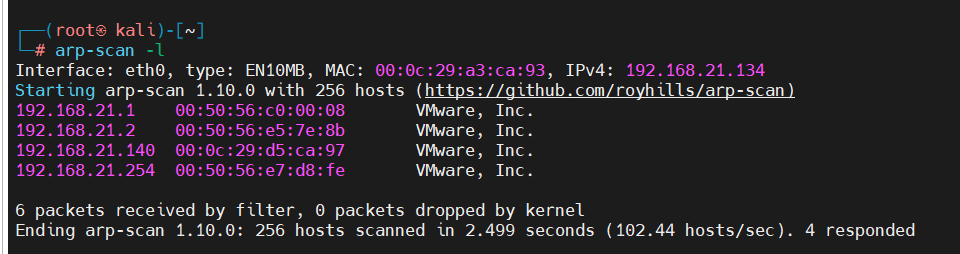
DEATHNOTE: 1

难度：easy

下载地址：<https://download.vulnhub.com/deathnote/Deathnote.ova>

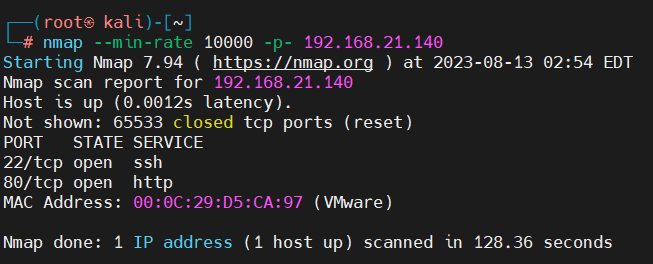
主机发现

arp-scan -l



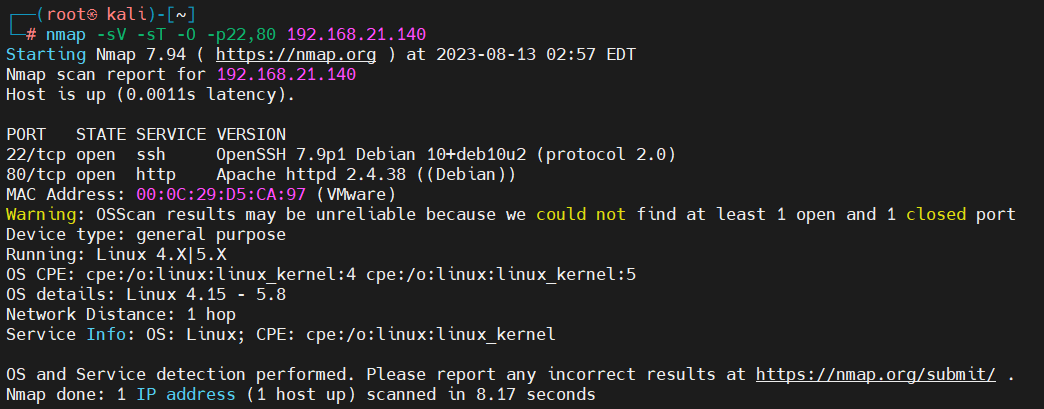
端口扫描

nmap --min-rate 10000 -p- 192.168.21.140



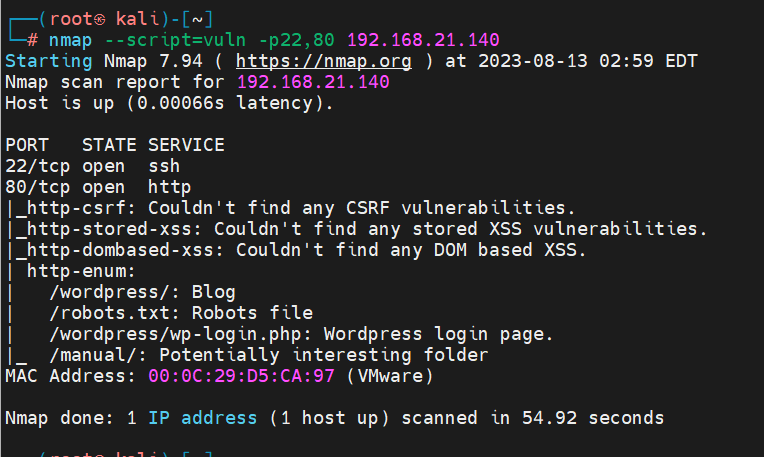
进一步查看目标的端口的服务和版本

nmap -sV -sT -O -p22,80 192.168.21.140

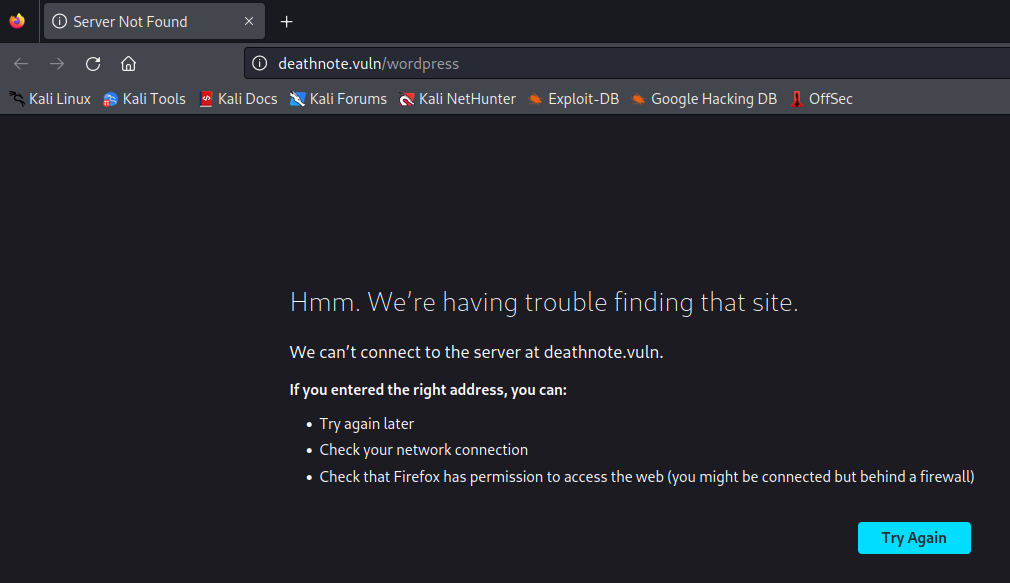


扫描端口的漏洞

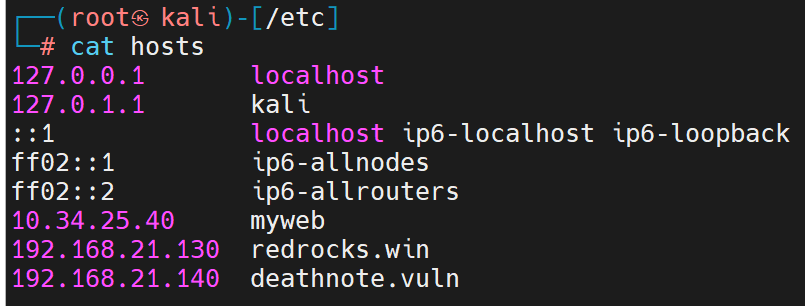
nmap --script=vuln -p22,80 192.168.21.140

