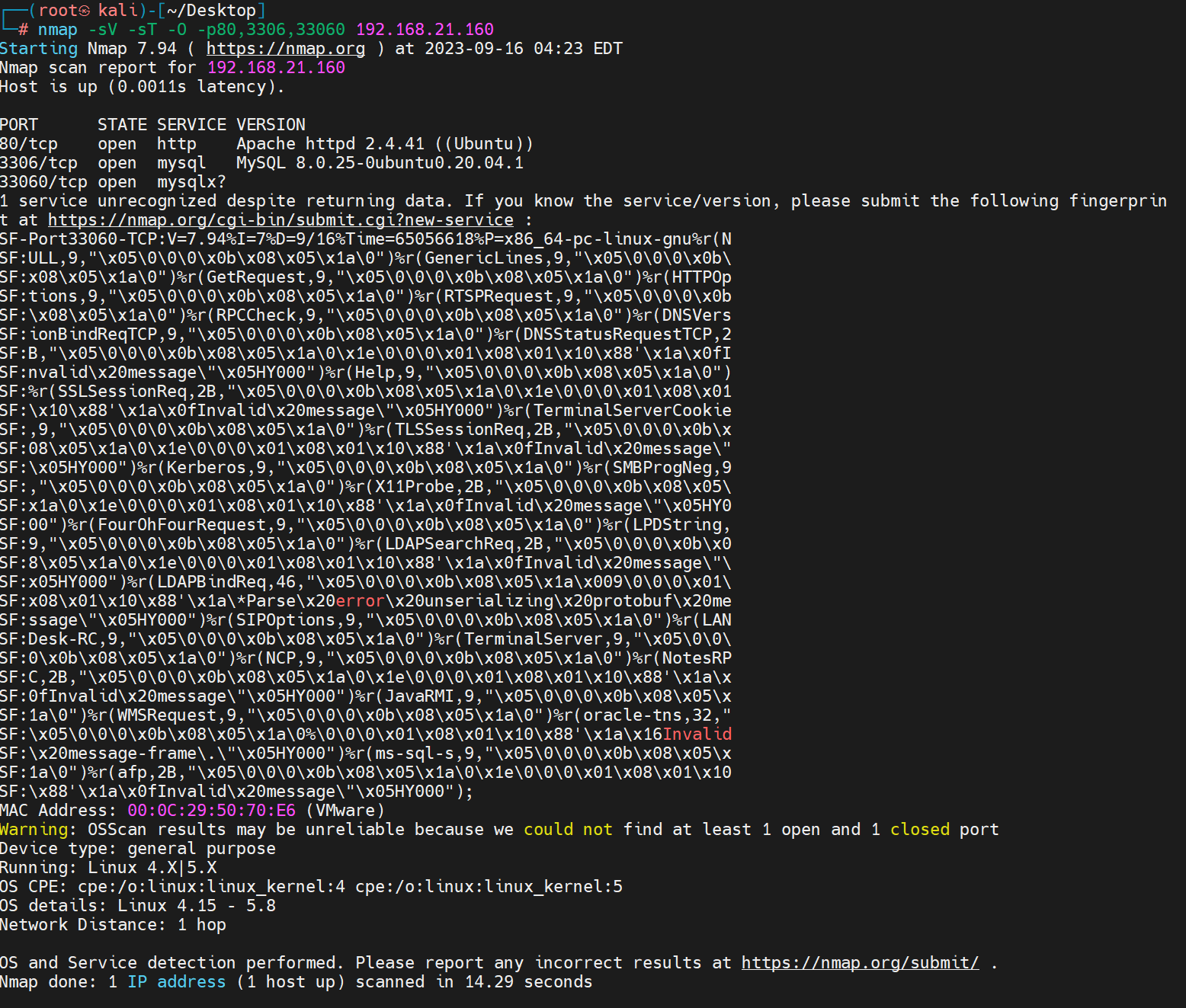
端口扫描

nmap --min-rate 10000 -p- 192.168.21.160



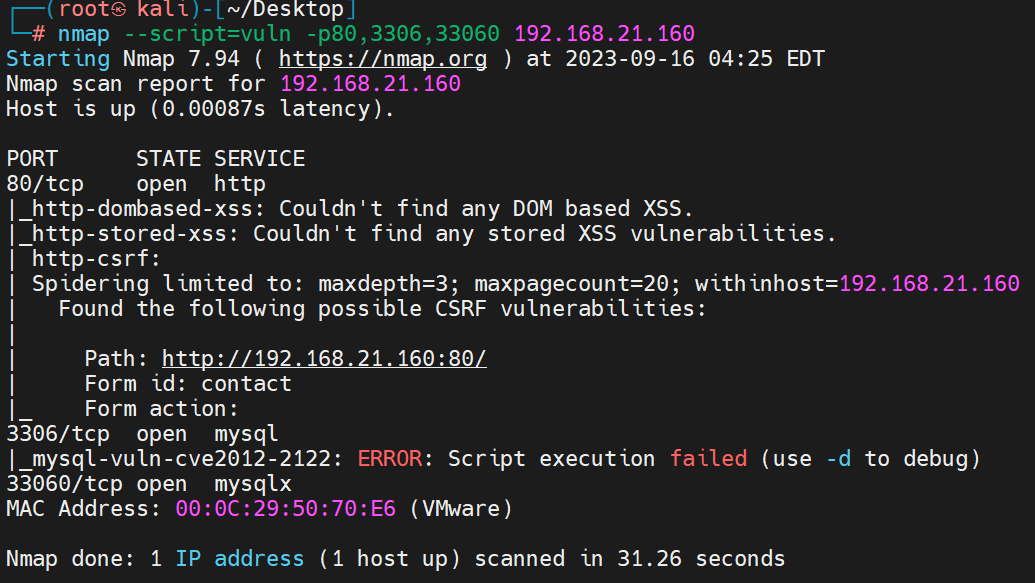
服务扫描

nmap -sV -sT -O -p80,3306,33060 192.168.21.160

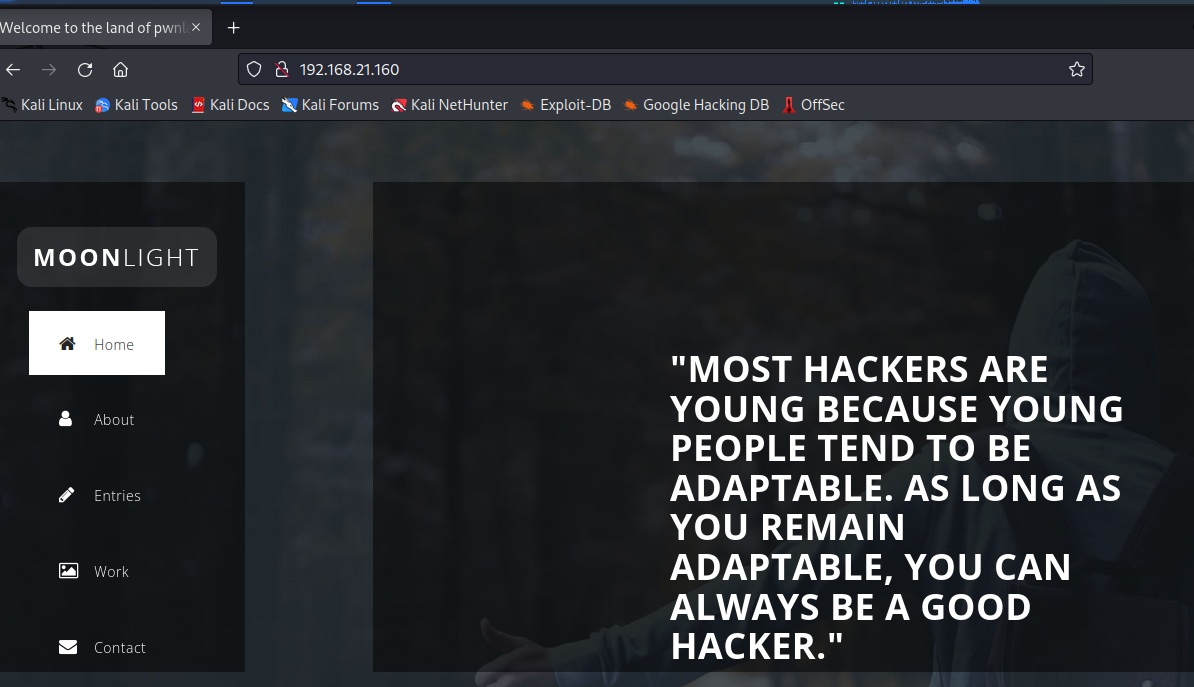


漏洞扫描

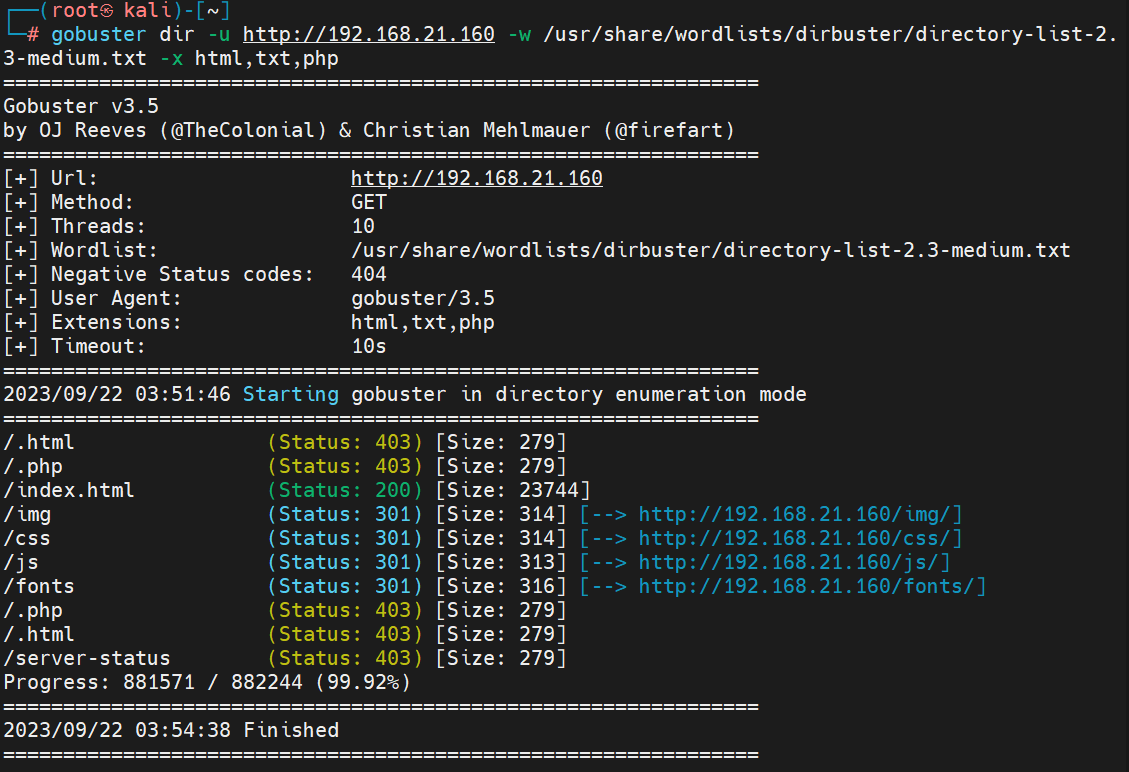
nmap --script=vuln -p80,3306,33060 192.168.21.160



