Task 'Mid Module Assignment Security Risk Identification and Technical Design Analysis' Unit 3

Mid Module Assignment Security Risk Identification and Technical Design Analysis

1. Introduction

Due to the value of financial data and sensitive data being processed in Fintech, such companies are desired targets for threat actors. Effective risk management, robust security design, continuous vulnerability assessment, and planning according to industry security best practices are essential. This technical analysis evaluates the security posture of the Zero Bank web application; a vulnerable online banking platform used for security training and assessment. This report identifies and analyzes key security threats and vulnerabilities present within Zero Bank through ethical vulnerability scanning and manual analysis conducted from a controlled virtual machine environment. Industry-standard tools such as Nessus assess network exposure, service misconfigurations, and application-layer weaknesses. In addition, the Fintech industry is highly regulated one, for instance the EU GDPR, DORA and many more.

(NCSC, 2022; NIST, 2021)

2. Scope and Objectives

The scope of this assessment is limited to ethical and non-intrusive scanning and analysis of the publicly accessible Zero Bank website. No denial-of-service testing or destructive exploitation was conducted.

The key objectives are to:

- Establish a baseline security assessment of the Zero Bank application.
- Identify potential threats and vulnerabilities.
- Evaluate and reference the technical design, architecture and security controls in place.
- Assess the effectiveness and limitations of selected security tools.
- Propose remediation recommendations aligned with best practices.

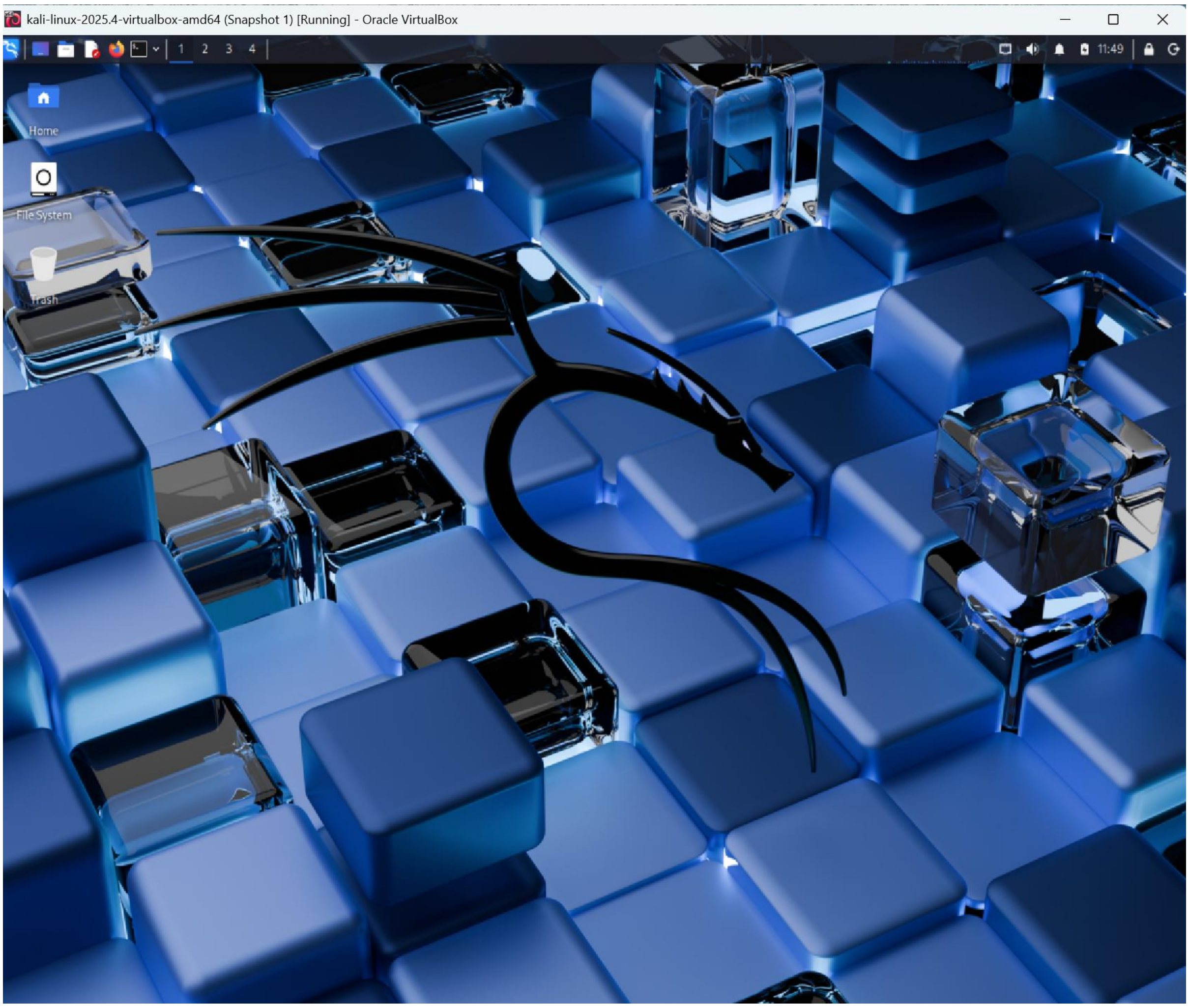
(NIST, 2021)

