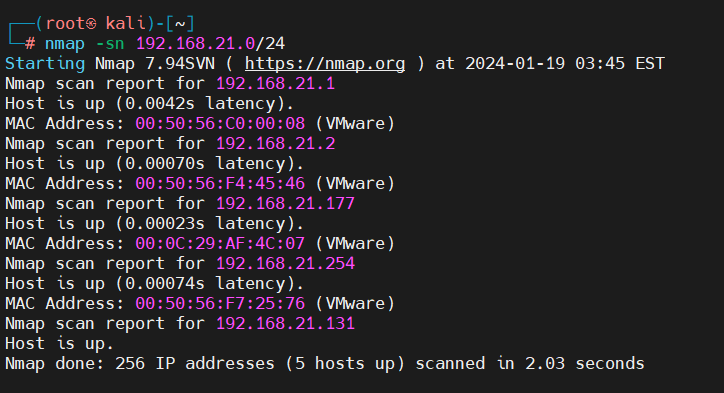
BlueSky

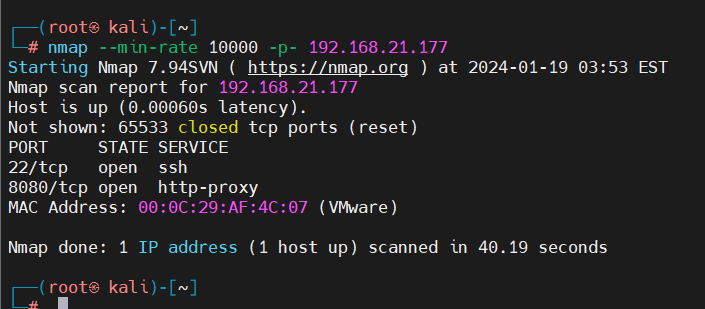
下载地址：<https://www.vulnhub.com/entry/bluesky-1,623/>

