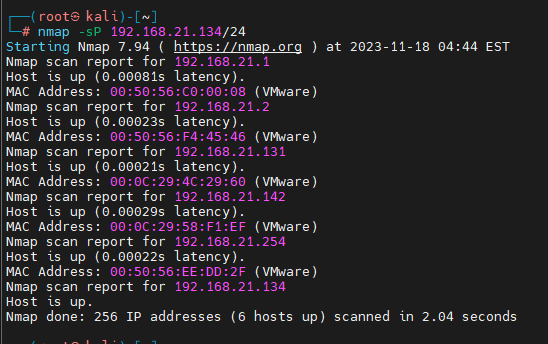
HotelWW

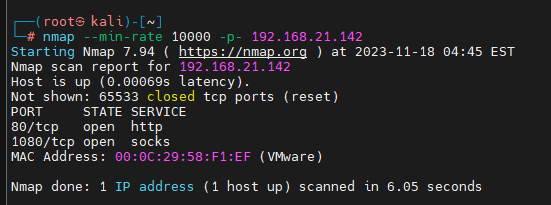
下载地址：https://download.vulnhub.com/worstwesternhotel/HotelWW.ova

主机发现

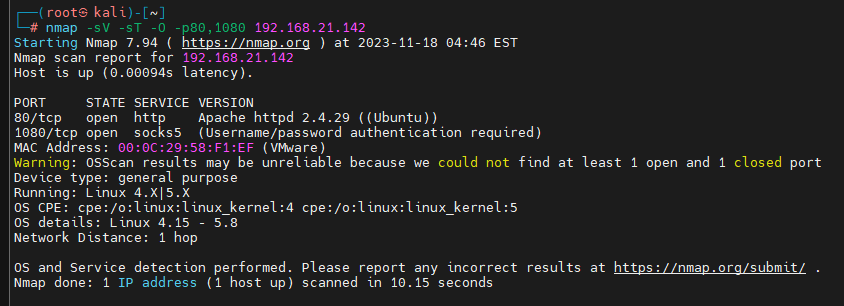


目标142

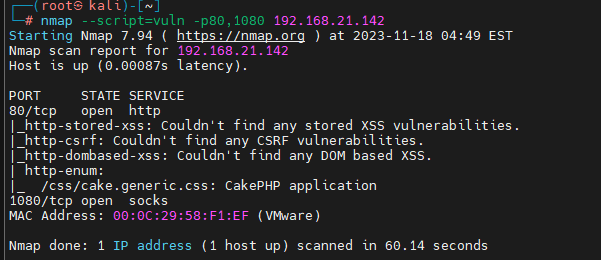
端口扫描



服务版本扫描



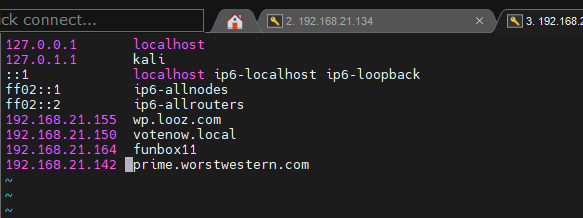
漏洞扫描

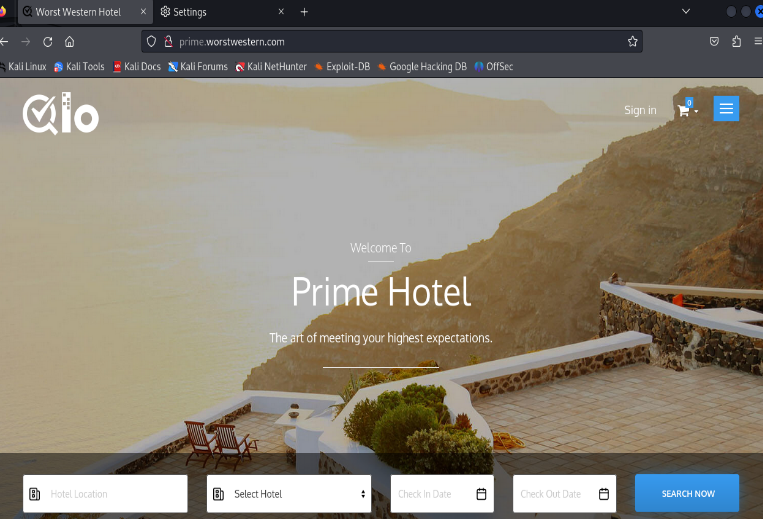


看一下web

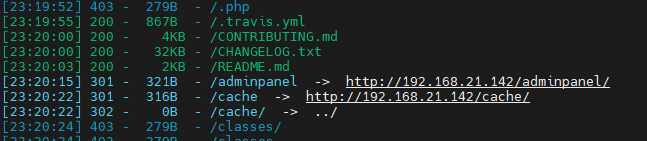


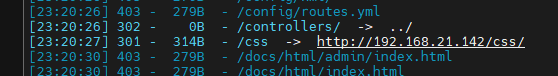
好好好这么玩改host

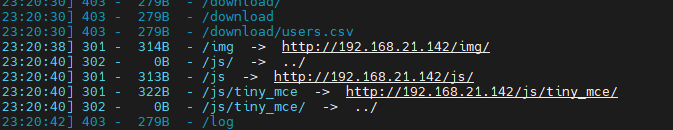


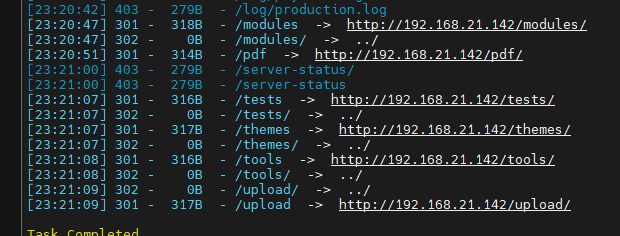


啥也没有先做个目录爆破

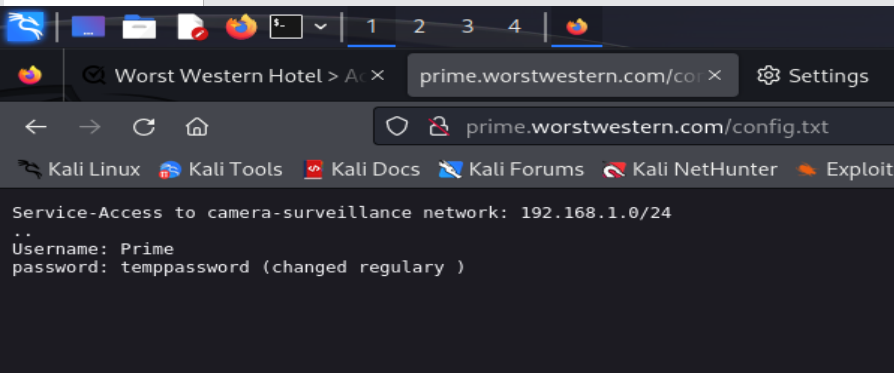








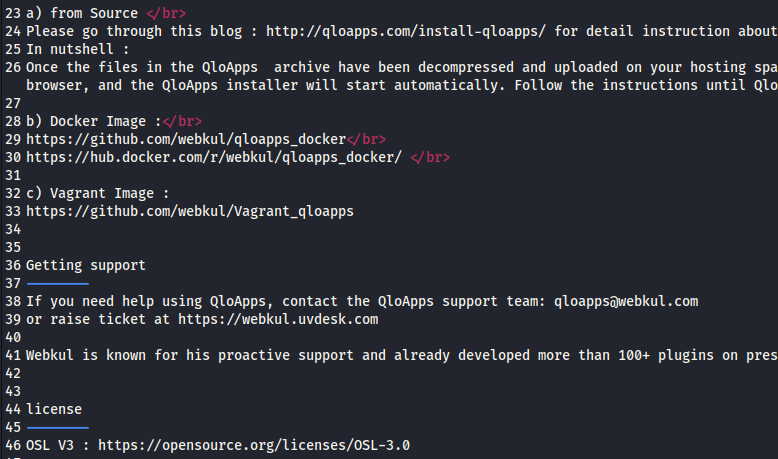
扫描太慢我就没看了看几个重点的txt（robot,config，readme）（边看边扫）