3. Methodology – Rules of Engagement

The assessment followed a smaller scope vulnerability assessment lifecycle which is based on the NIST SP 800-115 Testing Guide methodologies. Testing will be conducted using a Kali Linux virtual machine and will maintain ethics.

(NIST, 2021)

Task ‘Mid Module Assignment Security Risk Identification and Technical Design Analysis’ Unit 3



kali-linux-2025.4-virtualbox-amd64 (Snapshot 1) [Running] - Oracle VirtualBox

Figure 1: Installed Kali VM

The methodology included

1. Reconnaissance and passive, automated vulnerability scanning using Nessus.
2. Risk evaluation and impact analysis based on findings.
3. Documentation of findings and remediation guidance.

Overview of Ethical Assessment Approach

All scanning activities will be performed in an ethical manner, reducing impact on the availability, integrity, or confidentiality of any assets as much as possible. Automated scans were supplemented with manual inspection to reduce false positives and better understand application logic flaws such as broken access control and cross-site scripting.

(NCSC, 2022; NIST, 2021)

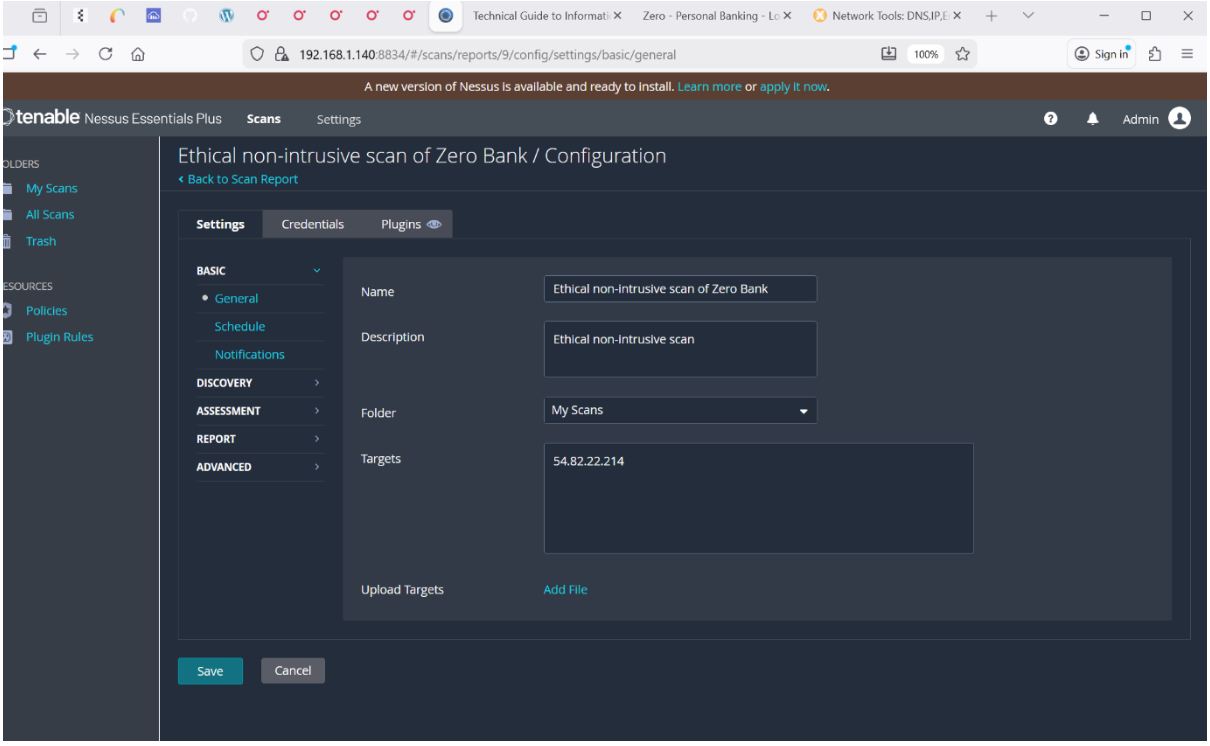
Ethical Vulnerability Analysis Report: Zero Bank

