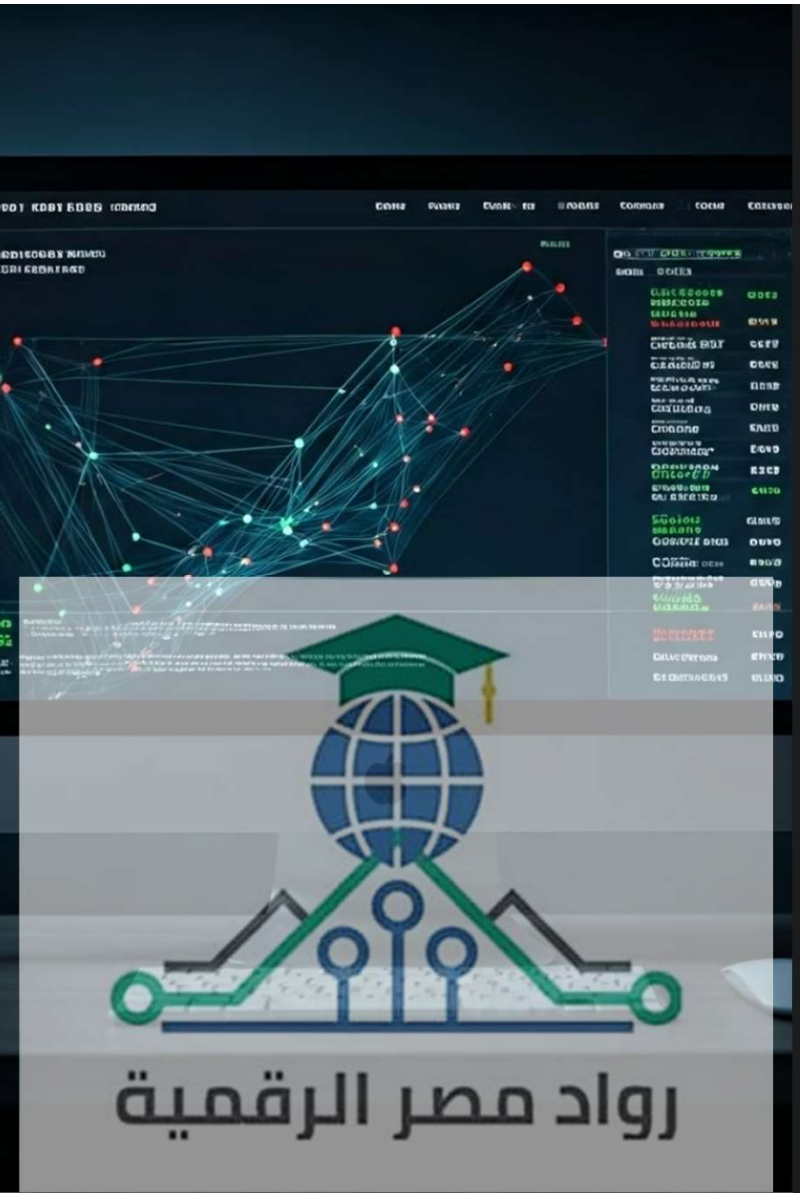


DEPI Penetration Testing Report

This report details the findings of a penetration test conducted on the Trickster machine from Hack The Box. The assessment, completed on October 21, 2024, uncovered multiple critical vulnerabilities that pose significant risks to system security. These issues range from exposed sensitive data to remote code execution possibilities, highlighting the urgent need for remediation to prevent potential breaches and unauthorized access.

Team Members

Ayman Abdelmonsef Mojahid (Leader)
Ahmed Mahmoud Ajmed Aboshady
Ahmed Abdelrahman Abdelrahman
Jihad Reda Adel
Eslam Mahmoud Amin
Mohammed Elsayed Ahmed Saber

Executive Summary

1 Multiple Vulnerabilities Identified

The penetration test revealed several critical security flaws in the Trickster machine, including exposed .git directories, insecure configurations, and remote code execution vulnerabilities.

