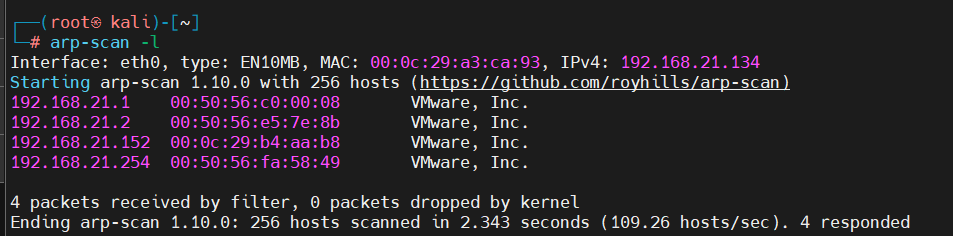
Vegeta

下载地址：<https://www.vulnhub.com/entry/vegeta-1,501/>

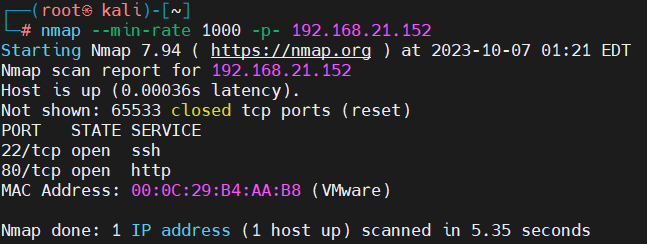
主机发现

arp-scan -l



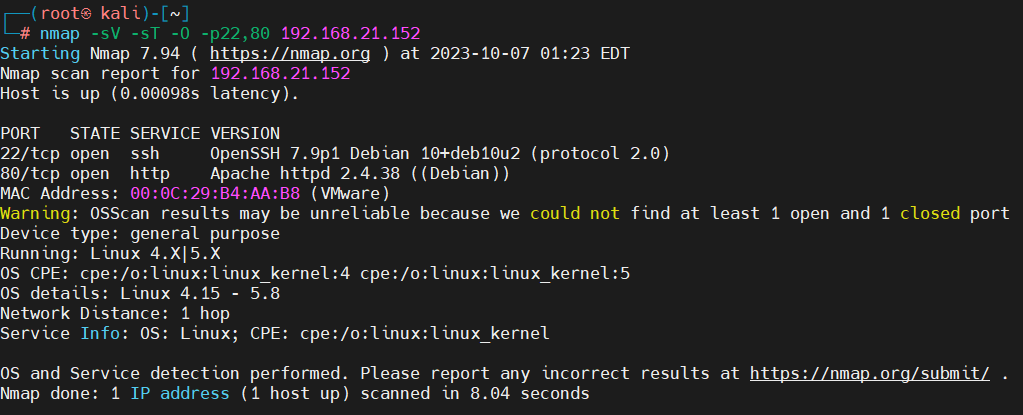
端口扫描