Website Technology Identification

During the initial reconnaissance and automated passive scanning, Nessus had identified the target as a Java-based web application on an Apache Tomcat server . Its architecture follows a traditional web application design. The server exposes HTTP interface which is misconfigured or insufficiently protected.

(NCSC, 2022; NIST, 2021)

4. Target Scan Setup Screenshots



192.168.1.140:8834/#/scans/reports/9/config/settings/basic/general

A new version of Nessus is available and ready to install. Learn more or apply it now.

tenable Nessus Essentials Plus · Scans · Settings · Admin

Ethical non-intrusive scan of Zero Bank / Configuration

‹ Back to Scan Report

Settings · Credentials · Plugins

BASIC: General, Schedule, Notifications · DISCOVERY · ASSESSMENT · REPORT · ADVANCED

Name: Ethical non-intrusive scan of Zero Bank

Description: Ethical non-intrusive scan

Folder: My Scans

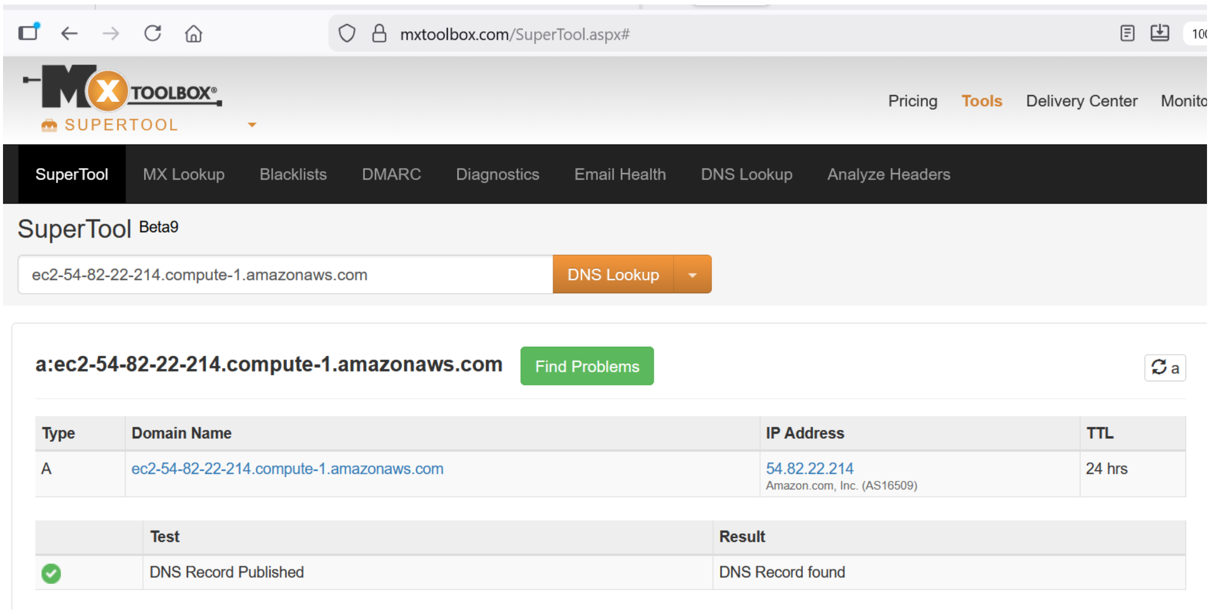
Targets: 54.82.22.214

Upload Targets: Add File

Save · Cancel

Figure 2: Nessus scan setup

(Tenable, 2026)