2 Potential for Unauthorized Access

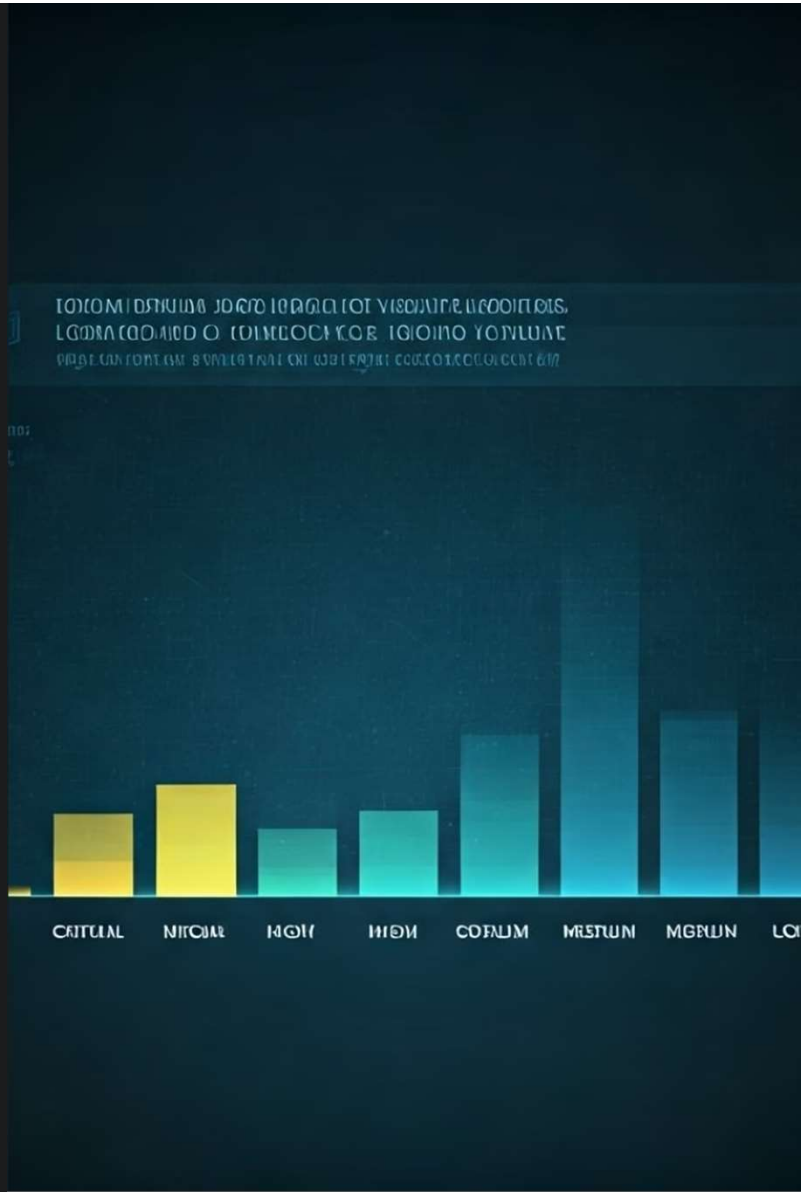
Exploiting these vulnerabilities could lead to unauthorized system access, data breaches, and compromise of system integrity.

3 Urgent Remediation Required

The identified issues pose significant threats to system security and require immediate attention to prevent potential exploitation.

Vulnerability Overview

ID	Vulnerability Name	Severity
1	Accessing .git Directory	(Medium)
2	PrestaShop XSS (CVE-2024-34716)	(High)
3	Database Credentials in PHP Configuration File	(High)
4	Access to Docker Services	(Medium)
5	ChangeDetection Arbitrary File Write SSTI (CVE-2024-32651)	(High)
6	Exposed Backup Files	(High)
7	PrusaSlicer Command Injection (CVE-2023-47268)	(Critical)



Methodology

1. **A1: Injection**

   Exploited command injection vulnerabilities in the system.