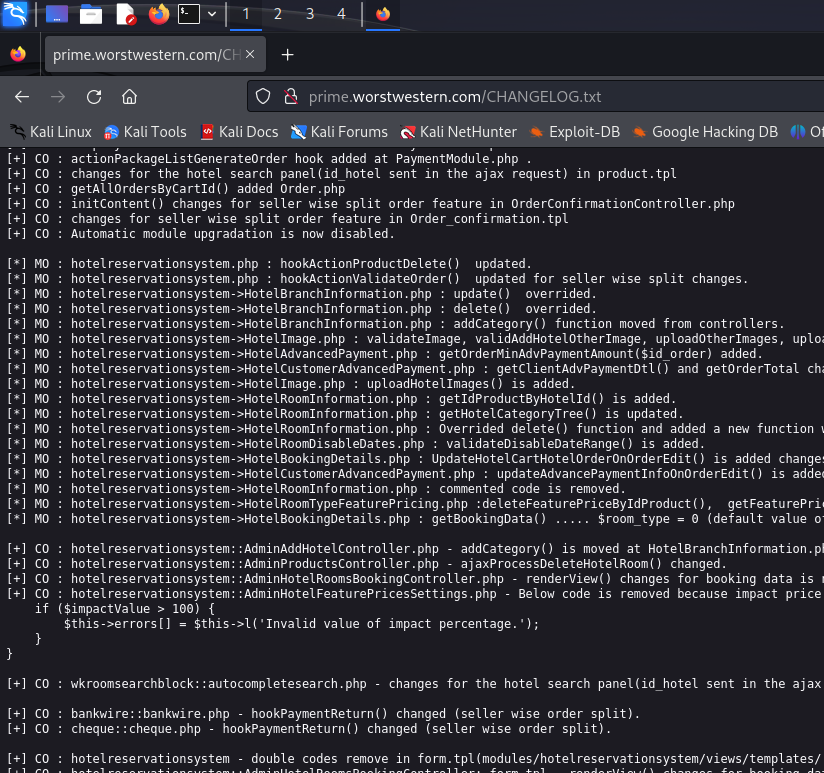
看到密码了（但是被改了，可以用用户去爆破）

应该是1080端口登入

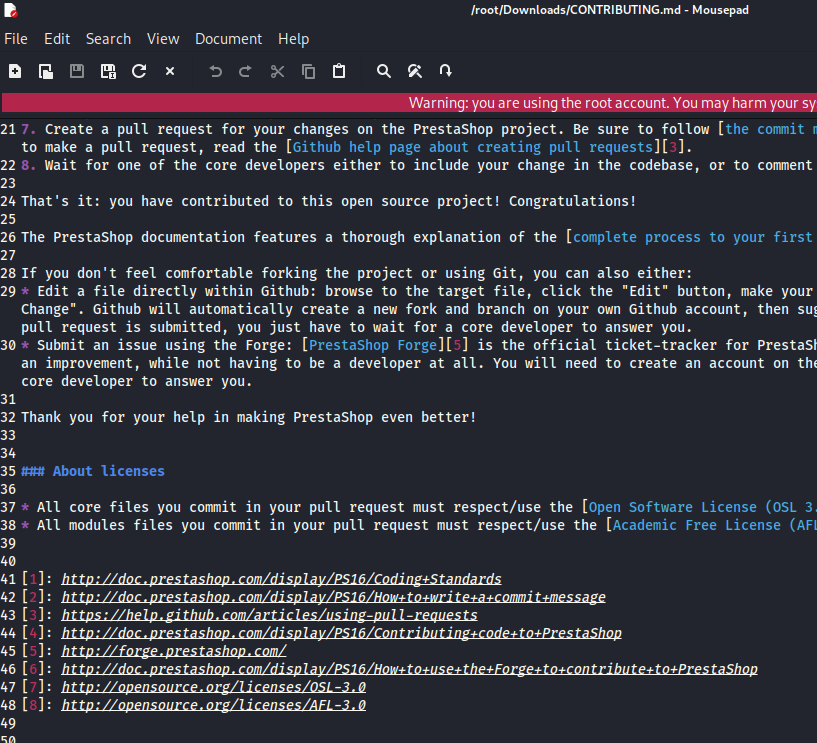
然后里面有readme.md文件，这里泄露了源码

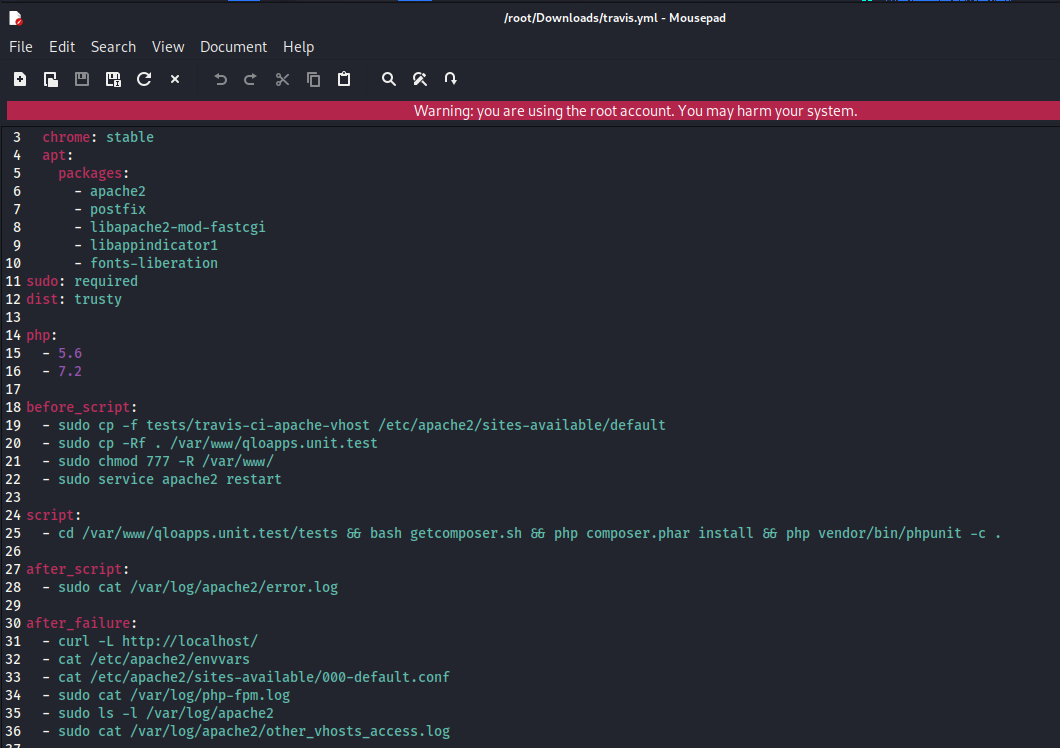


再看一下别的东西



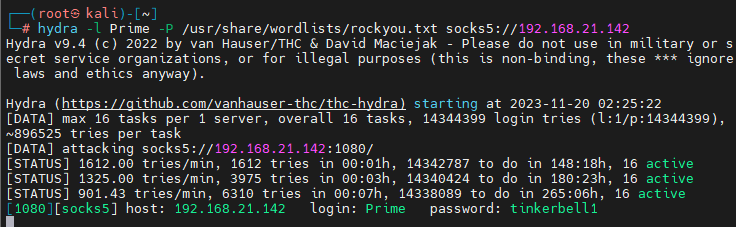
好部分php文件也来了





拿到这玩意就不用多说了吧

接下来socks5爆破



tinkerbell1（爆出来就停，这玩意就是慢）

登入登入登入！！！！

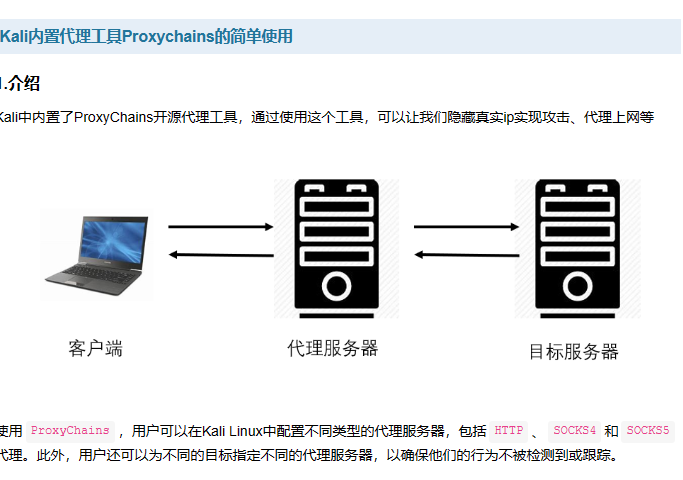
在此之前socks5

[Socks5工作原理与搭建\_東魔的博客-CSDN博客](https://blog.csdn.net/CZD__CZD/article/details/120493190)



简单点说这玩意就是代理

[Kali内置代理工具Proxychains的简单使用 - junlin623 - 博客园 (cnblogs.com)](https://www.cnblogs.com/junlin623/p/17442091.html)



