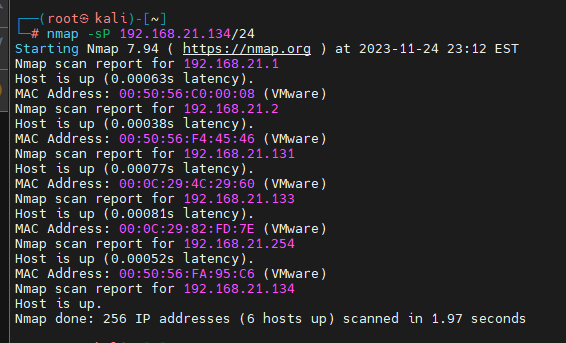
Aragog-1.0.2

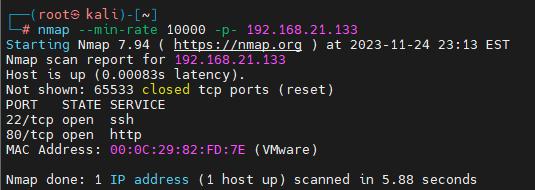
靶机下载：https://download.vulnhub.com/harrypotter/Aragog-1.0.2.ova

主机发现

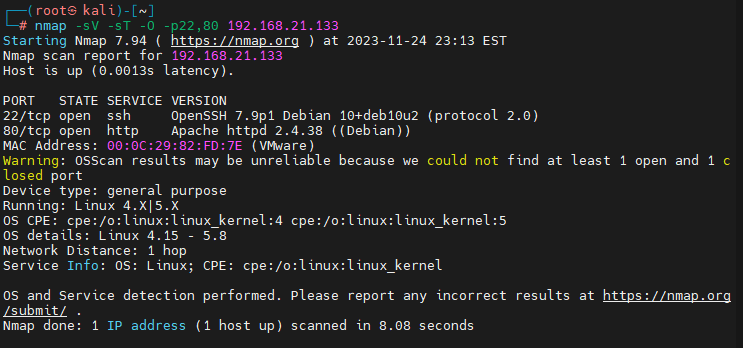


目标133

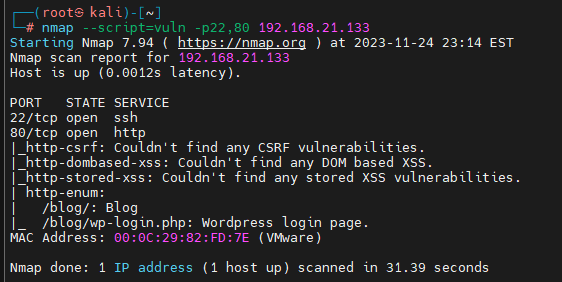
端口扫描



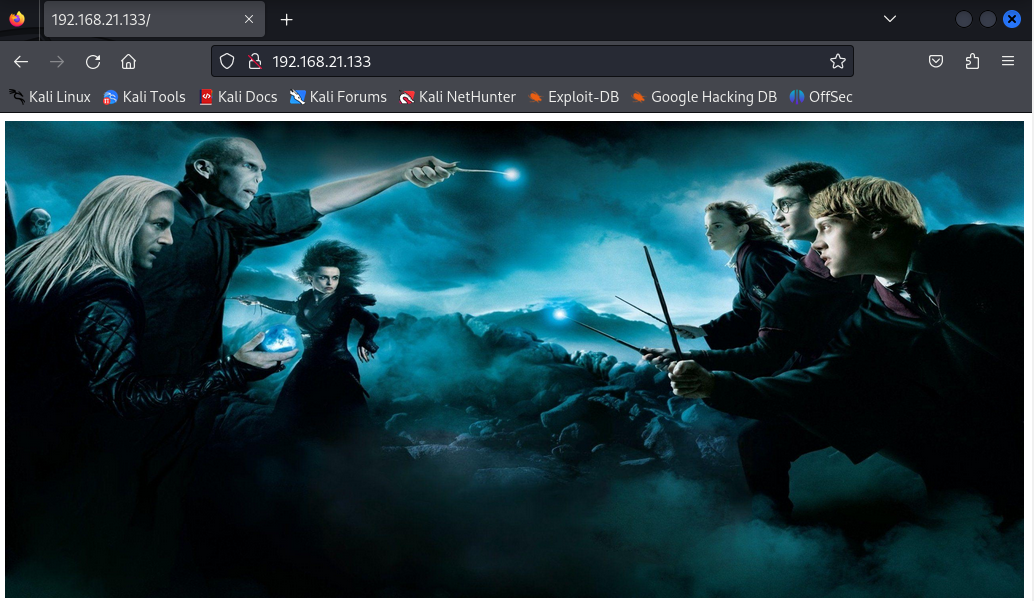