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.

Critical Vulnerabilities: Part 1

Accessing .git Directory

Exposed source code and sensitive configuration files, potentially revealing system architecture and security measures.

PrestaShop XSS (CVE-2024-34716)

Allowed remote command execution as the www-data user, posing a significant threat to system integrity.

Database Credentials in PHP Configuration File

Enabled unauthorized access to database contents, potentially exposing sensitive user data.

Critical Vulnerabilities: Part 2

Access to Docker Services

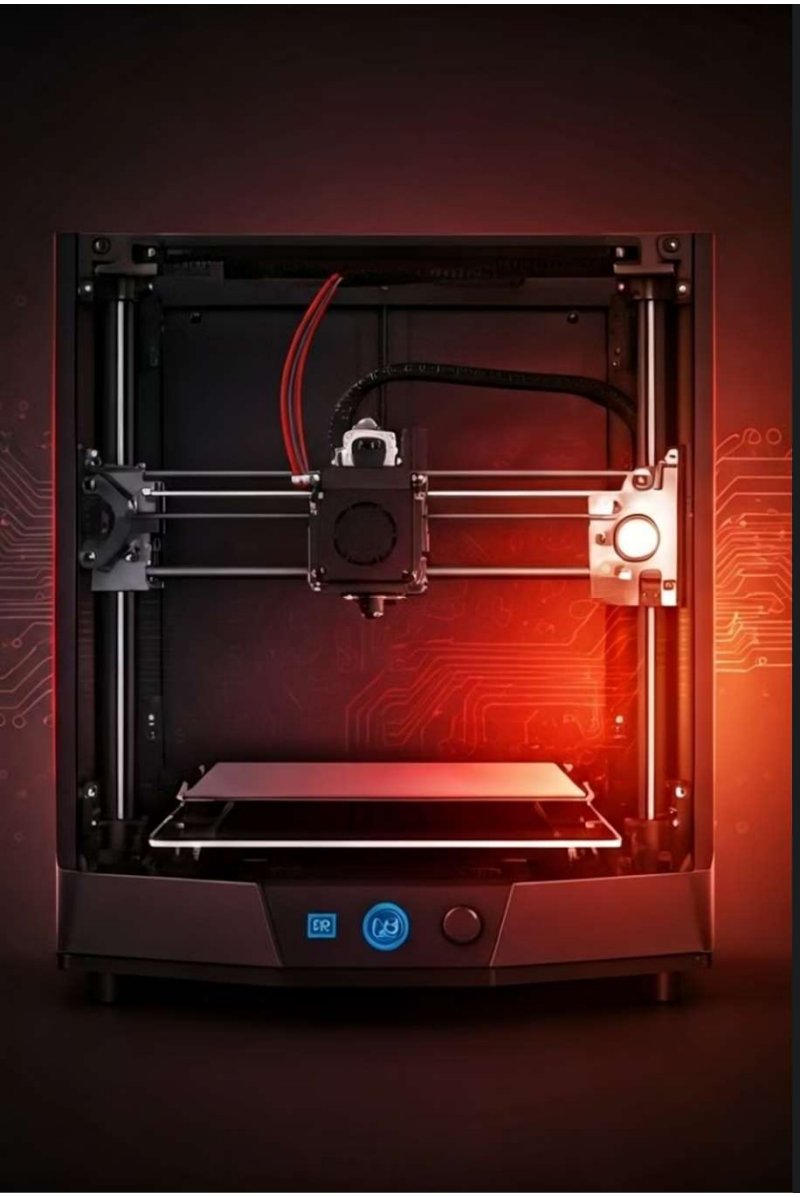
Allowed lateral movement within the system, potentially compromising multiple containers.

ChangeDetection Arbitrary File Write SSTI (CVE-2024-32651) 32651)

Permitted file manipulation within a Docker container, potentially leading to further system compromise.

Exposed Backup Files

Provided access to higher privileged user credentials, enabling escalation of privileges.