nmap --min-rate 1000 -p- 192.168.21.152



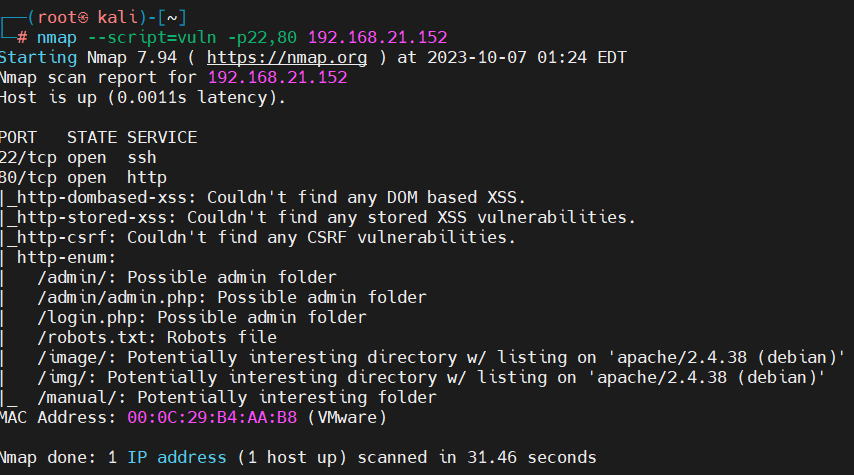
端口服务扫描

nmap -sV -sT -O -p22,80 192.168.21.152

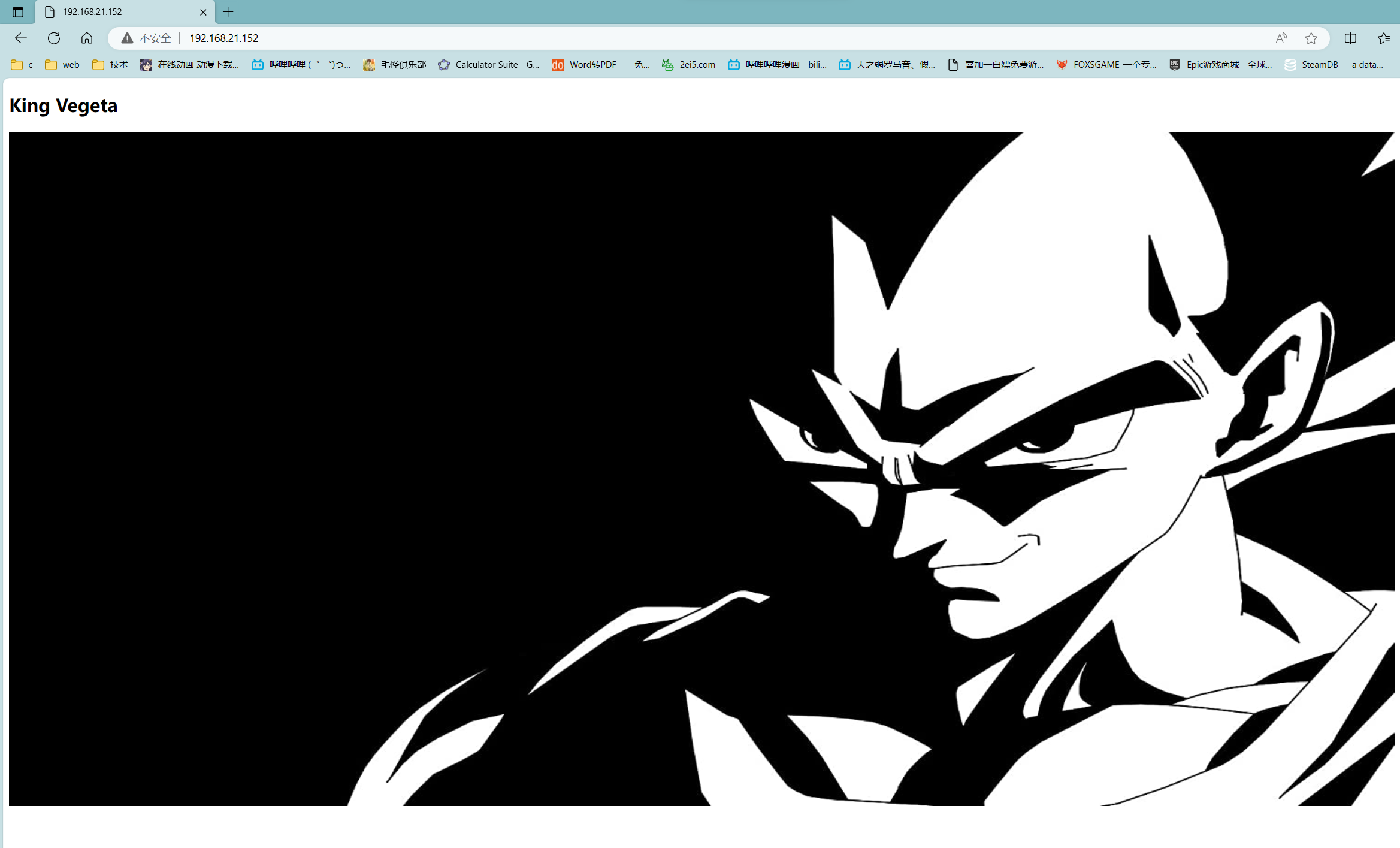


漏洞扫描

nmap --script=vuln -p22,80 192.168.21.152