端口服务扫描



漏洞扫描

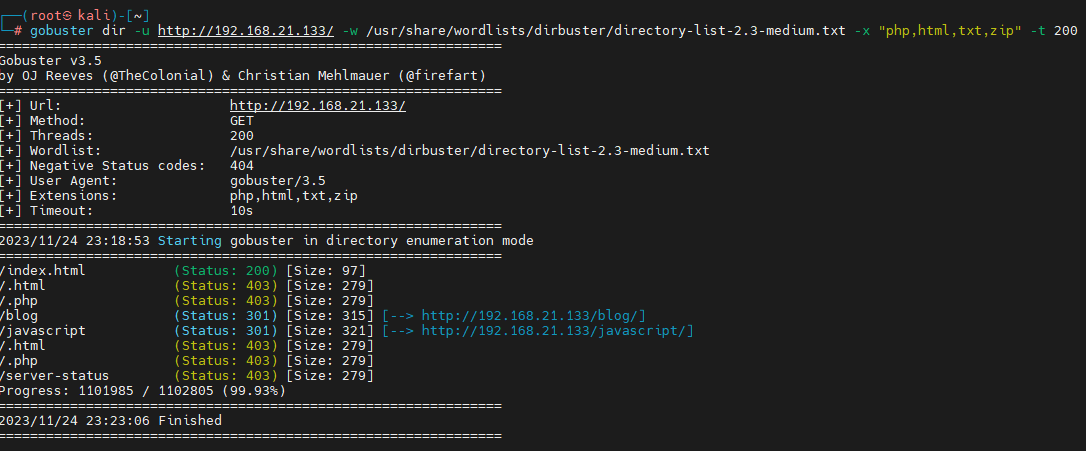


去看web



就一个图片

直接目录扫描

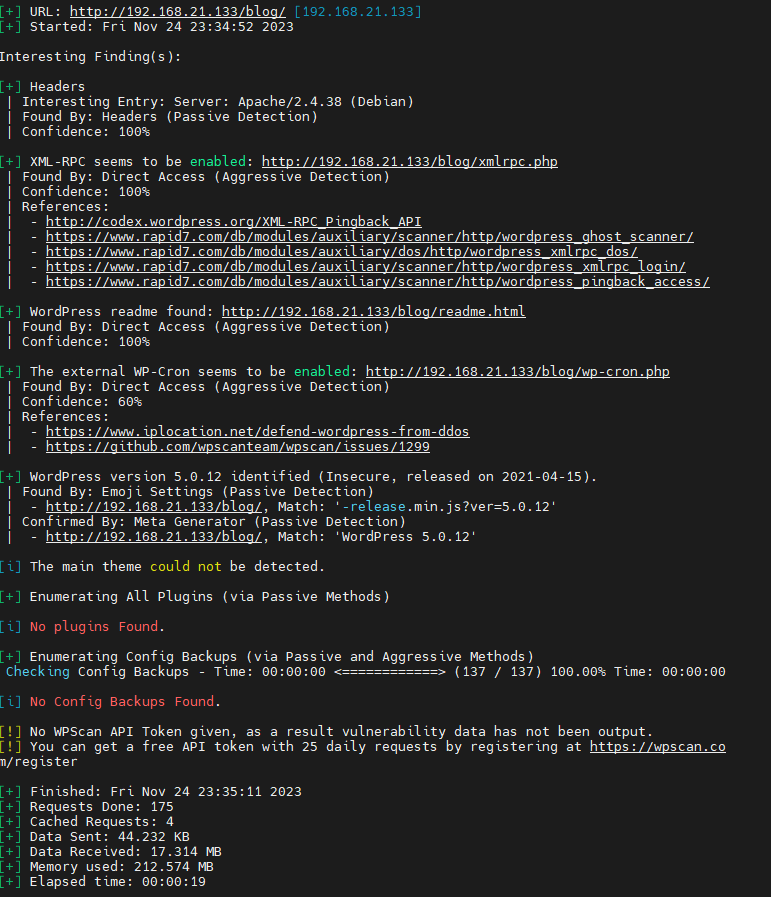


有点东西一个一个看（blog里面有东西）

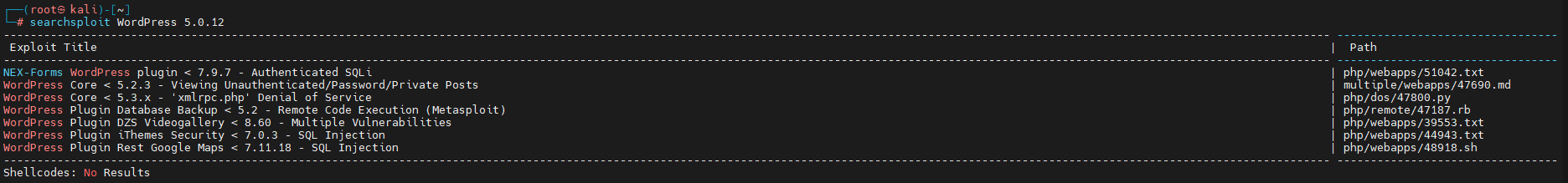


这里面直接能看到wordpress

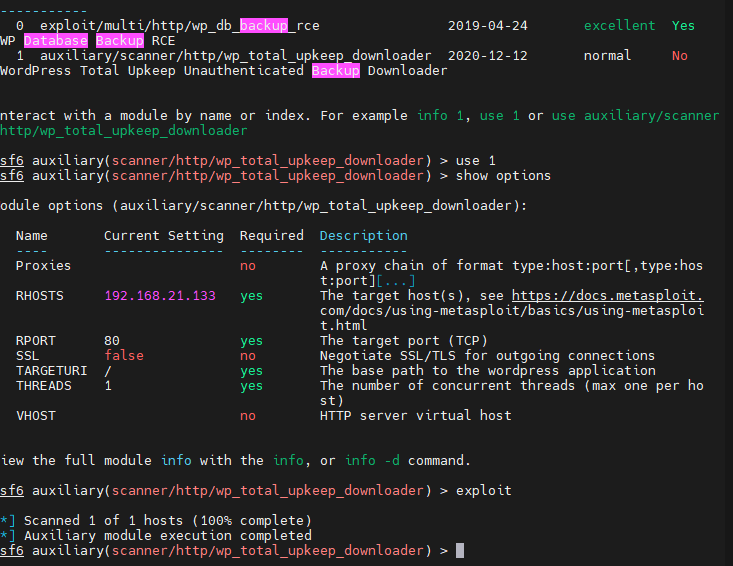
直接用wpscan扫



看到了版本去看一下有没有漏洞