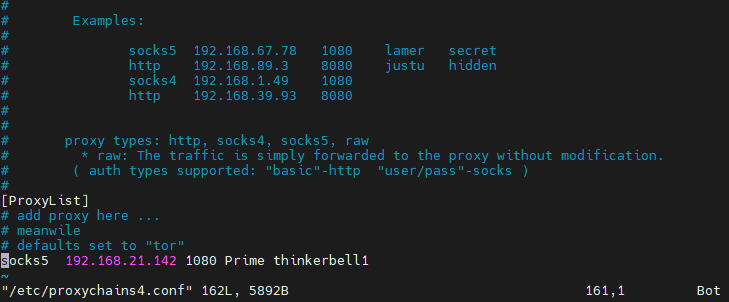
工具也能找到，修改配置文件用我们爆破到的东西做代理



修改一下配置文件开启dynamic\_chain

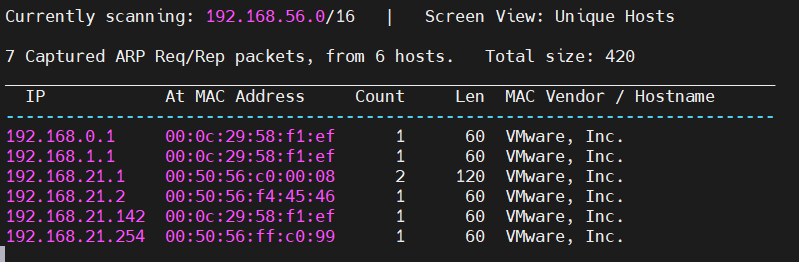


代理记得写用户名和端口



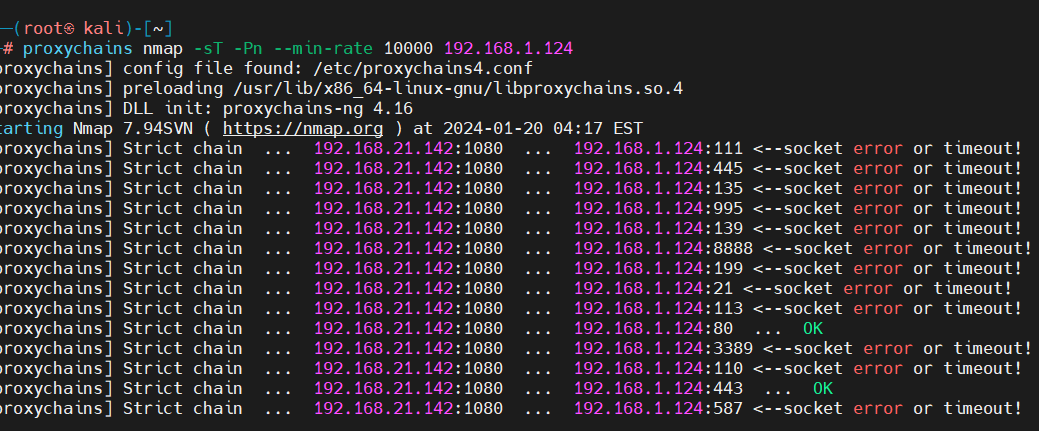
用proxychains扫描，注意一下这里nmap扫描存活主机是利用icmp包扫描的，但是这玩意代理不了icmp包只能直接利用端口扫描来判断主机是否存活（注意要升级工具！一定要升级！！！）

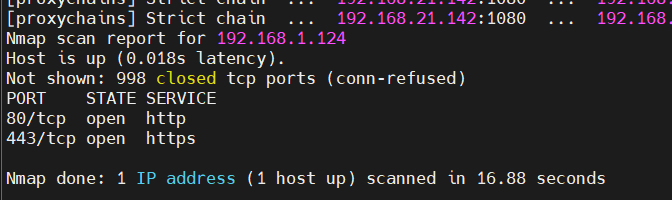
主机发现一下



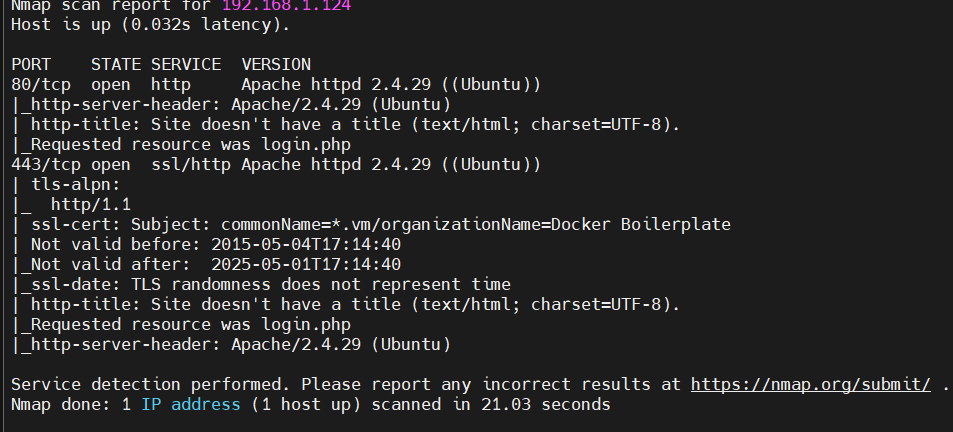


等一下就出来了





服务扫描

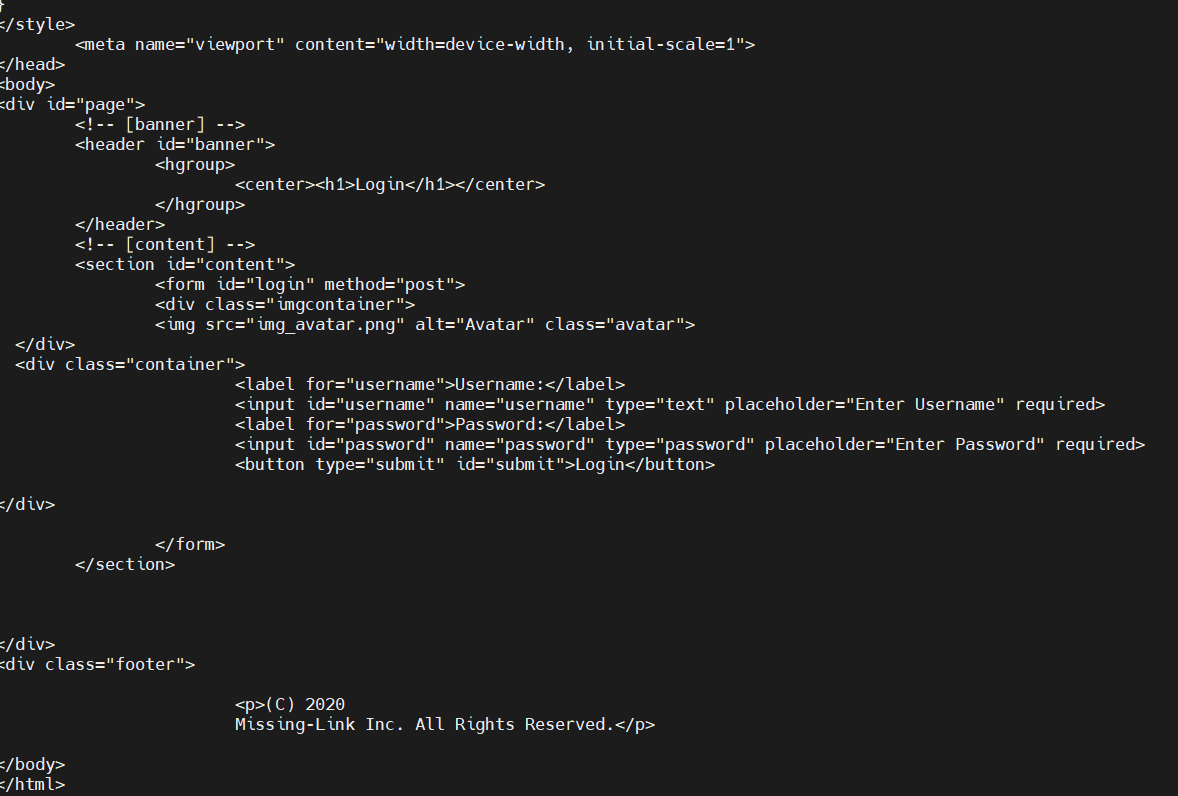


看一下web



做个目录爆破

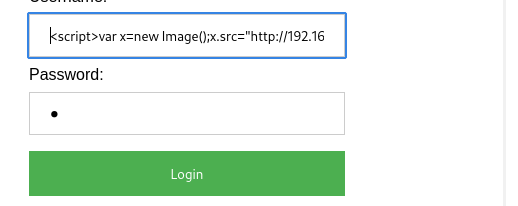
里面有xss

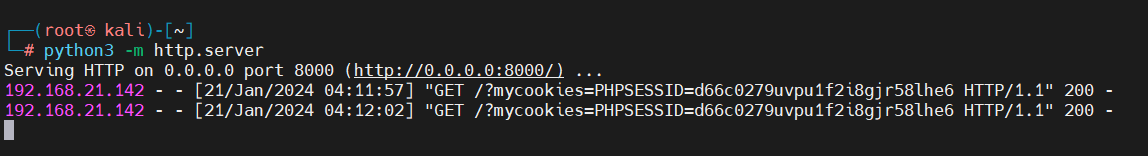


注意一下要在kai里面用



xss利用



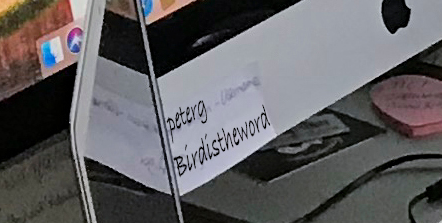


改cookie就能登入

mycookies=PHPSESSID=97sdv5cao935djcfkfqi7dav4u

http://192.168.1.124/4063830e548b8aea3586473c668aac826516be33/c49675b5b5ef6ac738587d12051b607b13c78c79.jpg