mxtoolbox.com/SuperTool.aspx#

SuperTool Beta9

ec2-54-82-22-214.compute-1.amazonaws.com · DNS Lookup

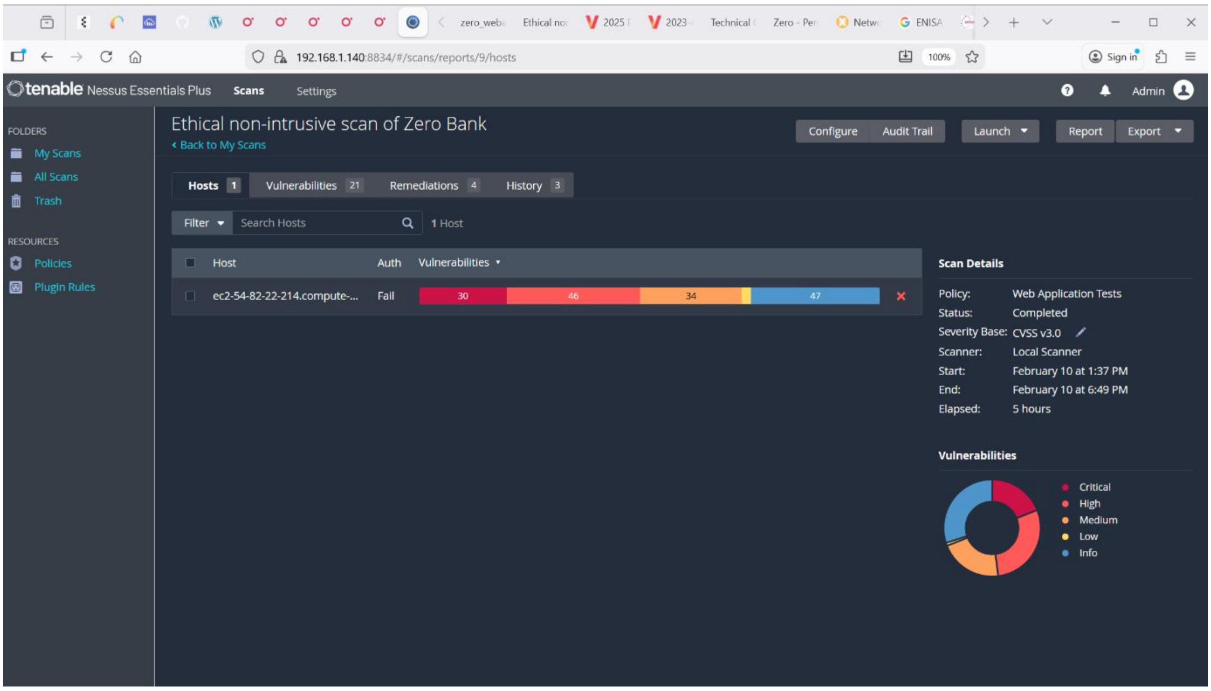
a:ec2-54-82-22-214.compute-1.amazonaws.com · Find Problems

Type	Domain Name	IP Address	TTL
A	ec2-54-82-22-214.compute-1.amazonaws.com	54.82.22.214 Amazon.com, Inc. (AS16509)	24 hrs

	Test	Result
✓	DNS Record Published	DNS Record found

Figure 3: DNS Lookup

(MXToolbox.com, 2021)