有一个能直接能利用的先去看看

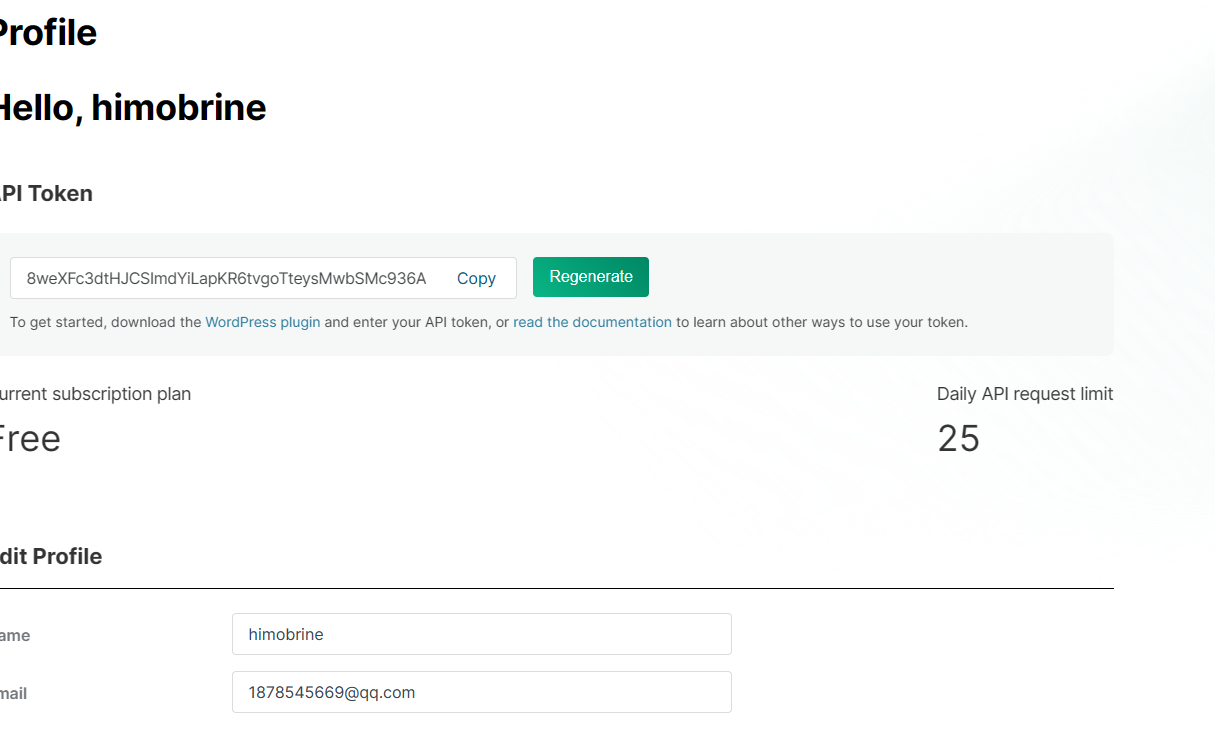


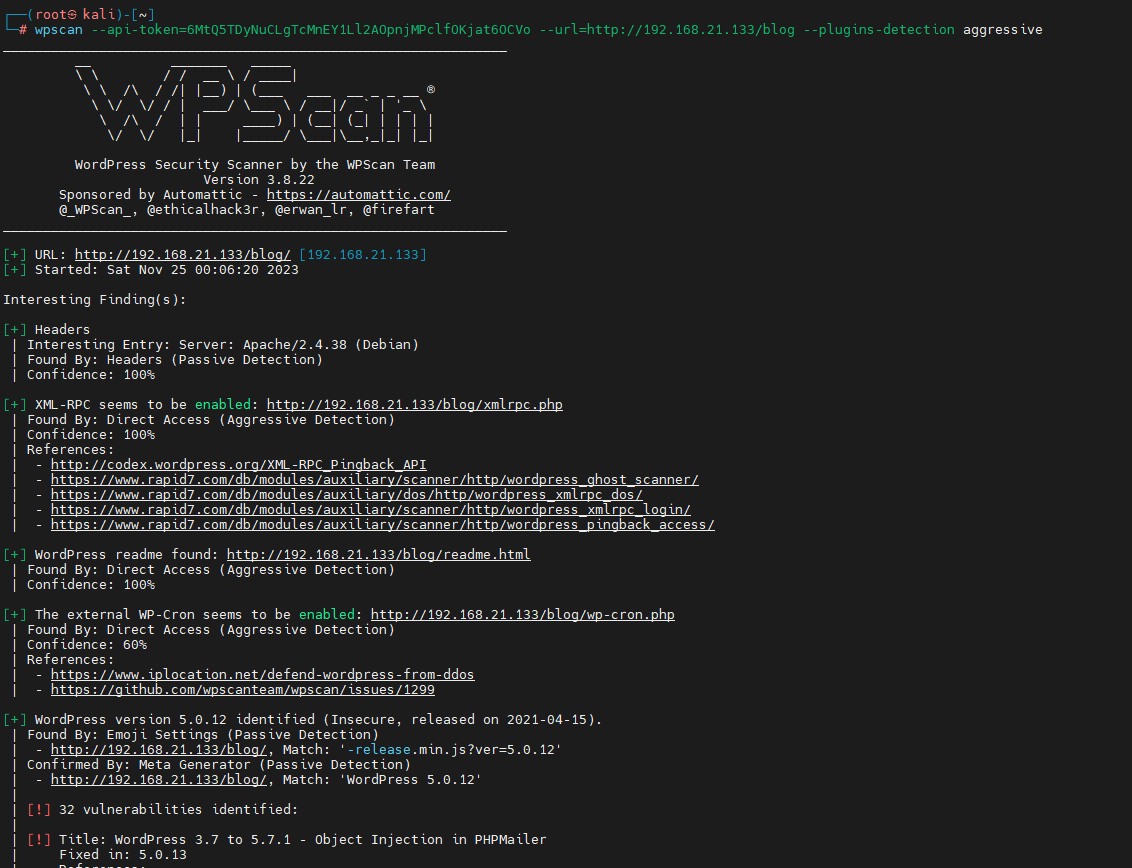
经典有问题

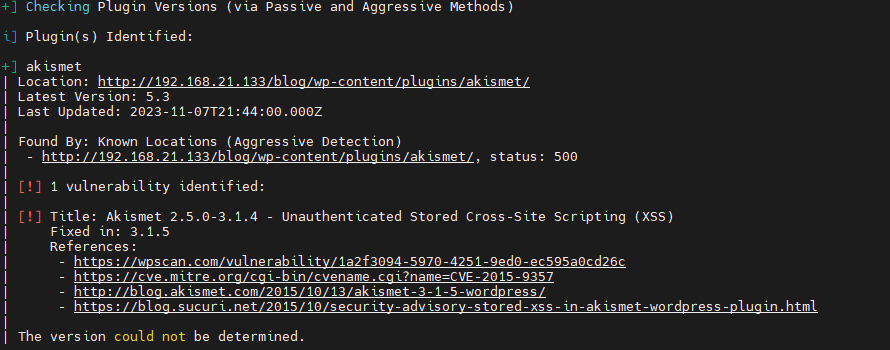
还是从wpscan下手，它默认是扫描wp框架的，去弄个tooken

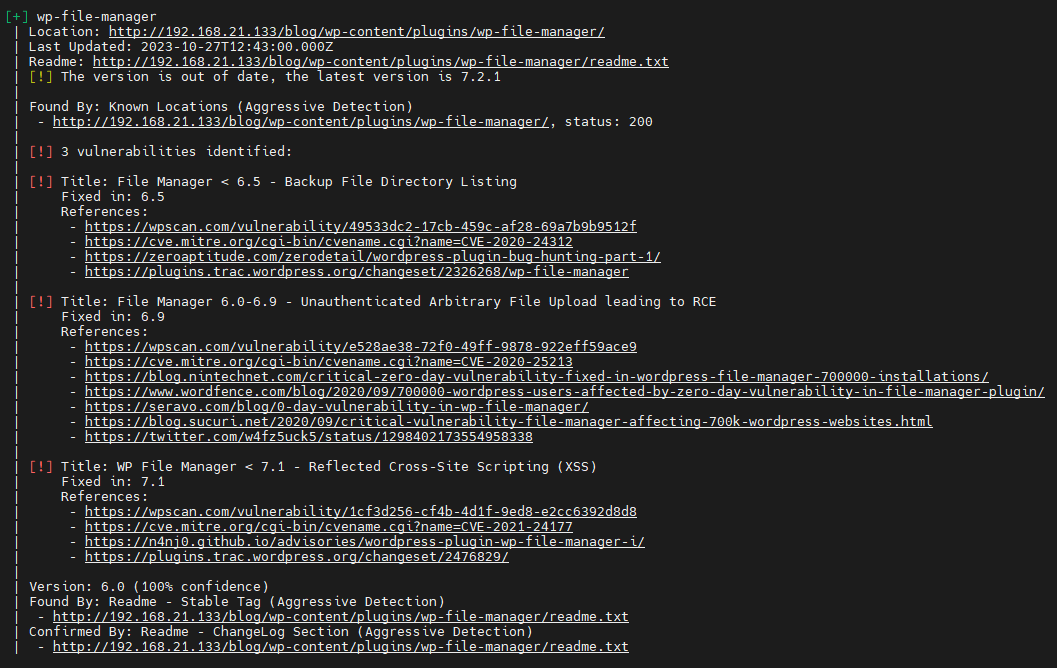
[WPScan: WordPress Security Scanner](https://wpscan.com/)