先去看web

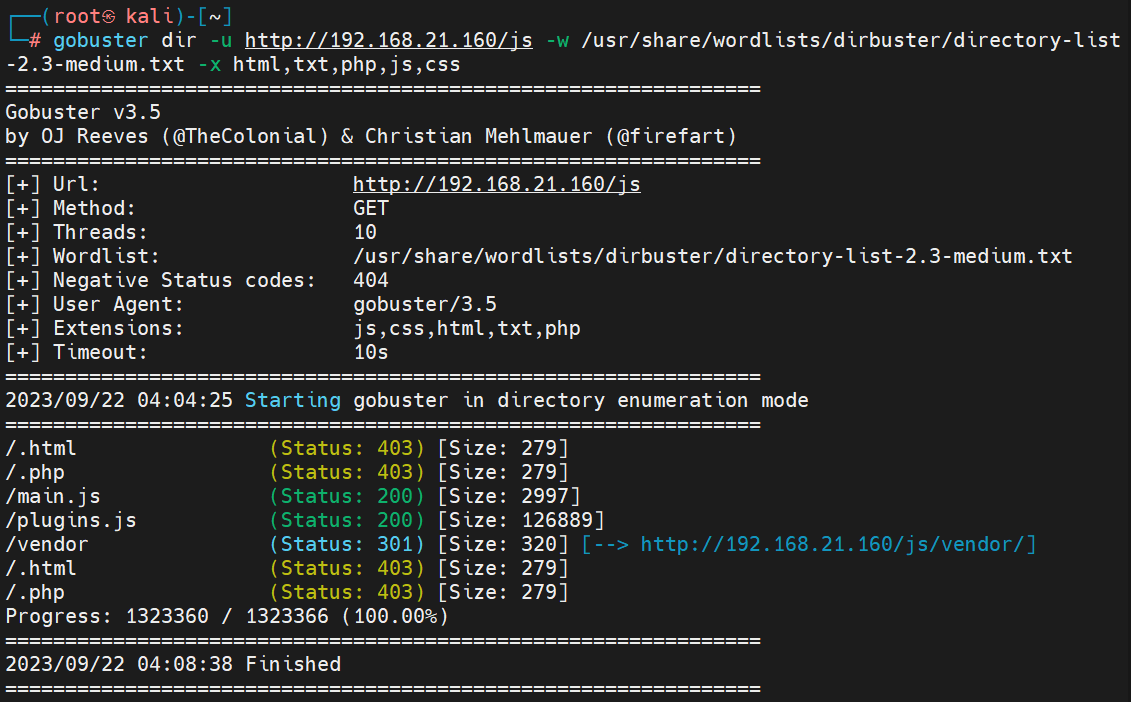


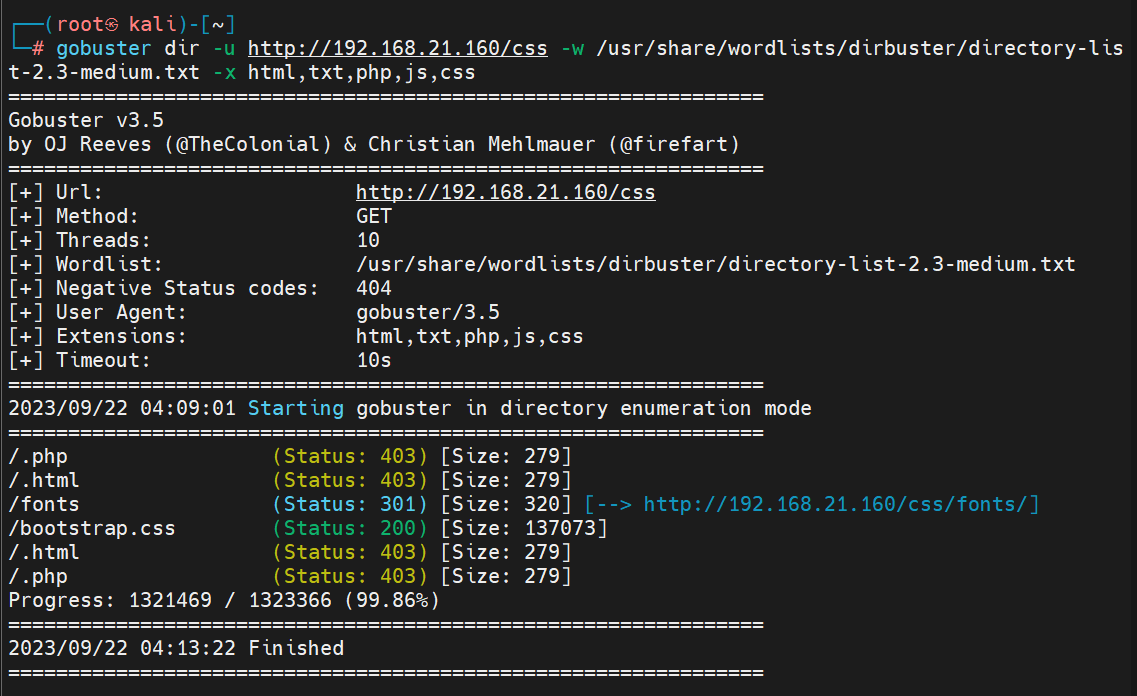
先做一个爆破目录

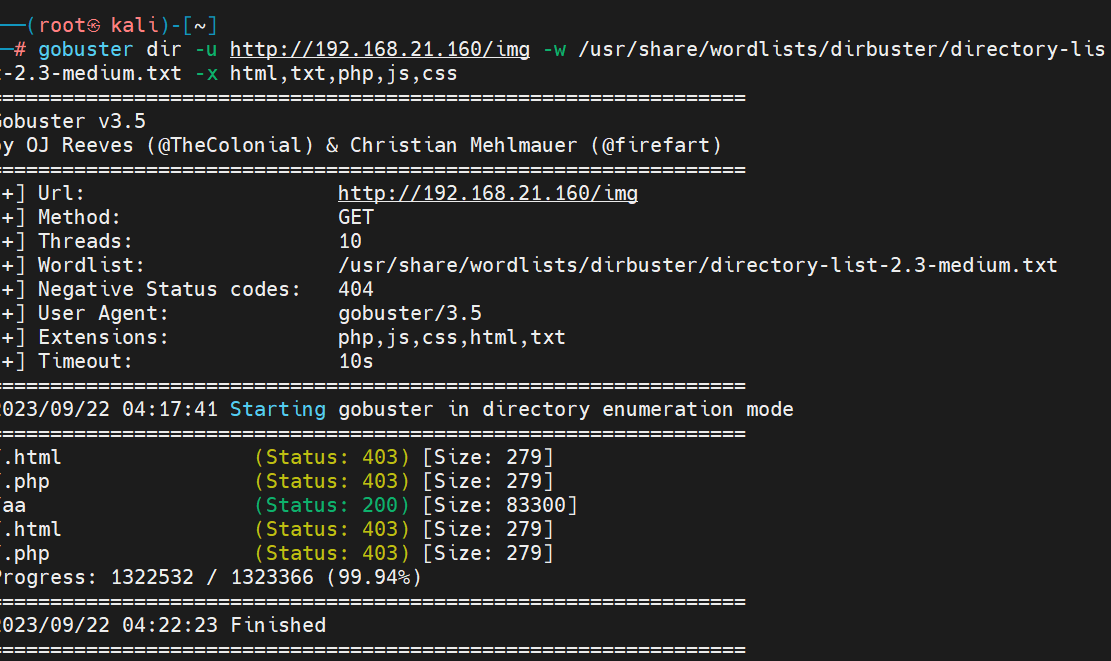


这里面都挺正常，接着往下面扫吧

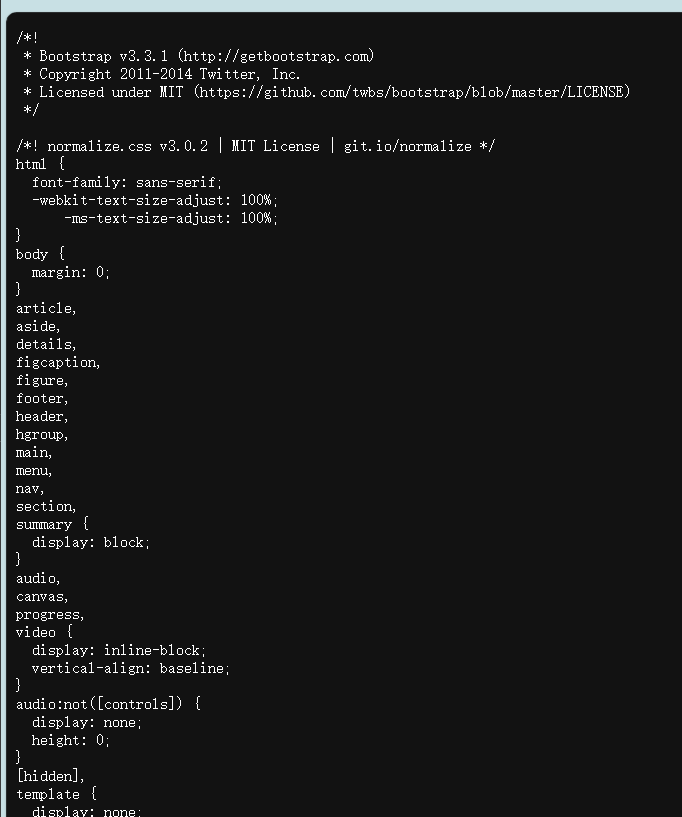
先去js看看







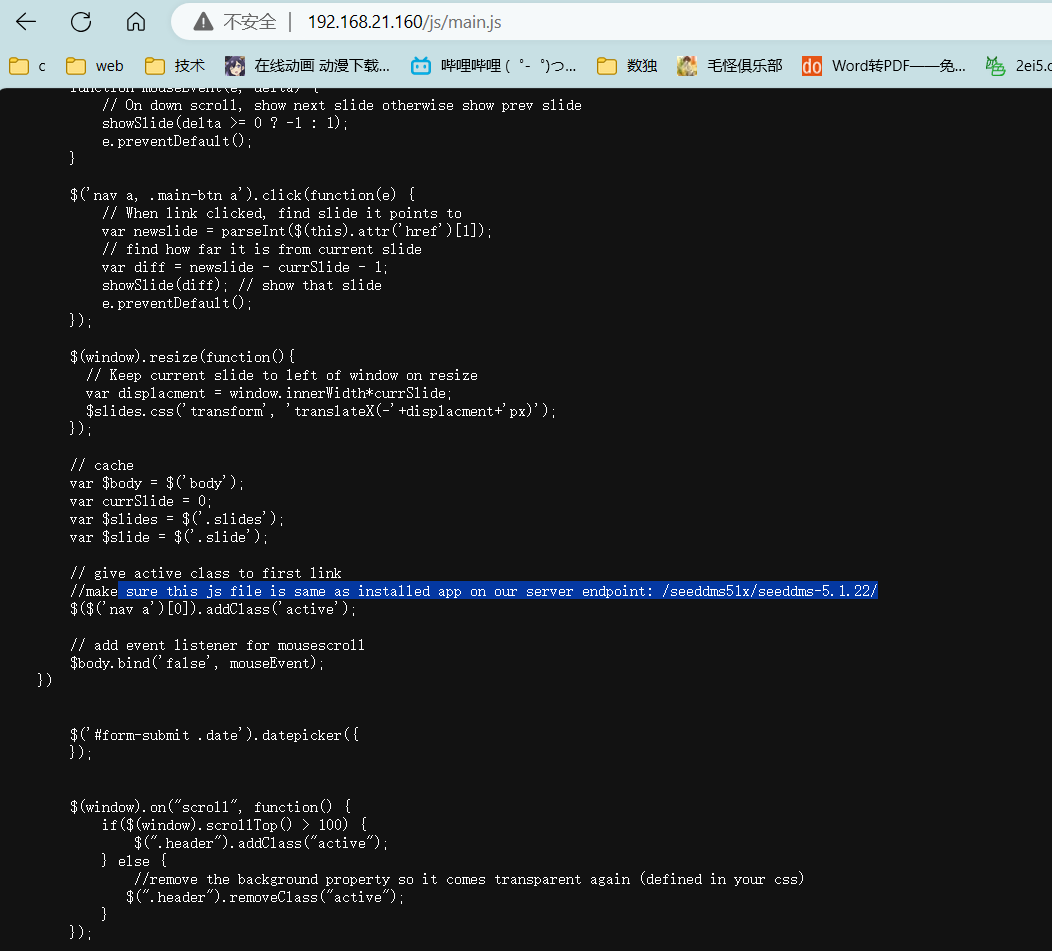
css



这里是利用的github的源码

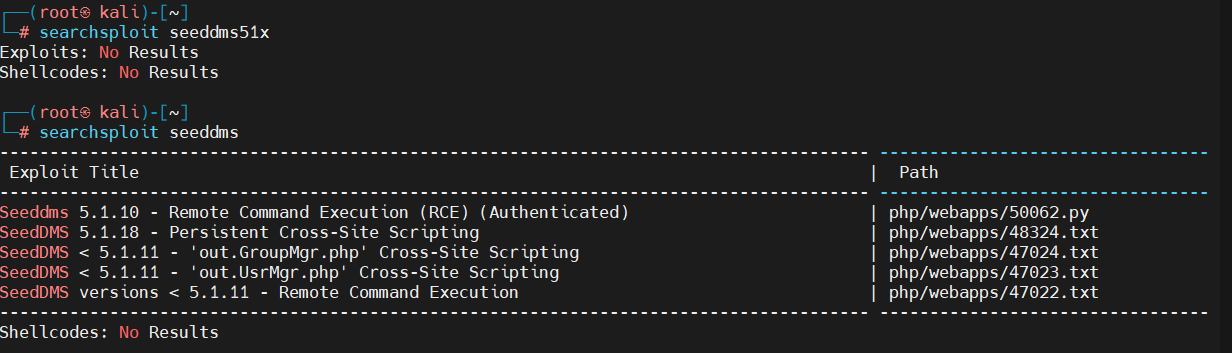
