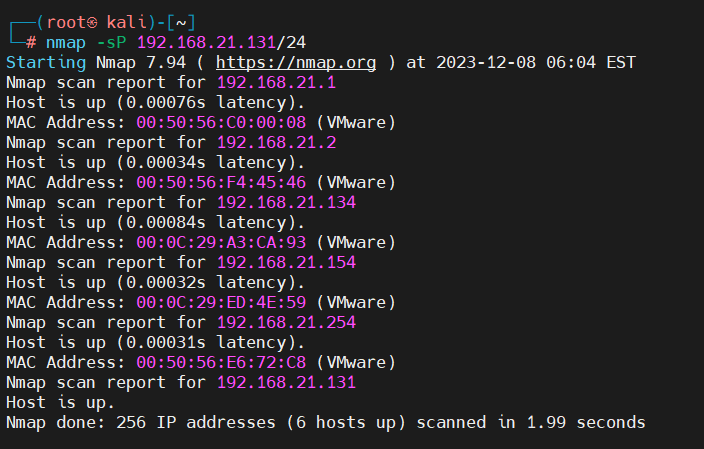
Phineas

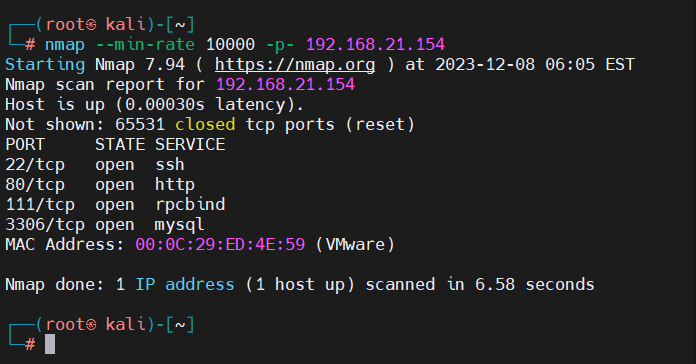
下载地址：<https://download.vulnhub.com/phineas/Phineas.ova>