PrusaSlicer Command Injection (CVE-2023-(CVE-2023-47268)

1

Vulnerability Discovery

Identified command injection flaw in PrusaSlicer application.

2

Exploitation

Successfully executed arbitrary commands through the vulnerable input.

3

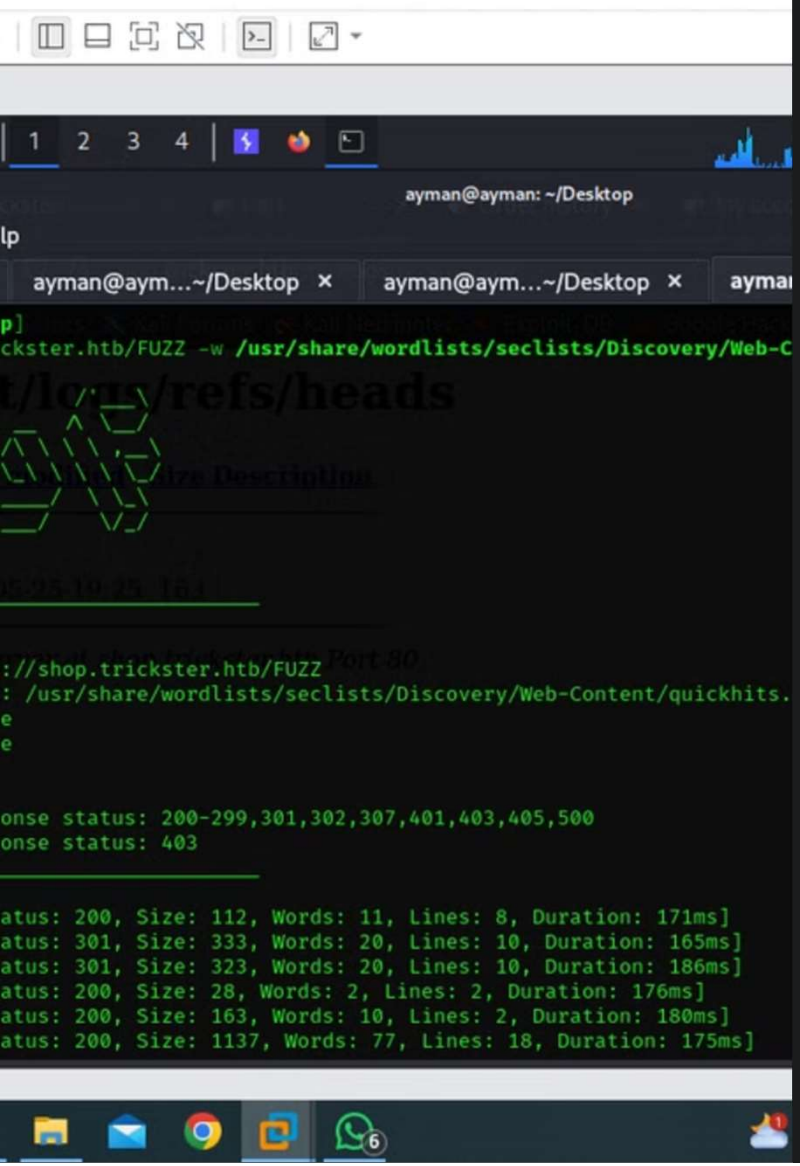
Privilege Escalation

Gained root-level access to system files via the injected commands.

4

Impact

Complete system compromise possible due to elevated privileges.



Exposed .git Directory

A medium severity vulnerability was discovered where the .git directory was publicly accessible. This exposure allows attackers to download source code and configuration files, potentially revealing sensitive data and system structure. The impact could lead to attackers gaining insights into the system's architecture and possibly uncovering hardcoded credentials or configuration flaws.