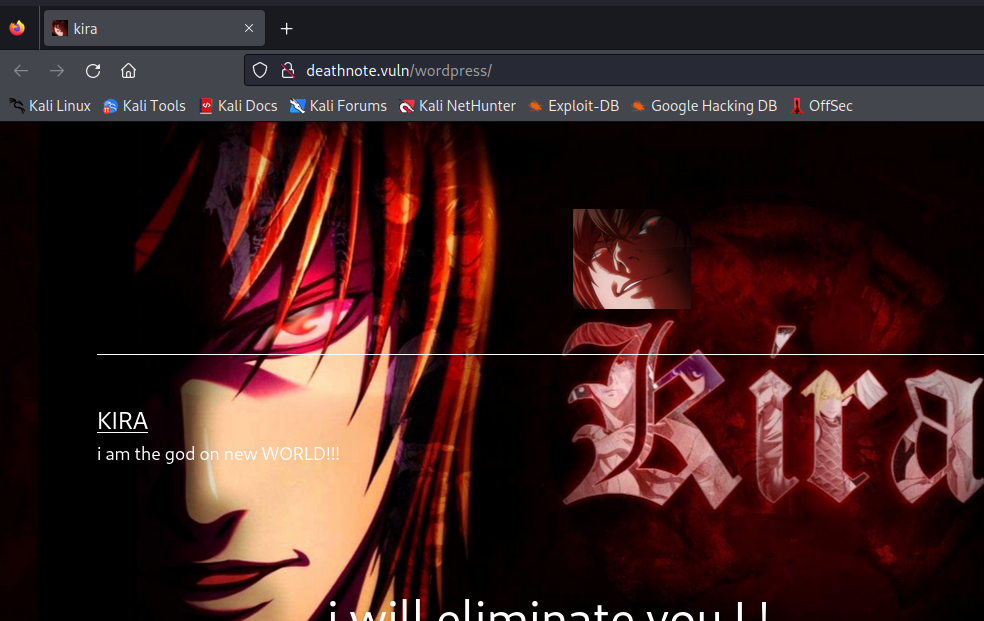


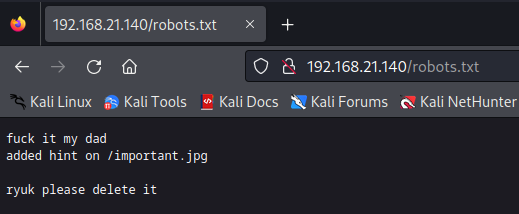
看到有robots先去看看



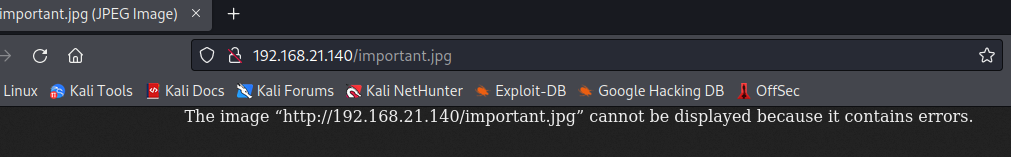
连不上改host