主机发现

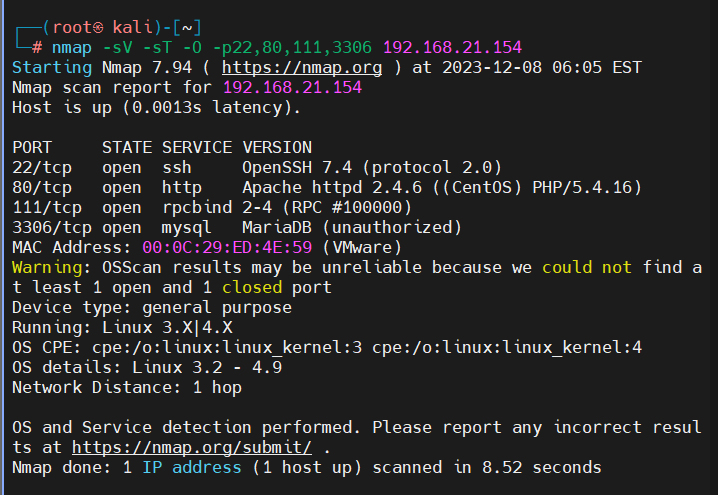


目标154

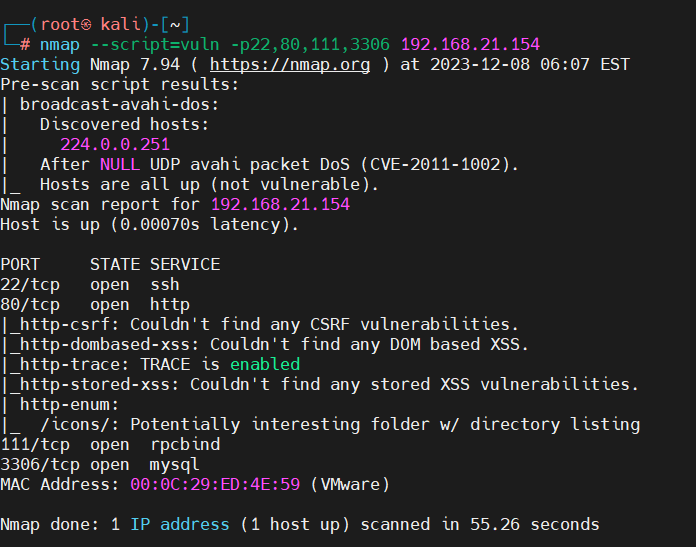
端口扫描

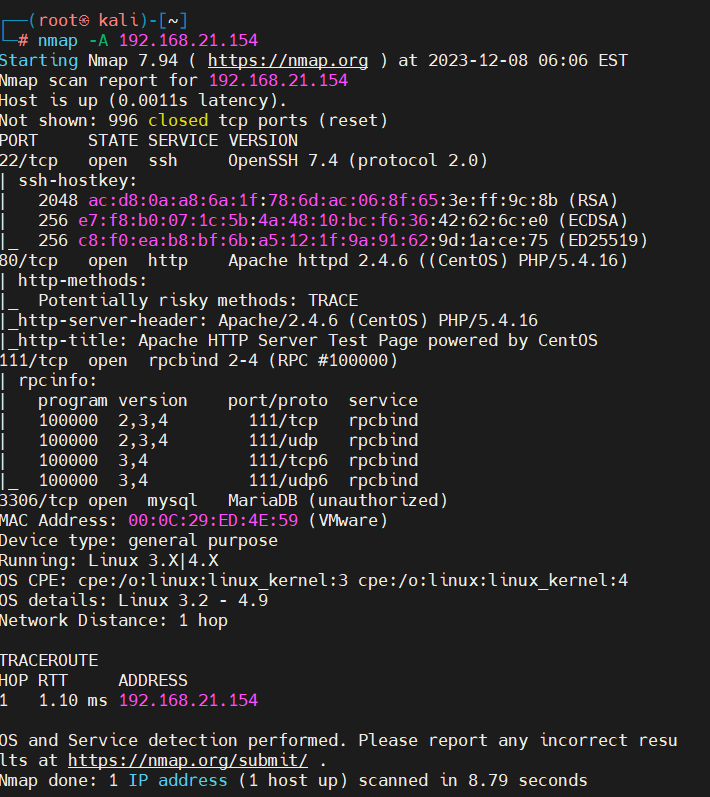


端口服务扫描

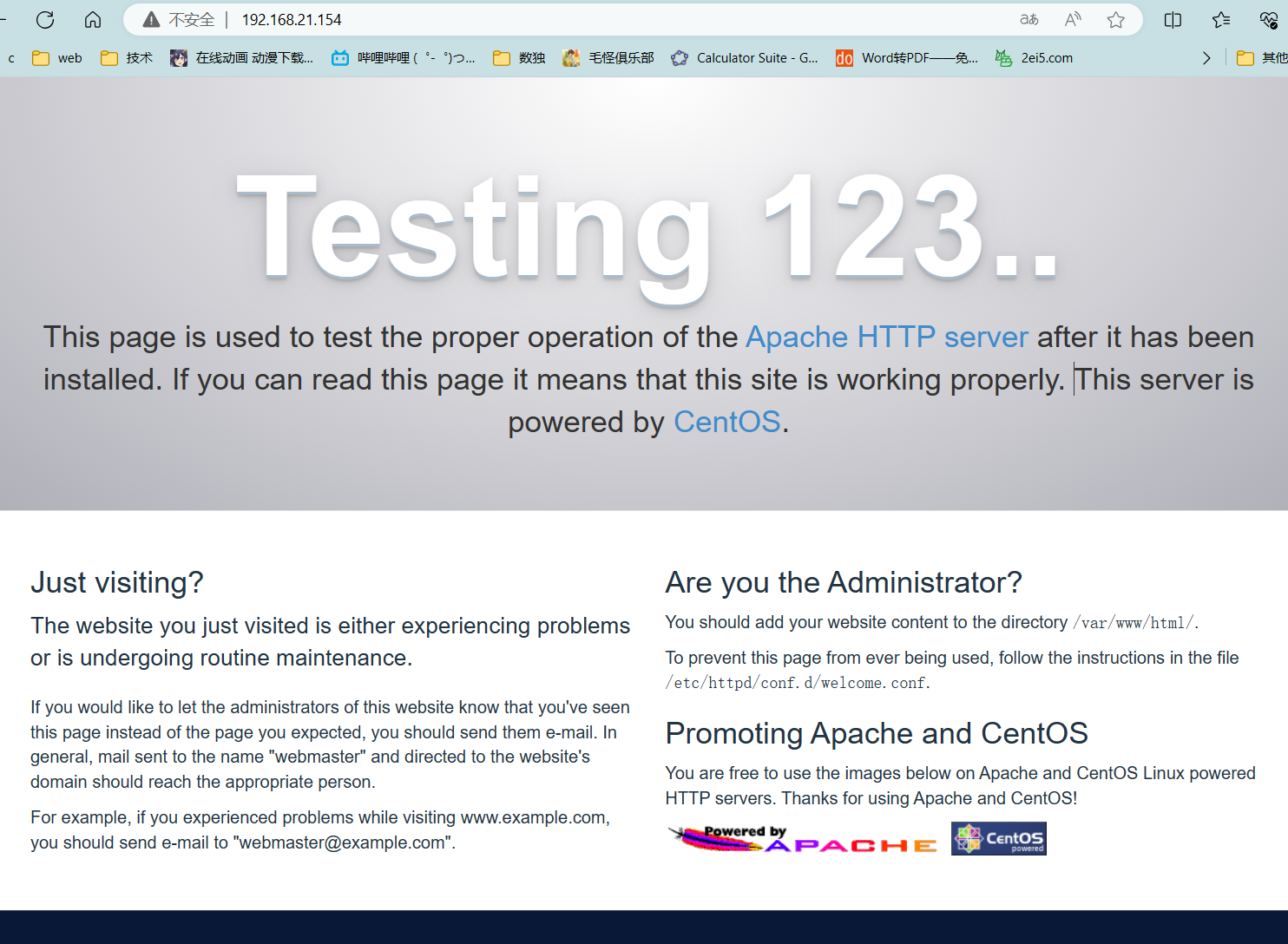


漏洞扫描

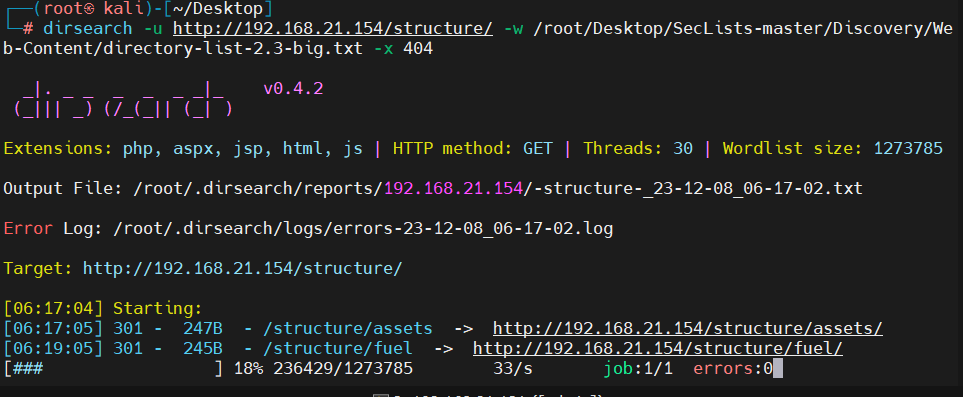


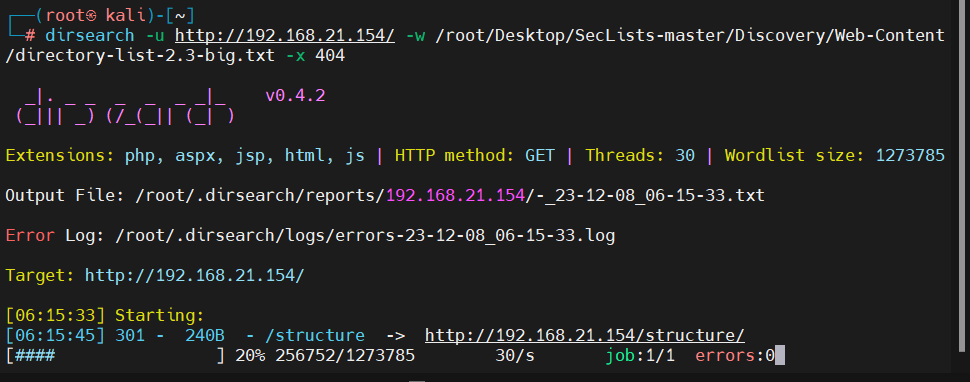


直接访问web