等等再看看看别的

js

****

注意高亮位置

这里疑似网站的cms



还真是，接下来注意版本

5.1.22的文件夹不一定是正确的版本

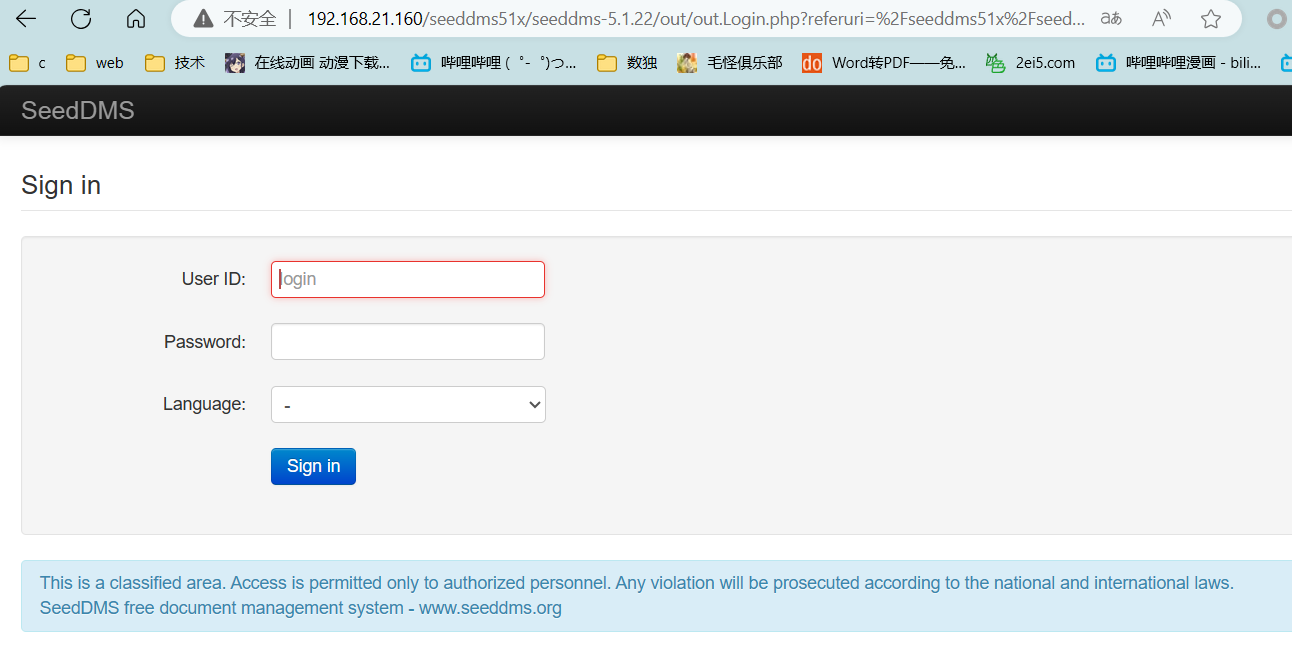
web搜一下



不太行

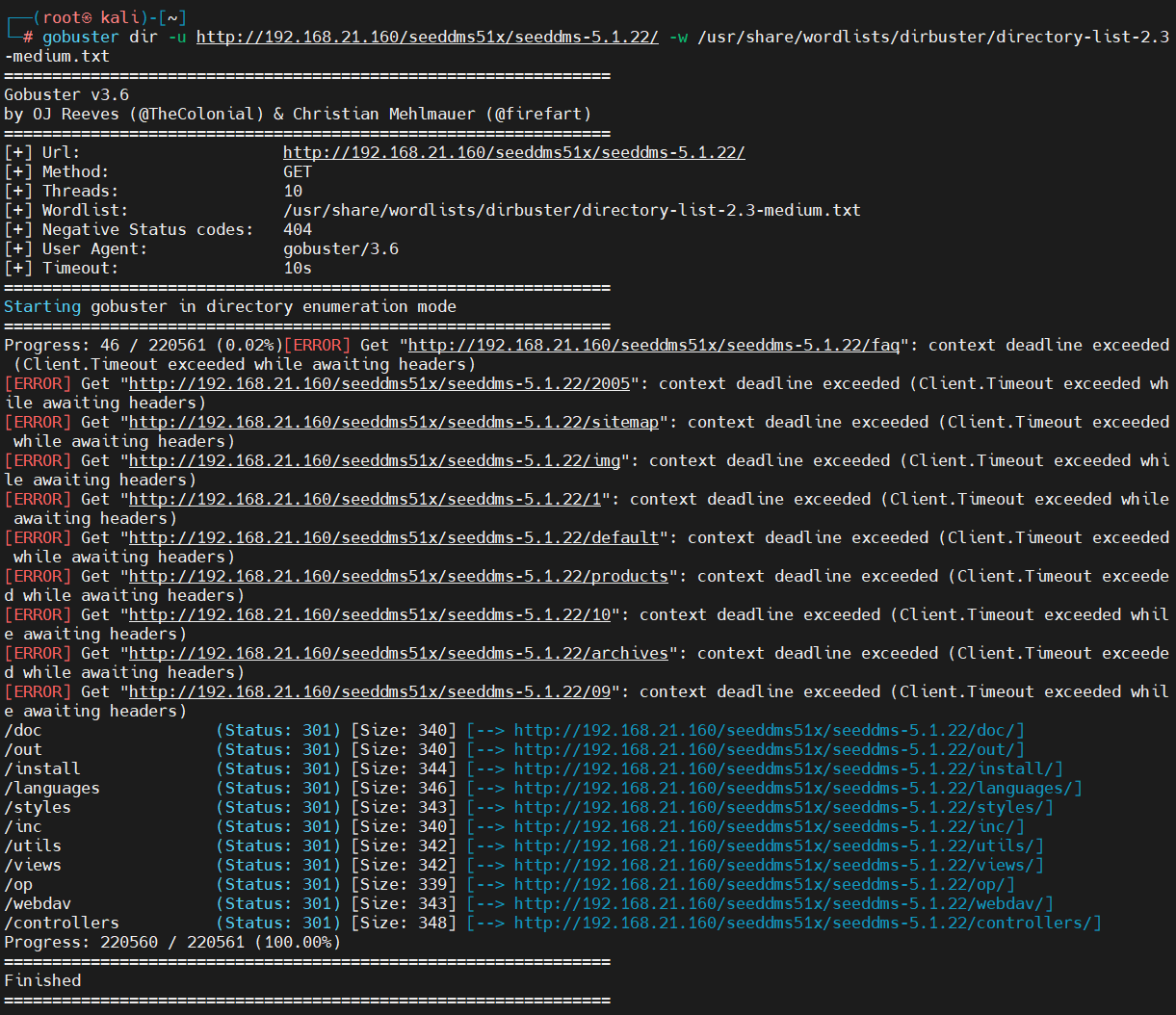
没有什么信息还是扫描一下网站

直接访问的话

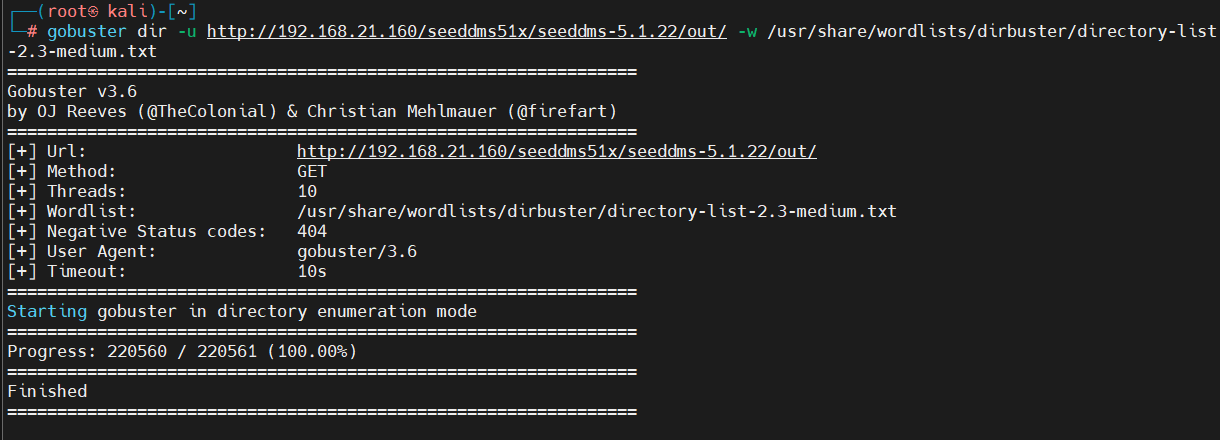


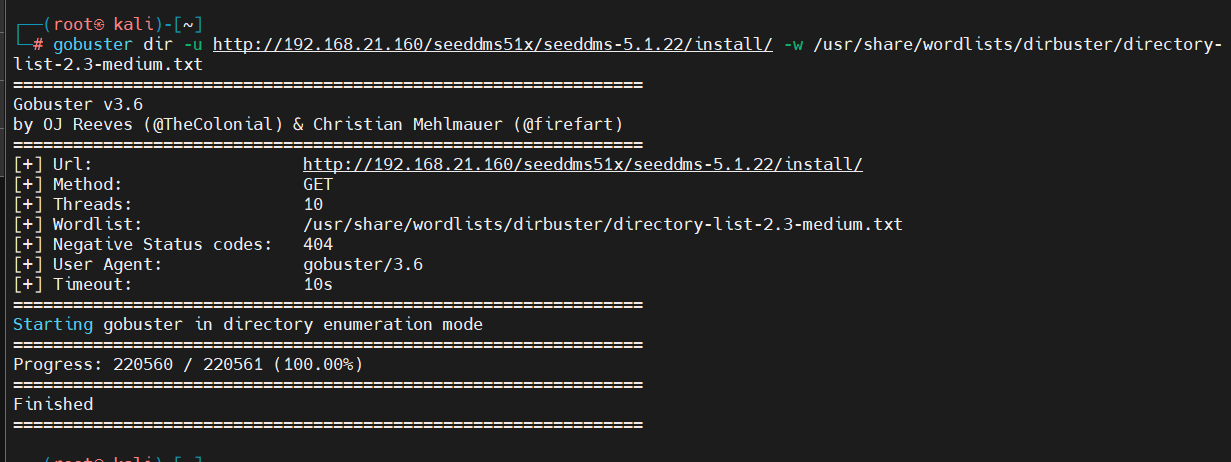
是一个后台登入界面