主机发现

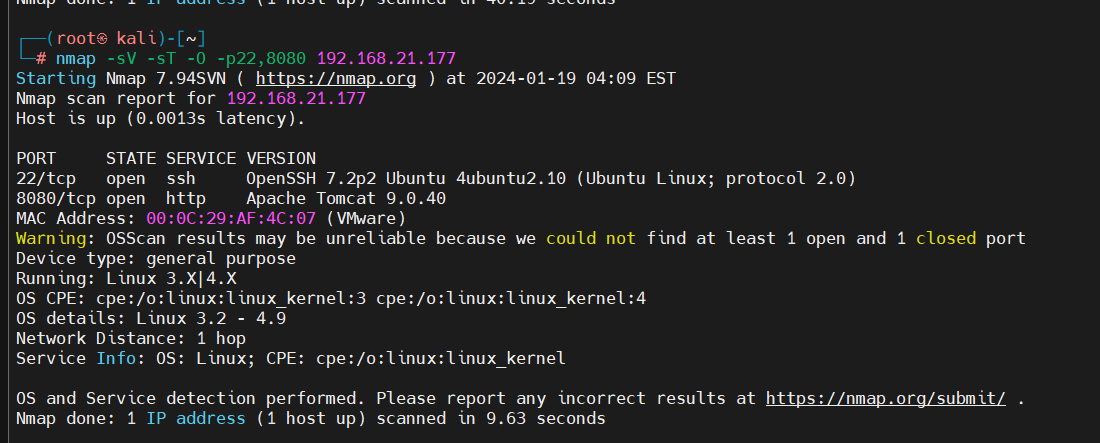


目标177

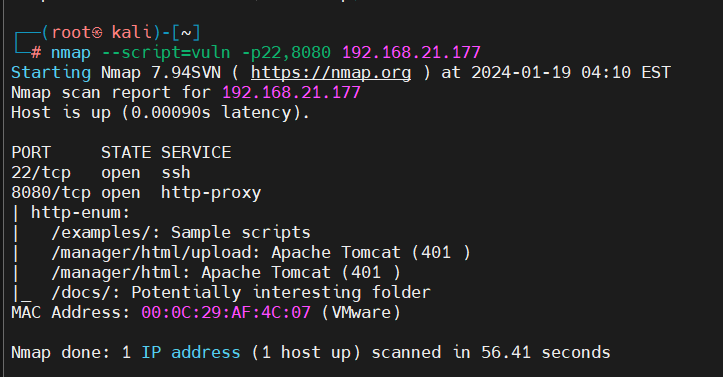
端口扫描



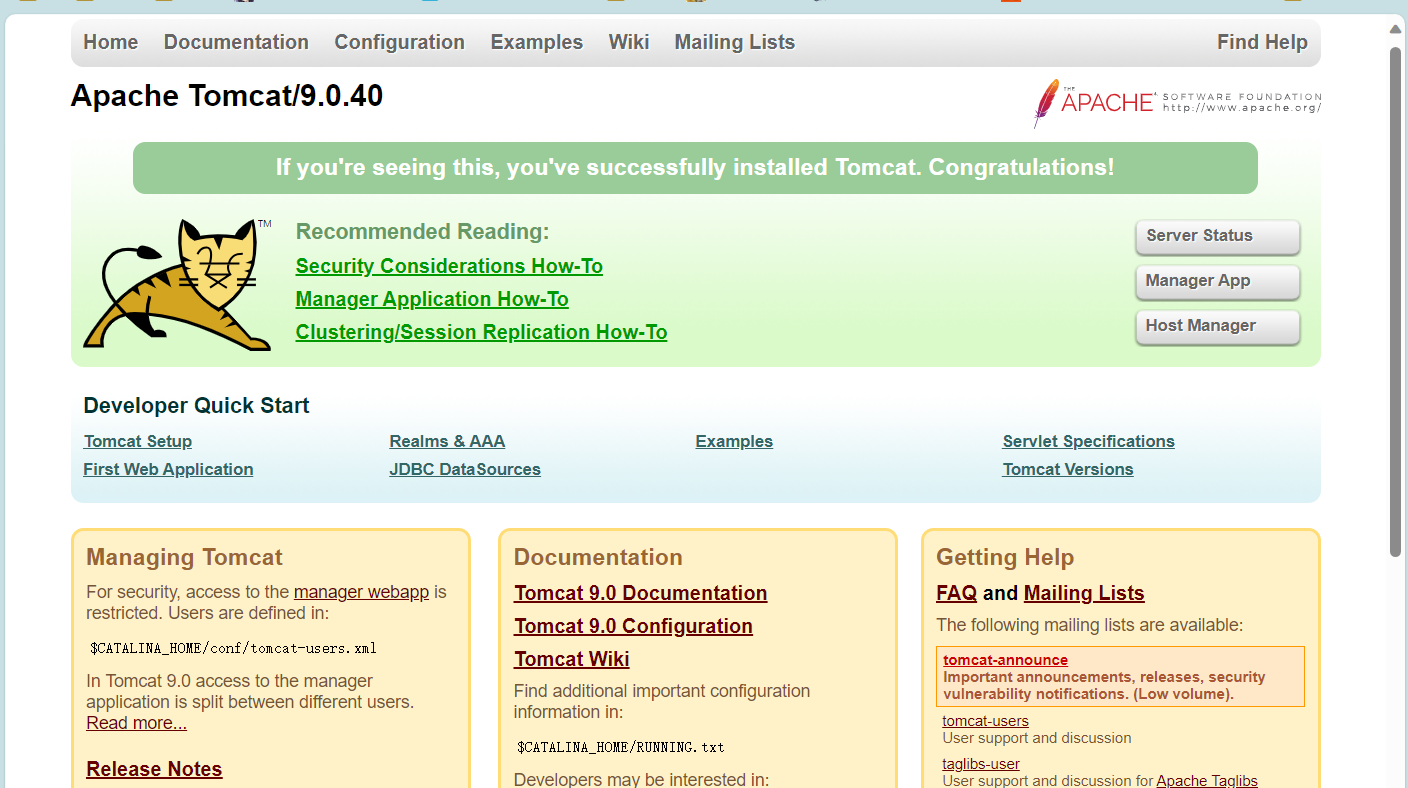
服务扫描



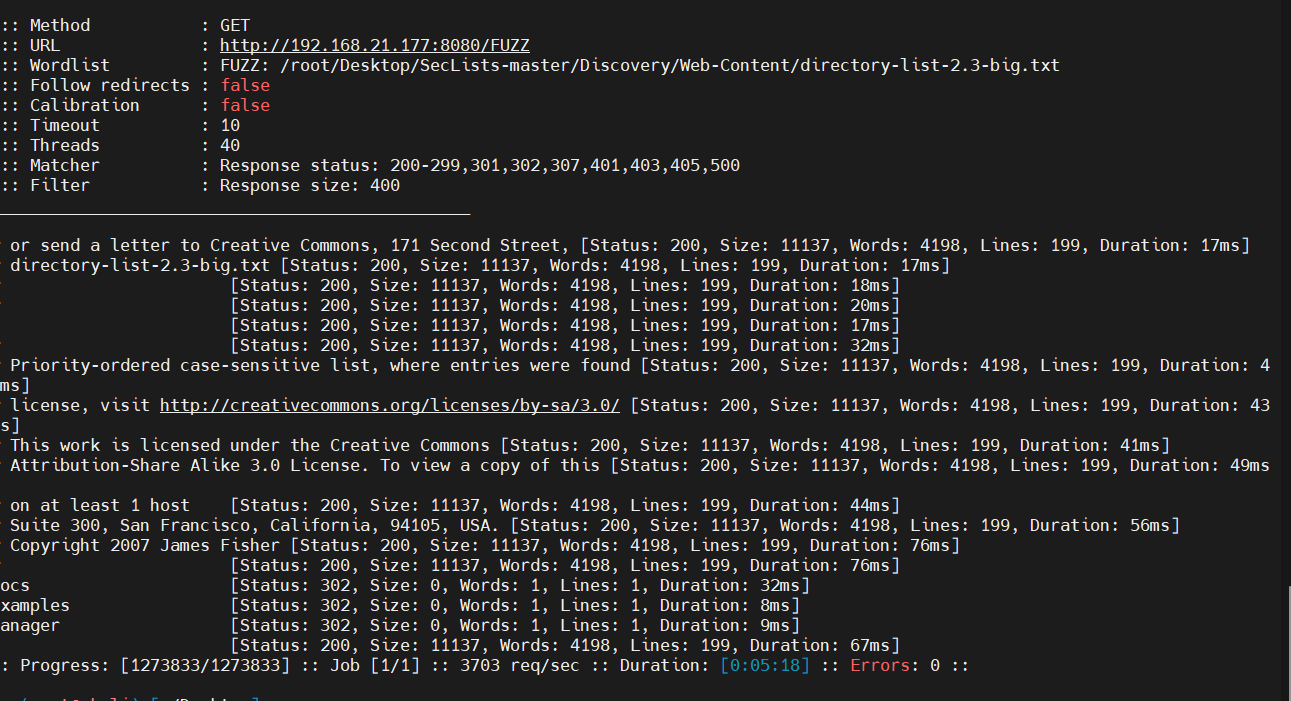