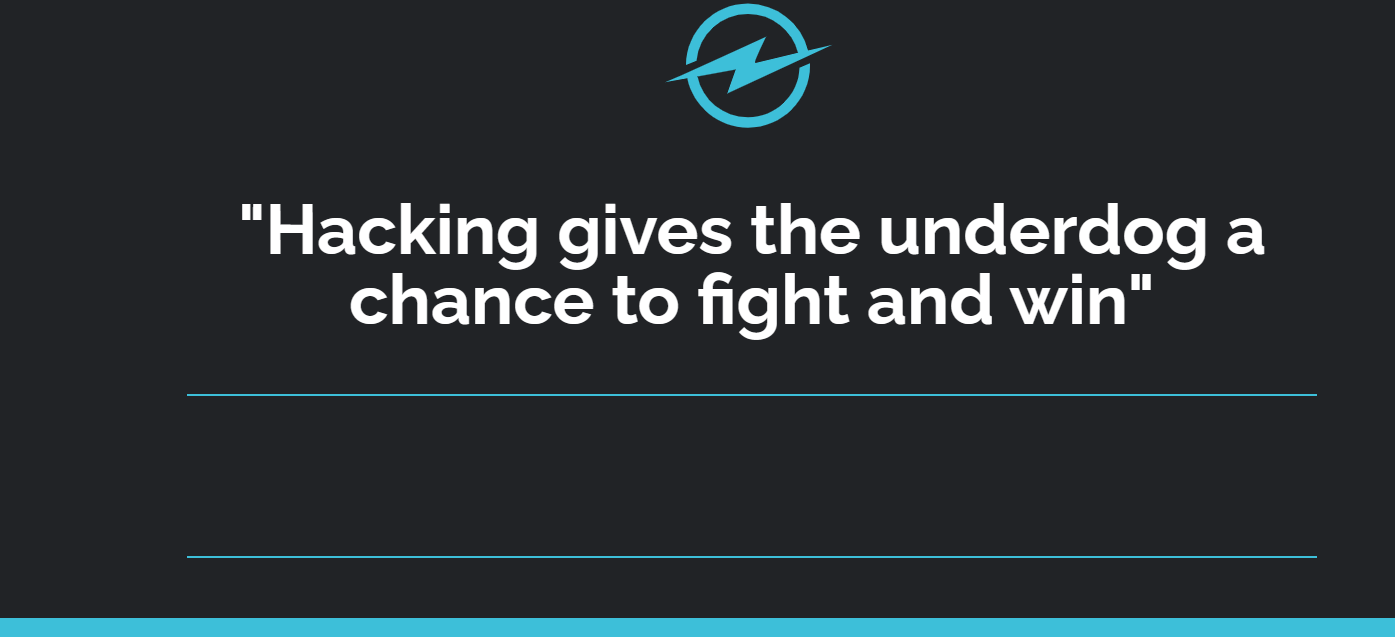


初始页面，我就不信没东西，开扫！

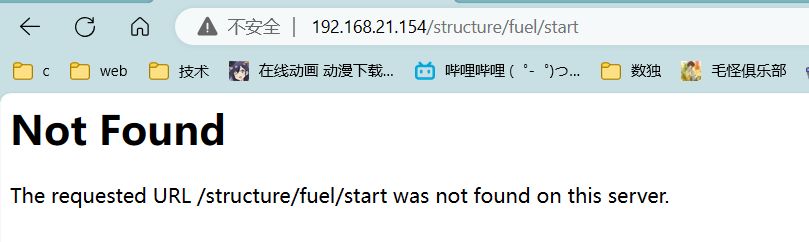




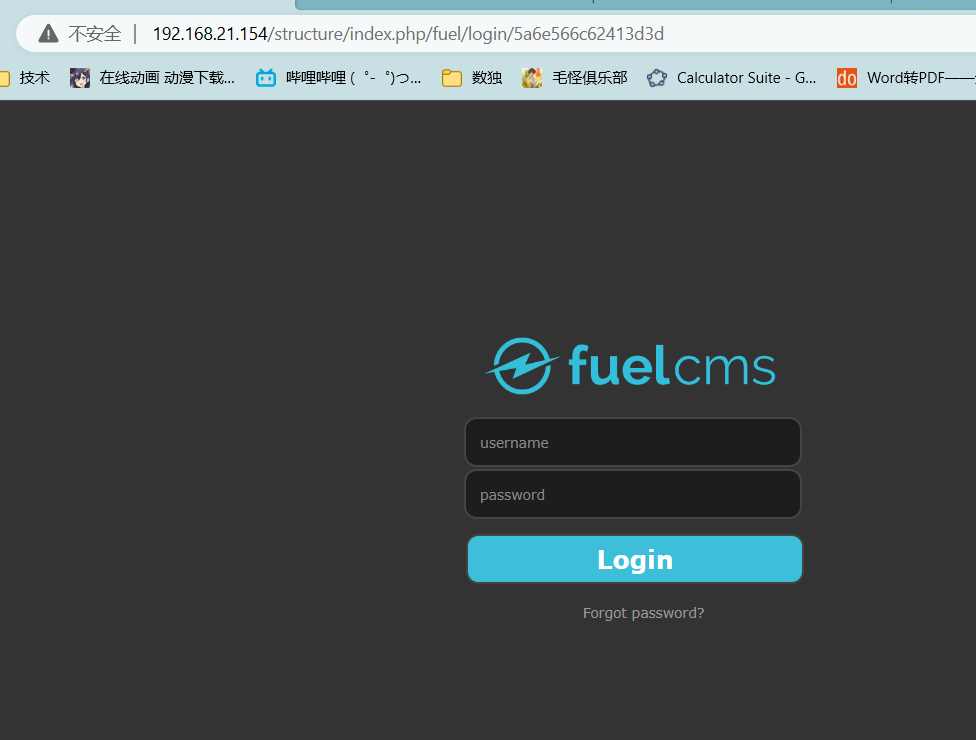
访问一下



访问fuel时候发现url变化了

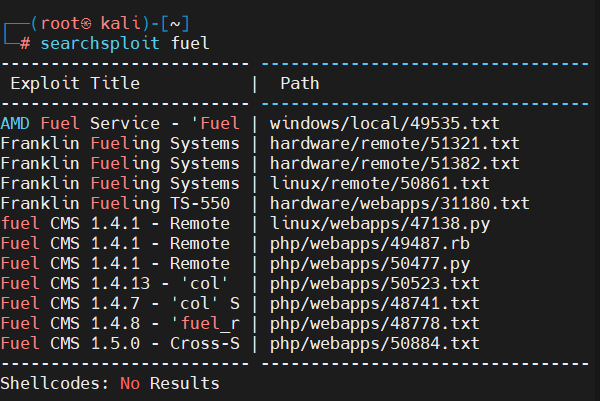


只能进行拼接url那就试一下凭借主页的文件（index.php）

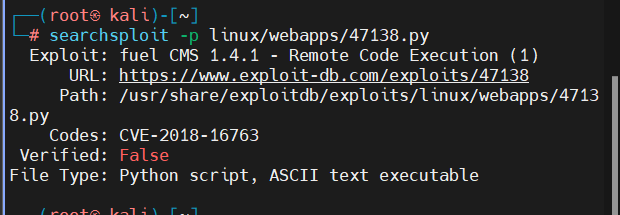


