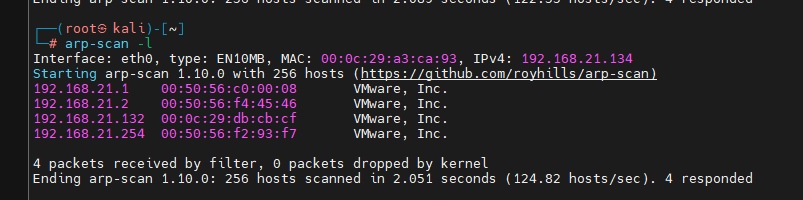
Venus

下载地址：<https://www.vulnhub.com/entry/the-planets-venus,705/>

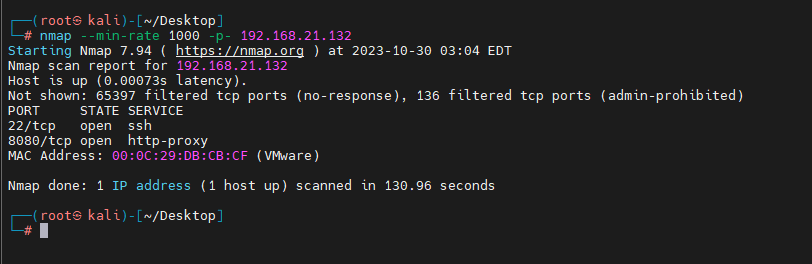
主机发现

arp-scan -l



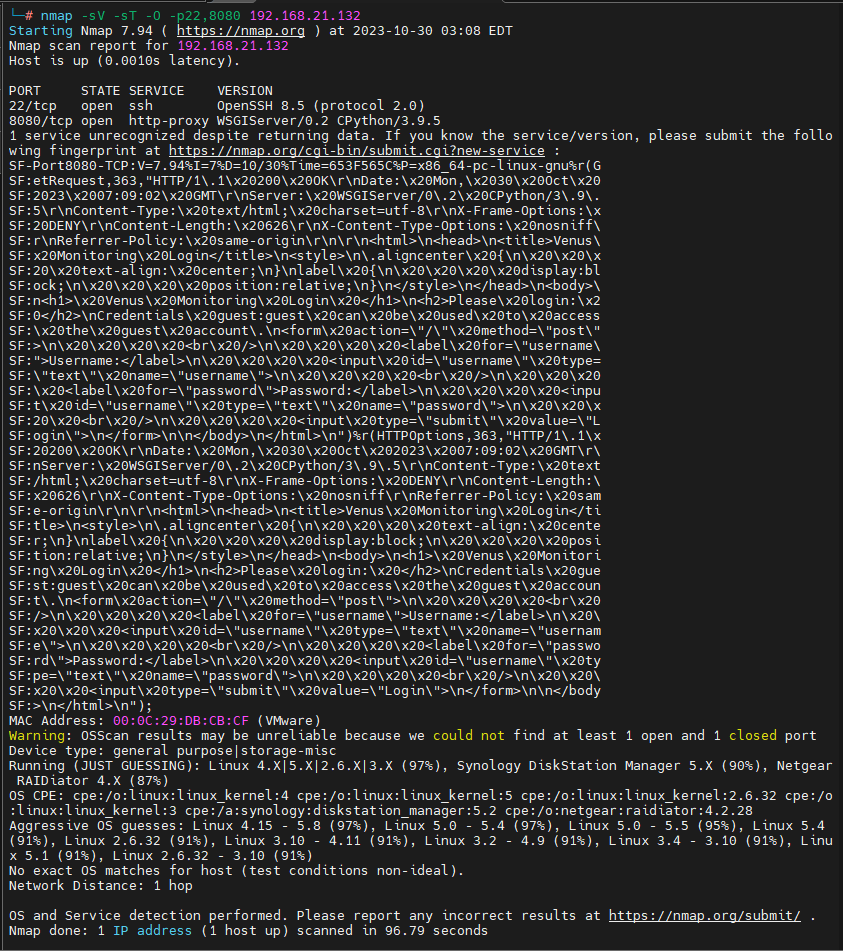
端口扫描

nmap --min-rate 1000 -p- 192.168.21.132



端口版本扫描

nmap -sV -sT -O -p22,8080 192.168.21.132



对于http-alt

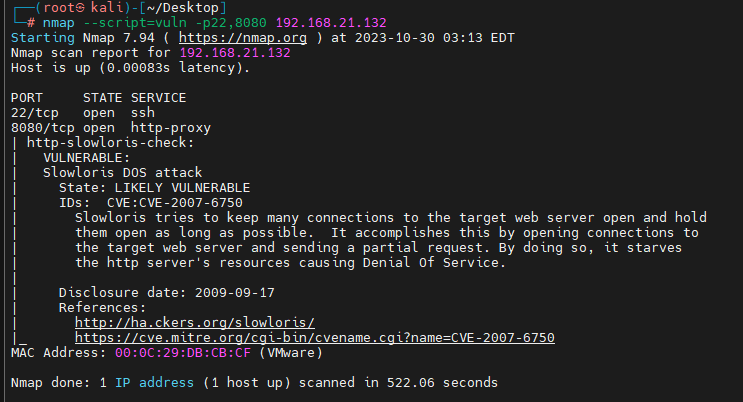
[HTTP Alternative Services 介绍 | JerryQu 的小站 (imququ.com)](https://imququ.com/post/http-alt-svc.html)

总结一下

2016年的协议，补充http服务端可以将自己的替代服务地址以协议规定的方式告诉浏览器，对于支持这个协议的浏览器来说，后续请求都会使用新地址。（这个石油安全隐患的）