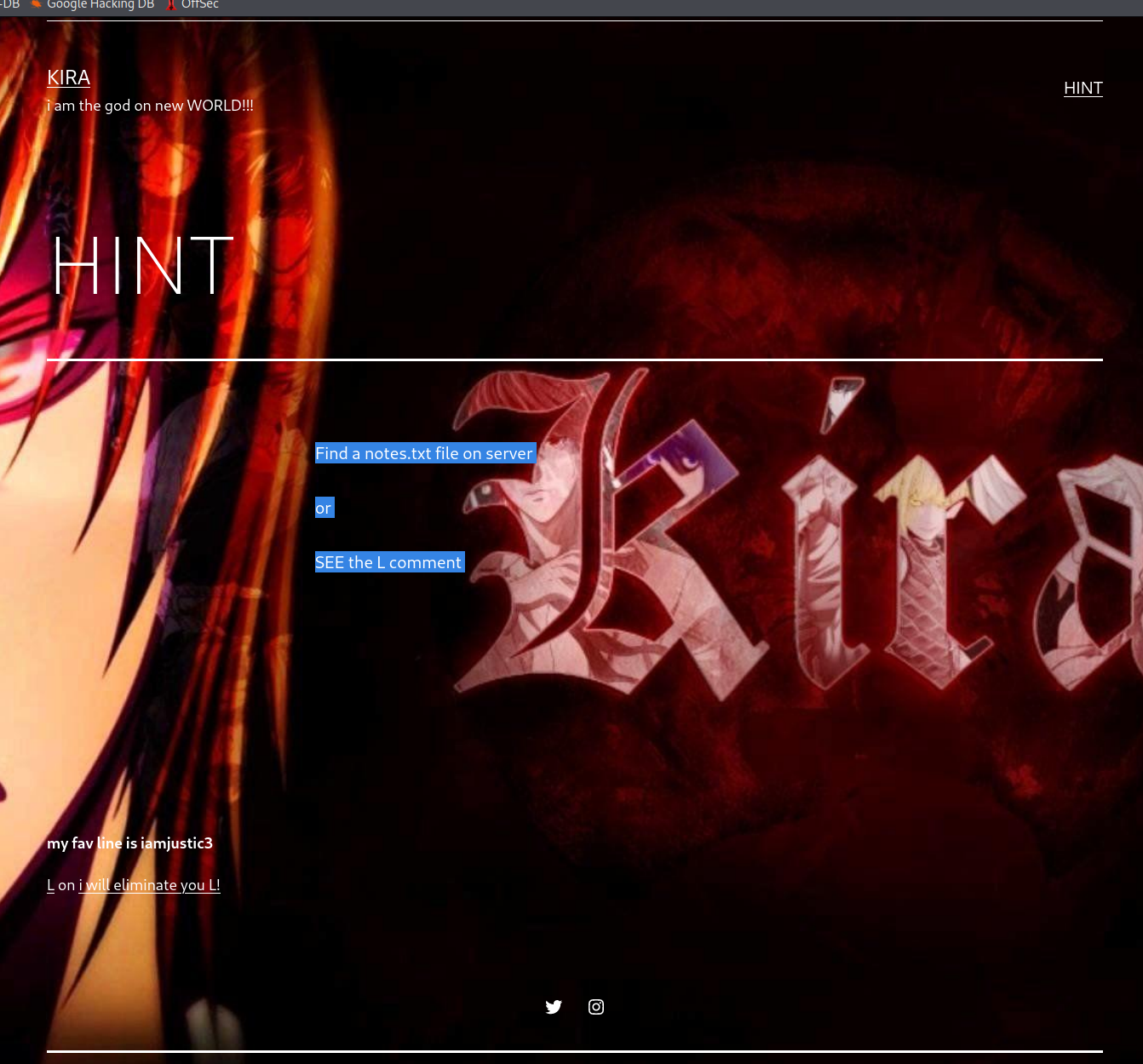




接着看



没有东西去网站碰运气，点了hint后发现这个



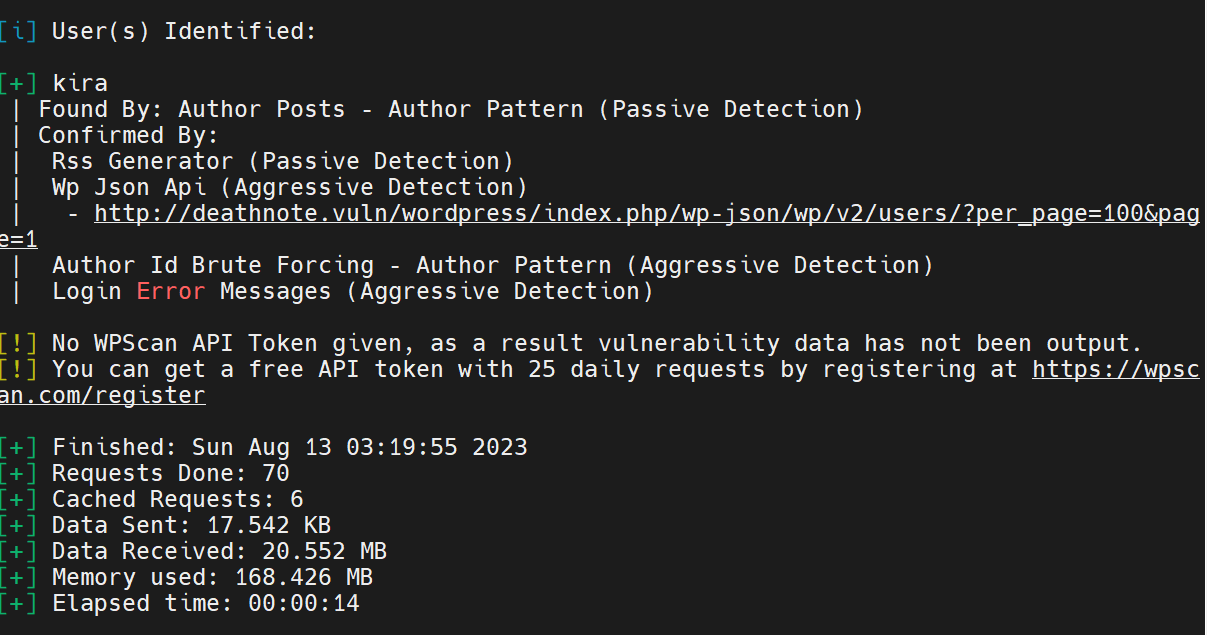
这个线索用过了，只能去wordpress看看有没有漏洞（网站是wordpress搭建的）