扫一下吧还是



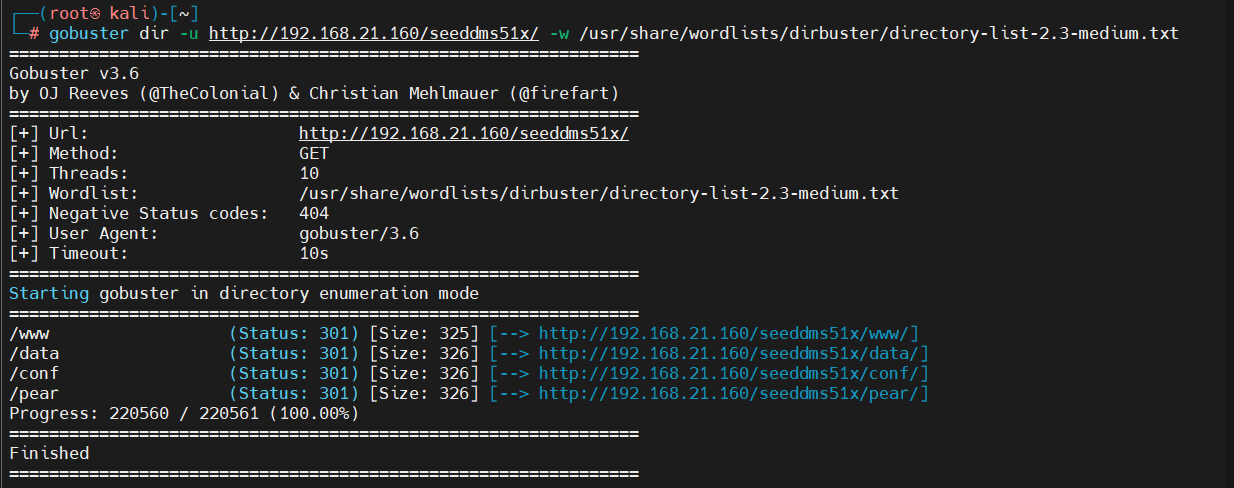
目前有两个想法一个是out文件夹的内容一个是install的内容



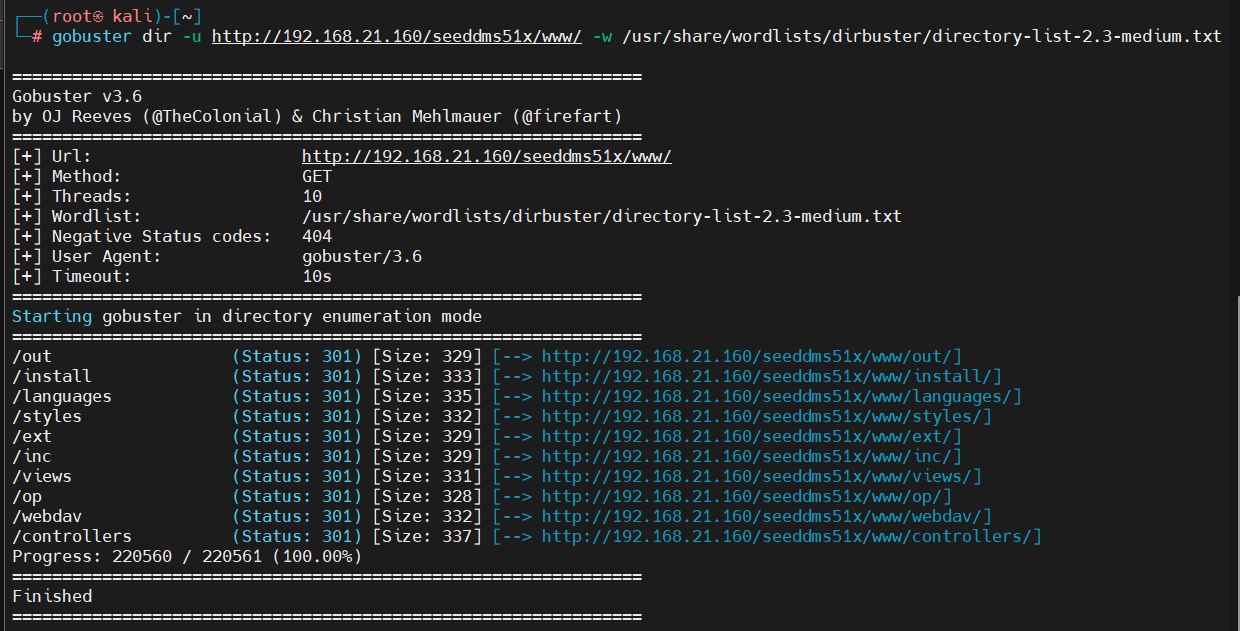


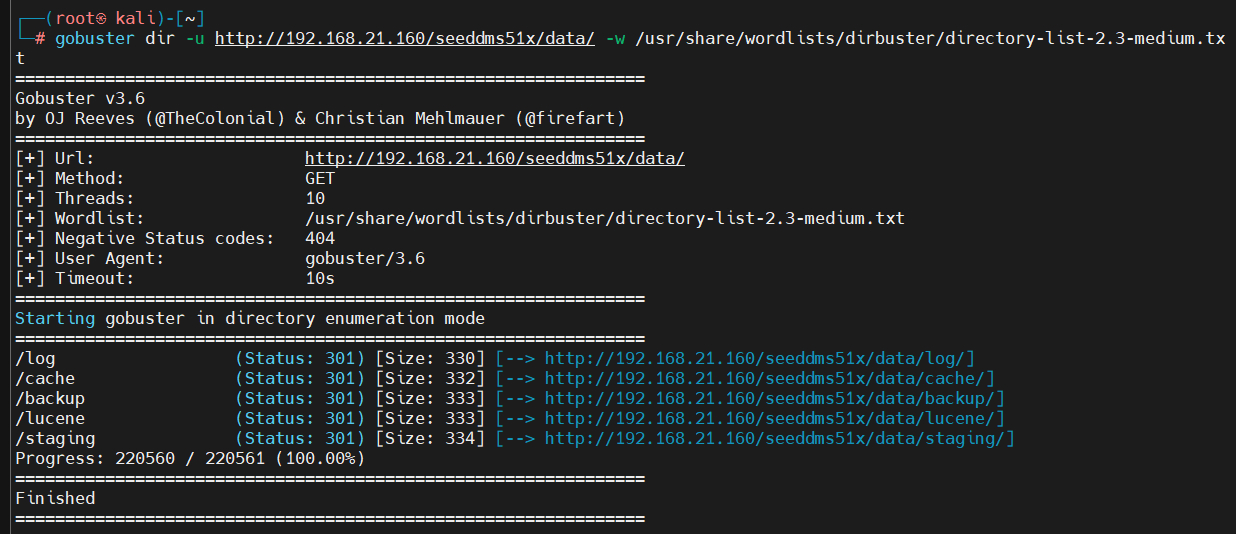
卡住了，但是发现一个疑点这个cms不因该没有config文件

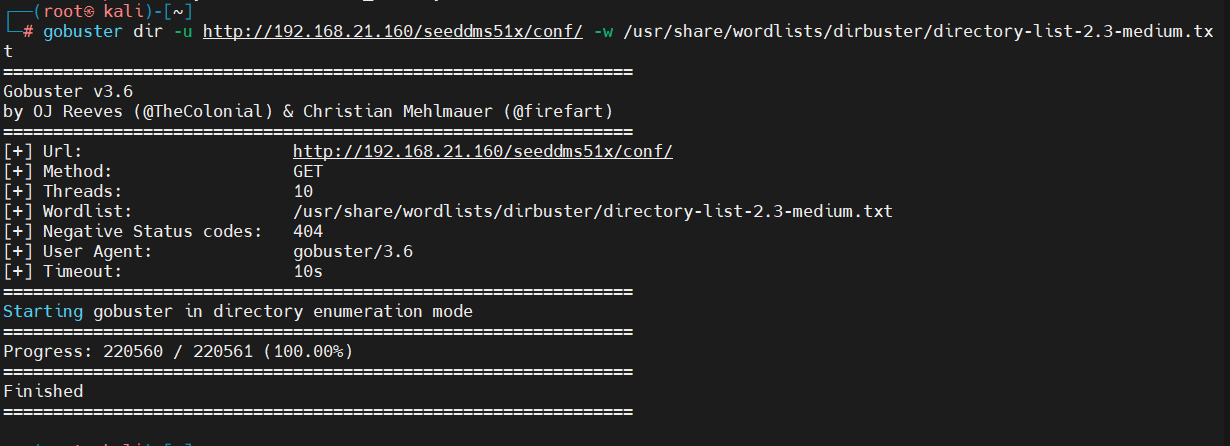
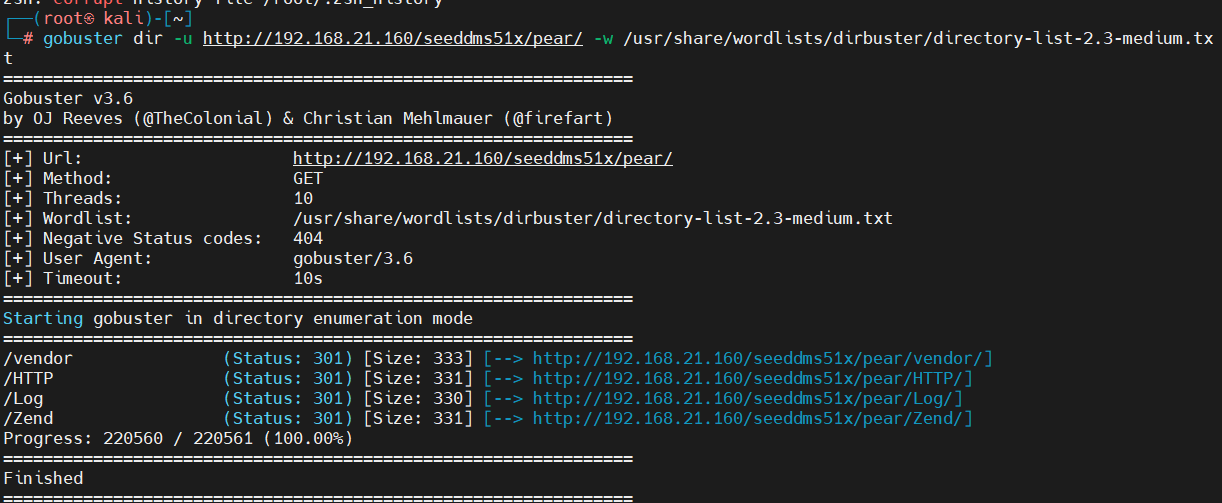
扫一下前一个目录（如果这个不行我们就搭一个）