Ethical non-intrusive scan of Zero Bank

‹ Back to My Scans

Hosts 1 | Vulnerabilities 21 | Remediations 4 | History 3

1 Host

Host	Auth	Vulnerabilities
ec2-54-82-22-214.compute-...	Fail	30 46 34 47

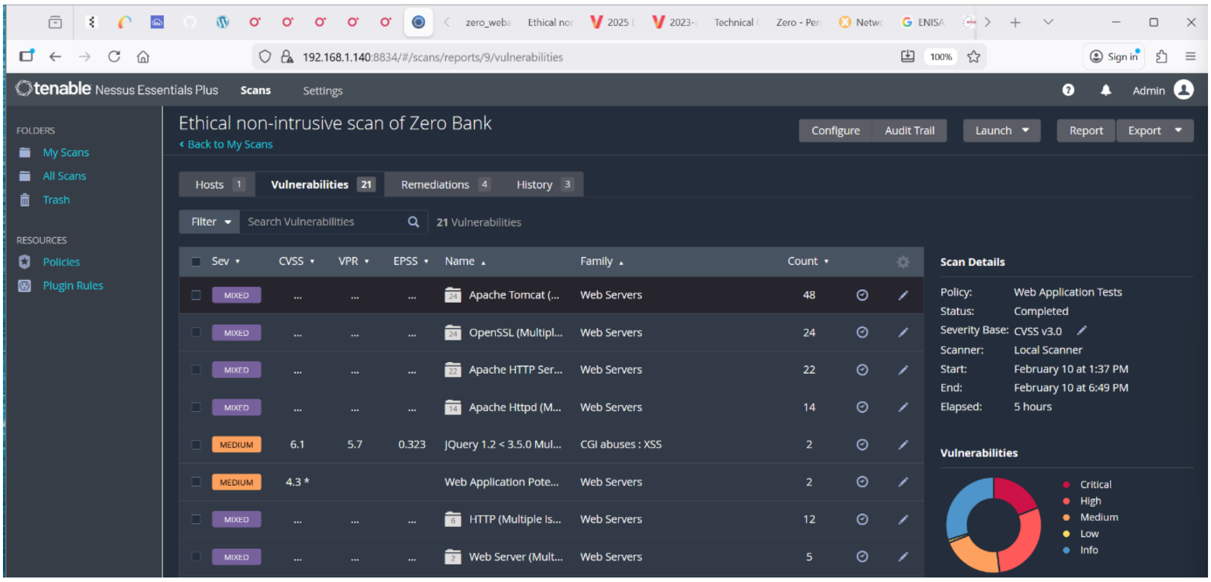
Scan Details

Policy: Web Application Tests
Status: Completed
Severity Base: CVSS v3.0
Scanner: Local Scanner
Start: February 10 at 1:37 PM
End: February 10 at 6:49 PM
Elapsed: 5 hours

Vulnerabilities

Figure 4: Nessus Findings Overview

(Tenable, 2026)



Ethical non-intrusive scan of Zero Bank

‹ Back to My Scans

Hosts 1 | Vulnerabilities 21 | Remediations 4 | History 3

21 Vulnerabilities

Sev	CVSS	VPR	EPSS	Name	Family	Count
MIXED	...	...	...	24 Apache Tomcat (...	Web Servers	48
MIXED	...	...	...	24 OpenSSL (Multipl...	Web Servers	24
MIXED	...	...	...	22 Apache HTTP Ser...	Web Servers	22
MIXED	...	...	...	14 Apache Httpd (M...	Web Servers	14
MEDIUM	6.1	5.7	0.323	JQuery 1.2 < 3.5.0 Mul...	CGI abuses : XSS	2
MEDIUM	4.3 *			Web Application Pote...	Web Servers	2
MIXED	...	...	...	6 HTTP (Multiple Is...	Web Servers	12
MIXED	...	...	...	2 Web Server (Mult...	Web Servers	5