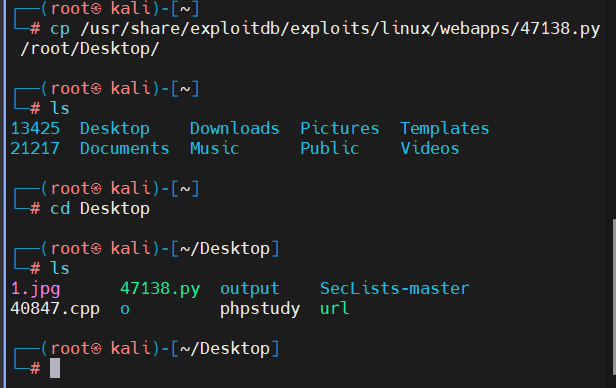
url变成这样了

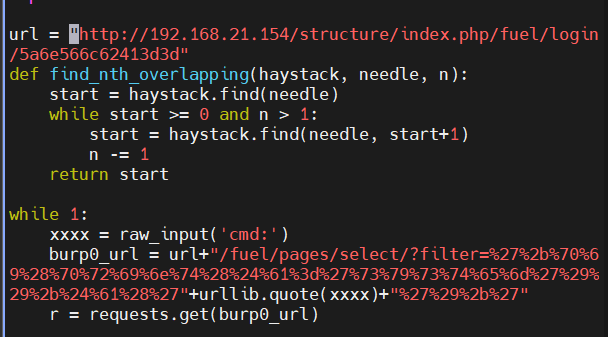
提示是fuel直接去查一下漏洞了



一个一个试

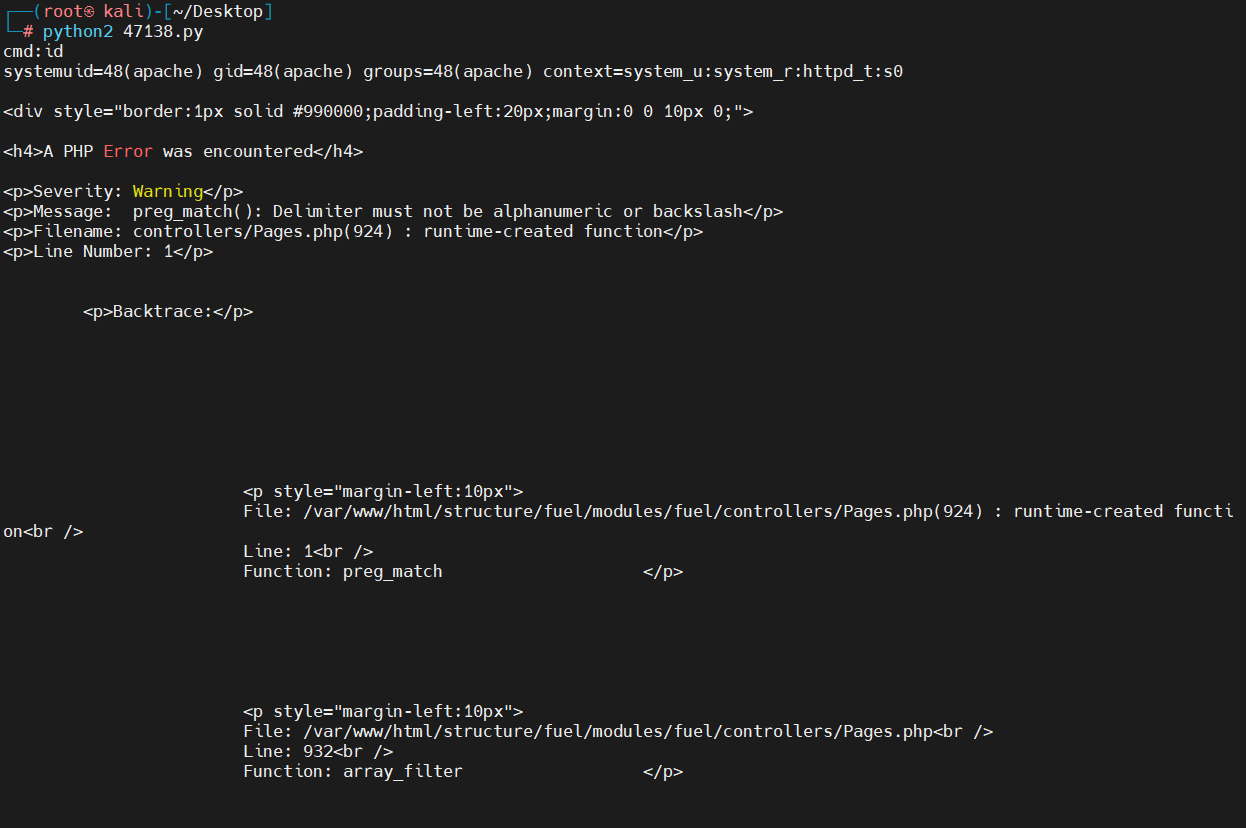


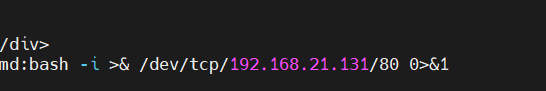




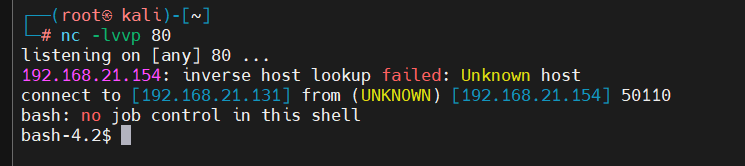
删掉代理，网站是登入页面的url



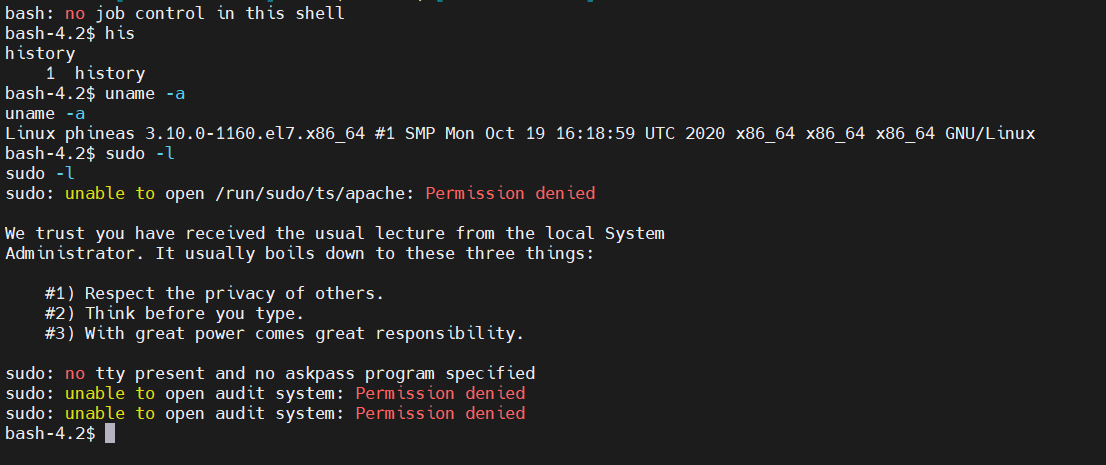