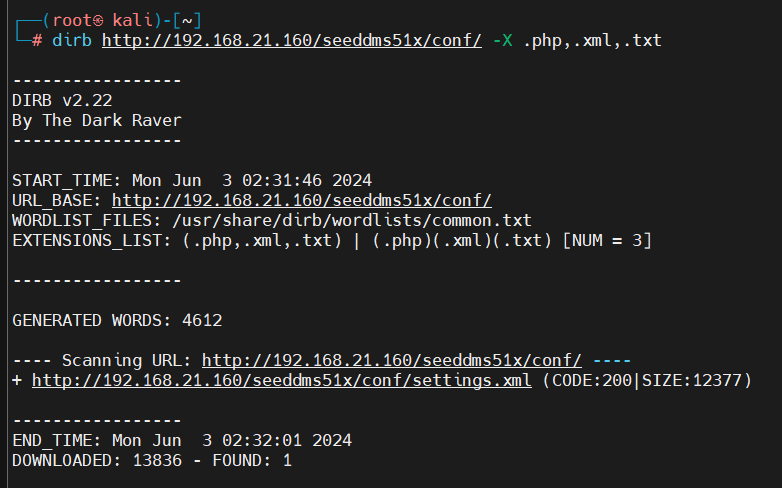
都扫一下吧



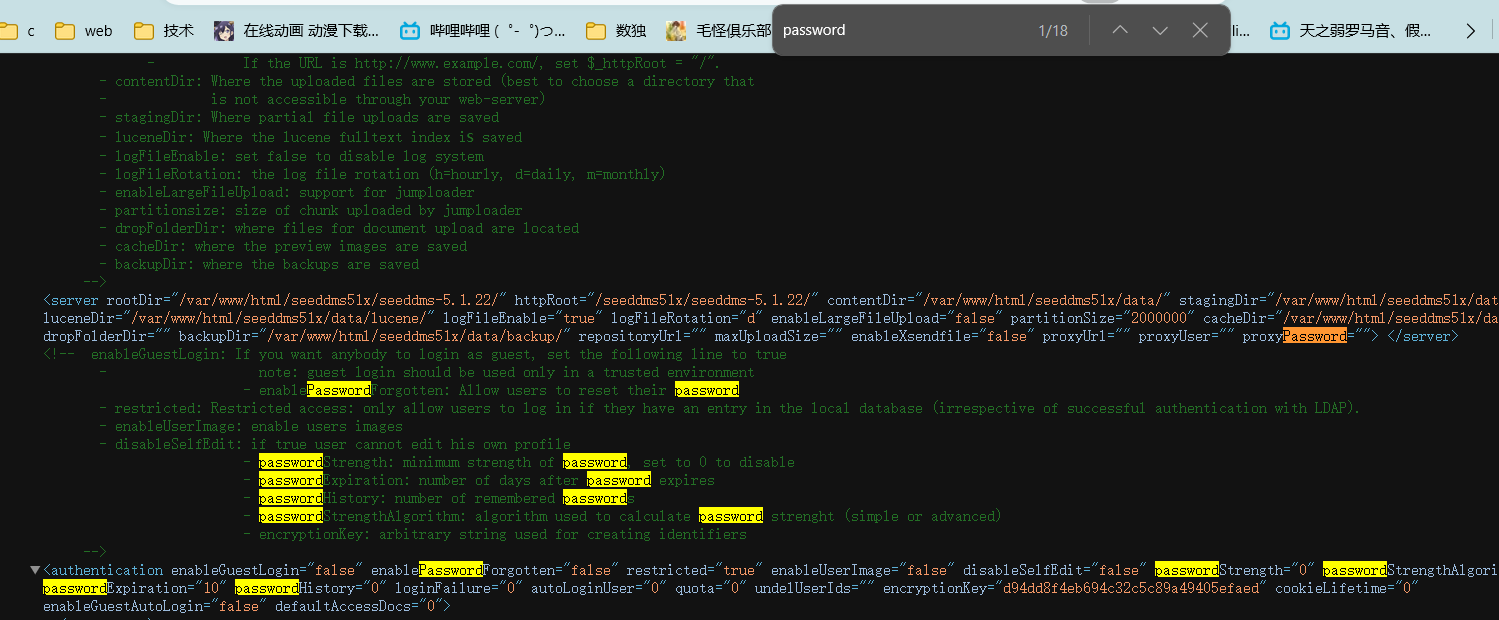


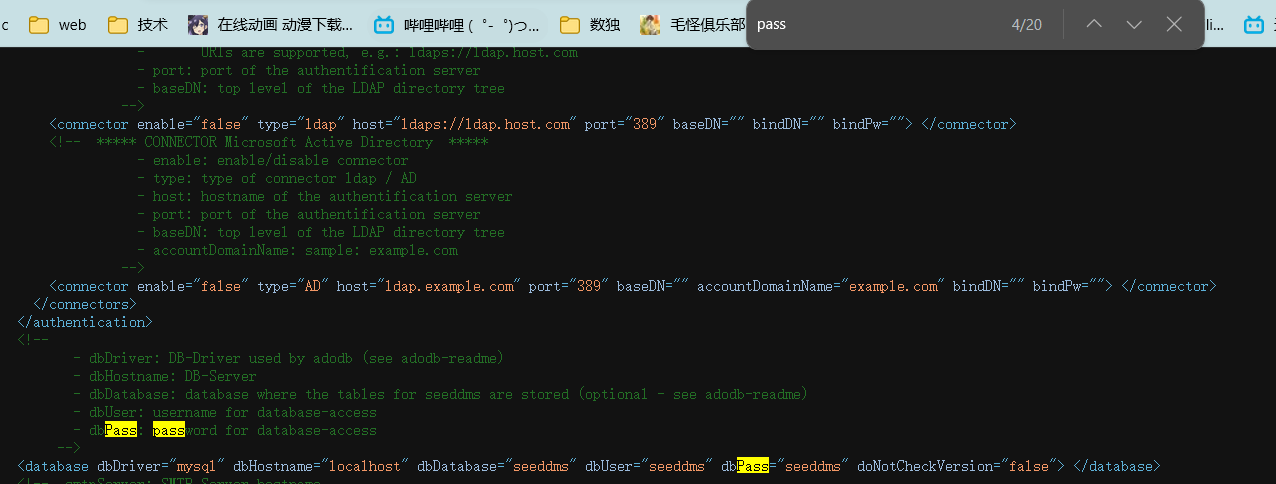
发现conf什么都没有换个扫描工具看看



看来没猜错要加后缀



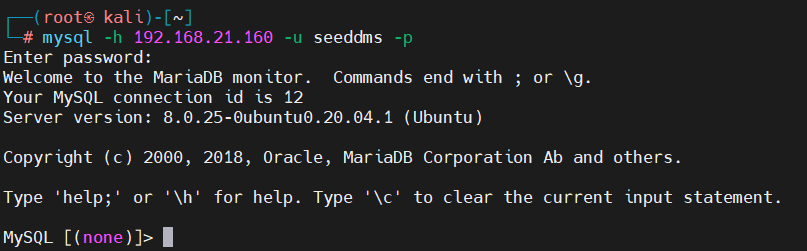
再筛选一下（太精细了）



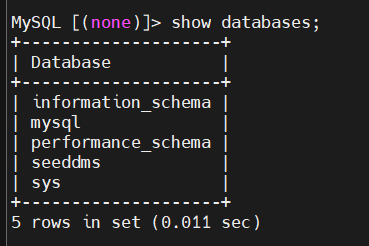
注意图片底

数据库账号到手

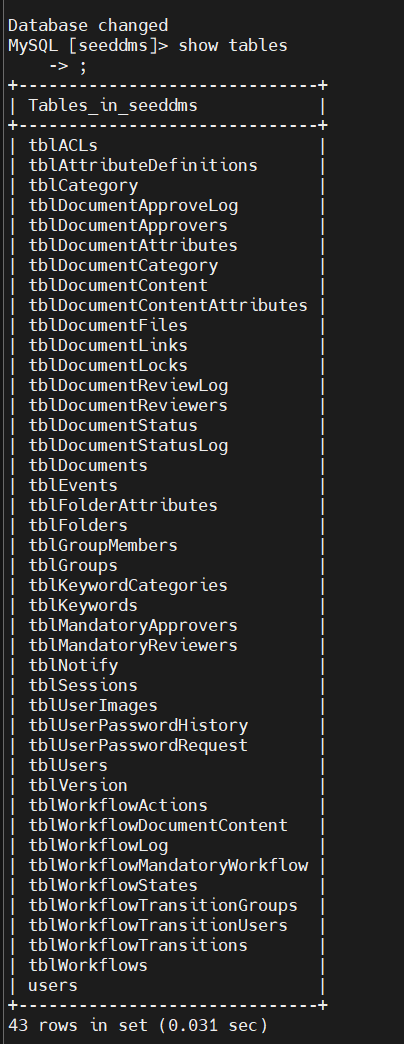
前面扫描到3306那么就远程连接



这里面就只剩下找密码了



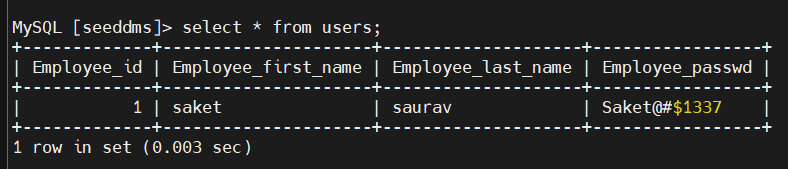