顺带一搜就找到工具了（wpscan）



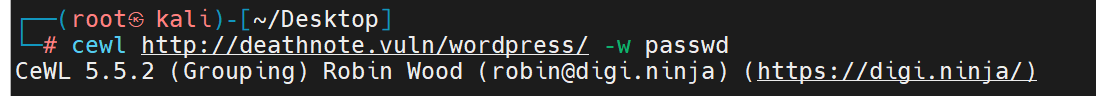
这里-e下面能直接爆破userid

wpscan --url http://deathnote.vuln/wordpress/ -e u



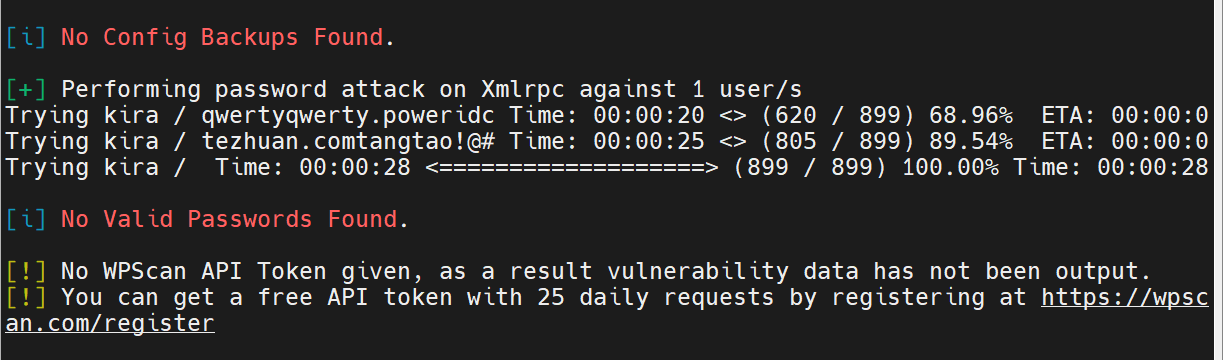
现在找到了用户名还差一个密码

cewl http://deathnote.vuln/wordpress/ -w passwd



再利用wpscan爆破密码

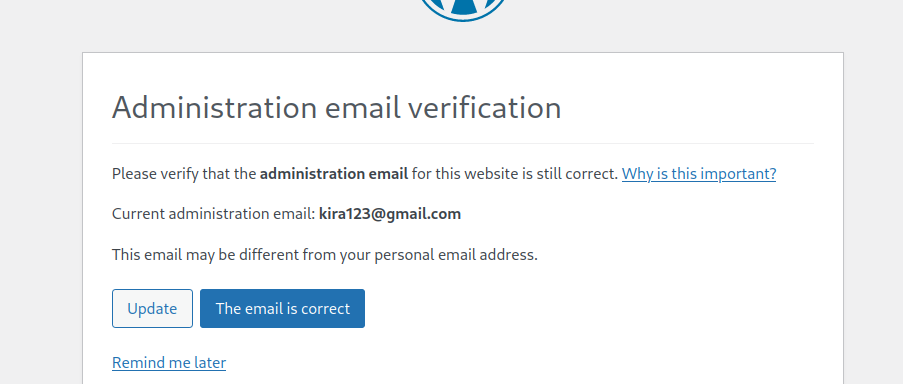
wpscan --url http://deathnote.vuln/wordpress/ -P password.txt -U kira