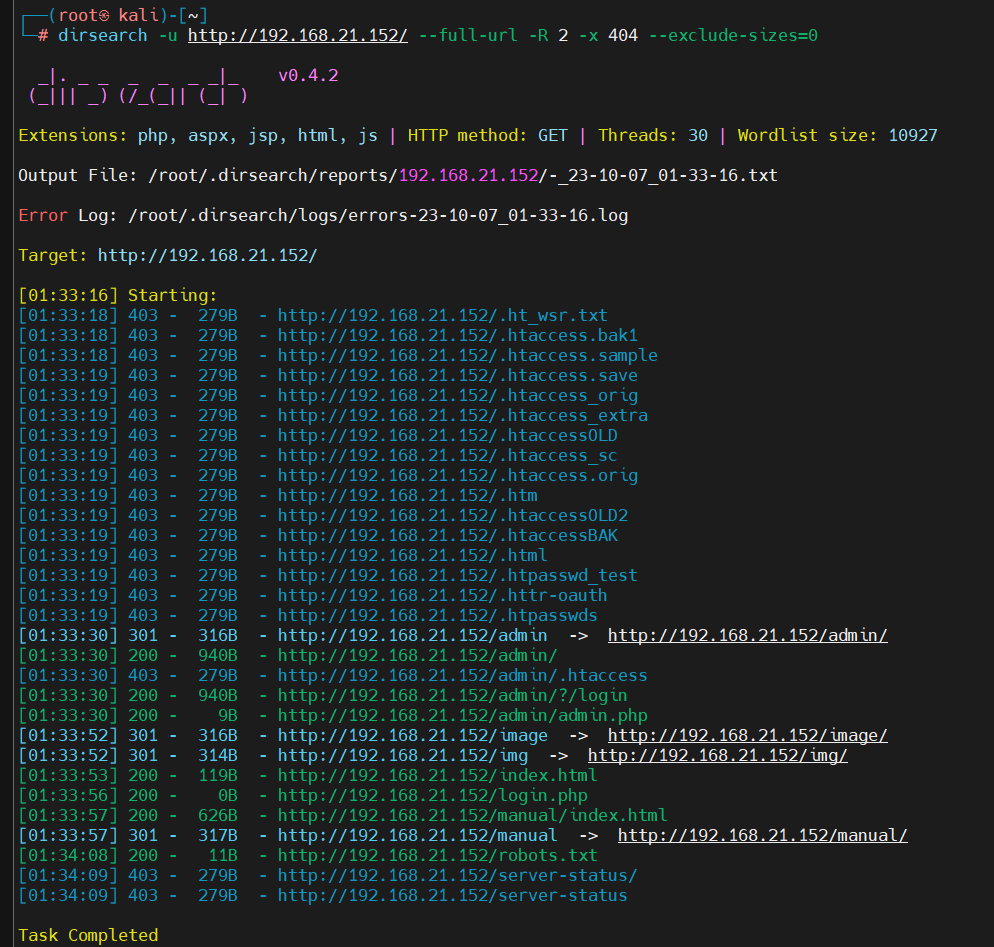


先去看看web

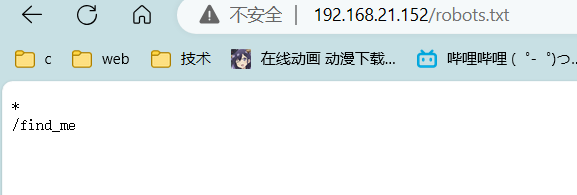


啥都没有，做一下目录爆破

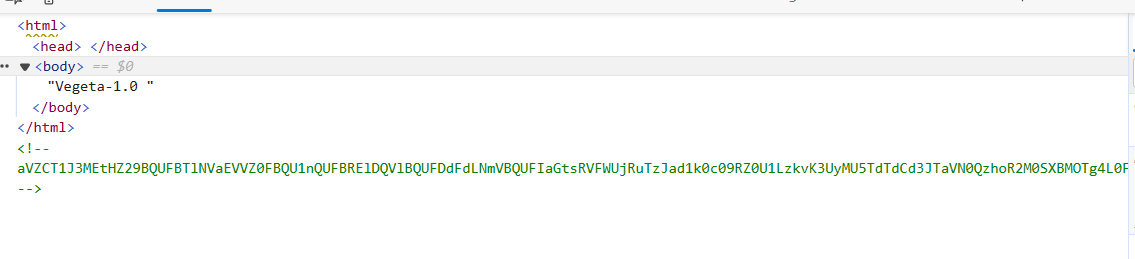
dirsearch -u http://192.168.21.152/ --full-url -R 2 -x 404 --exclude-sizes=0