Severity

Medium

Impact

Exposure of system structure and potential sensitive data

Recommendation

Configure web server to deny access to .git directory and implement proper ACLs

PrestaShop Remote Code Execution (CVE-2024-34716)

A high severity cross-site scripting (XSS) vulnerability was identified in PrestaShop versions 8.1.0 to 8.1.5 with the customer-thread feature flag enabled. This vulnerability allows attackers to upload malicious files containing XSS payloads, which can be executed when an admin opens the attached file in the back office. The exploit can access session data and security tokens, potentially leading to remote code execution.

1. **Vulnerability**

   XSS in PrestaShop's customer-thread feature

2. **Attack Vector**

   Malicious file upload through front-office contact form

3. **Execution**

   Admin opens attached file in back office, triggering XSS

4. **Impact**

   Potential shell access, data compromise, and privilege escalation

Database Credentials in PHP Configuration File

A high severity vulnerability was discovered where database credentials were hardcoded in the PHP configuration file (config.php). This exposure allows attackers to directly access the database using these credentials, potentially leading to unauthorized access, modification, or deletion of sensitive data stored in the database.

1 **Severity**

High

2 **Impact**

Unauthorized database access, potential data integrity loss, and exposure of user information

3 **Recommendation**

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

4 **Best Practice**

Avoid hardcoding sensitive information in configuration files

Access to Docker Services

A medium severity vulnerability was identified where Docker container services were accessible via IP 172.17.0.2 and port 5000. This exposure potentially allows attackers to exploit internal services running inside the Docker container, facilitating lateral movement and further system compromise.

Vulnerability Details

Docker container accessible via IP 172.17.0.2 and port 5000

Potential Impact

Lateral movement and exploitation of internal services

Recommendations

Implement network segmentation and apply firewall rules to control traffic between containers

ChangeDetection Arbitrary File Write (CVE-2024-32651)

A high severity vulnerability was discovered in changedetection.io, an open-source web page change detection and notification service. The vulnerability involves a Server Side Template Injection (SSTI) in Jinja2, allowing for Remote Command Execution on the server host. Successful exploitation provided root access within the Docker environment, leading to potential system compromise.

Update Software

Update ChangeDetection to the latest secure version

Implement Security

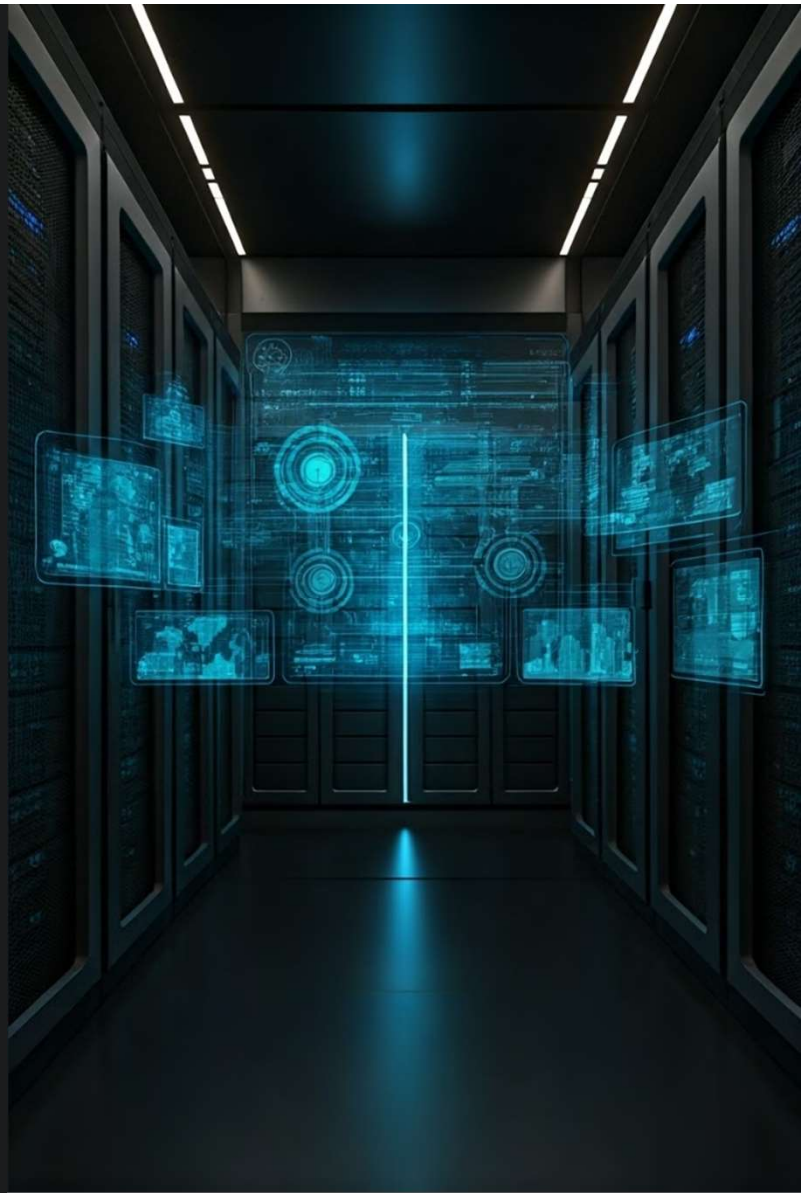
Use input validation and sandboxing techniques