醉了没有



这里应该是密码

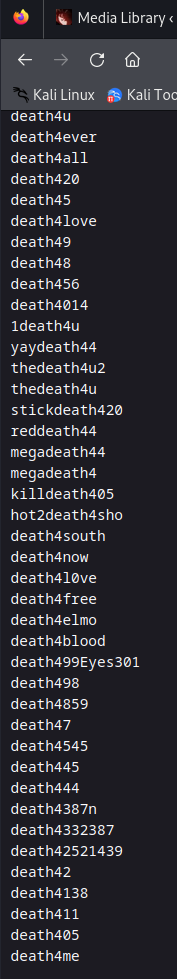


登入成功

找找有用的东西

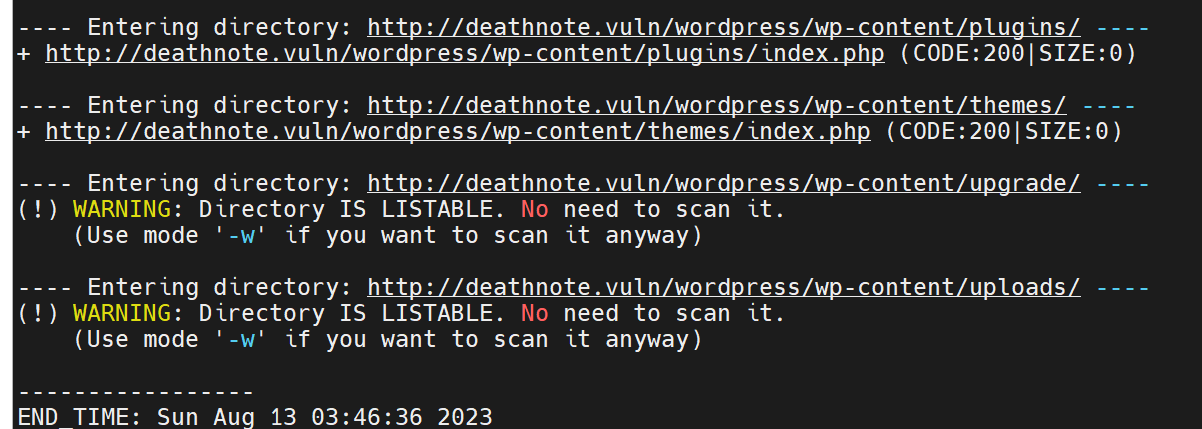
在media里面发现文件

http://deathnote.vuln/wordpress/wp-content/uploads/2021/07/notes.txt

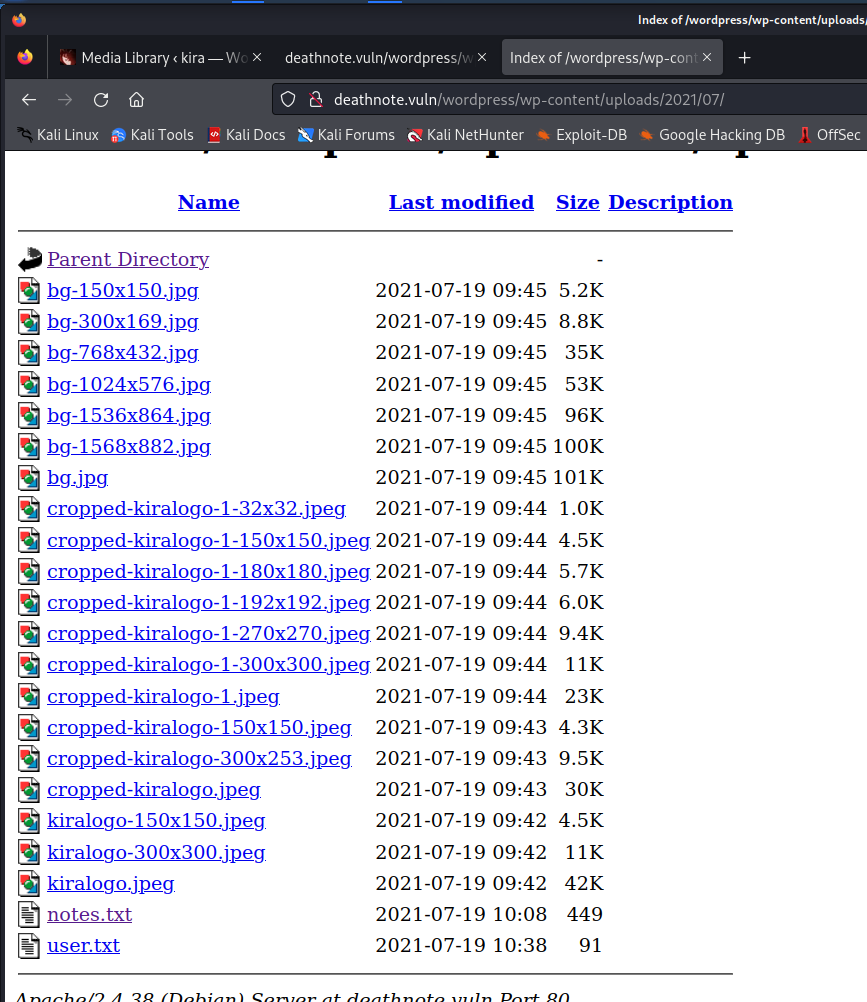


目前不知道用处，但是应该要目录扫描

dirb <http://deathnote.vuln/wordpress>



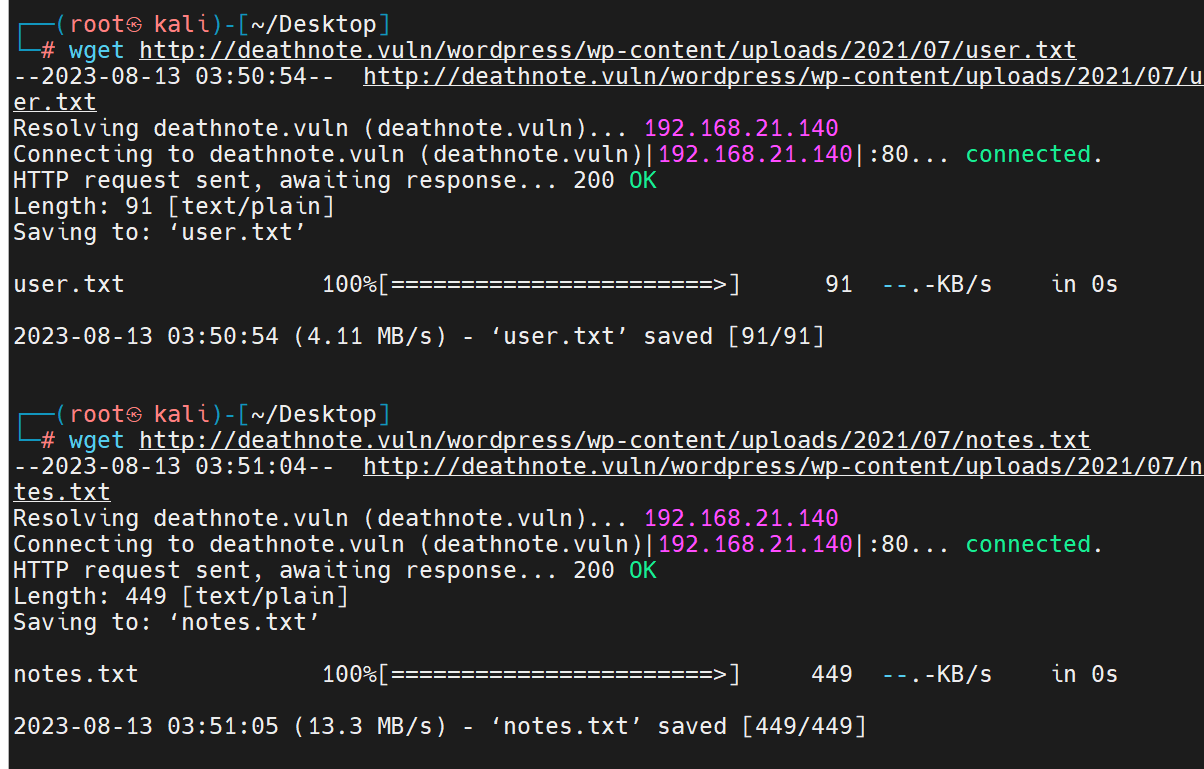
看到有uploads去看一下（我们看到notes.txt在这个文件夹里面）