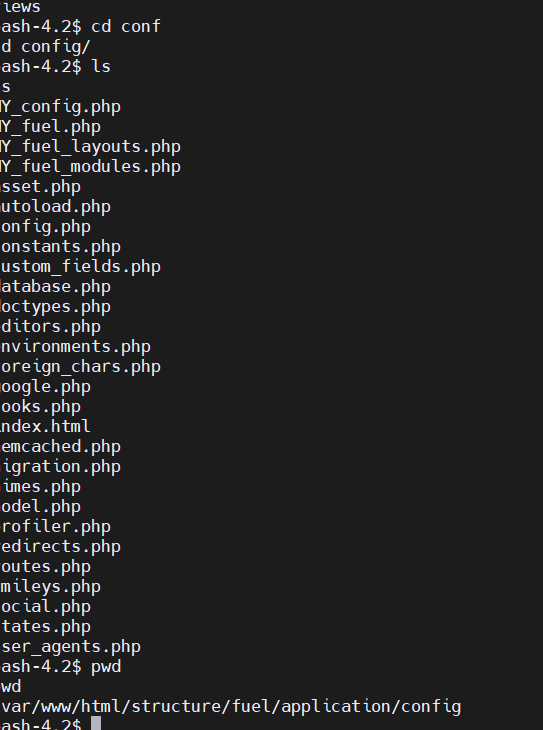


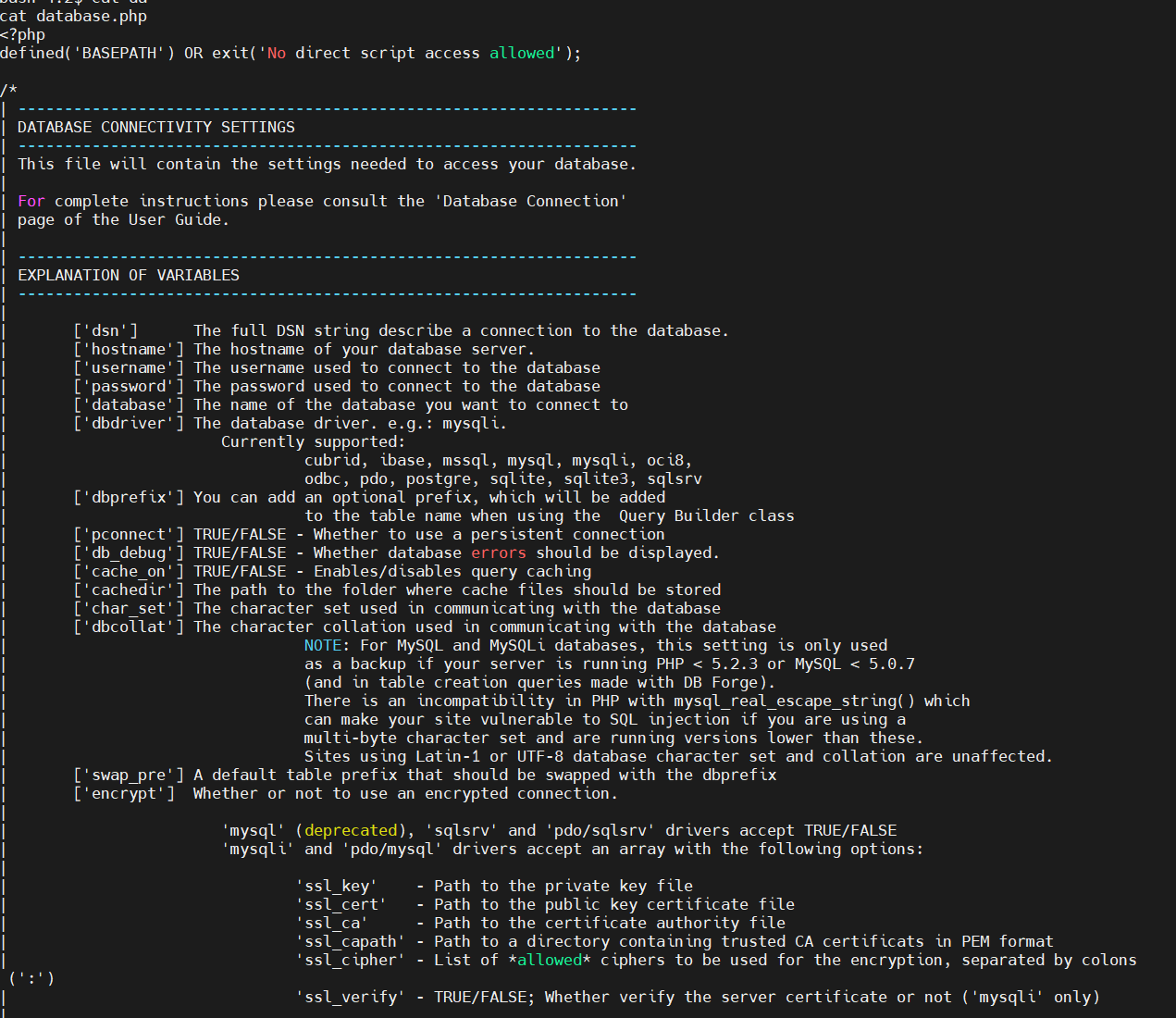
80端口能反弹shell

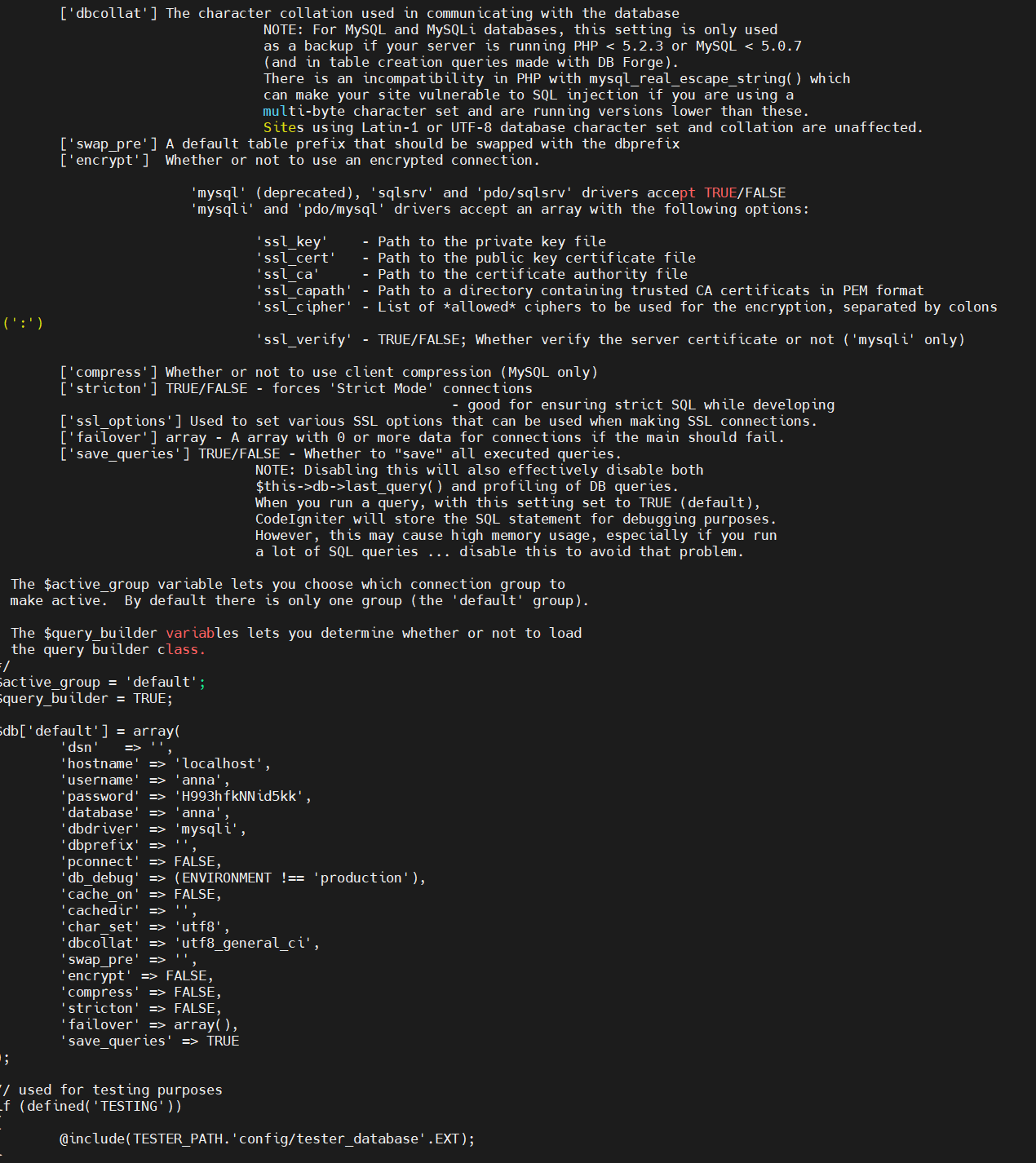


信息收集（其实apache账户没有什么收集的）

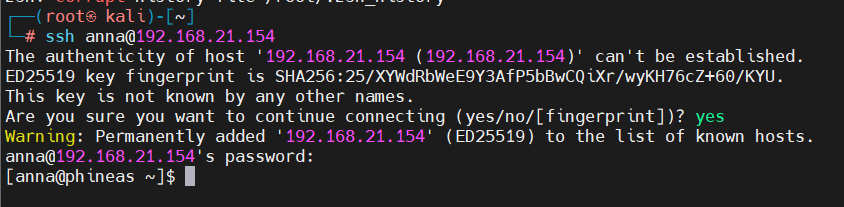






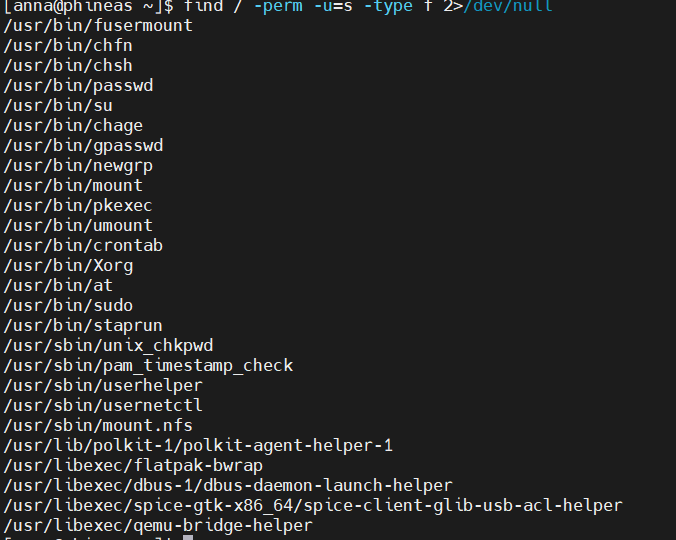


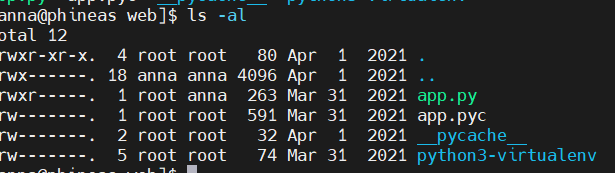
Ssh登入