注册的时候有点慢注意一下

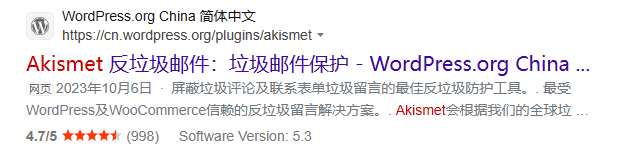


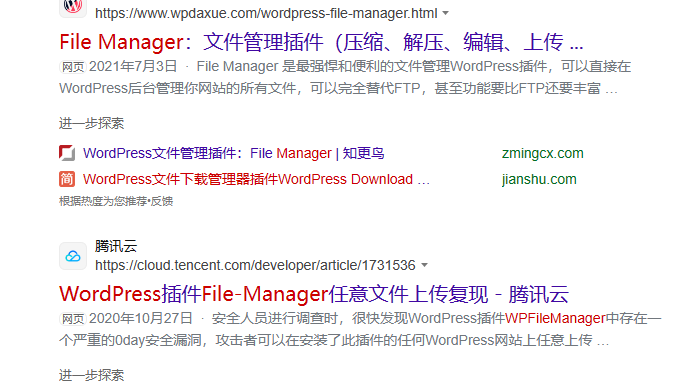






这里面发现发现了wp-file-manager和akismet

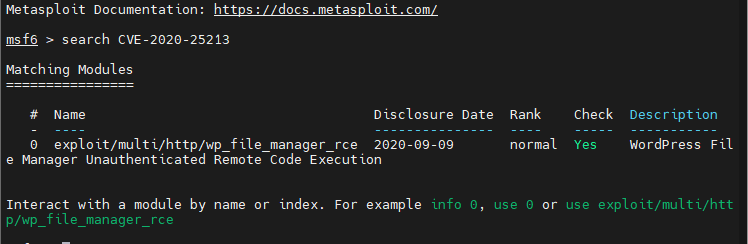




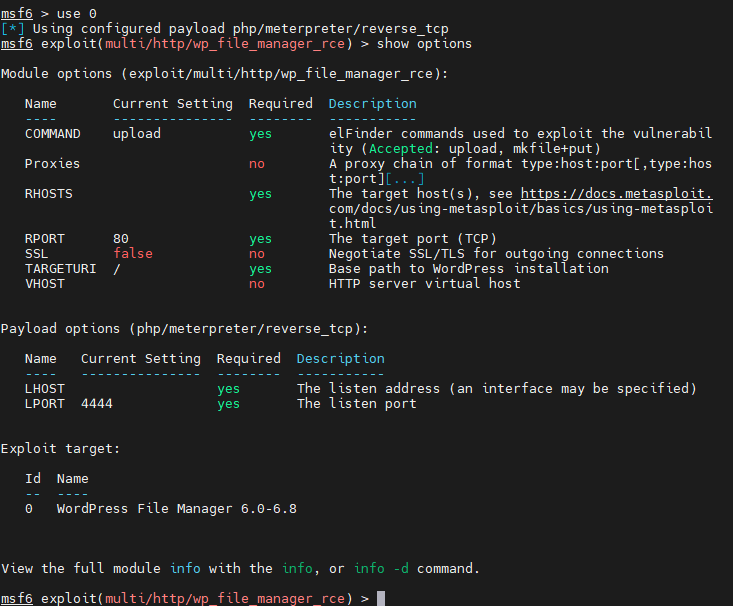
那应该是这个漏洞了经典文件上传

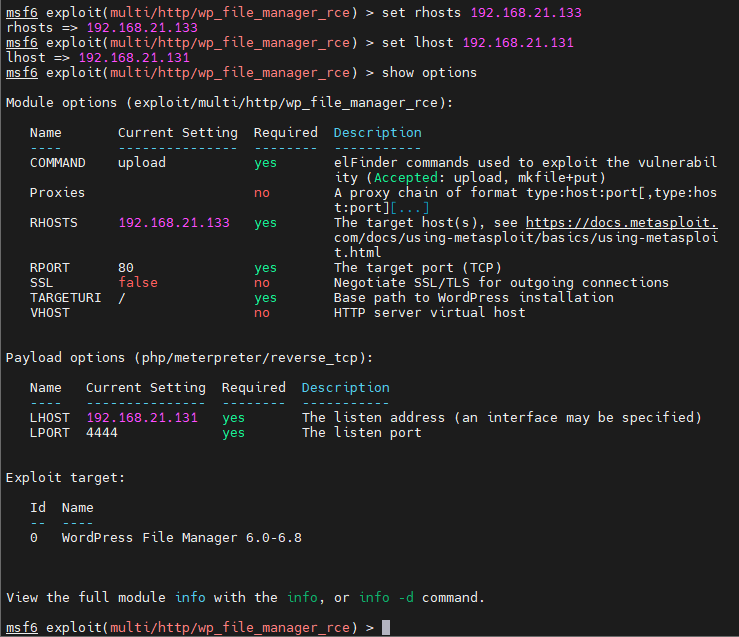
这里有网络连接注意一下去cve的网站

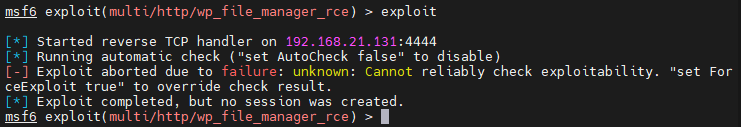