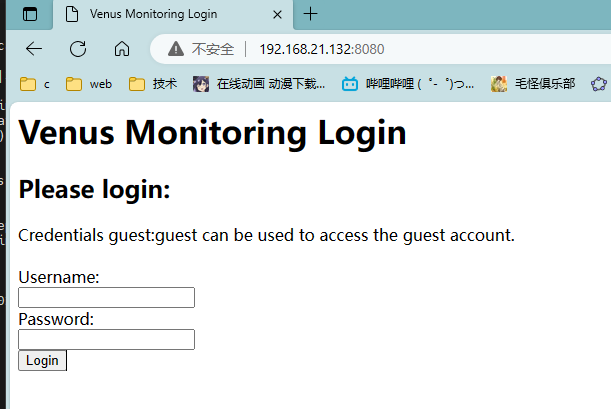
漏洞扫描

nmap --script=vuln -p22,8080 192.168.21.132

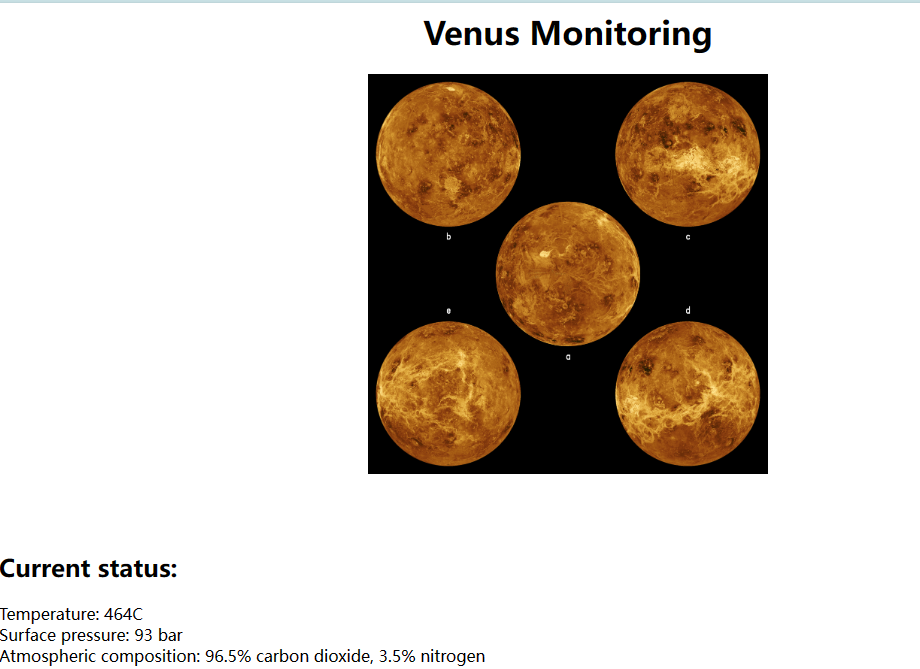


没用的dos漏洞

去看看web

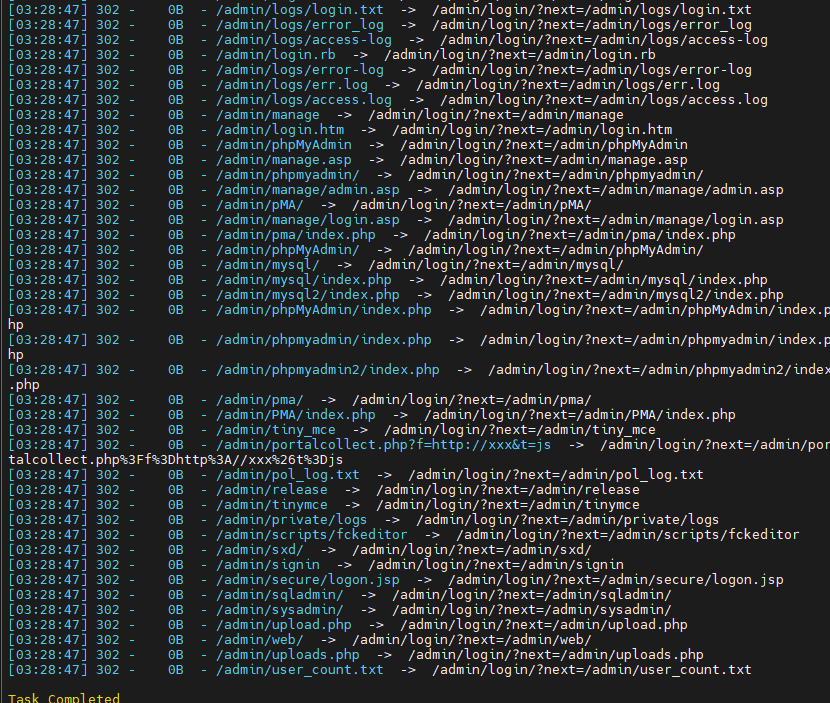


上面说能用guest登入看看



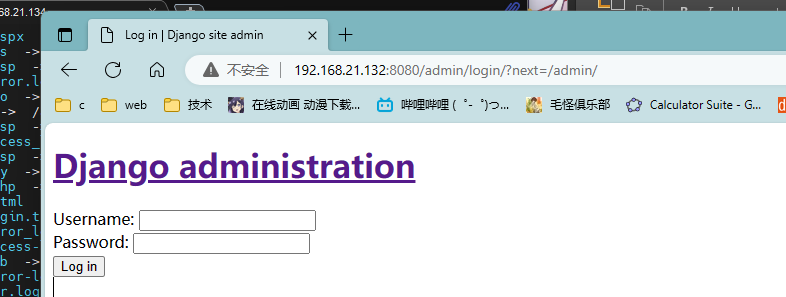