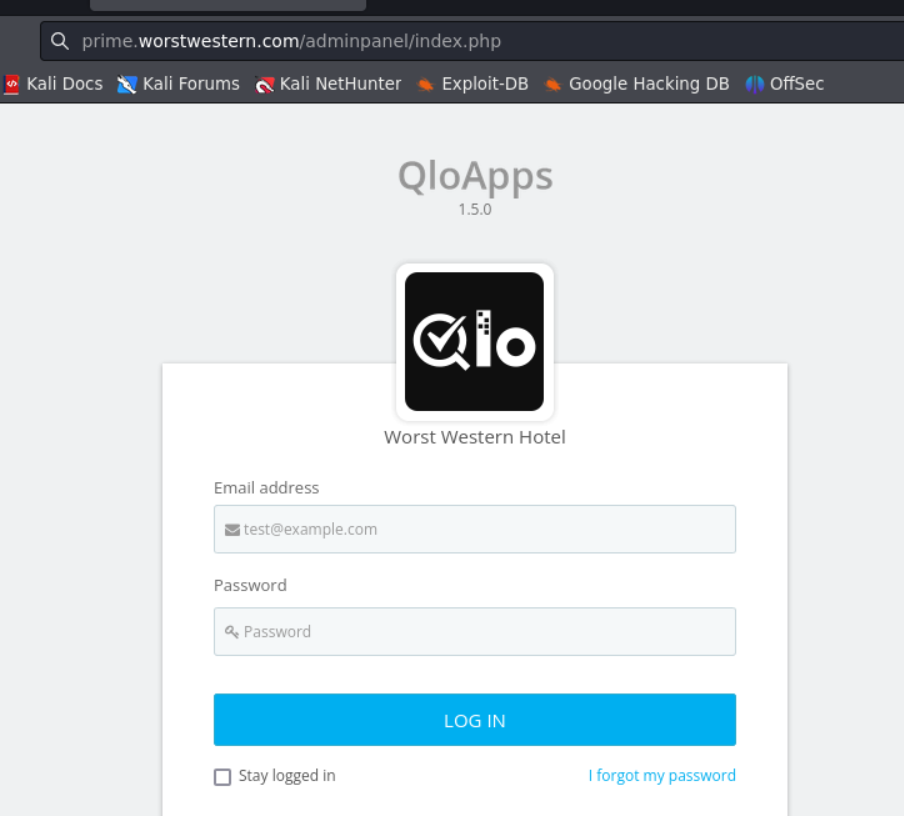
有个照片

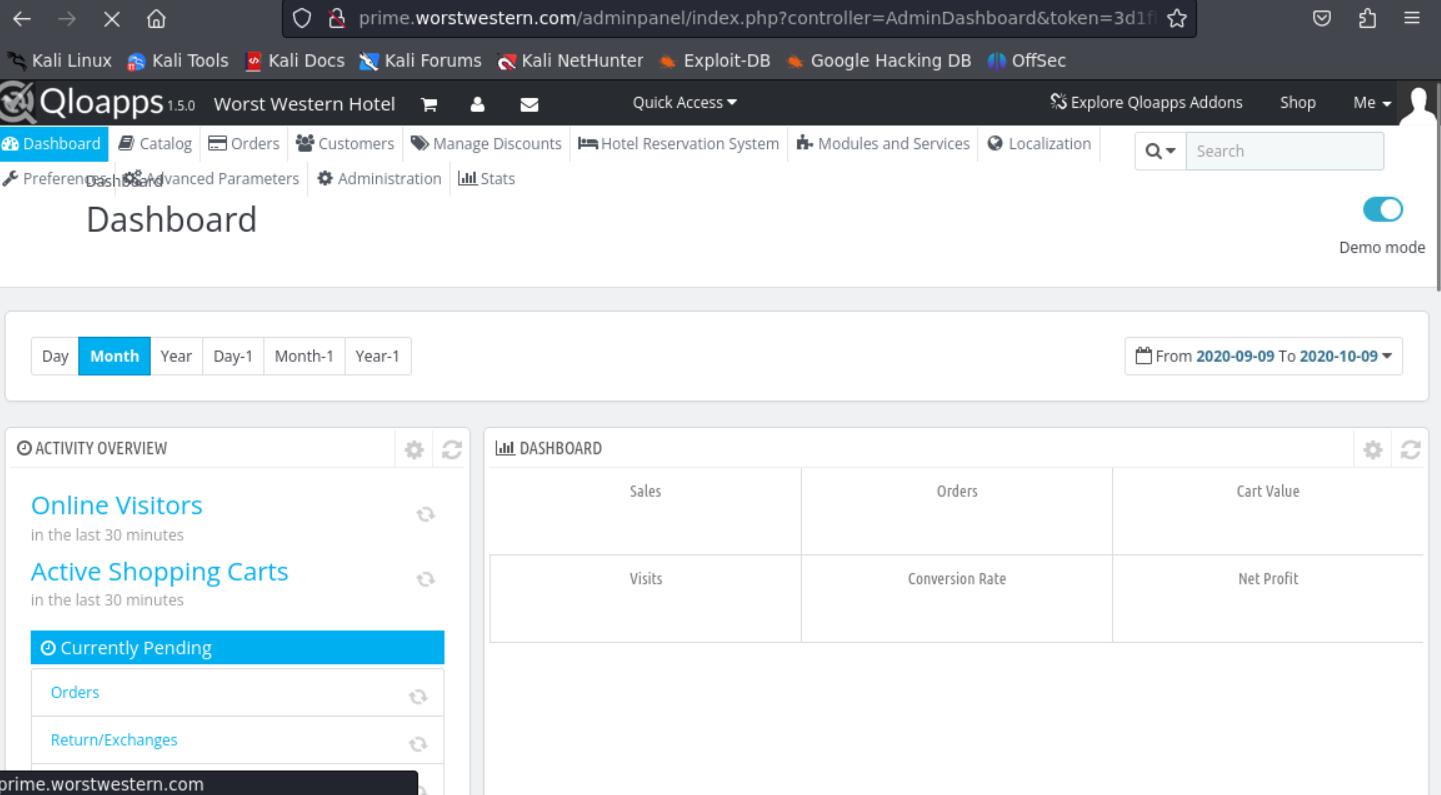


账号密码？

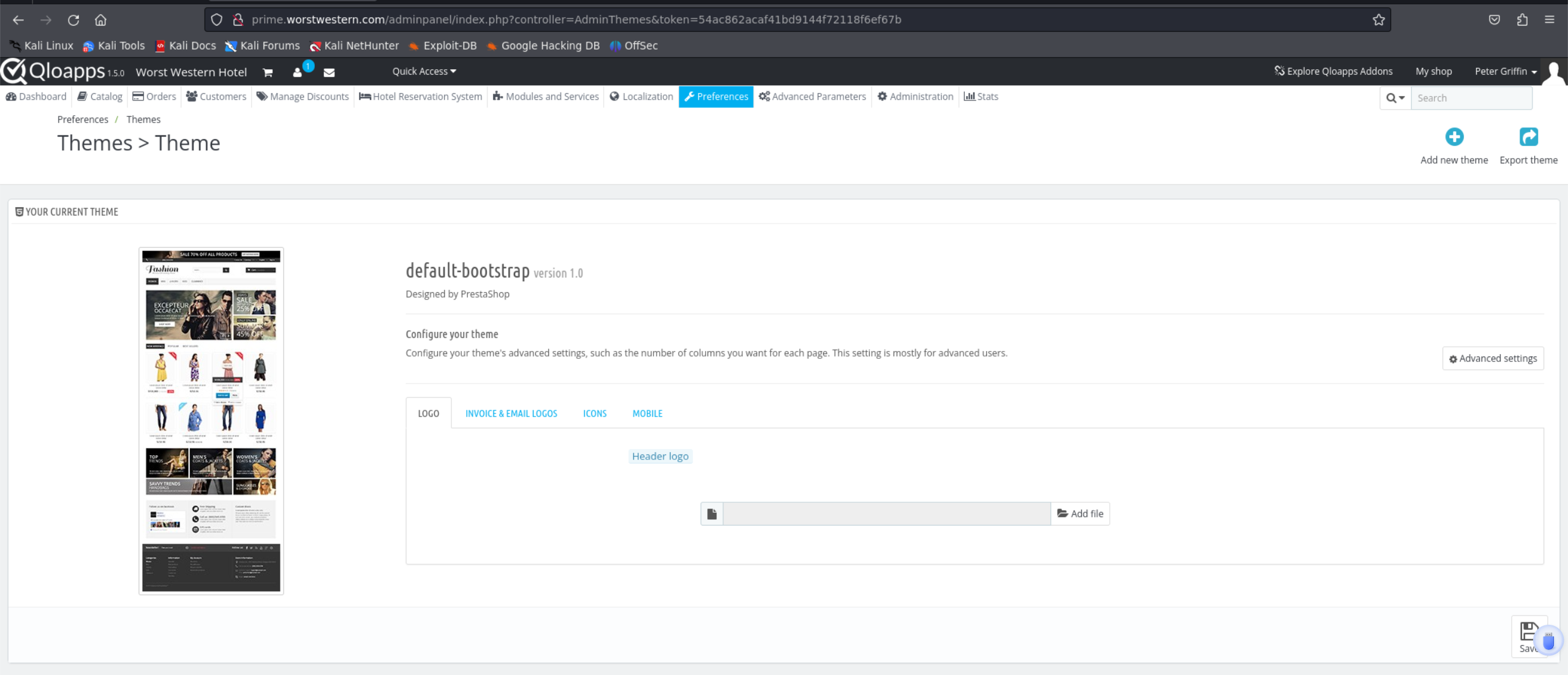
可以试试

前面的登入无法登入就能想到我之前扫出来的admin有关的字段能直接才出来那个应该是后台



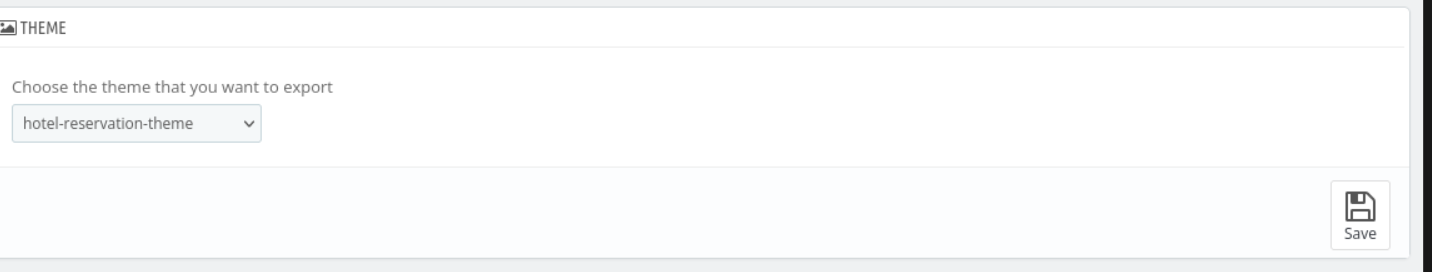


想着上传文件反弹shell，翻一下

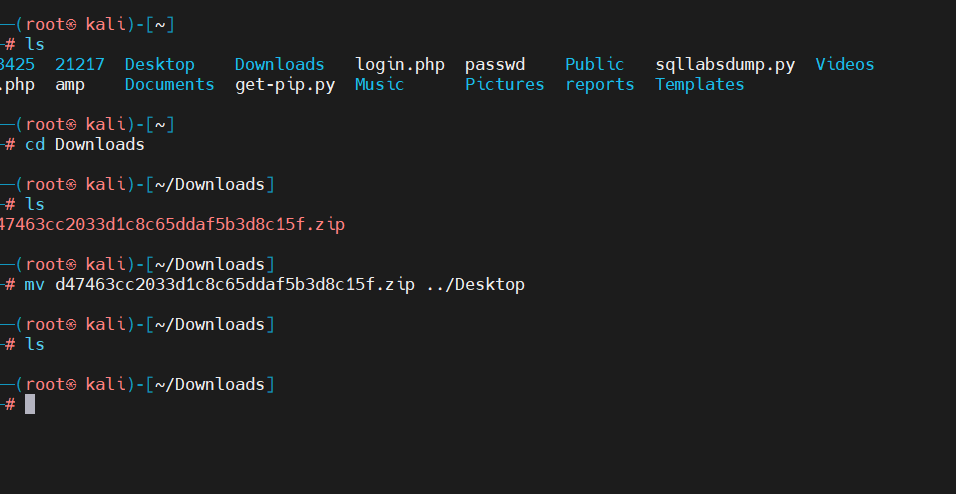


应该是这个，利用在线的反弹shell生成一个上传就可以

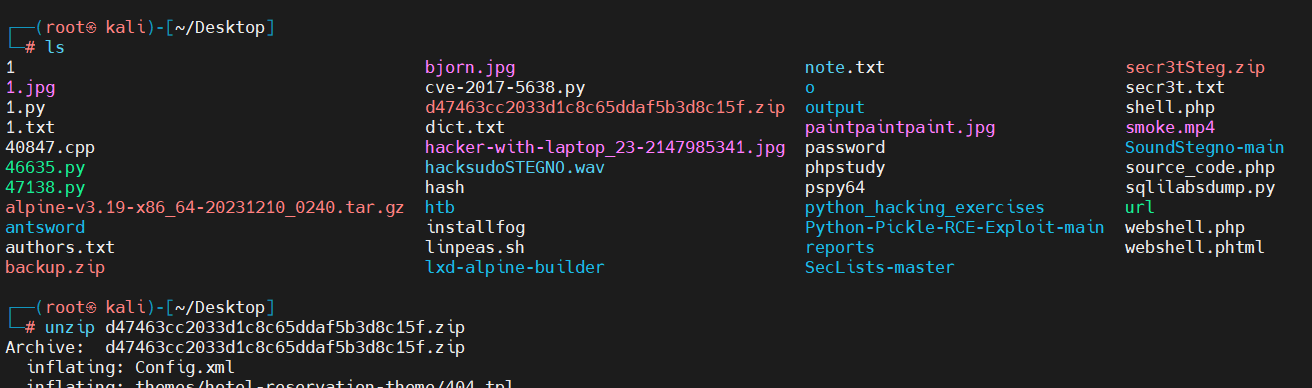