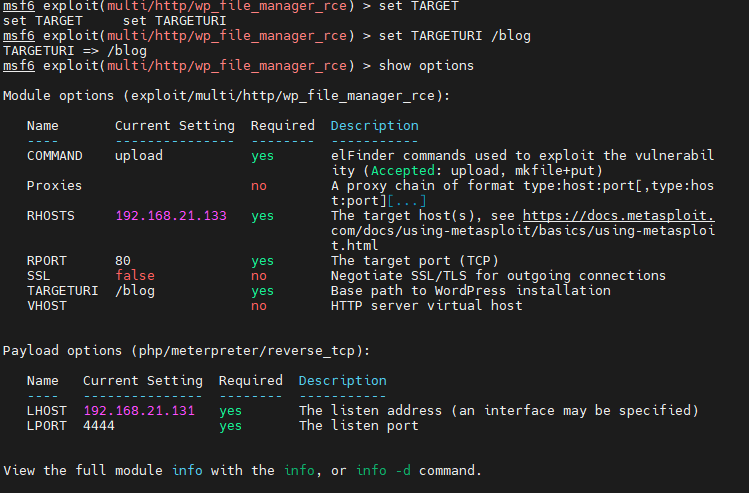
Msf有那就直接用了

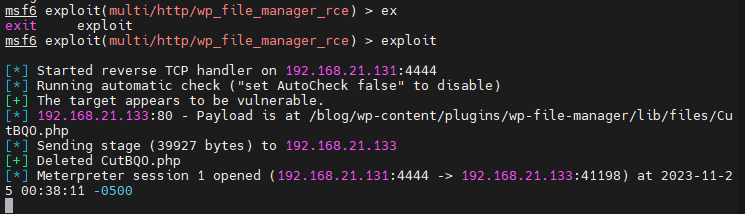






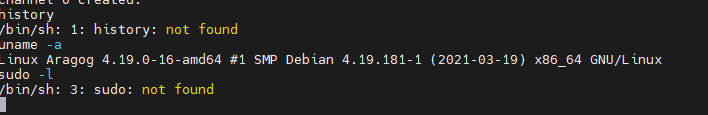
完蛋忘记了是blog文件夹





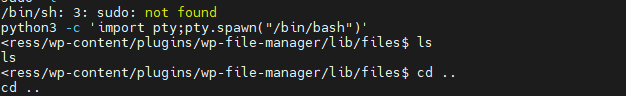
成功！（注意要大shell）

信息收集

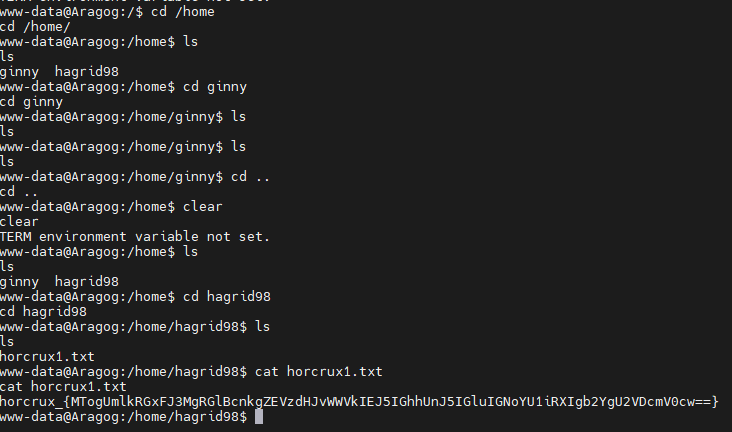


用python优化一下shell

python3 -c 'import pty;pty.spawn("/bin/bash")'