没有什么值得关注的，去看看robots



访问这个

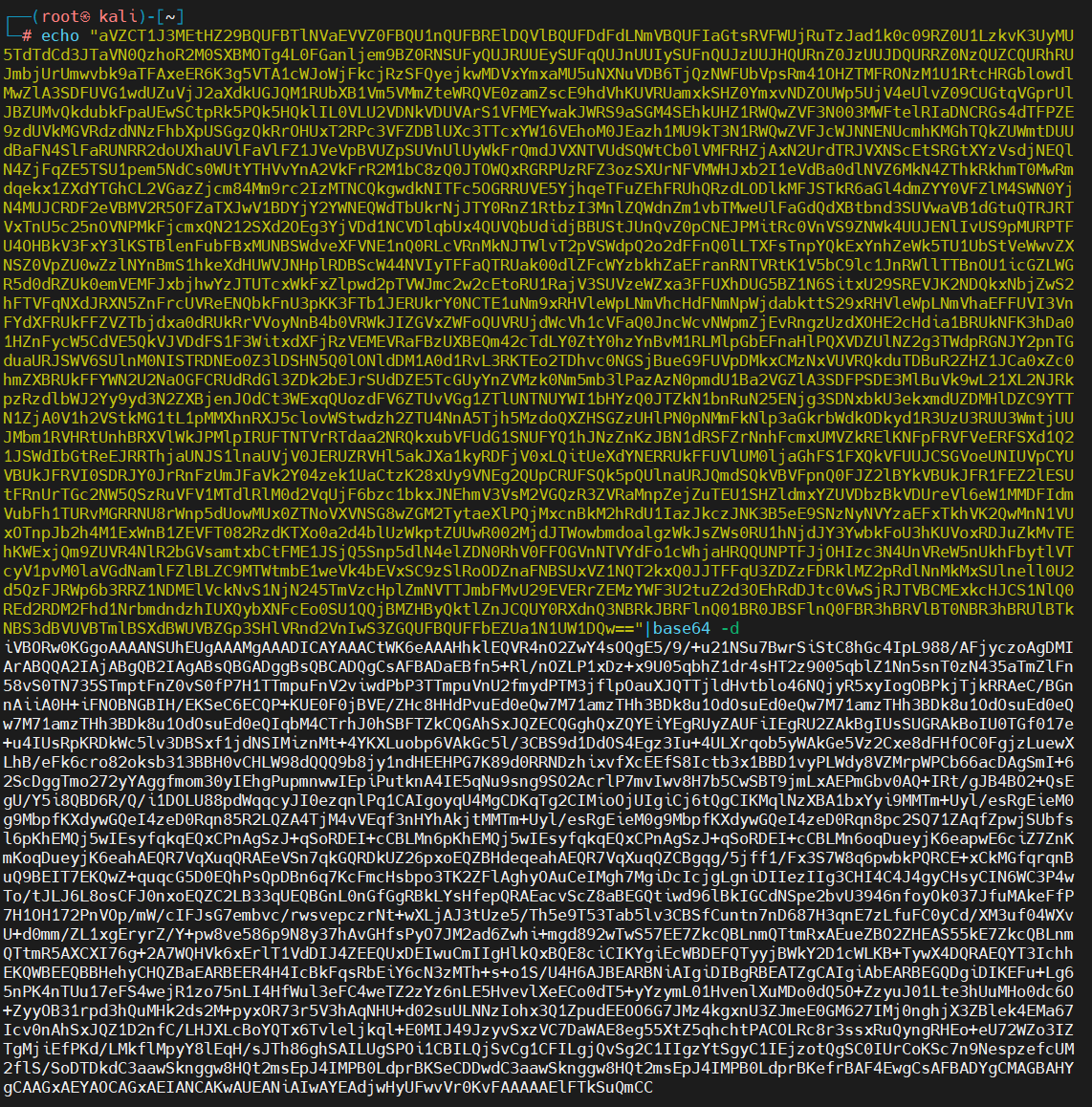


源码里面有个字符串



双等于结尾直接base64看看先

echo ""|base64 -d

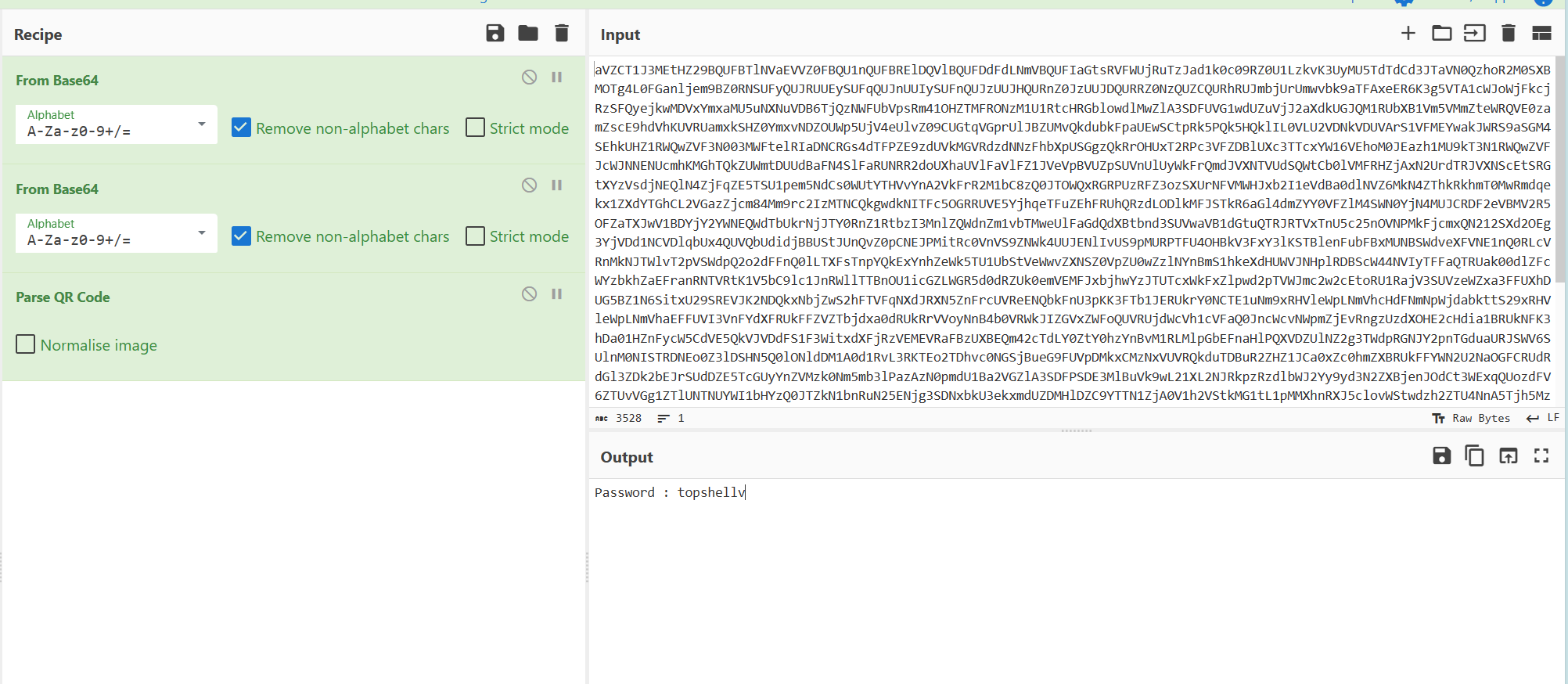