目标是seeddms



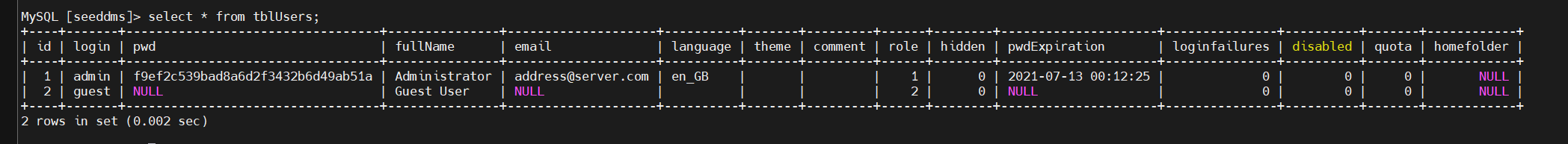
查询users咯

有两个表都看一下

我先看users

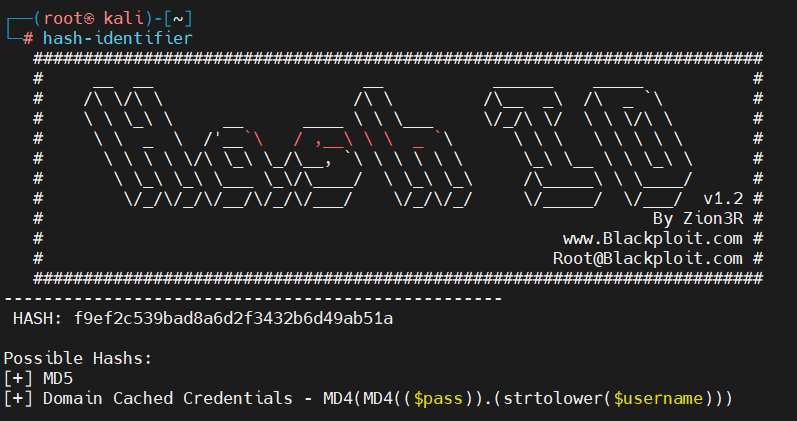


那就是另外一个

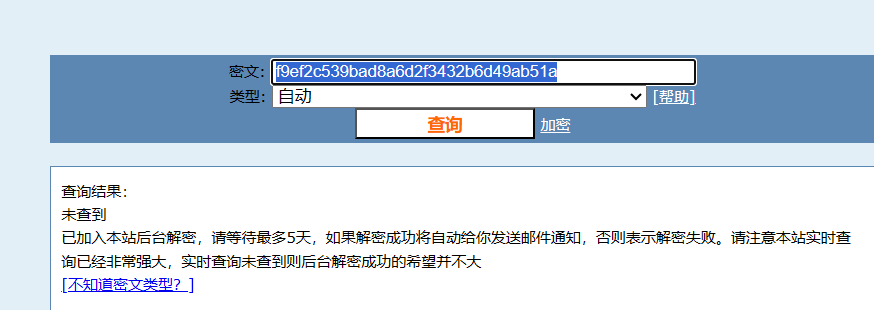


好东西，密码应该是md5加密

去检测一下

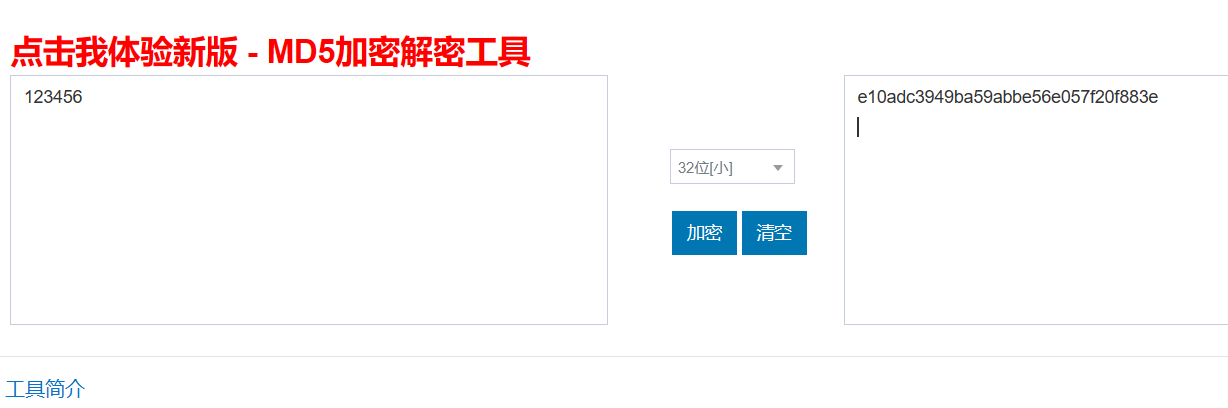


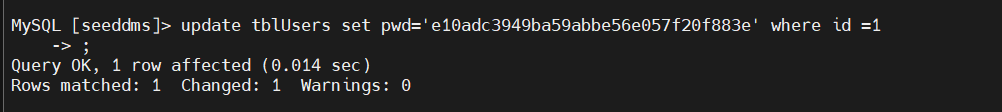
去web检测一下



好吧试一下吧

直接修改密码就行



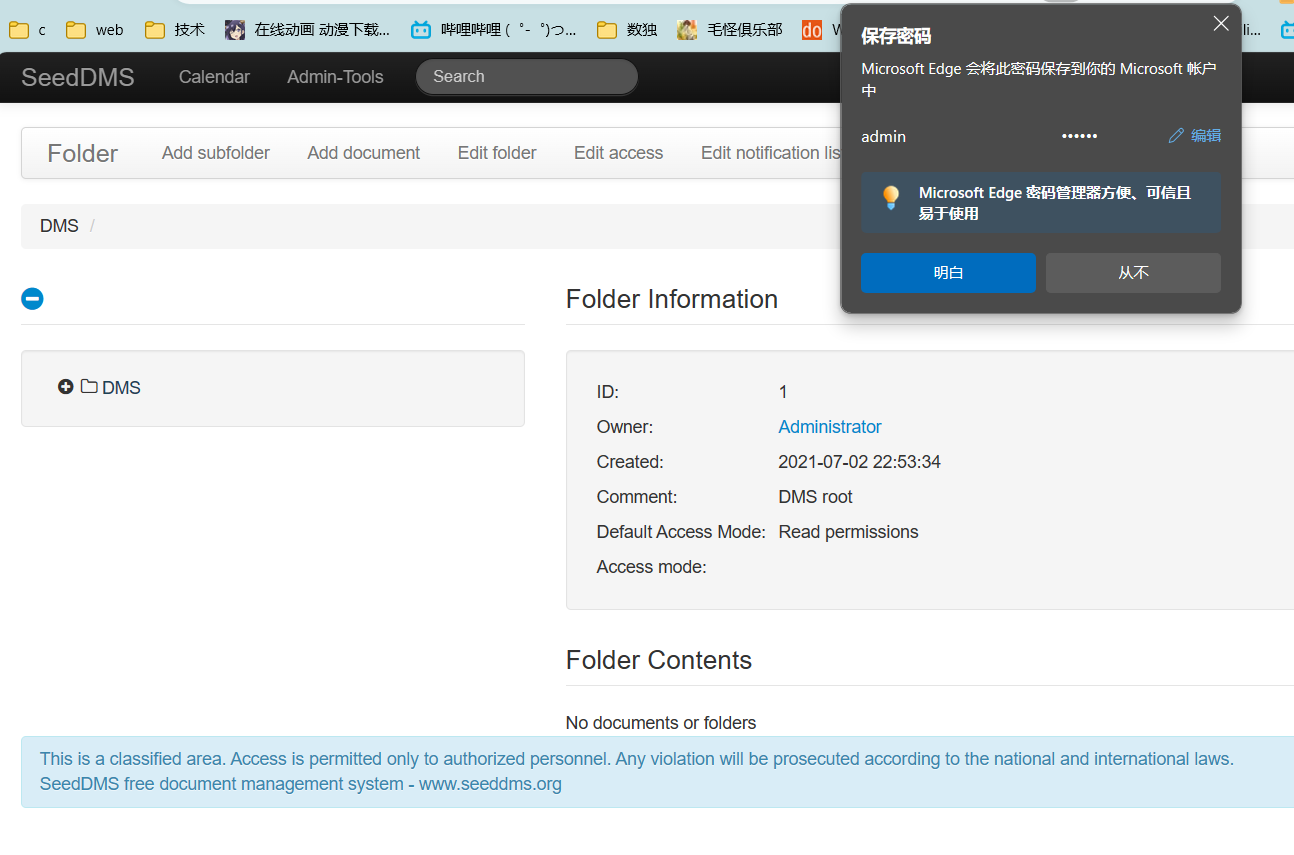


检查一下