Strengthen Authentication

Enable two-factor authentication (2FA)

Access Control

Ensure sensitive data is only accessible to authorized users



Exposed Backup Files Containing User Credentials

A high severity vulnerability was identified where backup files located in /datastore/Backups/ contained sensitive information, including credentials for the high-privileged user Adam. This exposure allows attackers to potentially log in as a high-privileged user, facilitating privilege escalation and broader system compromise.

1	2	3	4
Discovery	**Content**	**Risk**	**Mitigation**
Exposed backup files in /datastore/Backups/	Sensitive information including high-privileged user credentials	Unauthorized access and privilege escalation	Implement secure storage and restrict access to backup directories

PrusaSlicer Arbitrary Code Execution (CVE-2023-47268)

A critical vulnerability was discovered where PrusaSlicer was configured to run with sudo privileges without a password requirement. This configuration allows attackers to execute arbitrary commands as the root user, granting full control over the system. The impact of this vulnerability is severe, potentially leading to complete system takeover and access to all sensitive files.

Severity	Critical
Impact	Full system control and access to sensitive files
Recommendation 1	Limit sudo access to trusted users
Recommendation 2	Restrict use of sudo without passwords
Recommendation 3	Remove unnecessary sudo configurations for applications

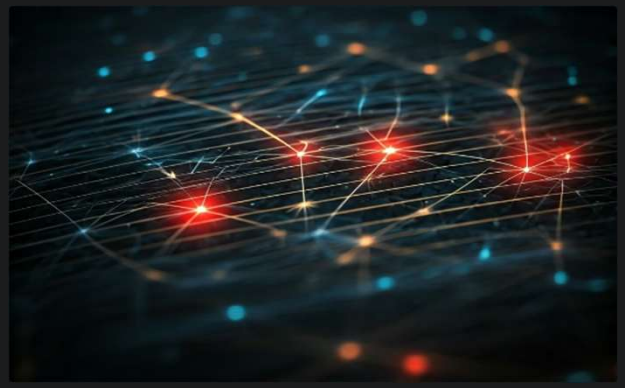
Conclusion and Tools Used

The assessment of the Trickster machine revealed several critical vulnerabilities that pose significant risks to system security. These issues range from exposed configurations and insecure services to critical vulnerabilities allowing remote code execution and privilege escalation. Prompt patching, secure system configuration, and regular security audits are strongly recommended to mitigate these risks.

The assessment utilized various tools including NMAP, FUFF, Git-dumper, Hashcat, Netstat, Arp, Brotli, Python server, and AI assistants like ChatGPT and GitHub Copilot for efficient vulnerability discovery and analysis.

Security Tools

Various tools used for vulnerability assessment and penetration testing



Vulnerability Map

Visual representation of identified vulnerabilities in the system

Secure Infrastructure

Ideal secure setup contrasting with the vulnerabilities found