这个因该还是64解码



这个比较怪异不知带是啥但是最后有iend结尾其实是png的文件格式这个就是一个文件

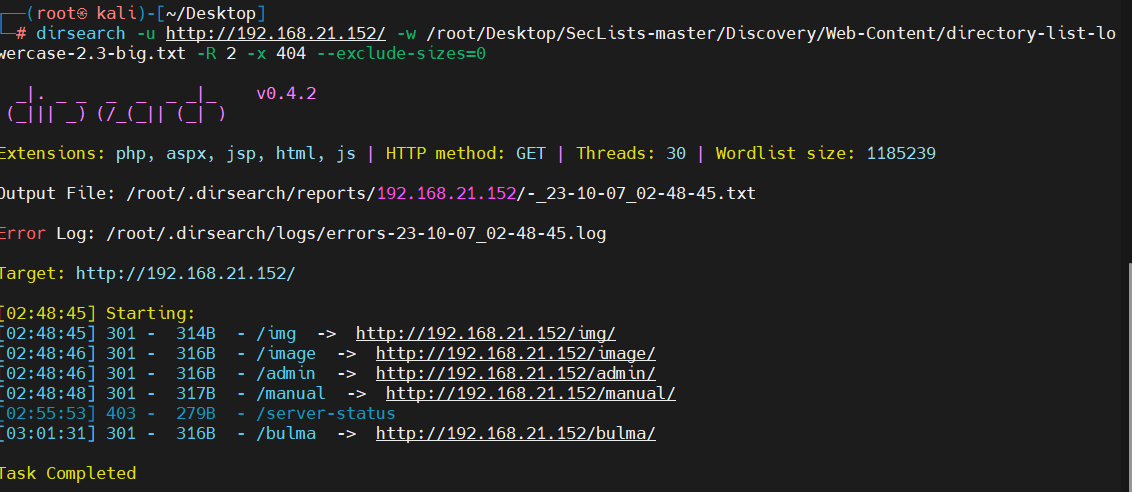
我猜是二维码



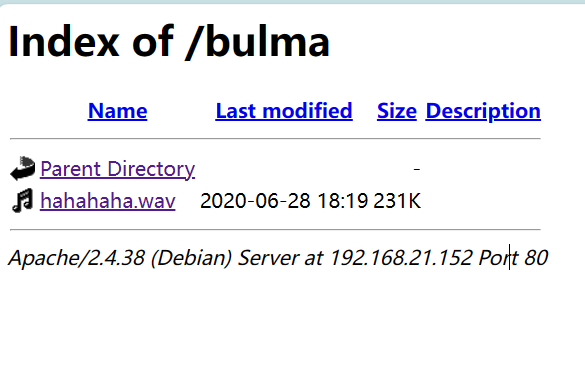
获得密码

到这里线索断了，大概率要重新扫描（要大量时间）

dirsearch -u http://192.168.21.152/ -w /root/Desktop/SecLists-master/Discovery/Web-Content/directory-list-lowercase-2.3-big.txt -R 2 -x 404 --exclude-sizes=0