修改完成

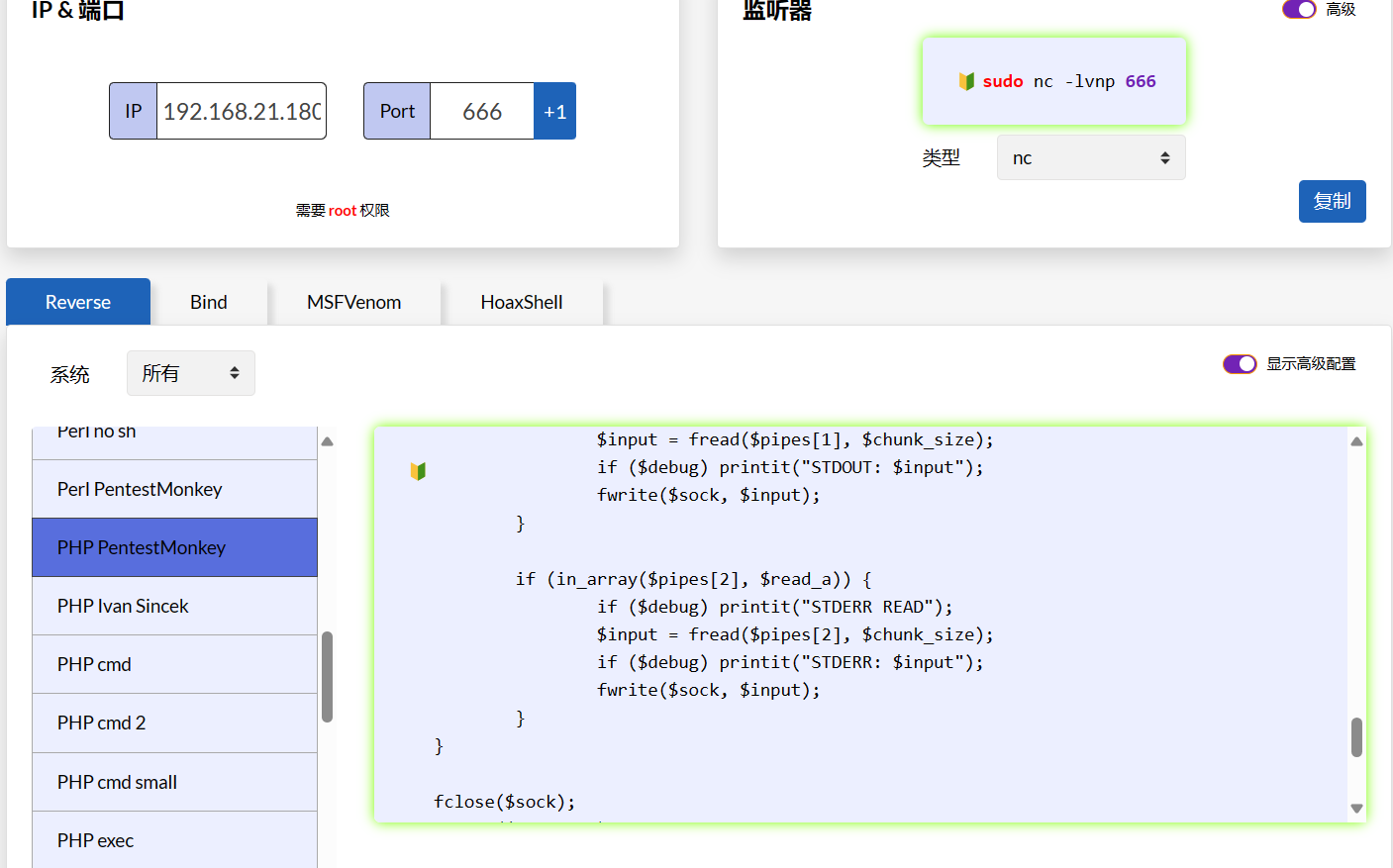
登入

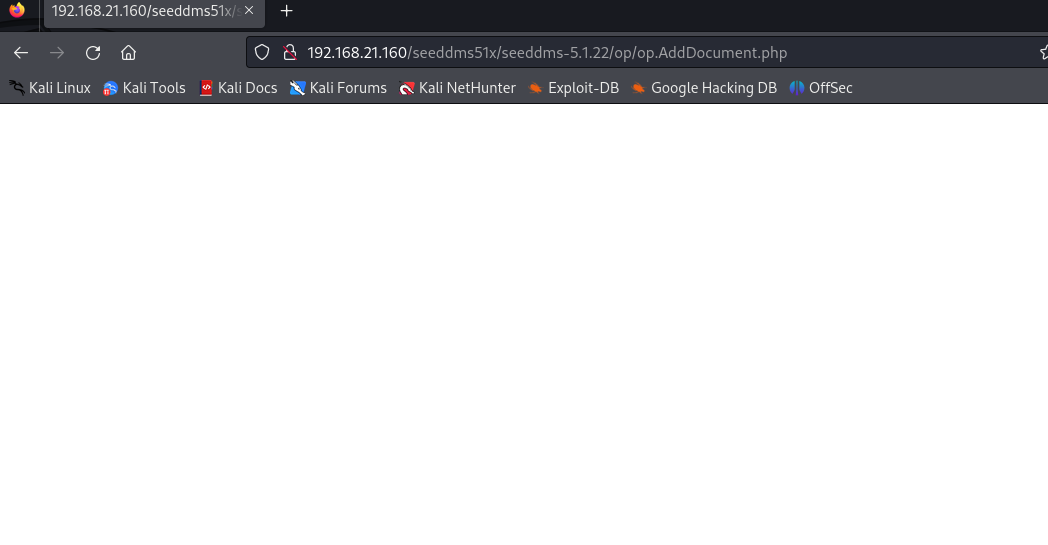


搞定

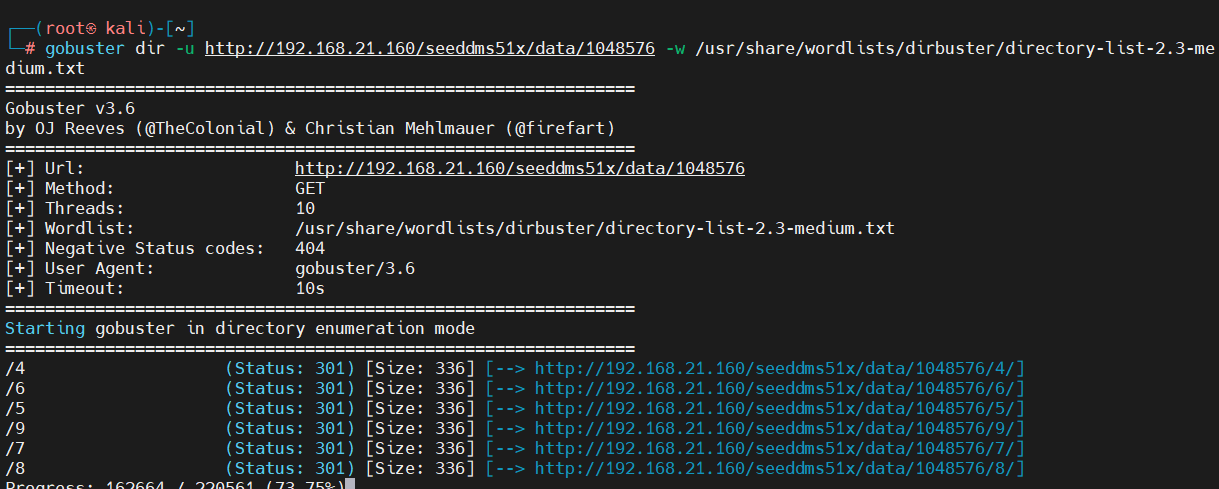
接下来长传shell

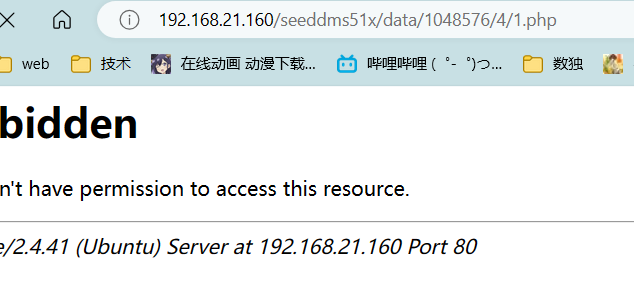
再添加文档里面上传shell

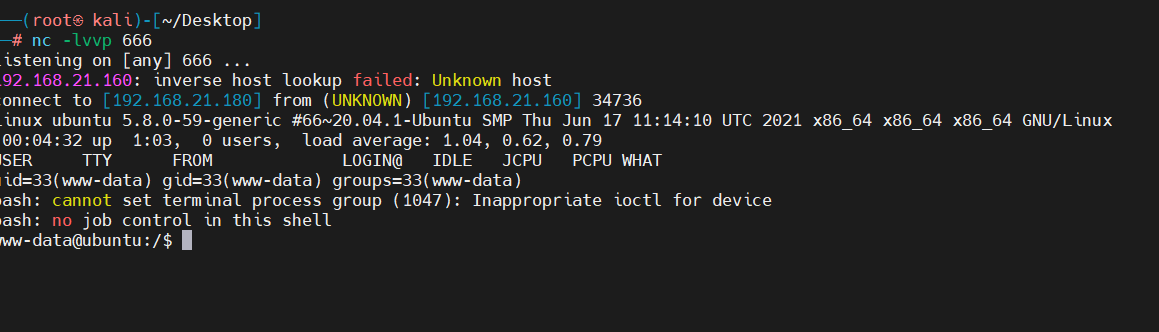




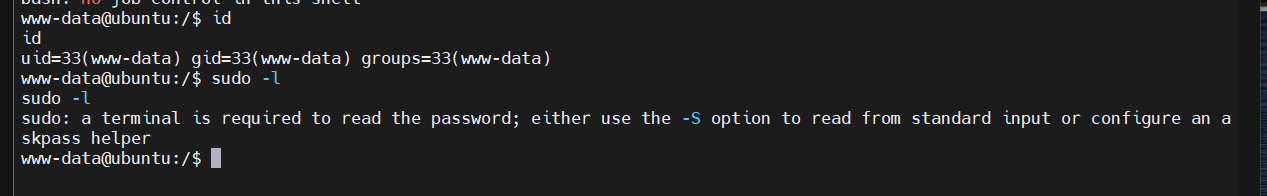


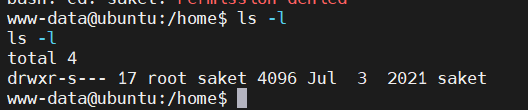




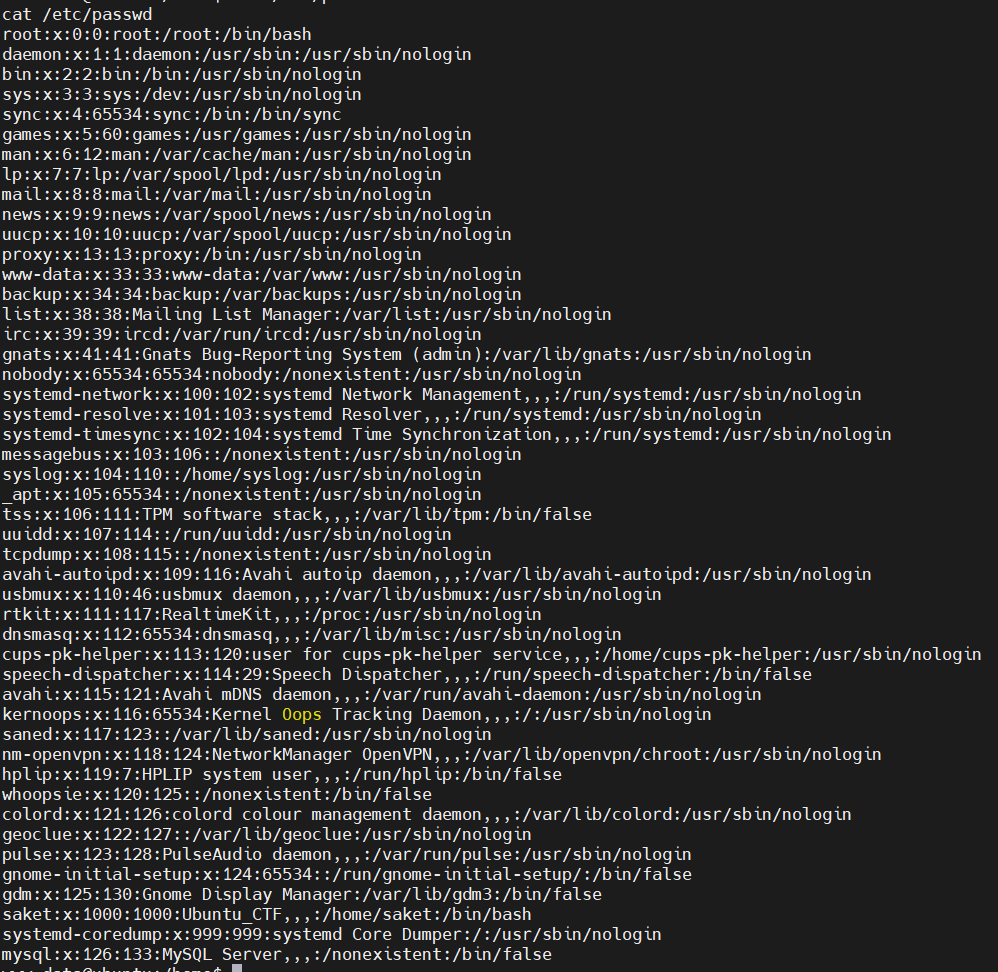