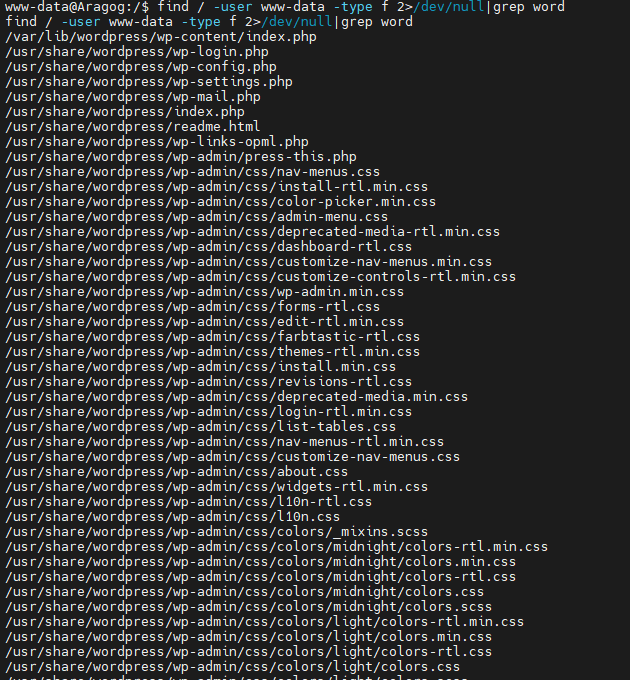


去拿flag（老是忘记）



接下来就是找文件权限的事情咯（其实就是找wp的数据库配置文件）

find / -user www-data -type f 2>/dev/null

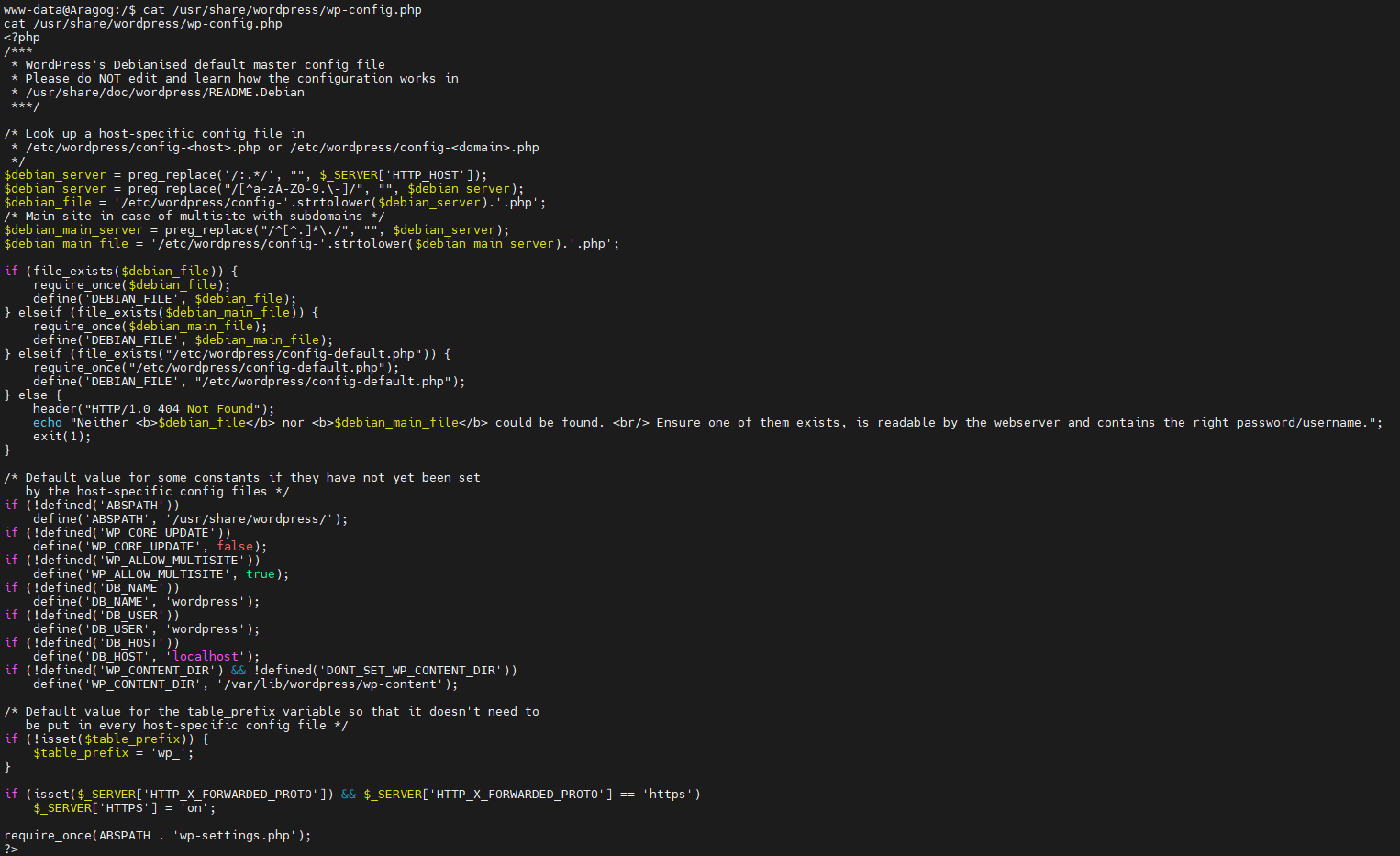


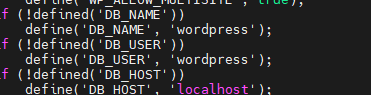
东西很多去找一下，一般是config文件（大不了网上搜，或者直接找数据库配置文件也可以）