线索断了，目录爆破吧

dirsearch -u <http://192.168.21.132:8080/>



全是admin这个文件夹的东西

进去看看

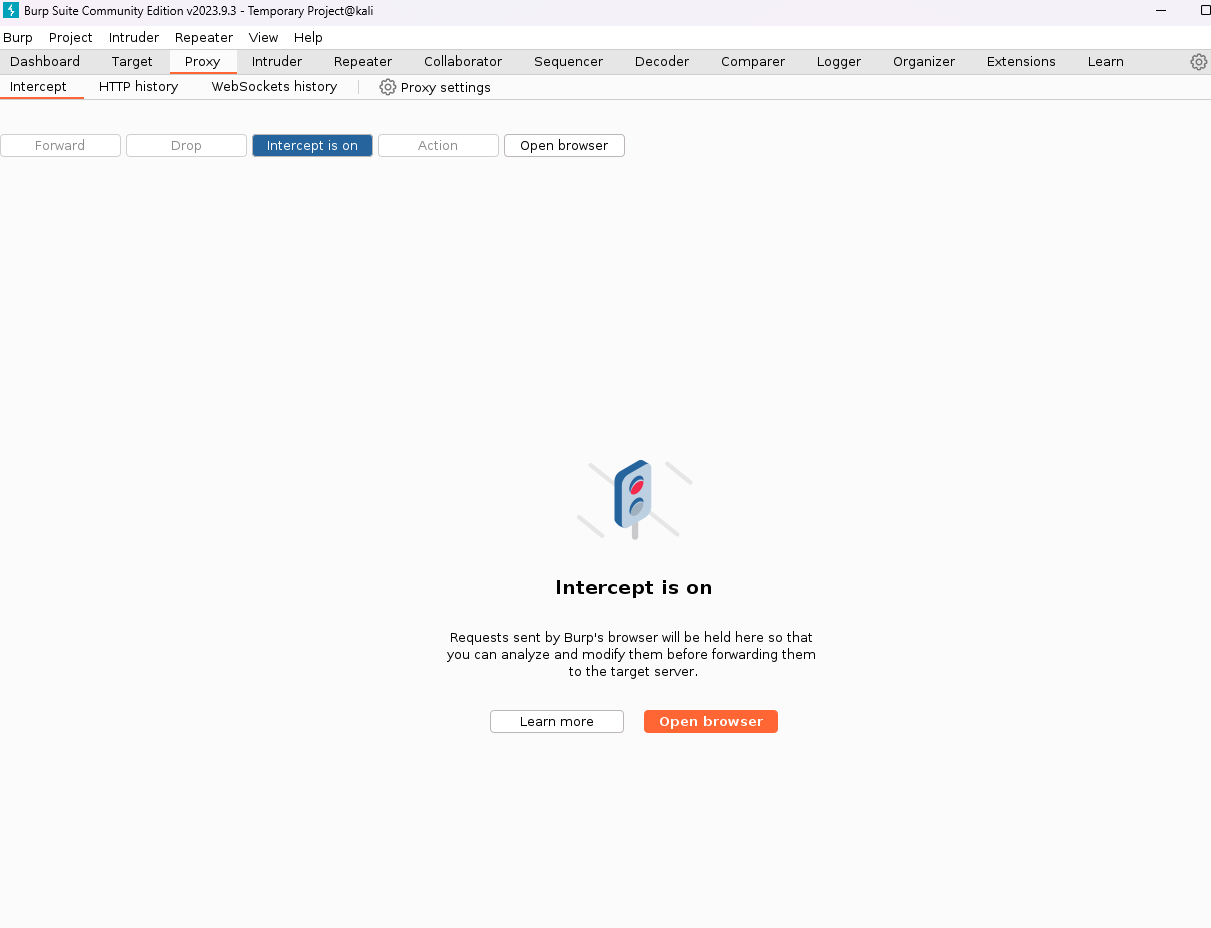


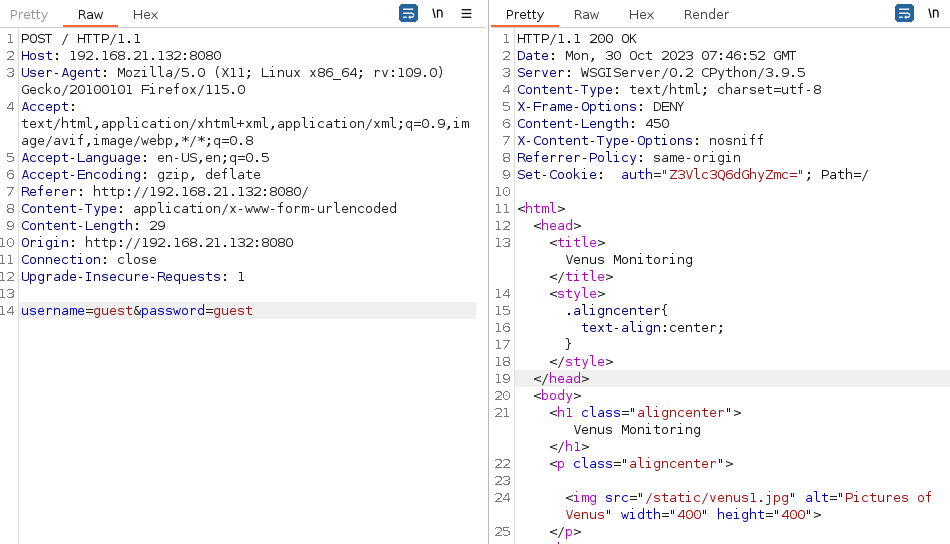


尝试登入发现直接报错

忘记了有抓包这个办法

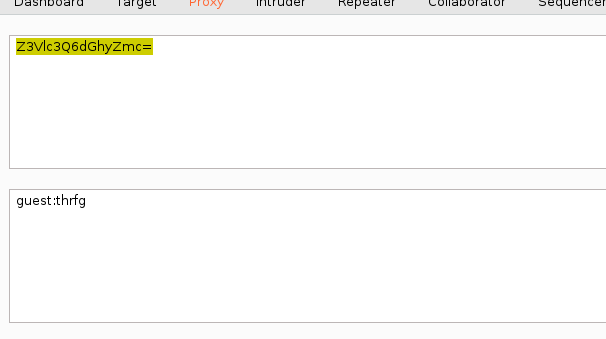
Burpsuite





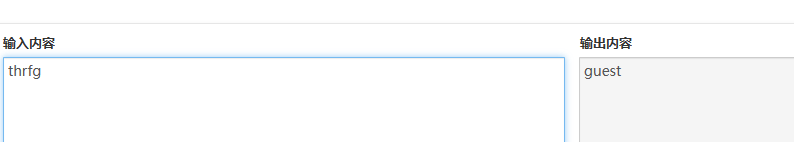
当我们guest登入成功时发现

Cookie是base64加密



这里密码是guest尝试加密方式（应该是对称加密）看着有点像凯撒

Rot13

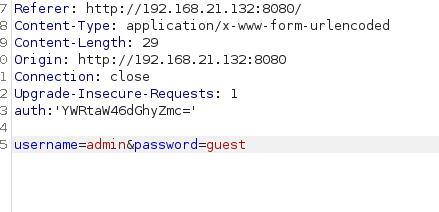


[ROT13加密/解密 - ROT13编码/解码—LZL在线工具 (lzltool.cn)](https://lzltool.cn/Tools/Rot13)