正好看到user.txt

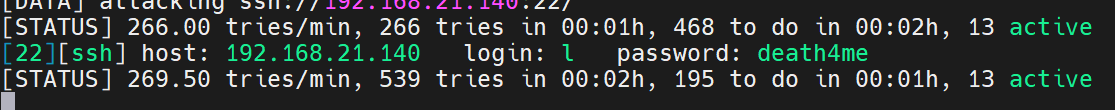
那么notes里面是有密码的

文件直接下下来



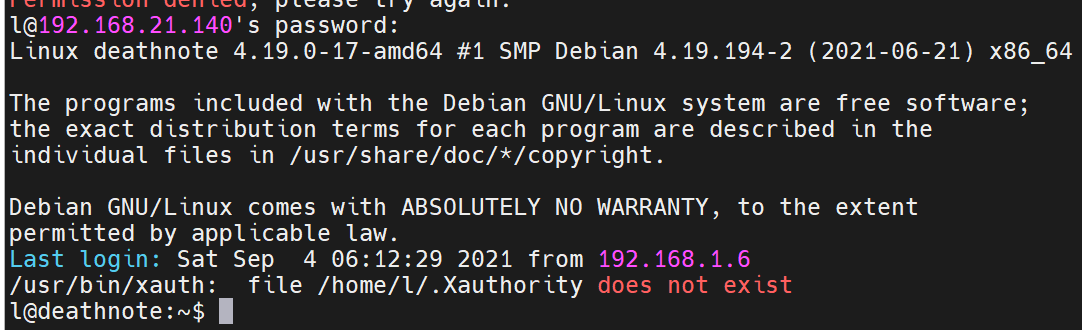
这里由于web已经结束了，因该是要我们去爆破ssh

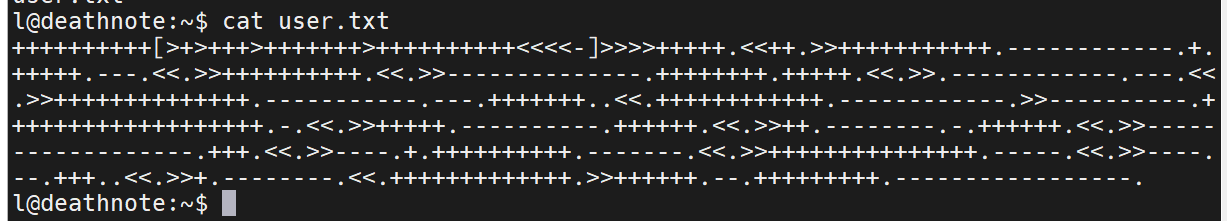
hydra -L user.txt -P notes.txt ssh://192.168.21.140



搞定ssh直接连

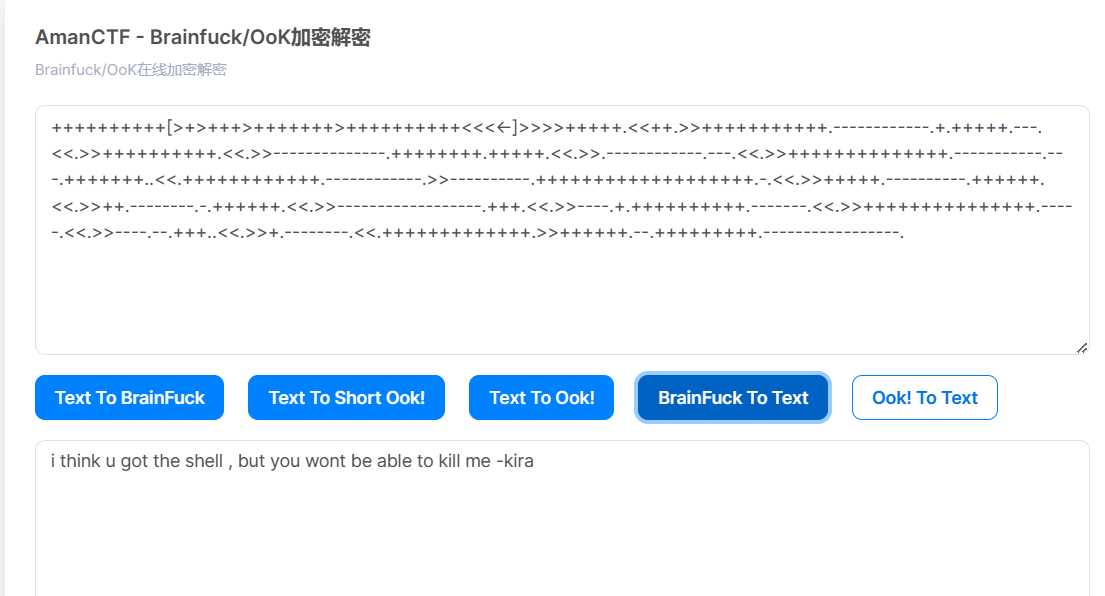
ssh [l@192.168.21.140](mailto:l@192.168.21.140)