漏洞扫描

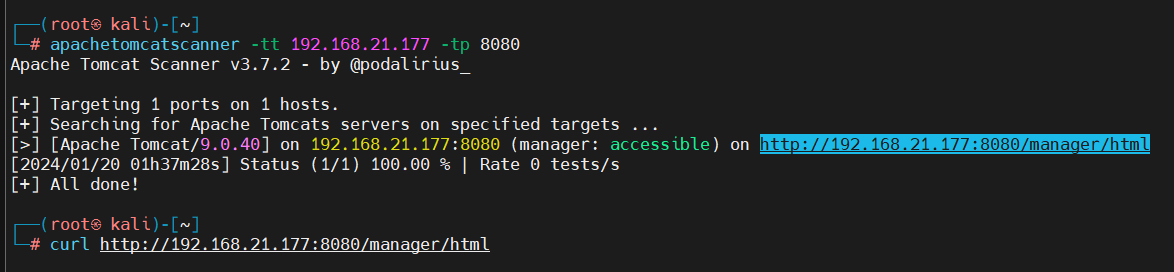


看web就不用我多说了吧

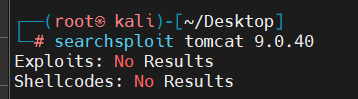


默认页面，爆破吧





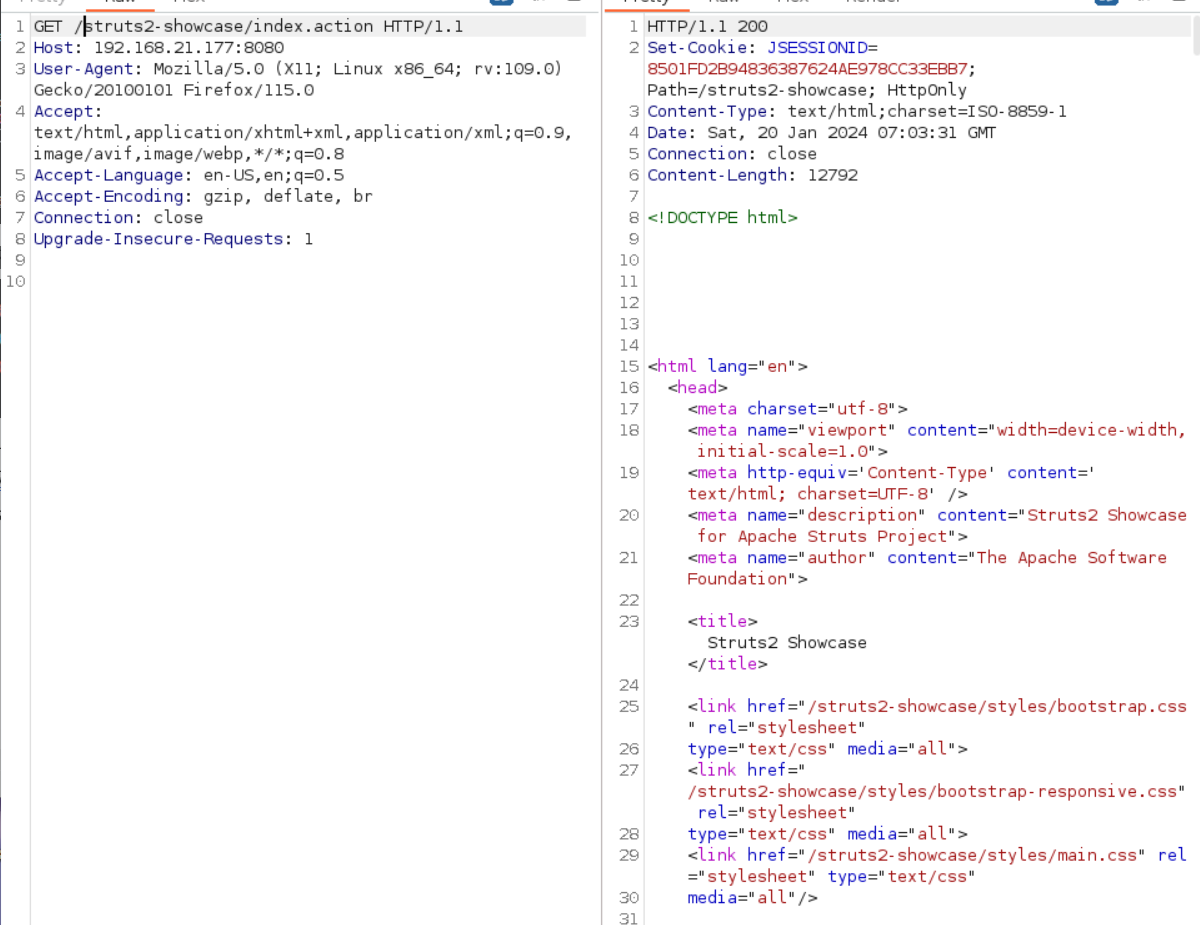
这个也没有扫出来