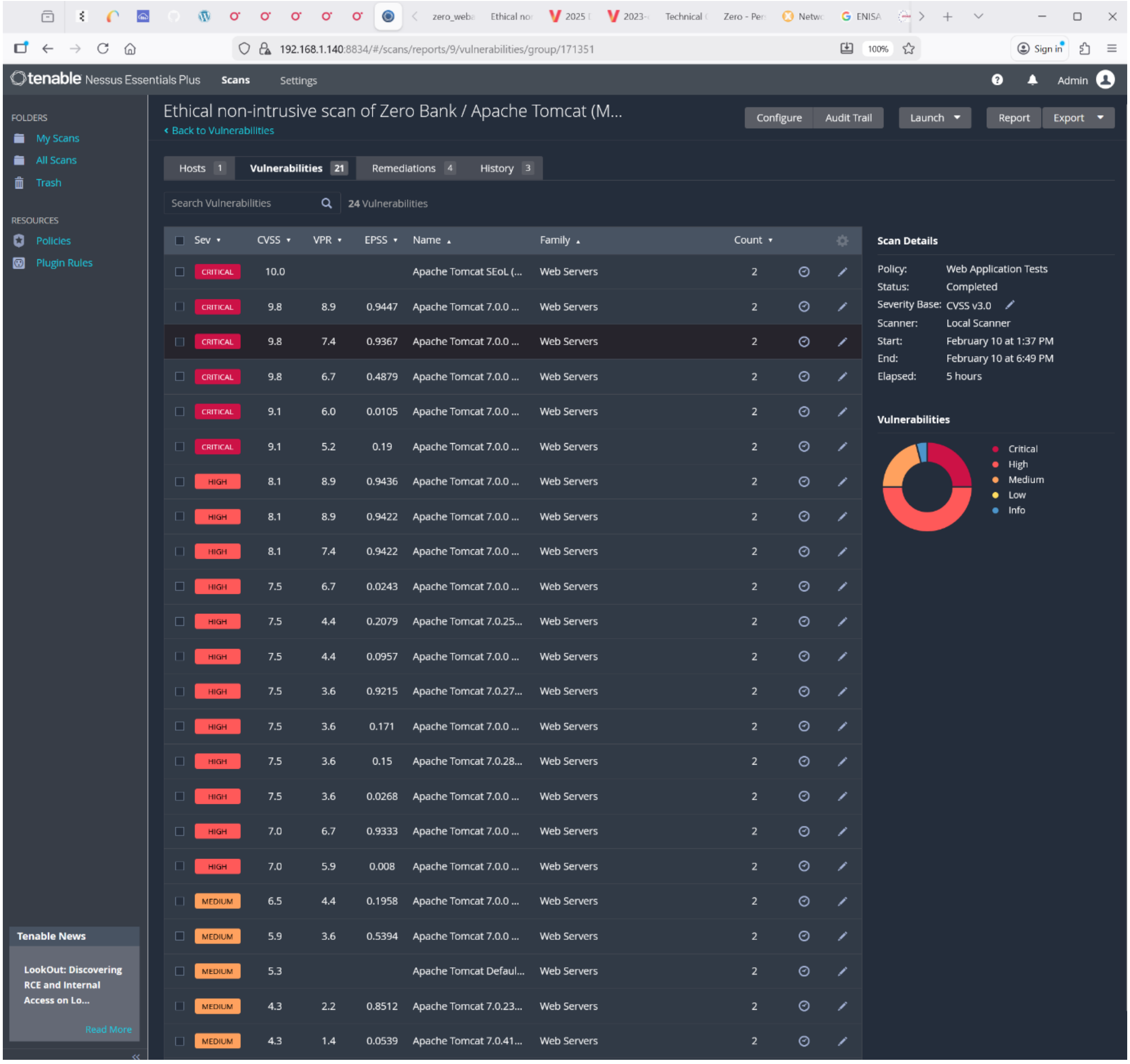
Scan Details

Policy: Web Application Tests
Status: Completed
Severity Base: CVSS v3.0
Scanner: Local Scanner
Start: February 10 at 1:37 PM
End: February 10 at 6:49 PM
Elapsed: 5 hours

Vulnerabilities

Figure 5: Nessus Finding 2 Mixed Collected

(Tenable, 2026)



Ethical non-intrusive scan of Zero Bank / Apache Tomcat (M...

‹ Back to Vulnerabilities

Hosts 1 | Vulnerabilities 21 | Remediations 4 | History 3

Search Vulnerabilities 24 Vulnerabilities

Sev	CVSS	VPR	EPSS	Name	Family	Count
CRITICAL	10.0			Apache Tomcat SEoL (...	Web Servers	2
CRITICAL	9.8	8.9	0.9447	Apache Tomcat 7.0.0 ...	Web Servers	2
CRITICAL	9.8	7.4	0.9367	Apache Tomcat 7.0.0 ...	Web Servers	2
CRITICAL	9.8	6.7	0.4879	Apache Tomcat 7.0.0 ...	Web Servers	2
CRITICAL	9.1	6.0	0.0105	Apache Tomcat 7.0.0 ...	Web Servers	2
CRITICAL	9.1	5.2	0.19	Apache Tomcat 7.0.0 ...	Web Servers	2
HIGH	8.1	8.9	0.9436	Apache Tomcat 7.0.0 ...	Web Servers	2
HIGH	8.1	8.9	0.9422	Apache Tomcat 7.0.0 ...	Web Servers	2
HIGH	8.1	7.4	0.9422	Apache Tomcat 7.0.0 ...	Web Servers	2
HIGH	7.5	6.7	0.0243	Apache Tomcat 7.0.0 ...	Web Servers	2
HIGH	7.5	4.4	0.2079	Apache Tomcat 7.0.25...	Web Servers	2
HIGH	7.5	4.4	0.0957	Apache Tomcat 7.0.0 ...	Web Servers	2
HIGH	7.5	3.6	0.9215	Apache Tomcat 7.0.27...	Web Servers	2
HIGH	7.5	3.6	0.171	Apache Tomcat 7.0.0 ...	Web Servers	2
HIGH	7.5	3.6	0.15	Apache Tomcat 7.0.28...	Web Servers	2
HIGH	7.5	3.6	0.0268	Apache Tomcat 7.0.0 ...	Web Servers	2
HIGH	7.0	6.7	0.9333	Apache Tomcat 7.0.0 ...	Web Servers	2
HIGH	7.0	5.9	0.008	Apache Tomcat 7.0.0 ...	Web Servers	2
MEDIUM	6.5	4.4	0.1958	Apache Tomcat 7.0.0 ...	Web Servers	2
MEDIUM	5.9	3.6	0.5394	Apache Tomcat 7.0.0 ...	Web Servers	2
MEDIUM	5.3			Apache Tomcat Defaul...	Web Servers	2
MEDIUM	4.3	2.2	0.8512	Apache Tomcat 7.0.23...	Web Servers	2
MEDIUM	4.3	1.4	0.0539	Apache Tomcat 7.0.41...	Web Servers	2