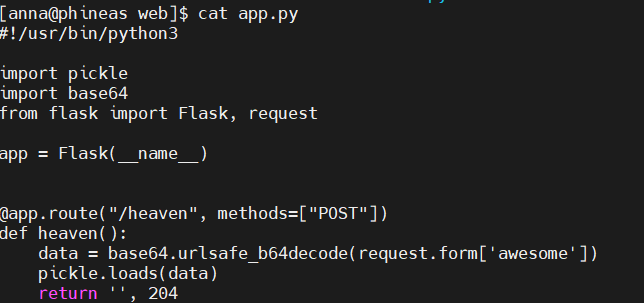


信息收集



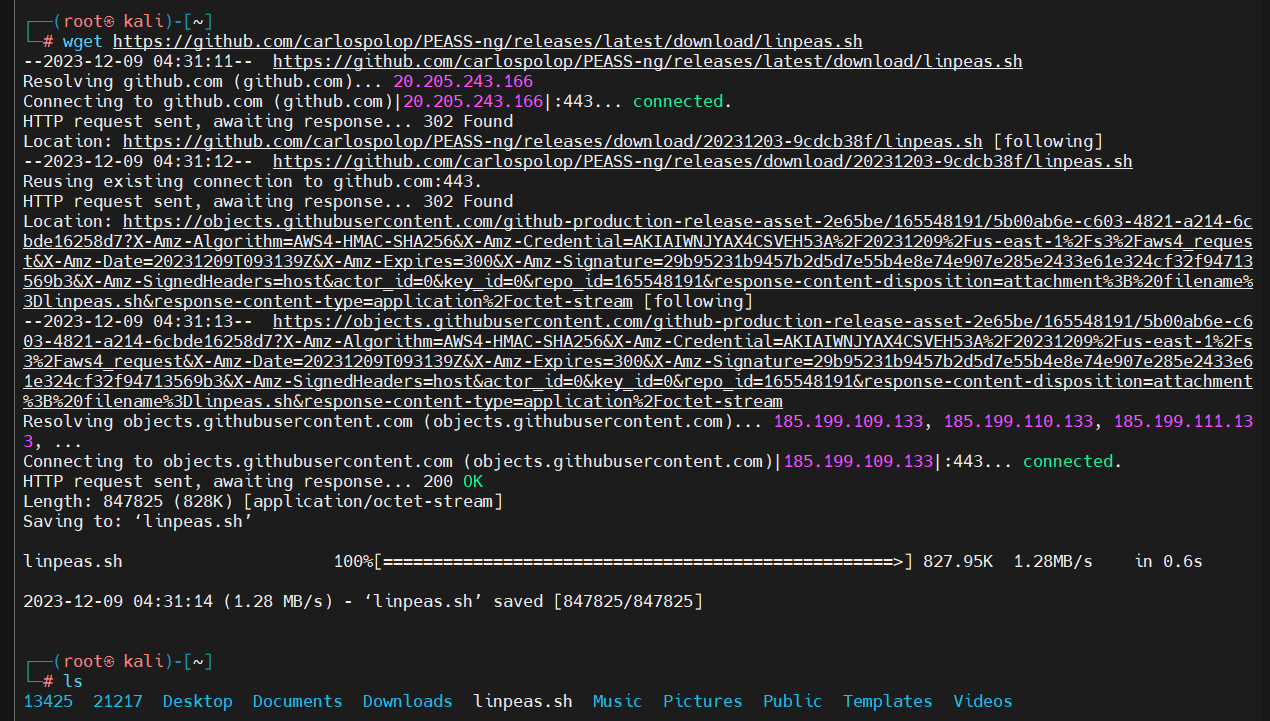


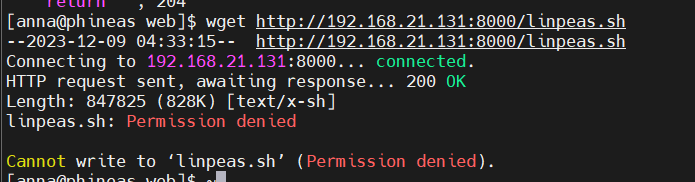




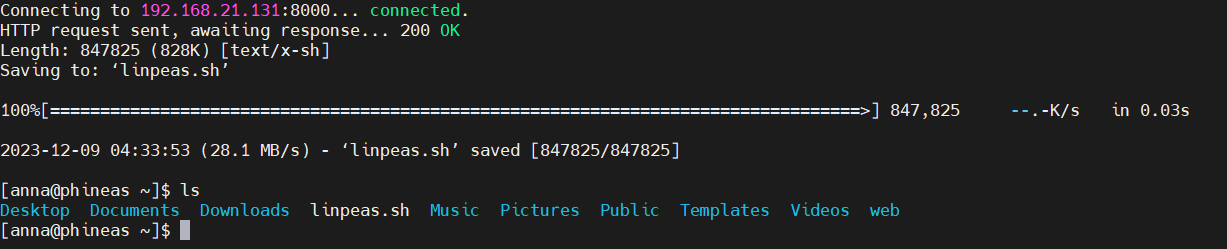
Pickle模块：[Python的pickle模块详解（包括优缺点及和JSON的区别）\_import pickle-CSDN博客](https://blog.csdn.net/Hardworking666/article/details/112754839)