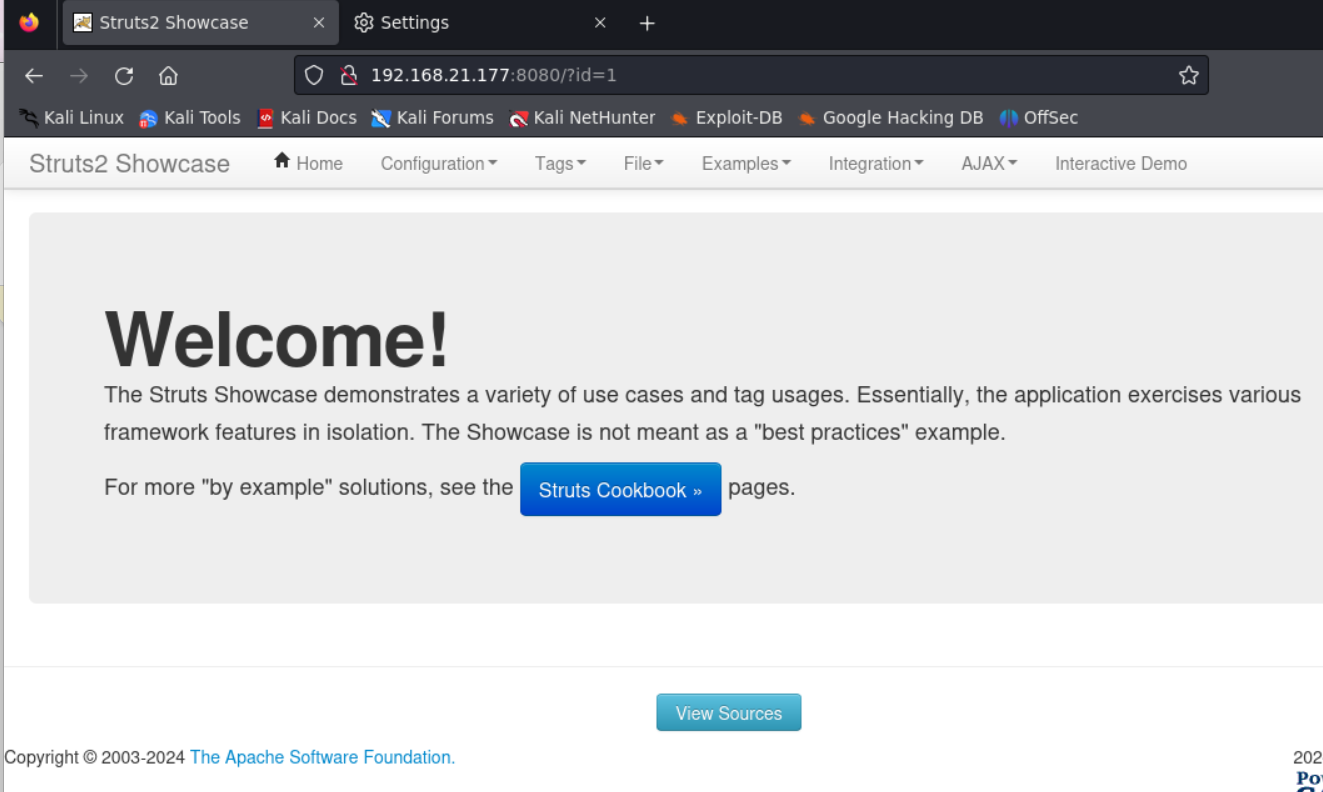


有manger/html但是没有任何返回值

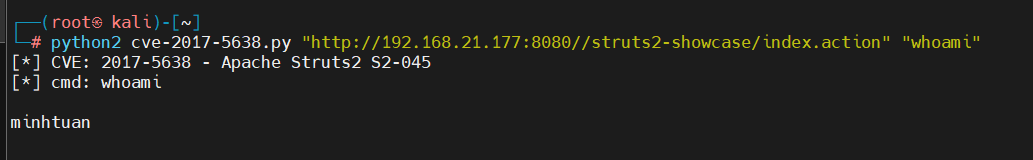
应该是限制本地访问或者禁掉了

网上直接用struts2-showcase这个洞了

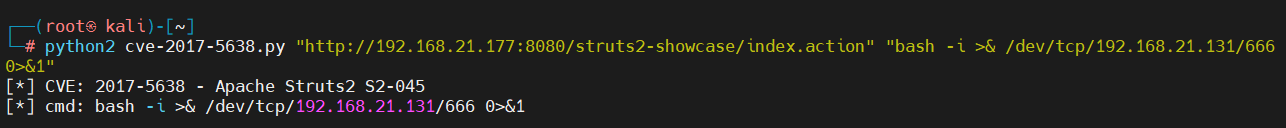


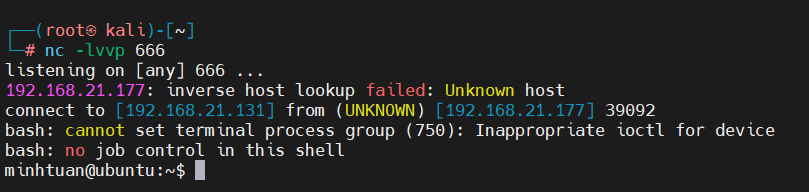
[cve-2017-5638/exploit/exploit.py at master · jrrdev/cve-2017-5638 (github.com)](https://github.com/jrrdev/cve-2017-5638/blob/master/exploit/exploit.py)