这里我们需要猜到用户名

先用admin

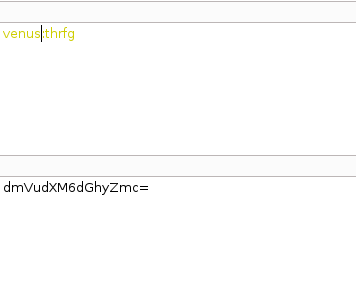


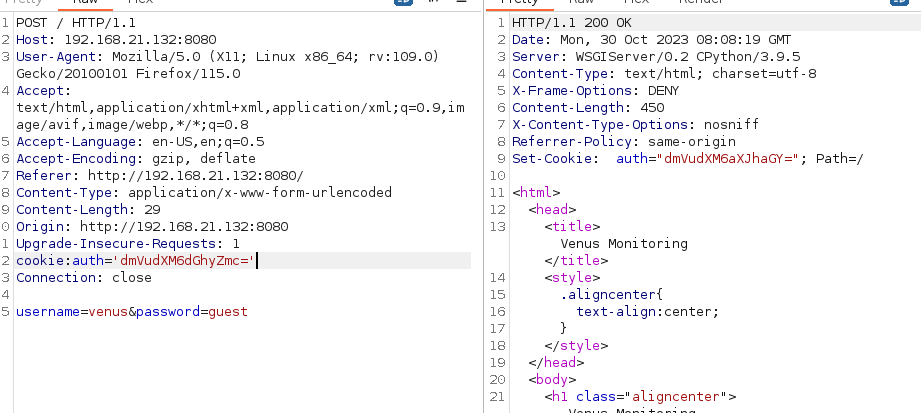


修改一下数据包

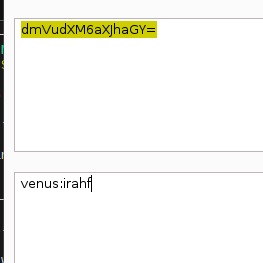


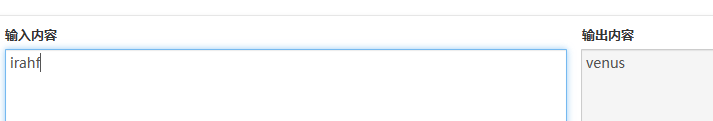
名字不对，试试这个靶机的名字，vulnhub经常就是靶机名字做username





对返回的cookie进行解密





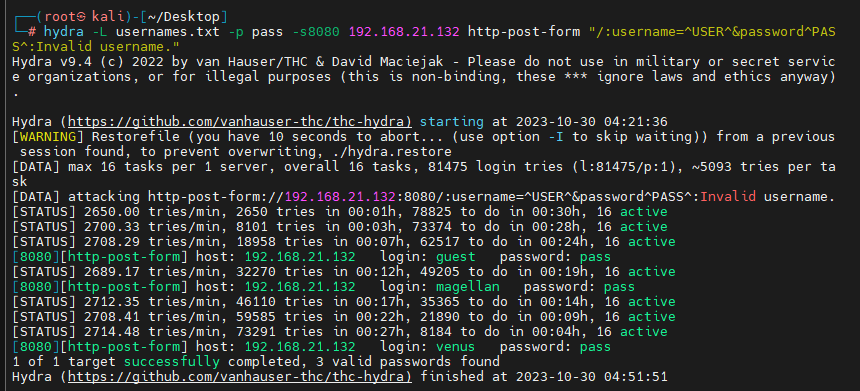
这个还是登入的主页面

没啥用