先导出方便点

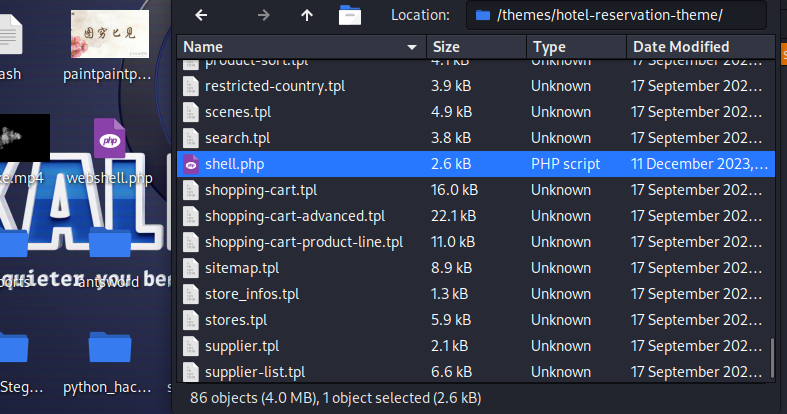


下载下来

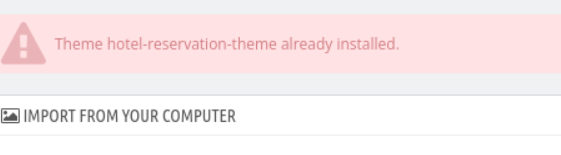


吧shell加进去

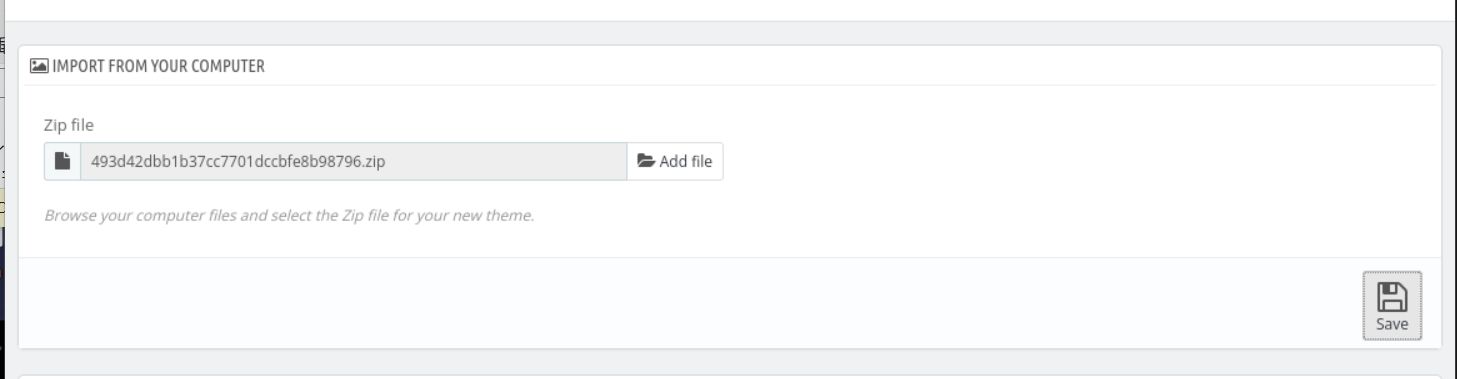


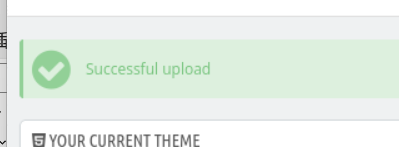


再上传就可以

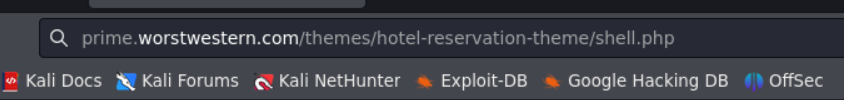


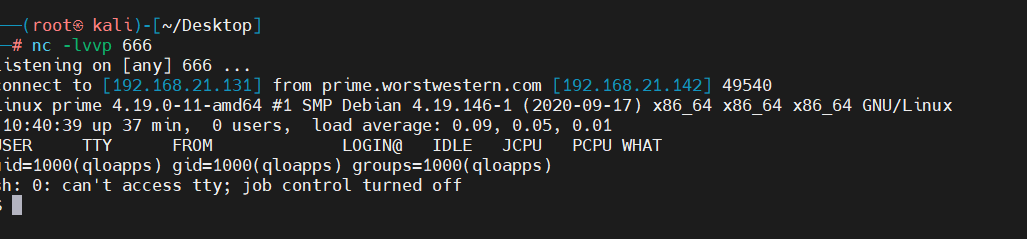
要改名字



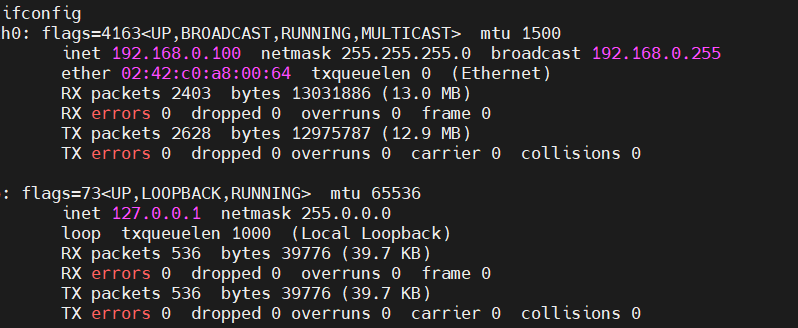