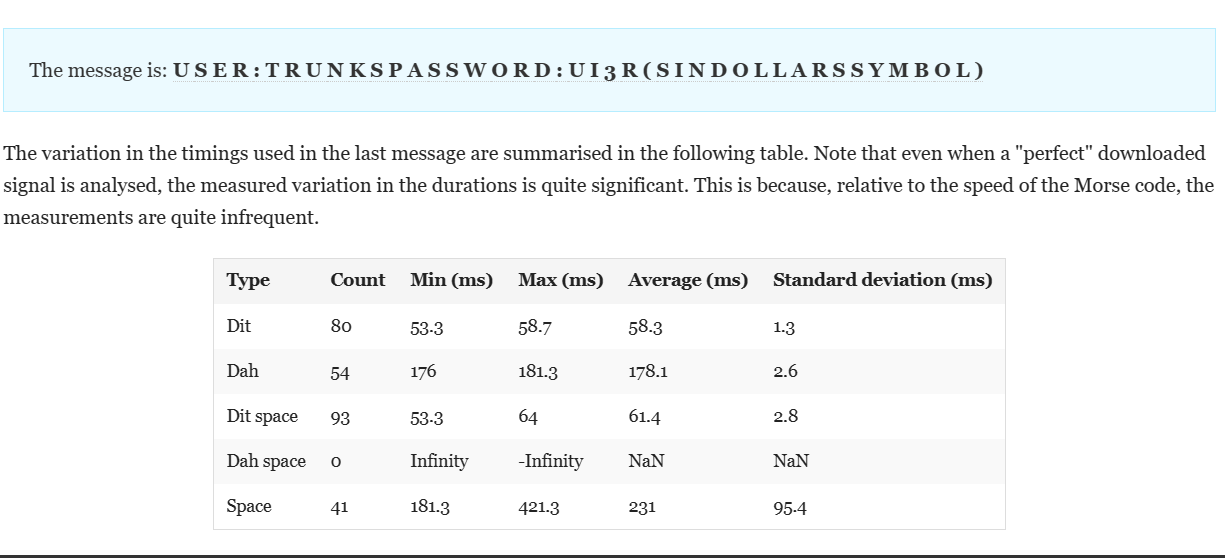


看来看去发现bulma里面有东西

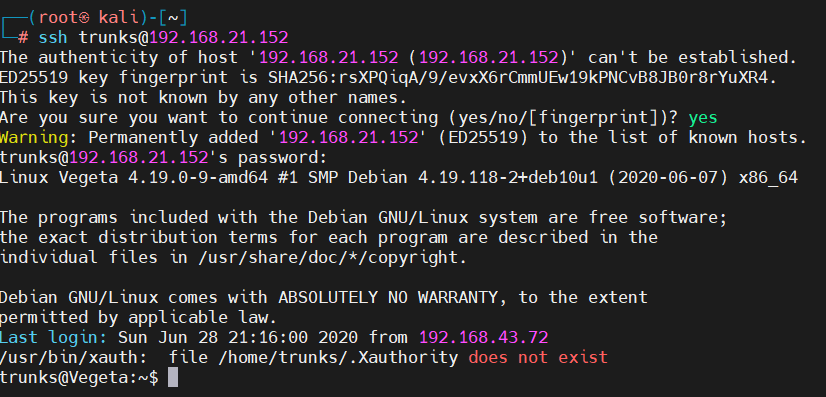


这个里面是典型的摩斯密码，建议用工具

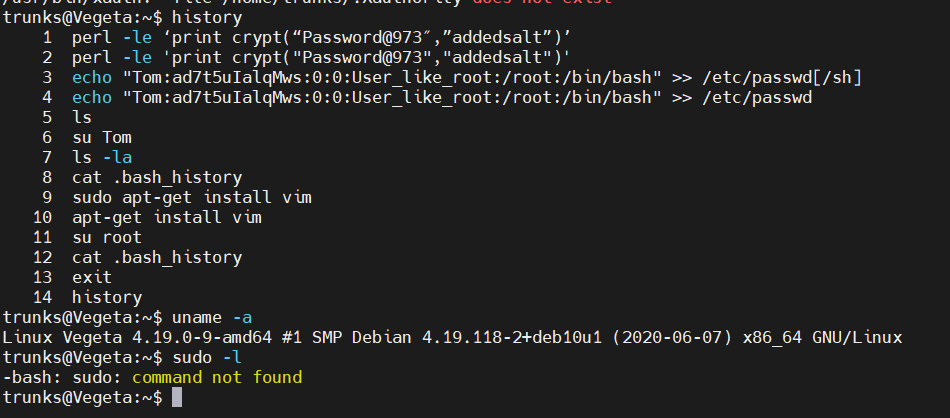
[Morse Code Audio Decoder | Morse Code World](https://morsecode.world/international/decoder/audio-decoder-expert.html)