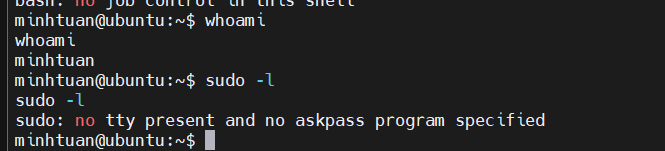
直接写进去

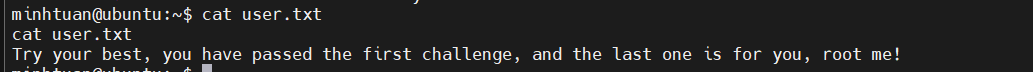


这里运用反弹shell



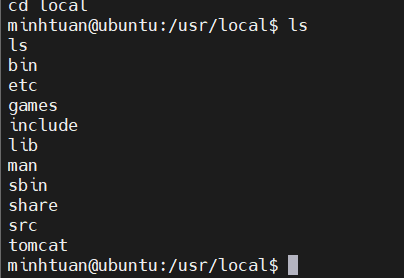


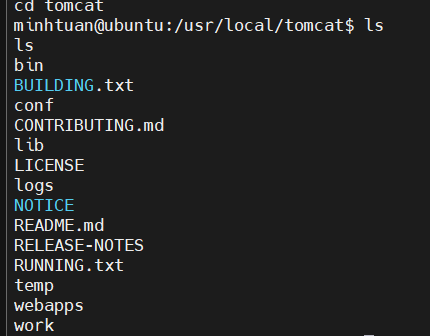


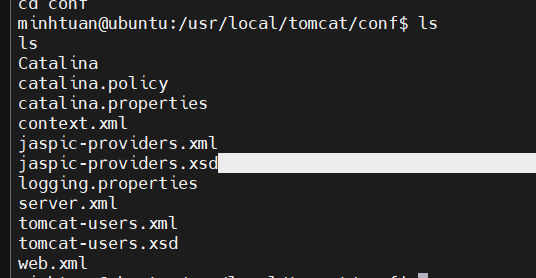


找密码

先去看看配置文件

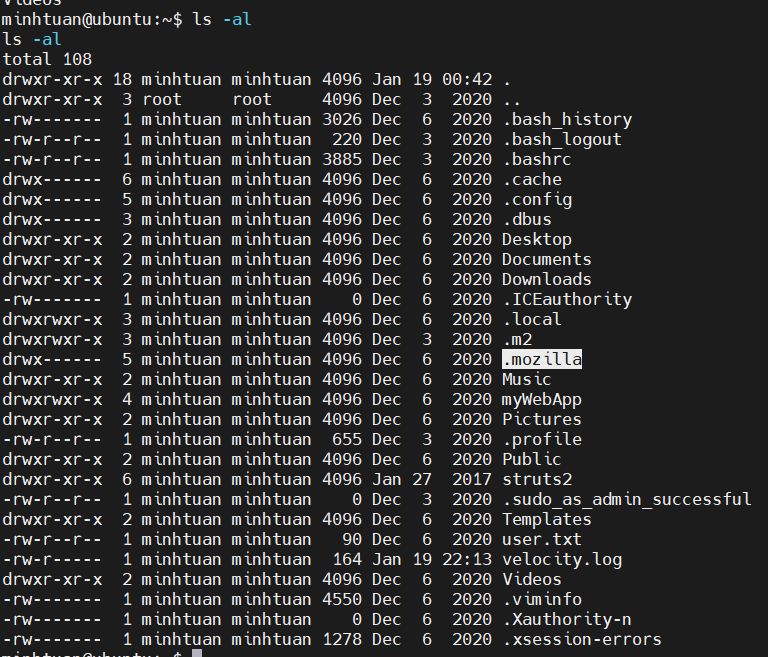