访问记得挂nc

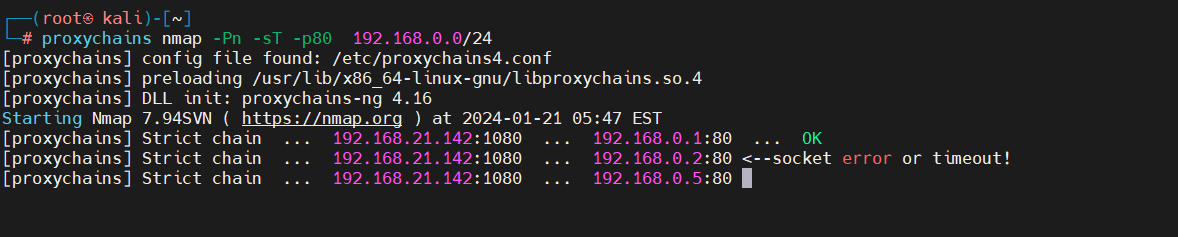




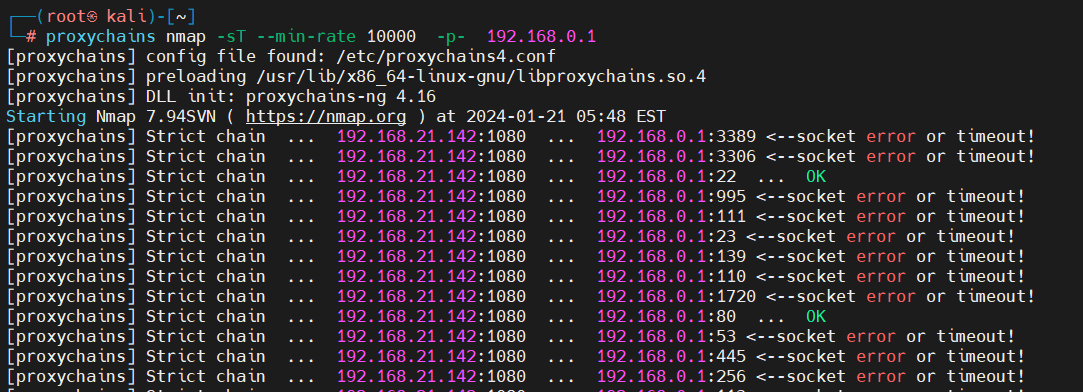




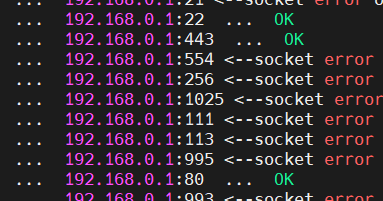
啊？又来



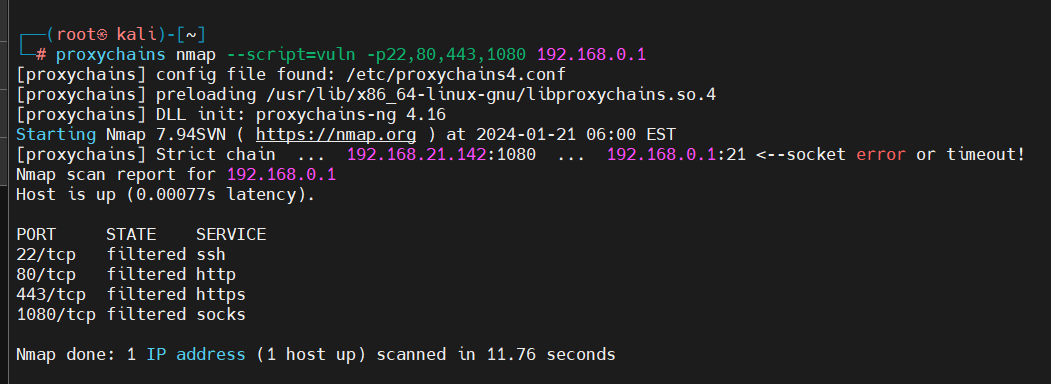
目标应该是这个之前网络发现也是看到了

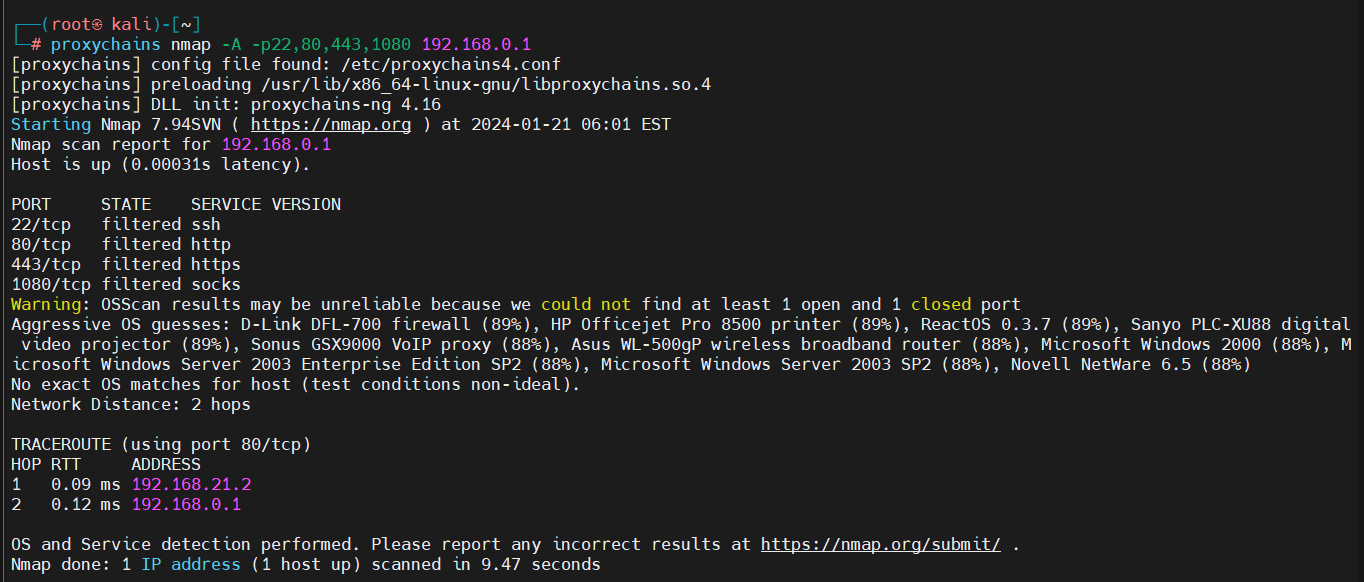






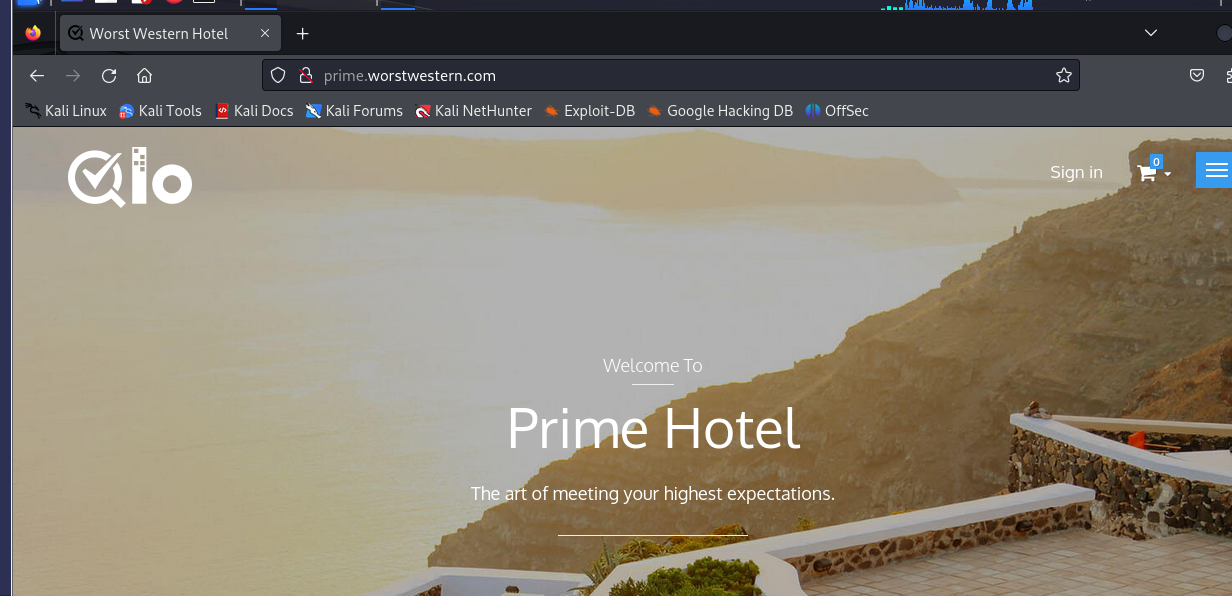
看一下服务



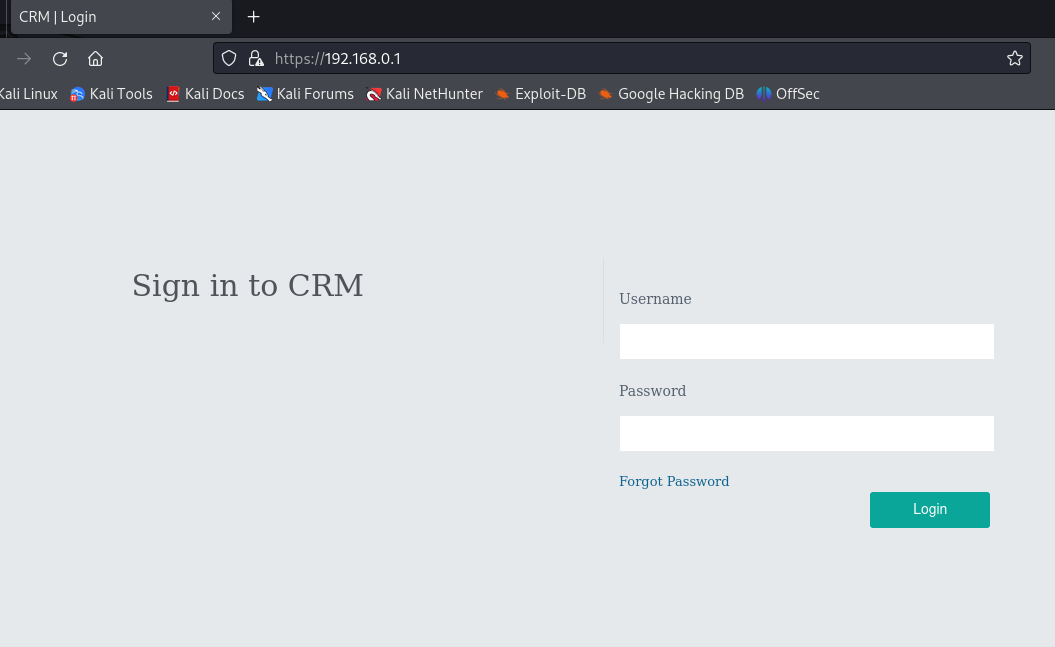