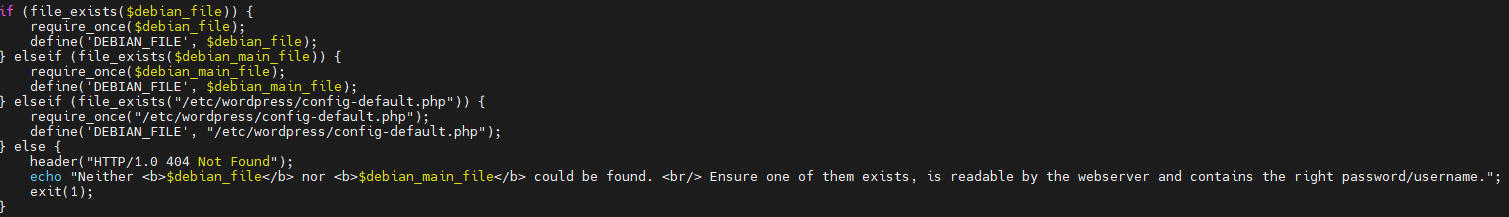




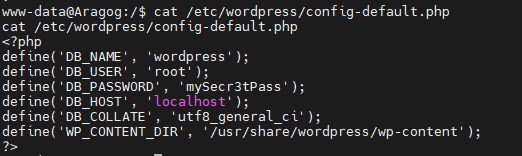
直接看





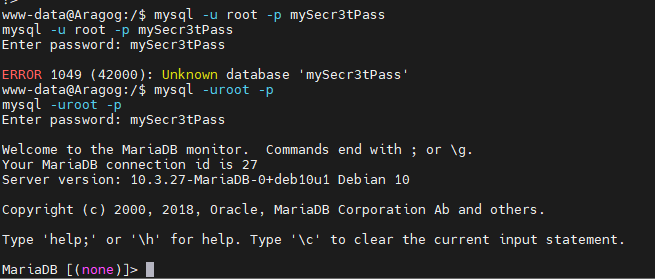


引用文件config-default.php

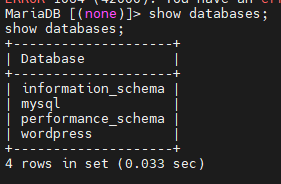


账号密码都来了

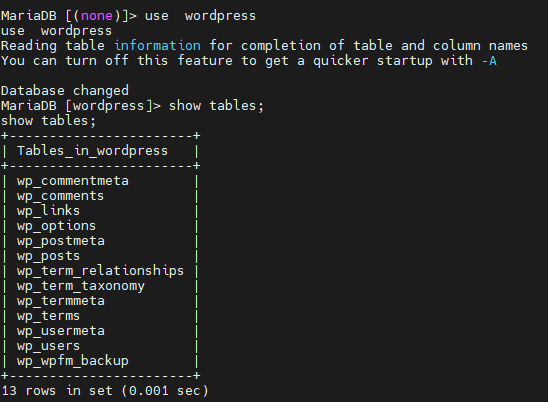
连接数据库



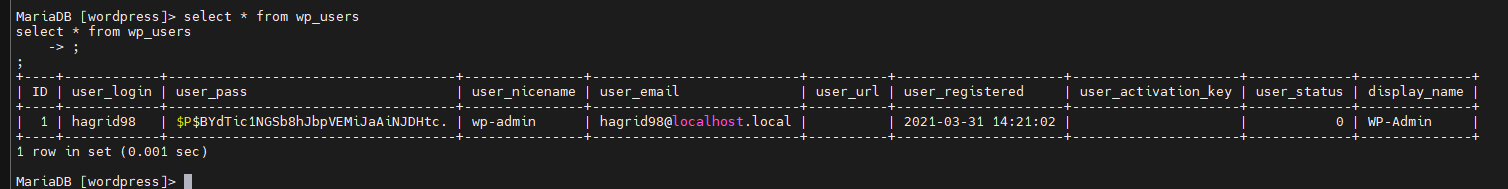
要在shell连（别问问就是host）



一定是wp

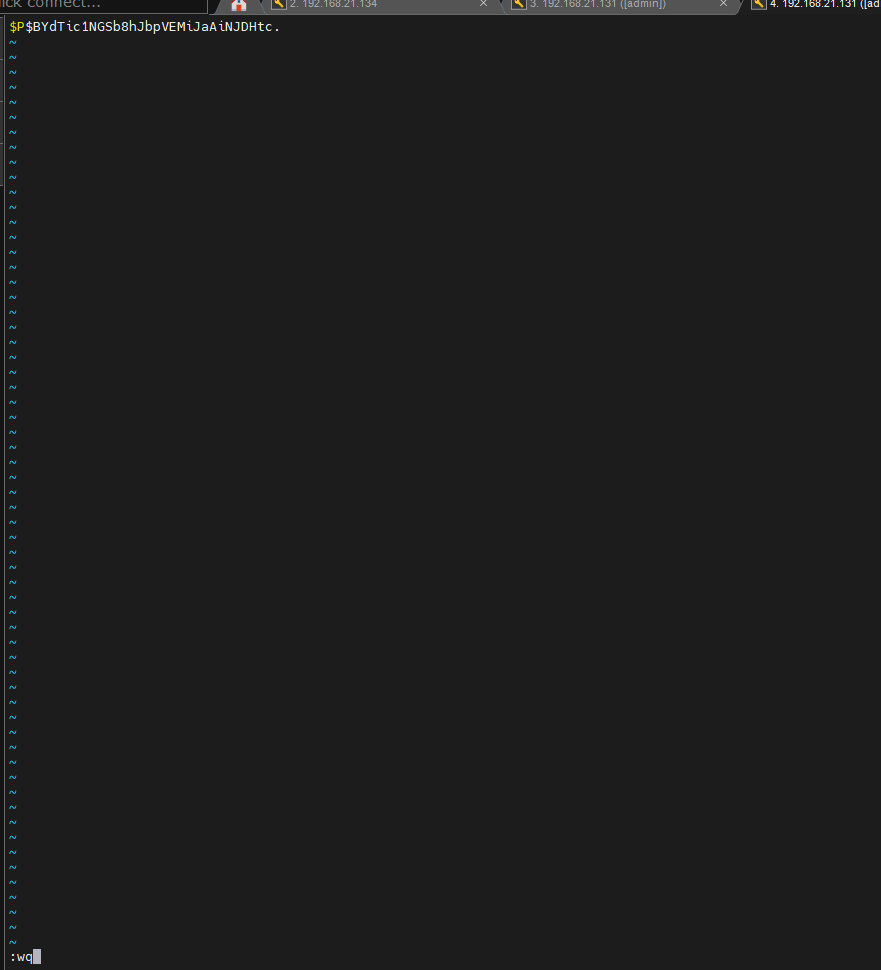


一定是用户密码



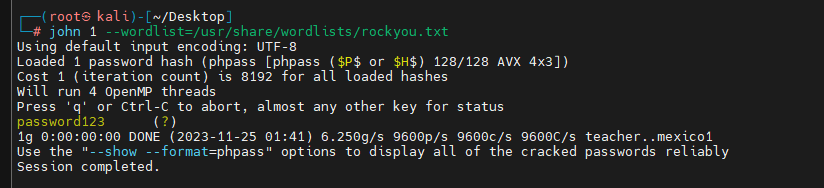
嘿嘿到手

走了解密