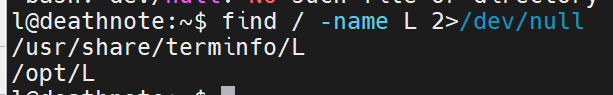


0ok加密

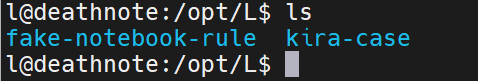
[Brainfuck/OoK加密解密 - Bugku CTF](https://ctf.bugku.com/tool/brainfuck)



L比较重要我就先扫描的l

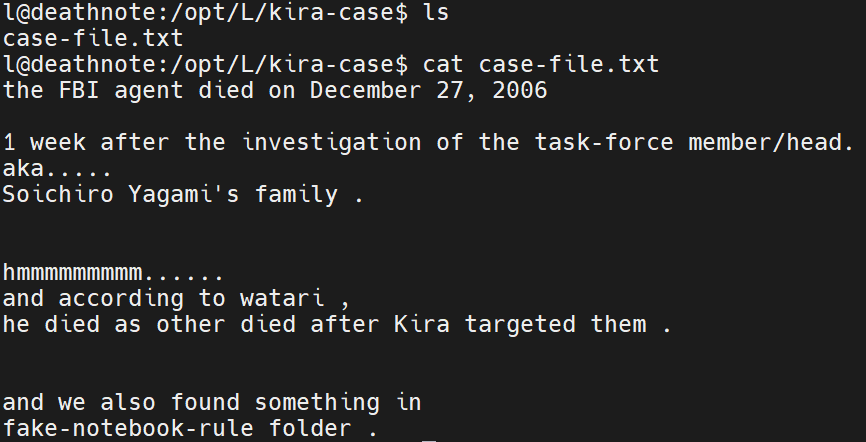


进去看

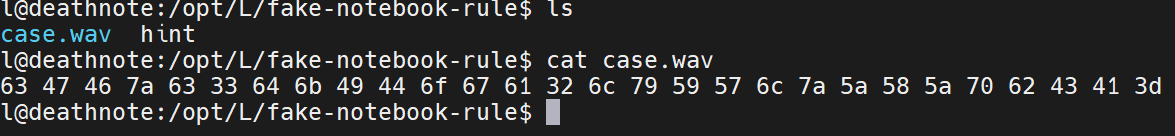