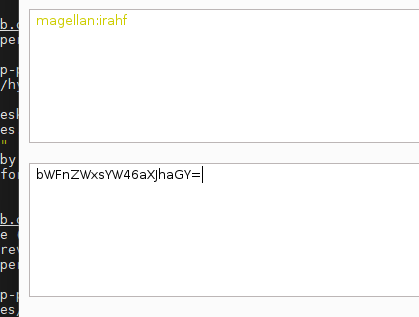
这里只能爆破用户名了

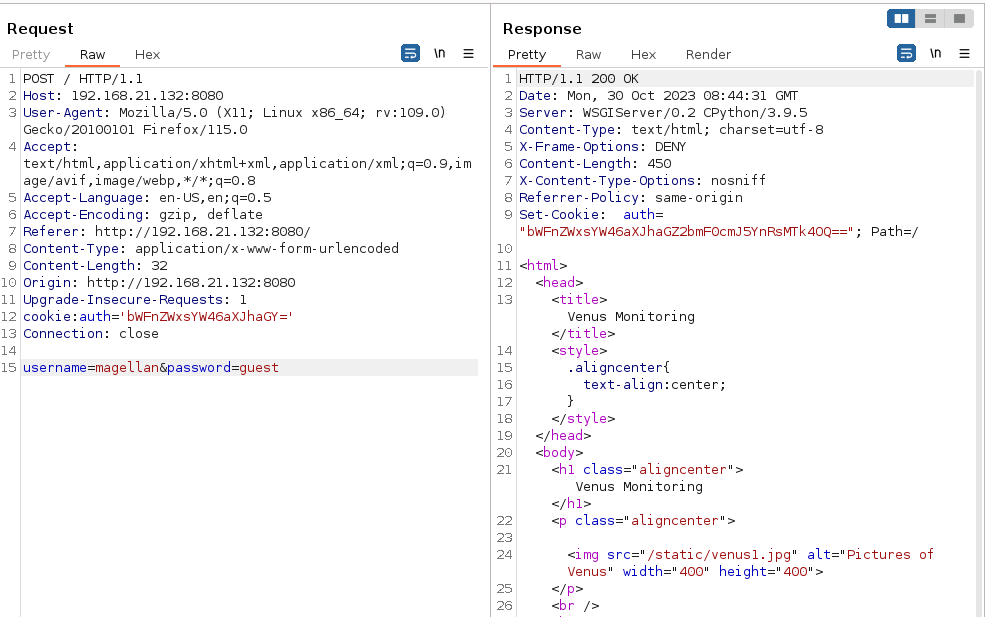
<https://github.com/jeanphorn/wordlist/blob/master/usernames.txt>

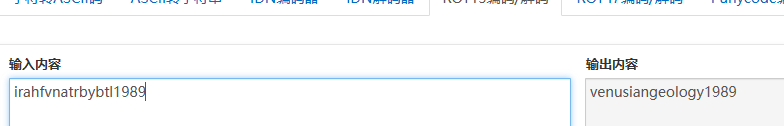
hydra -L usernames.txt -p pass -s8080 192.168.21.132 http-post-form "/:username=^USER^&password^PASS^:Invalid username."