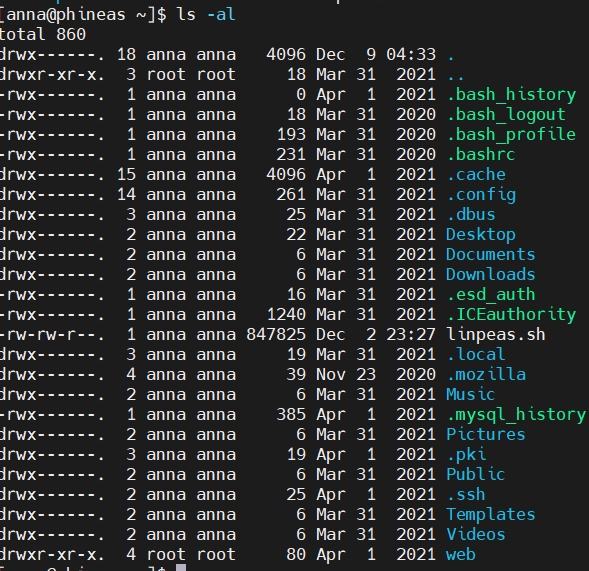
漏洞：[Python Pickle反序列化漏洞-CSDN博客](https://blog.csdn.net/qq_43431158/article/details/108919605)