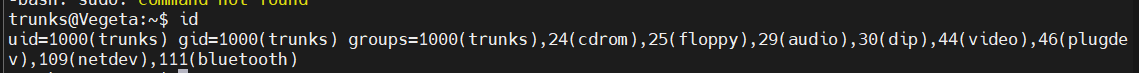


接下来ssh登入就可以



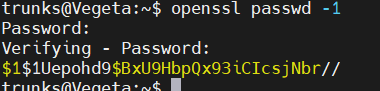
信息收集



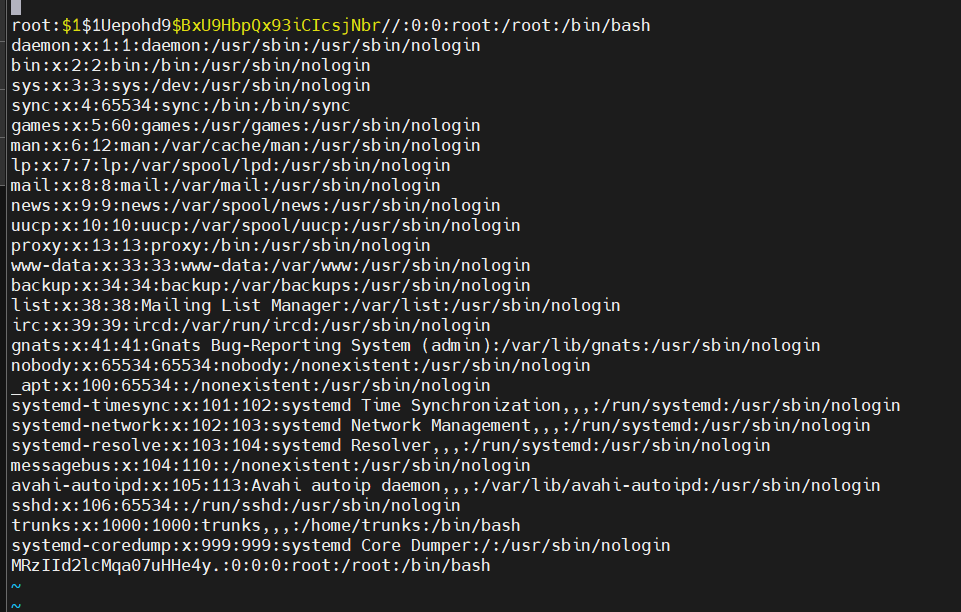


这里发现能对passwd进行操作（直接改root密码）

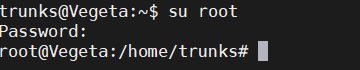
openssl passwd -1

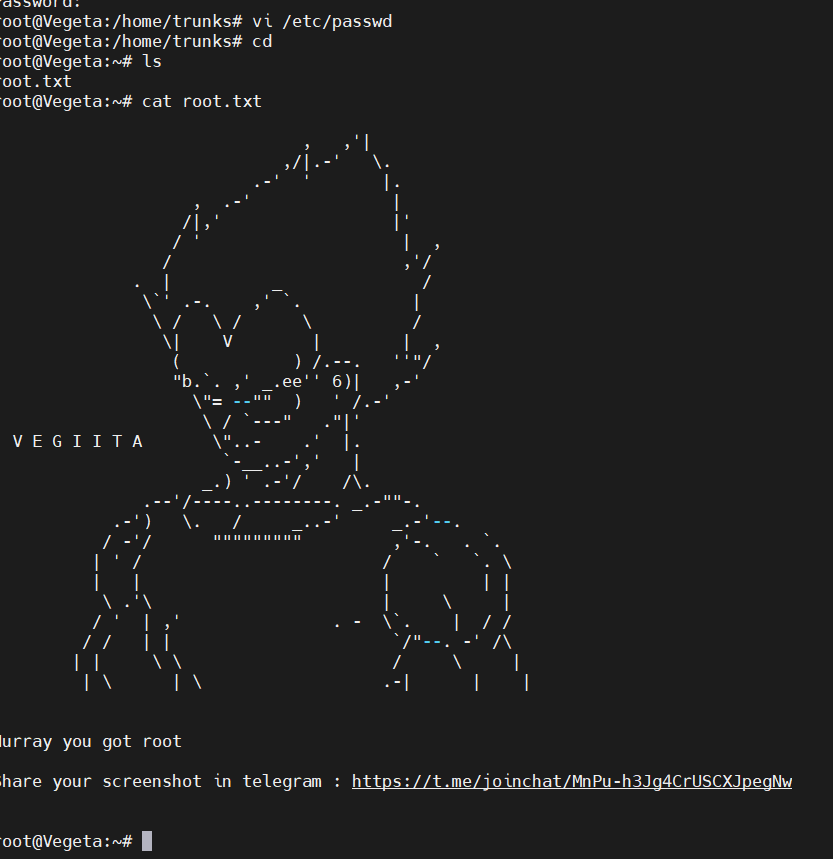


修改passwd文件



登入





解决