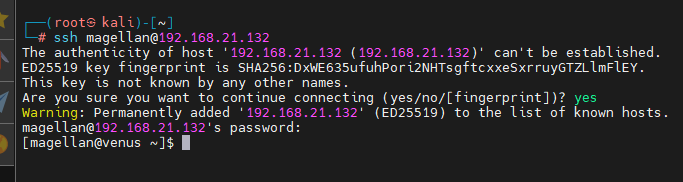
发现一个用户magellan



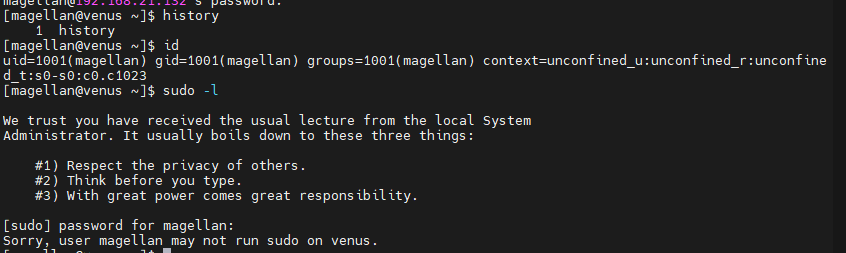


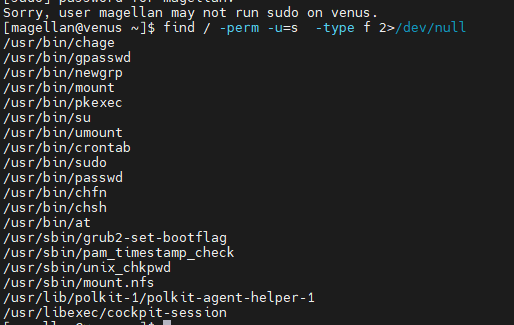


拿到密码，登入ssh

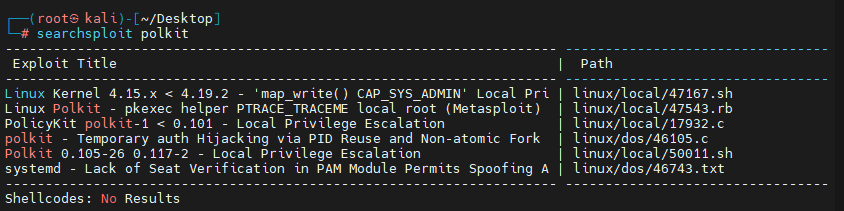


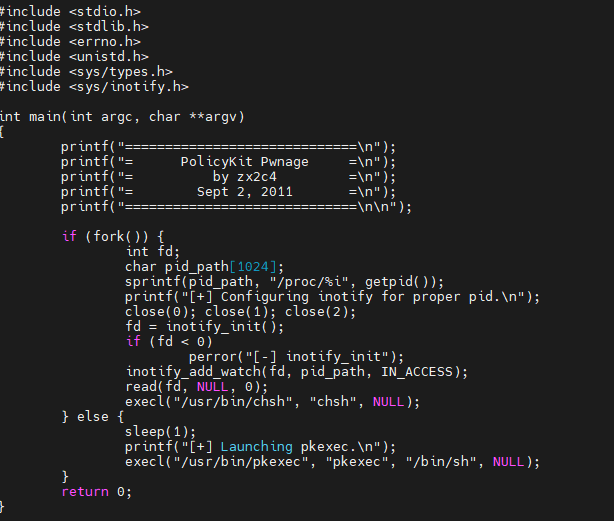
信息收集

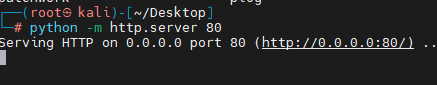




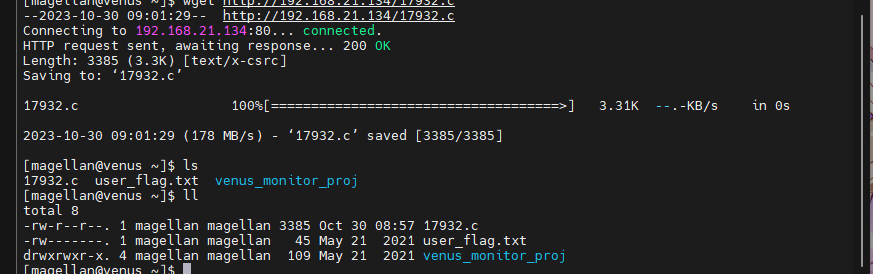
这里发现polkit有漏洞



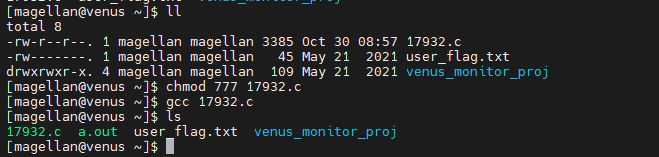


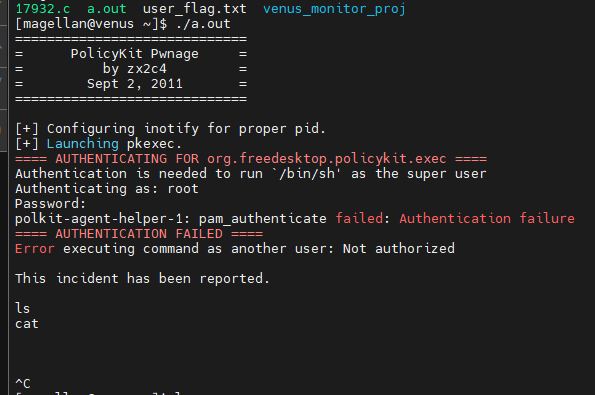


把这个放到python的web服务里面



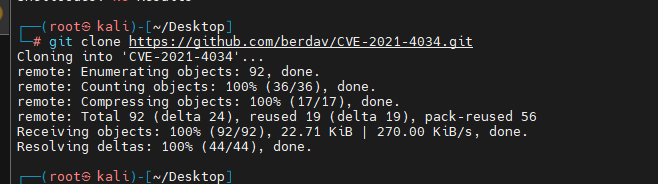