两个文件夹

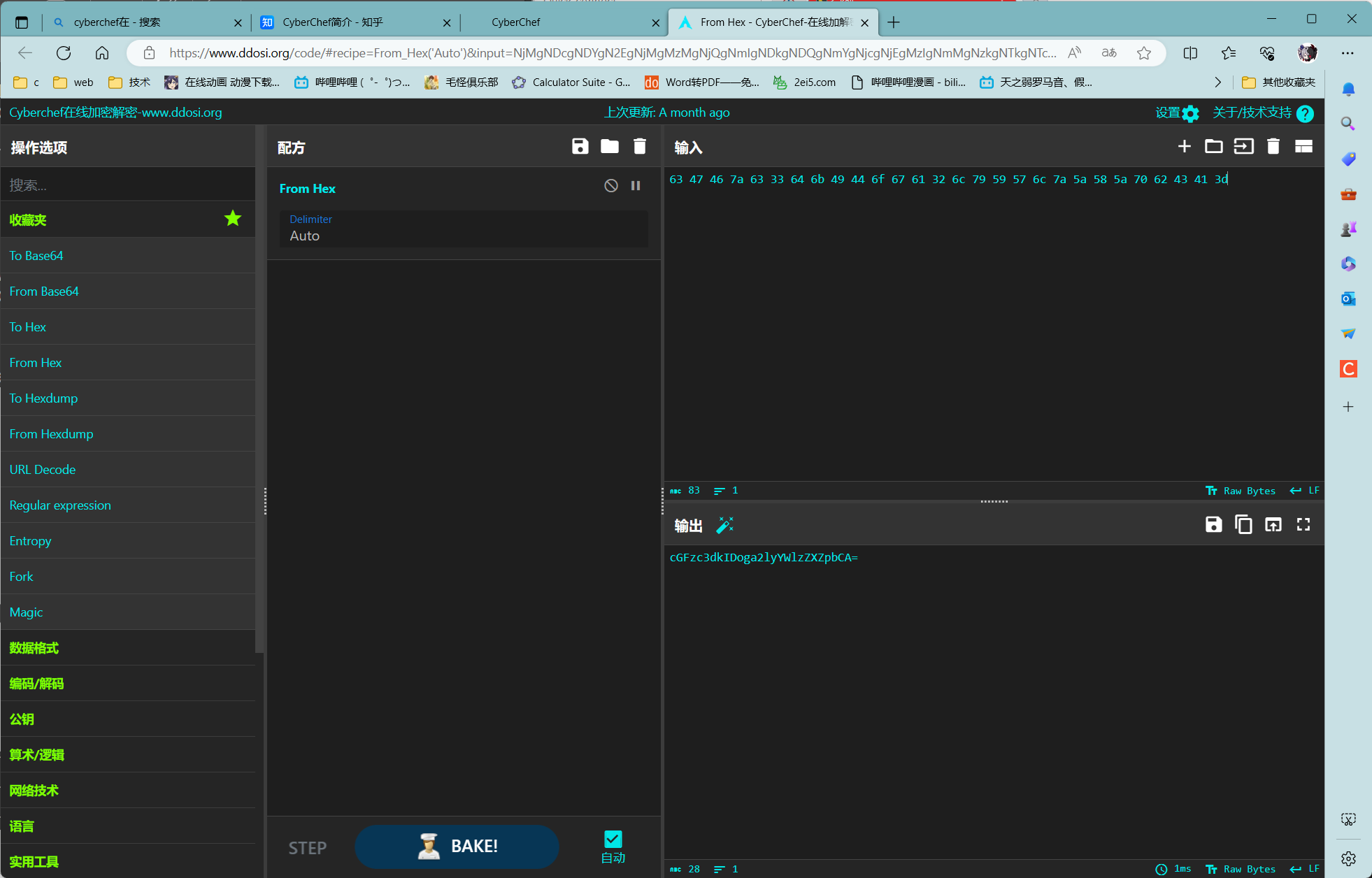
进kira看



这里面说去fake里面看

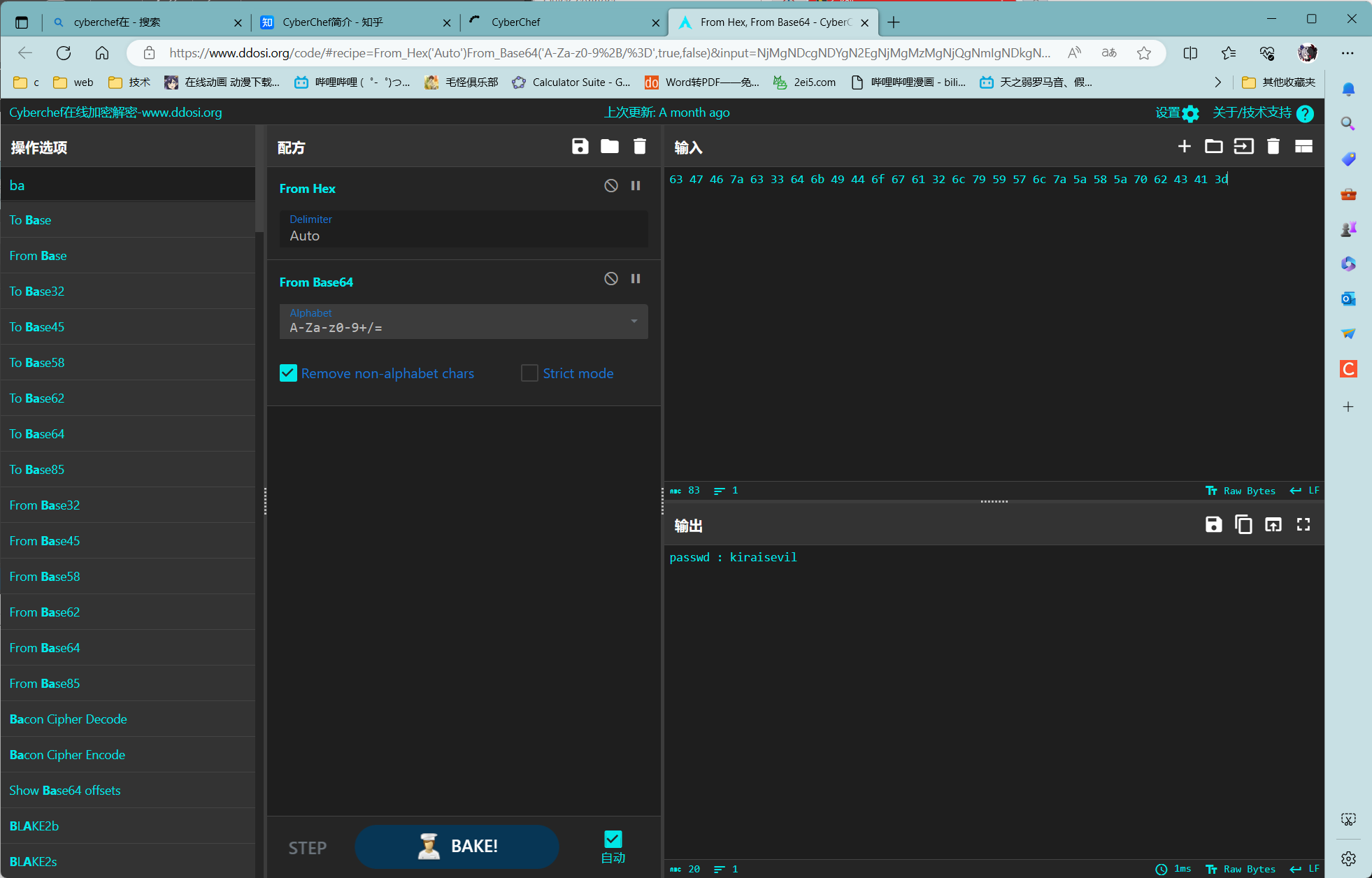


16进制数



cGFzc3dkIDoga2lyYWlzZXZpbCA=

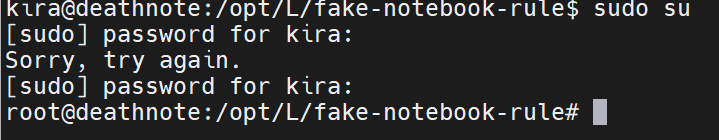
base64



Kiraisevil

密码拿到

这个就因该是root的密码（kira）



搞定