是说麻一般的扫描扫不了原来是防火墙真该死

去看看各个端口

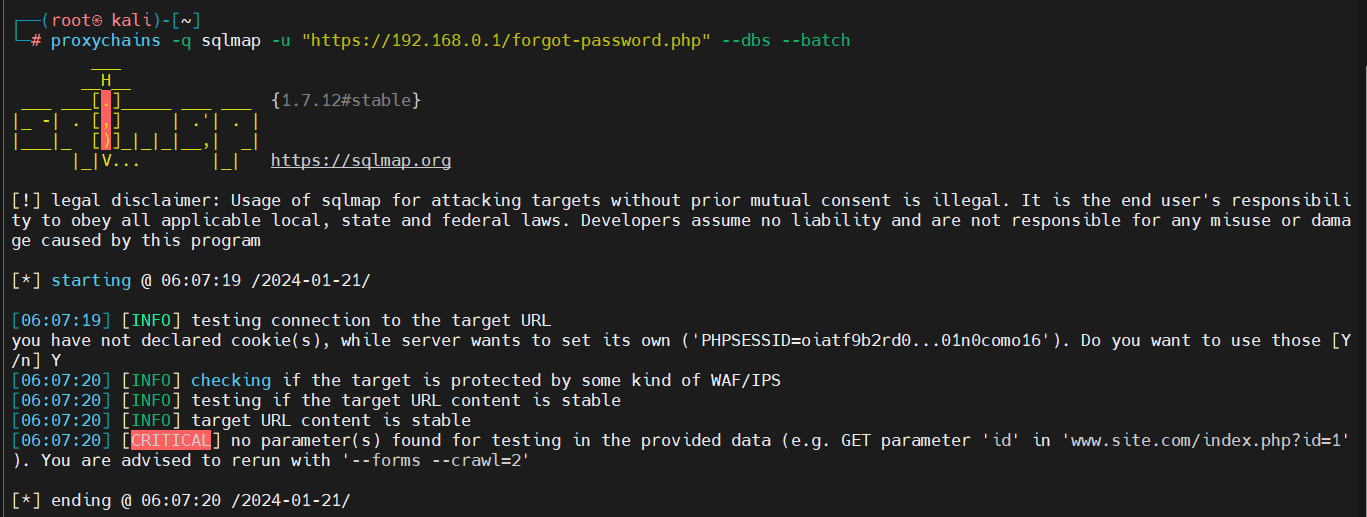


80还是和之前的一样



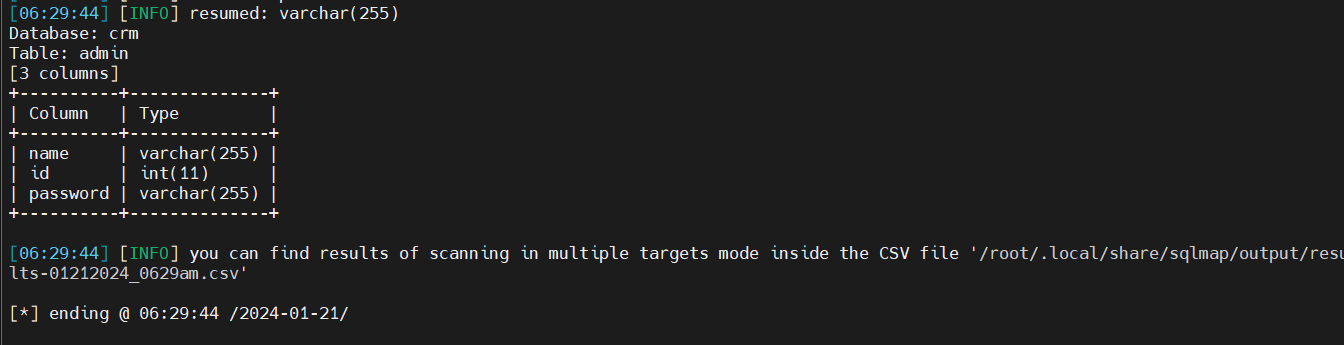
443还非要用https

盲猜是sql注入

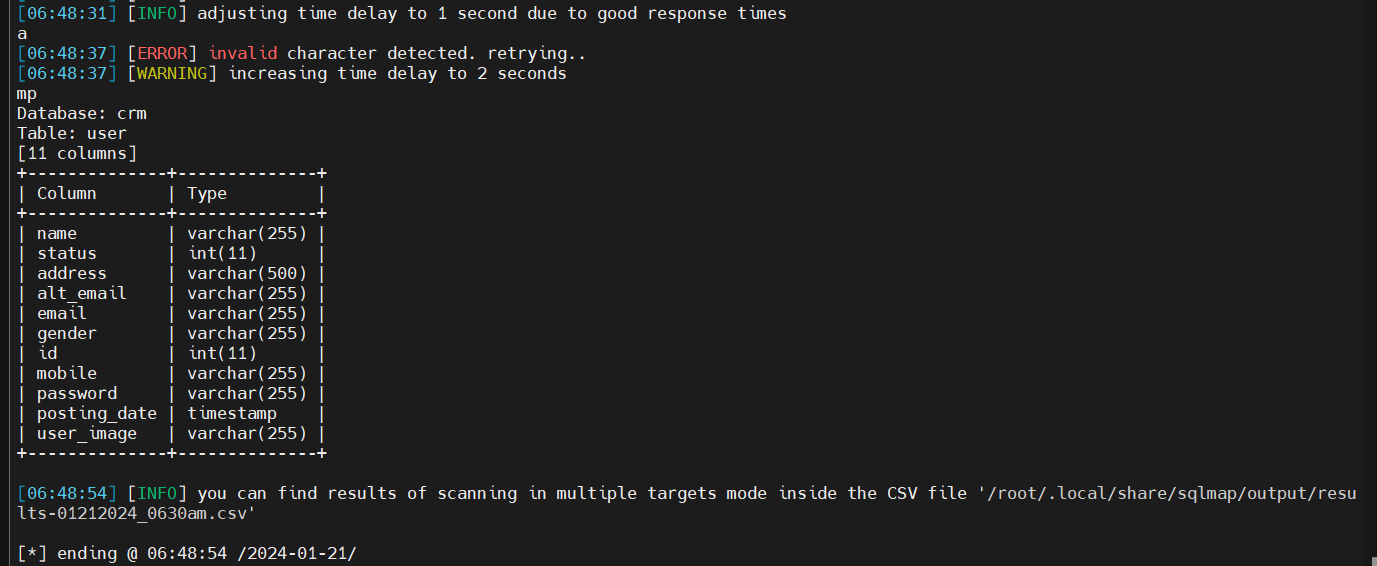


要加参数

admin

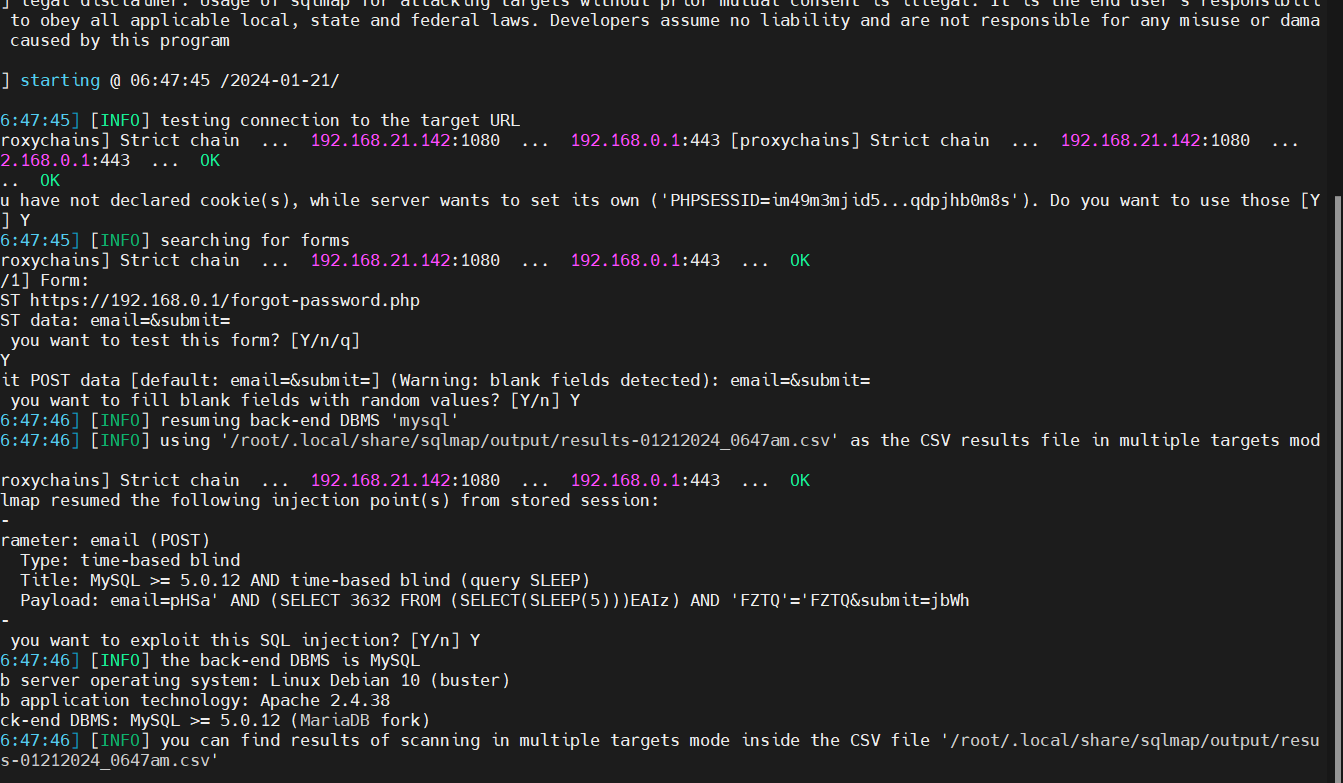


user

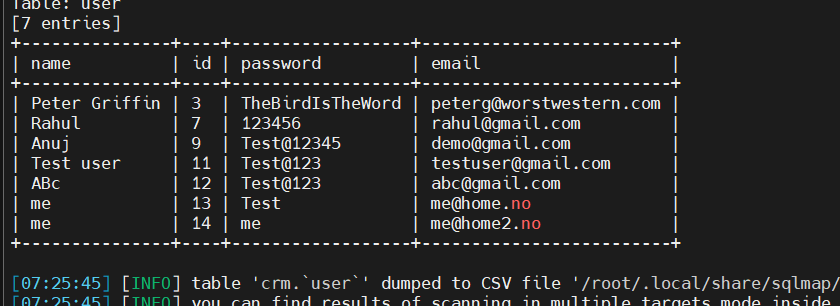


数据

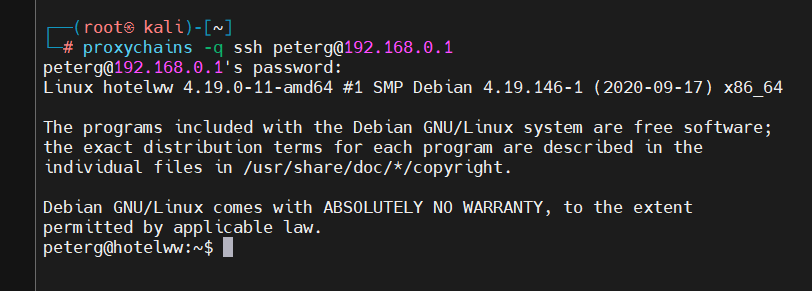
admin访问不了