修改权限，编译



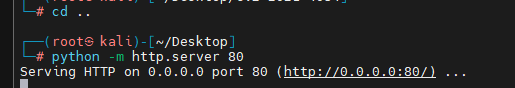


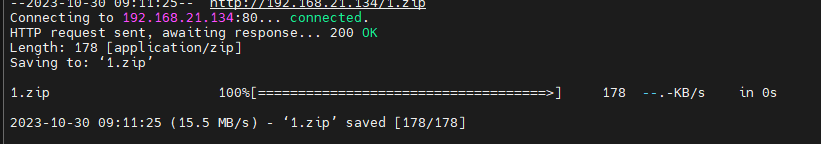
失败了去网上找找

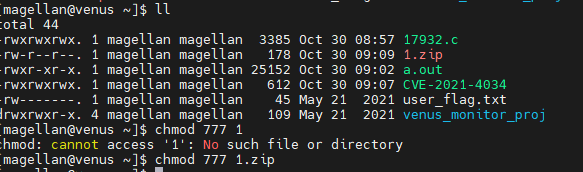
[GitHub - berdav/CVE-2021-4034: CVE-2021-4034 1day](https://github.com/berdav/CVE-2021-4034)

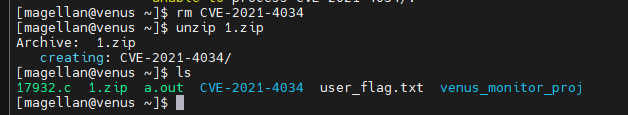


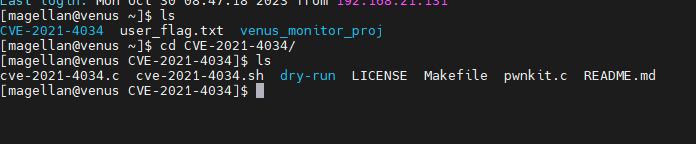
打包zip 1.zip cve-2021-4034

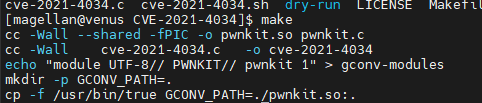


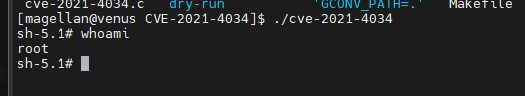


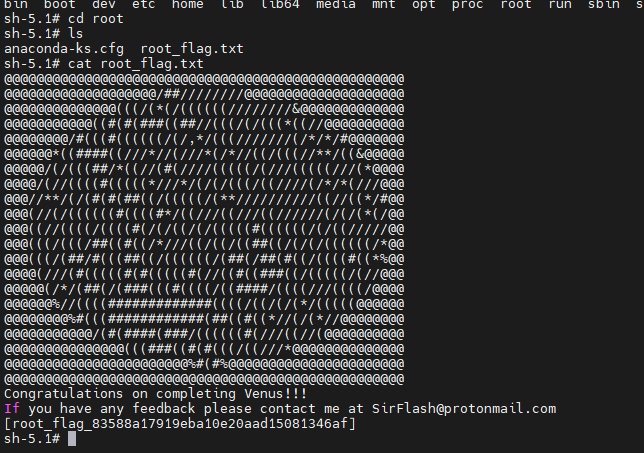












结束