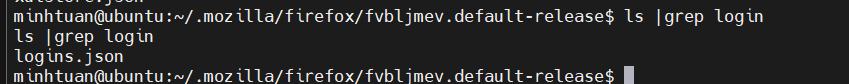
看一下users

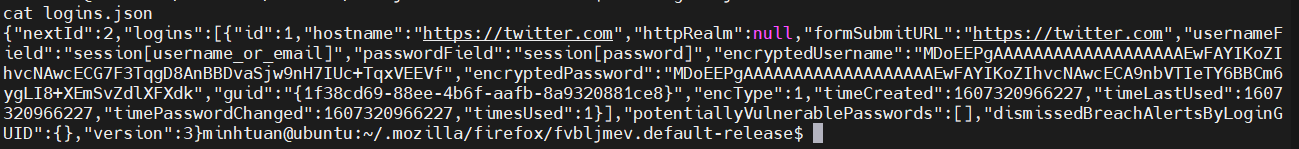




看到火狐的东西了，那么就是要找登入信息

在里面找一下





加密了



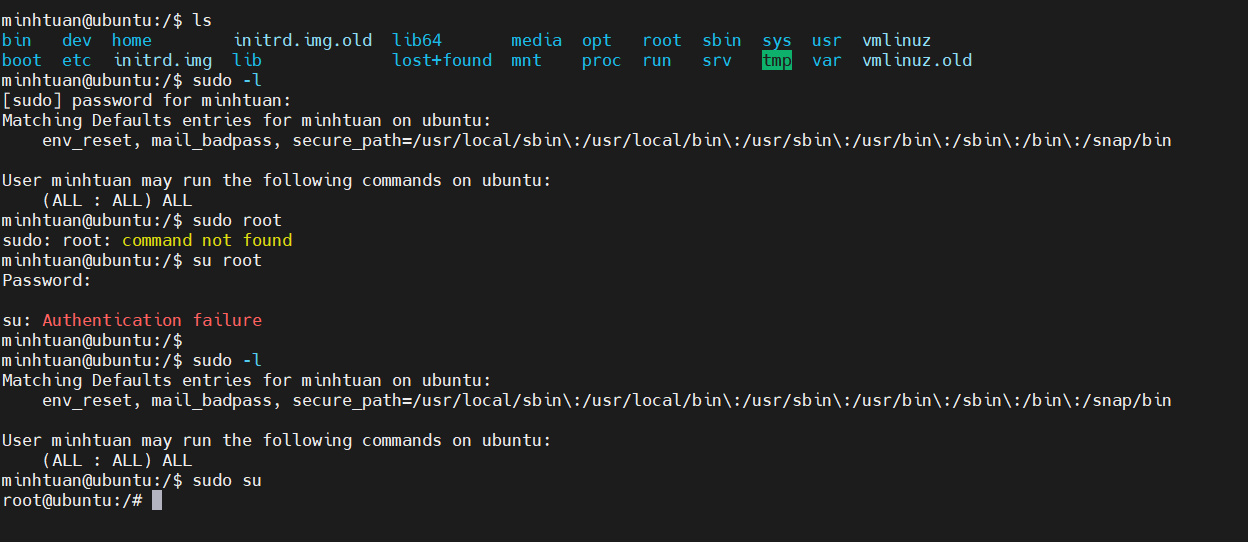
[渗透技巧-横向渗透-导出Firefox等浏览器中保存的密码 - 香农Shannon - 博客园 (cnblogs.com)](https://www.cnblogs.com/ethtool/p/12507649.html)



用户名：minhtuan

密 码：skysayohyeah

ssh登入



结束