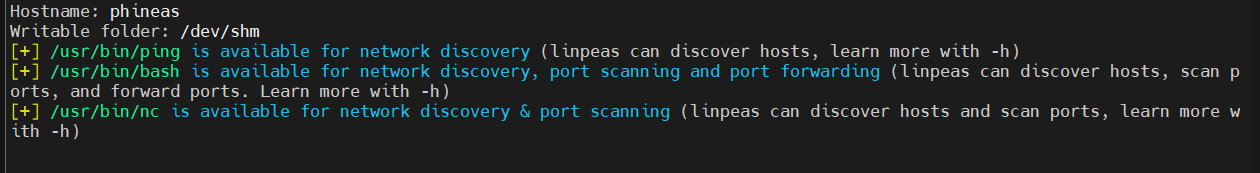


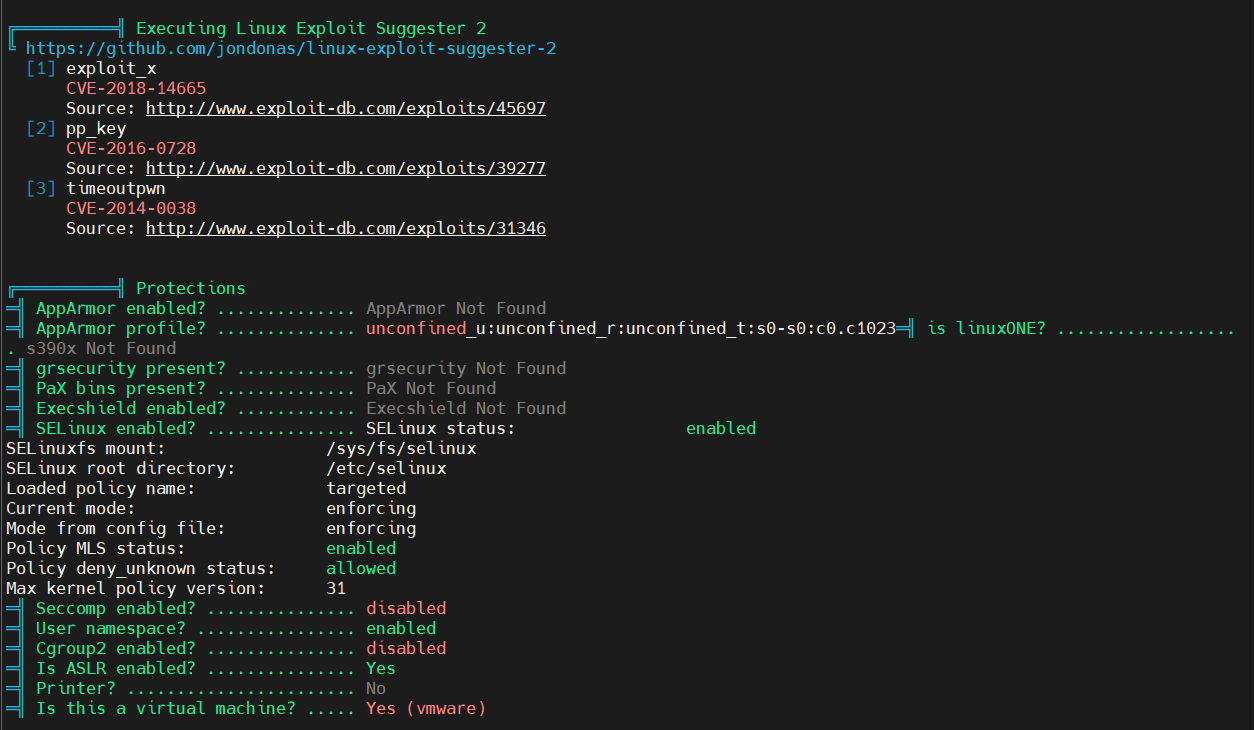
权限问题



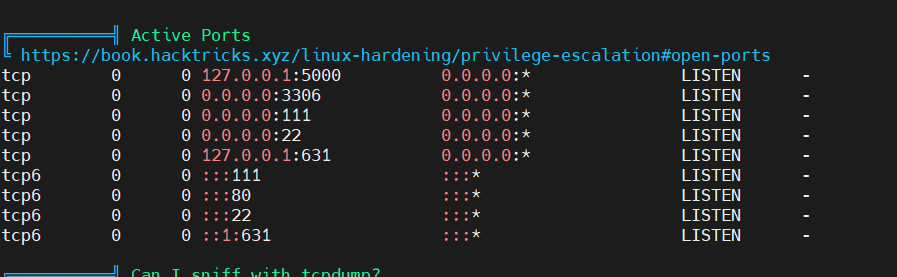




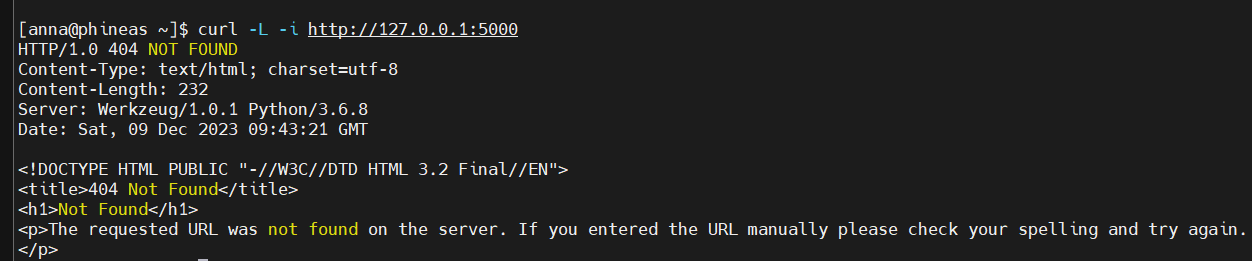




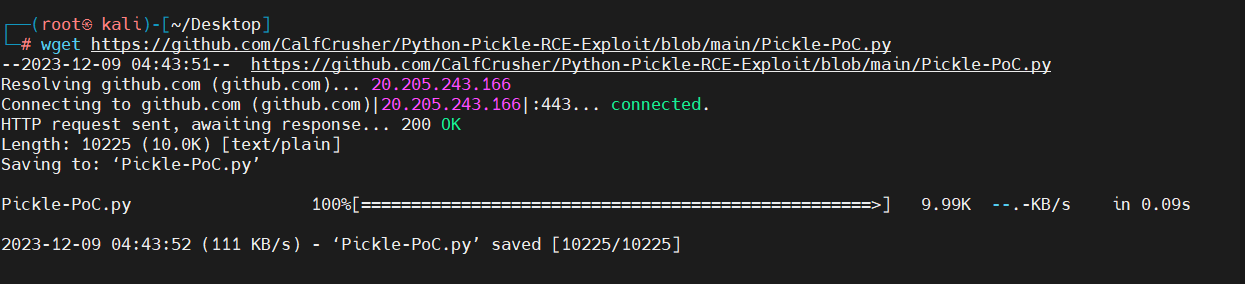
这玩意好猛



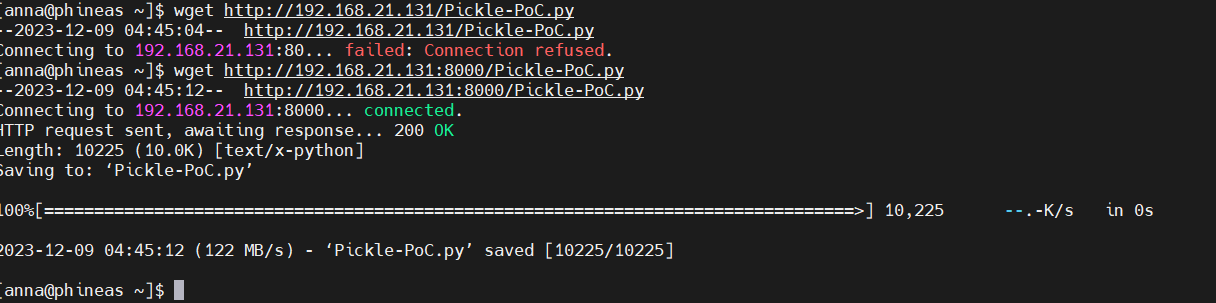
看一下5000端口是啥

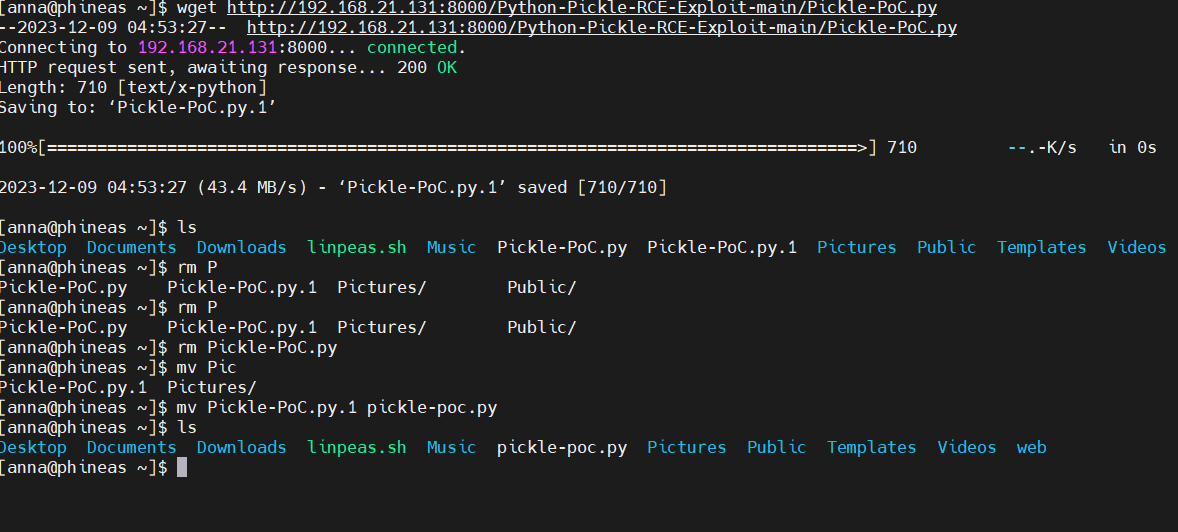


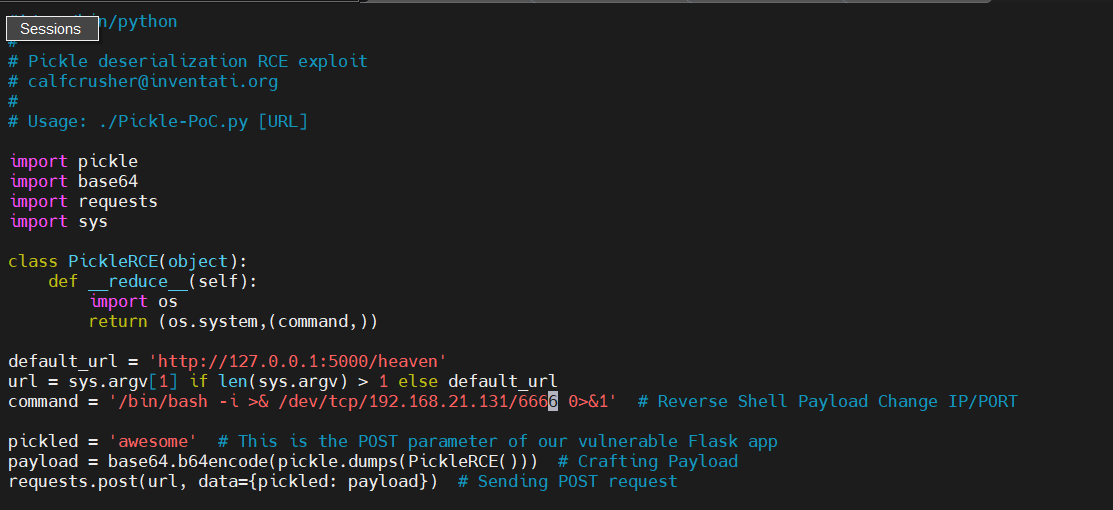
嗯是这个了

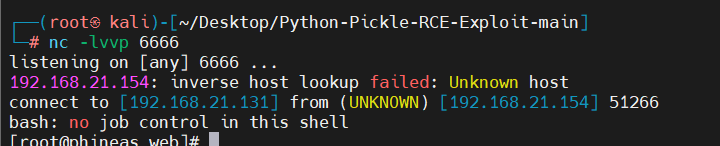


下一下工具









成功