Vim写文件

然后用john爆破

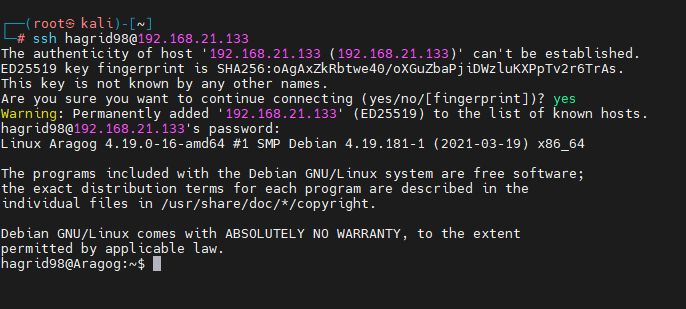


找到点有用的网站

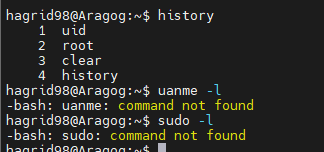




直接ssh登入

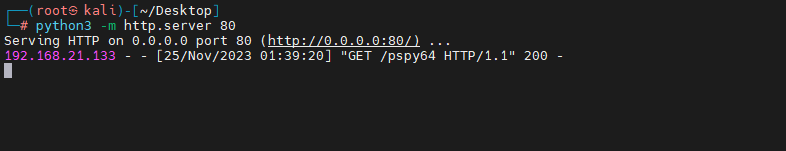


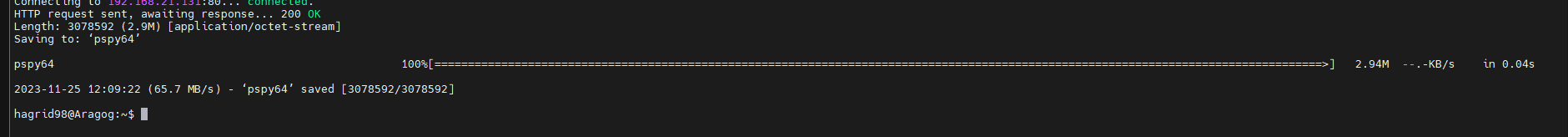
信息收集



啥都没有

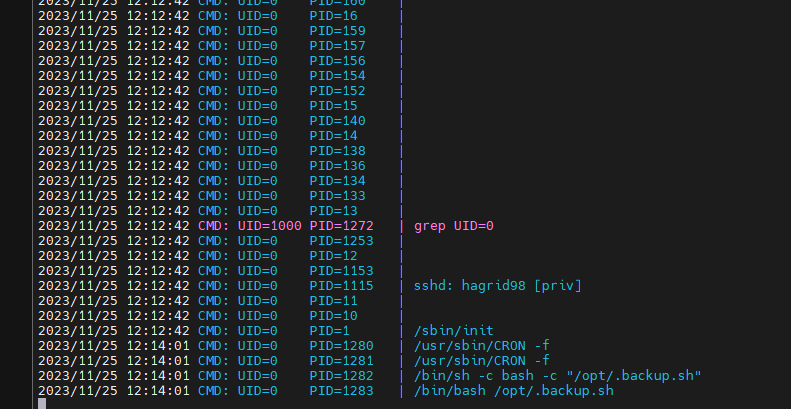
传个pspy吧

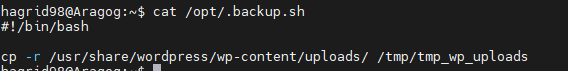




运行

等了一下发现点好东西



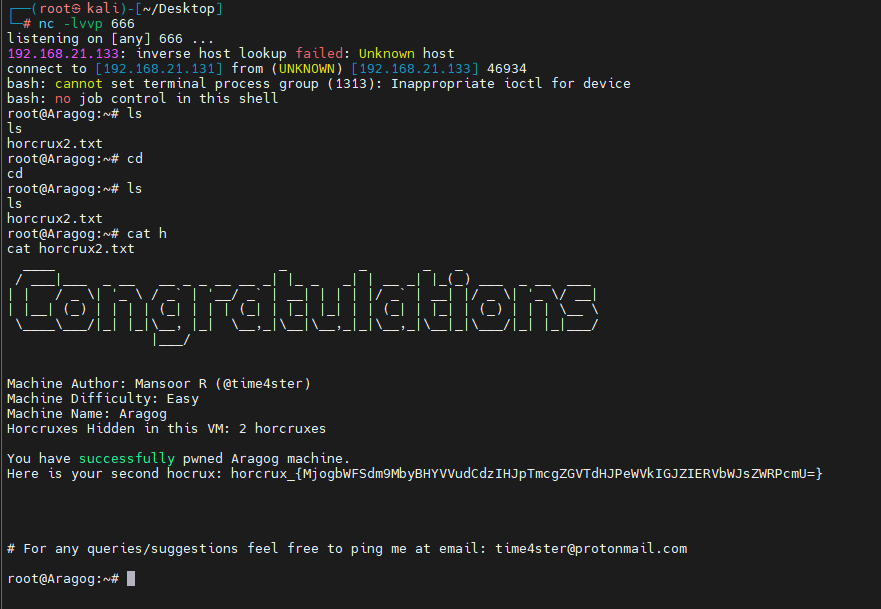


这里发现点好东西

直接改一下写个反弹shell（或者直接用upload的漏洞）



耐心等待一下就可以



结束！