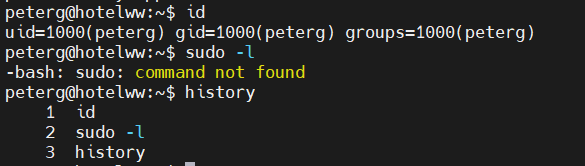


user数据

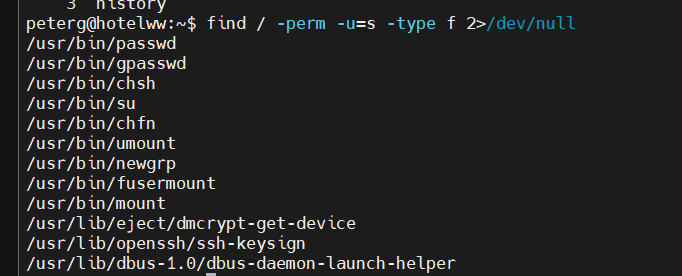


第一个就能登入进去了

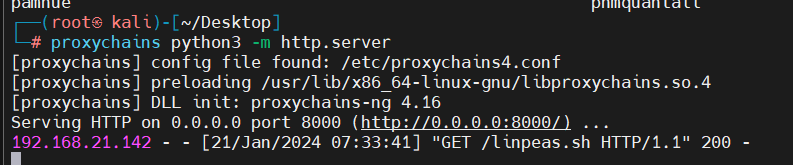


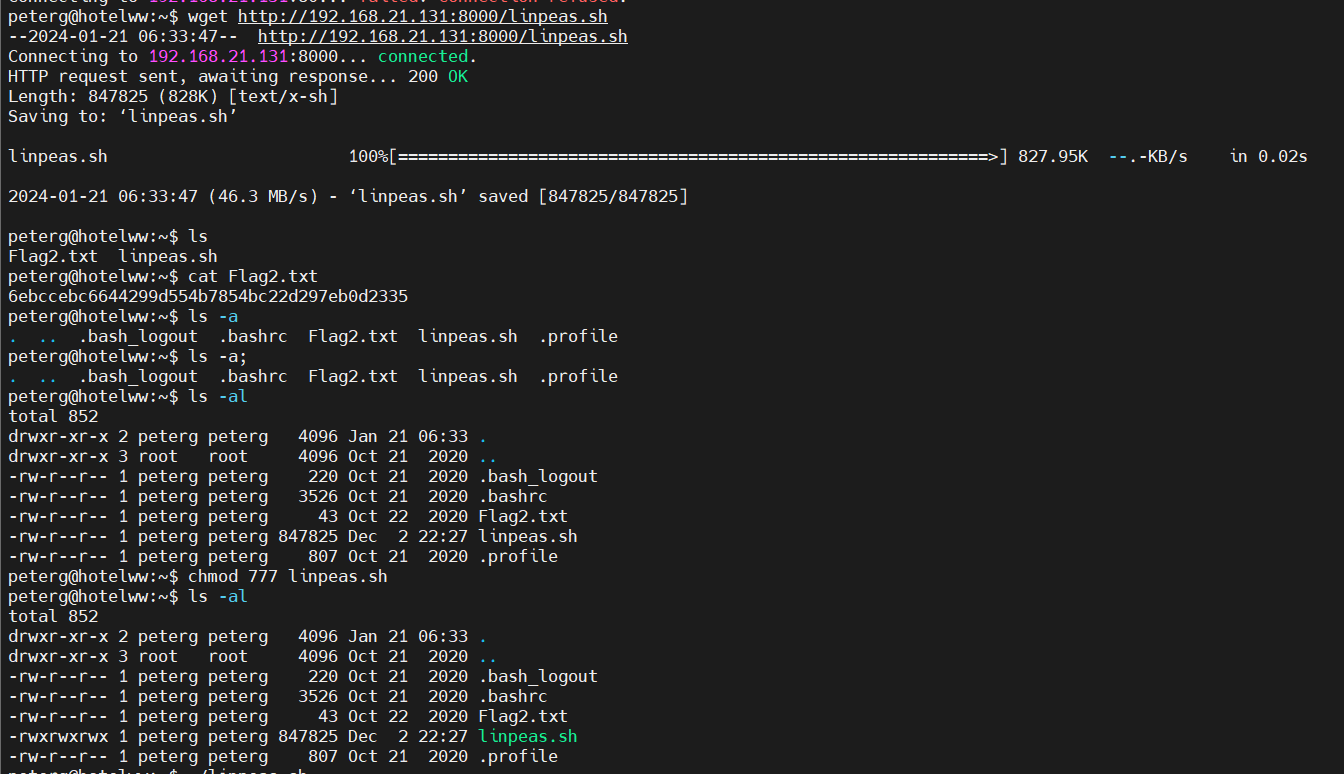




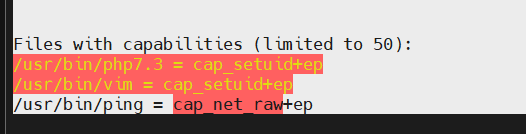


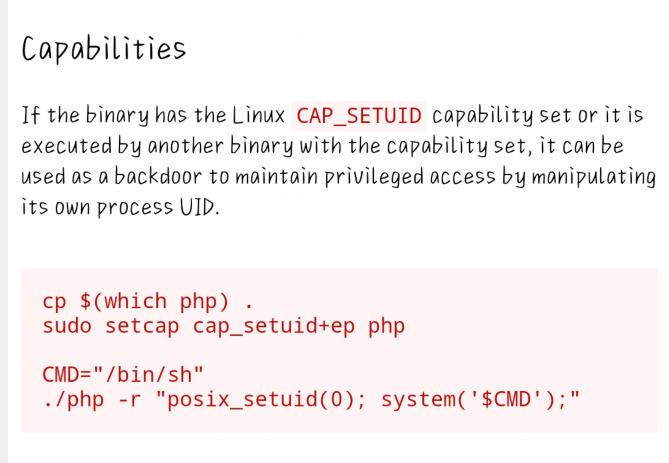
没什么思路用linpeas吧





运行





这个图是收集访问的见谅

利用这个就可以



烦人要严格按找上面的来，不然不行





结束