信息收集



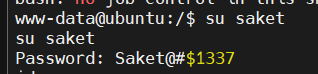


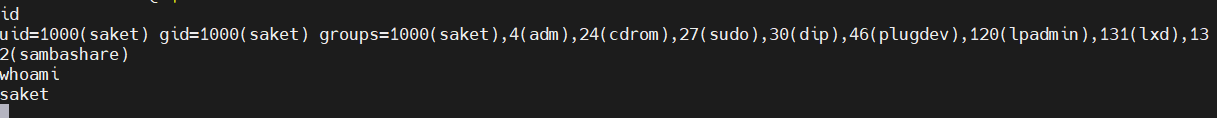
去看一下/etc/passwd



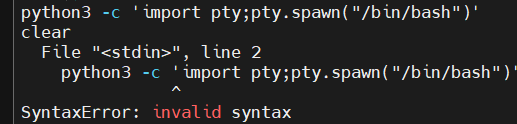
这个用户是有密码的

上面查过了



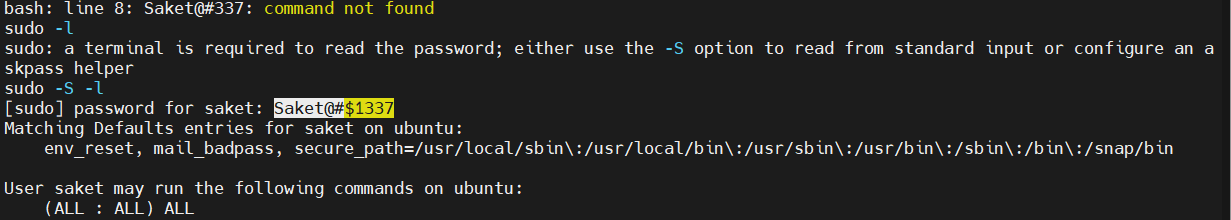


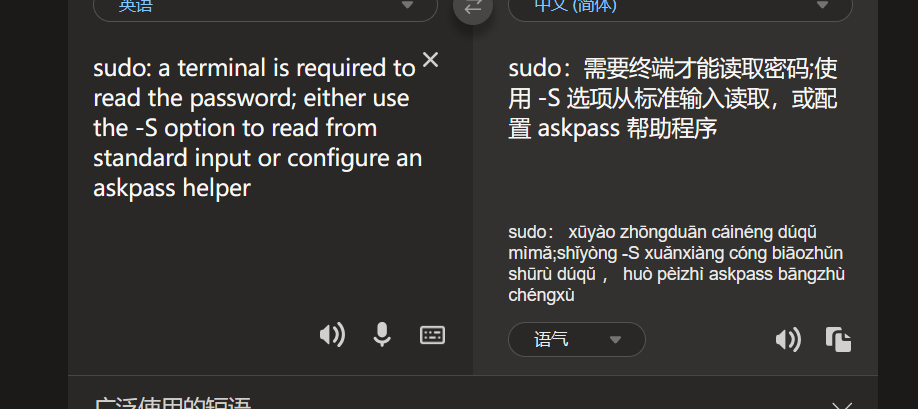
这里没有办法升级shell

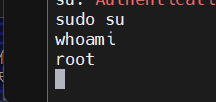


就这样用吧

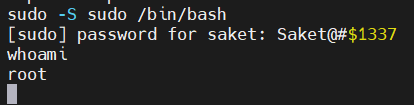
提权







这样也可以



没找到flag