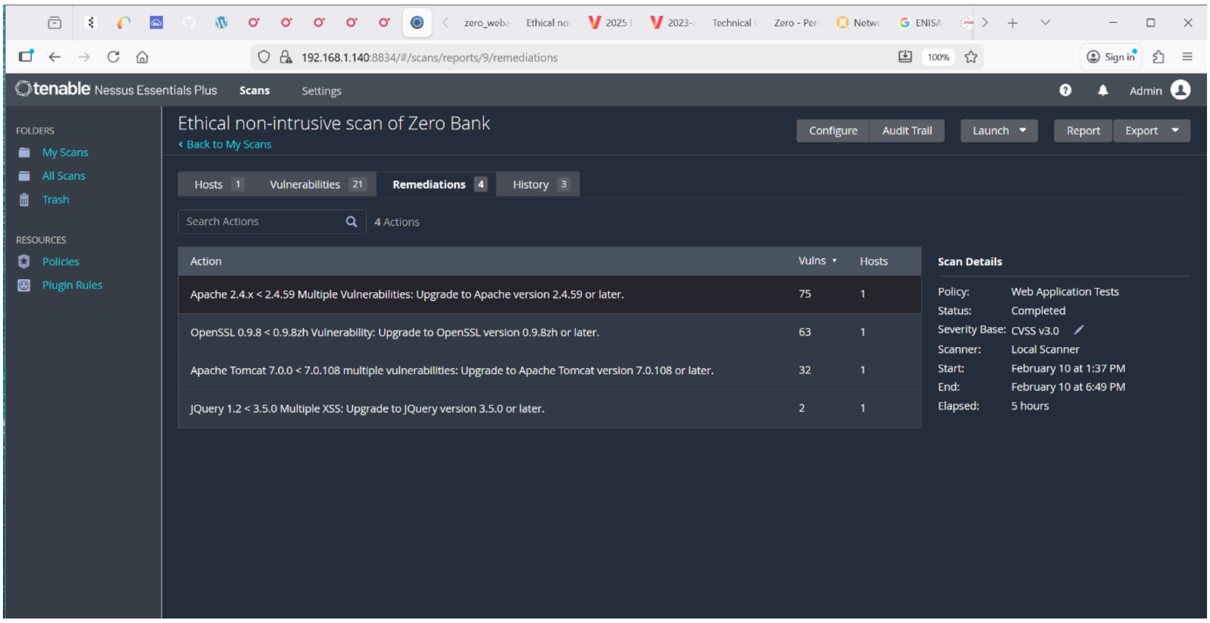
Scan Details

Policy:	Web Application Tests
Status:	Completed
Severity Base:	CVSS v3.0
Scanner:	Local Scanner
Start:	February 10 at 1:37 PM
End:	February 10 at 6:49 PM
Elapsed:	5 hours

Vulnerabilities

Figure 6: Apache Tomcat CVSS 10.0

(Tenable, 2026)



Ethical non-intrusive scan of Zero Bank

4 Actions

Action	Vulns	Hosts
Apache 2.4.x < 2.4.59 Multiple Vulnerabilities: Upgrade to Apache version 2.4.59 or later.	75	1
OpenSSL 0.9.8 < 0.9.8zh Vulnerability: Upgrade to OpenSSL version 0.9.8zh or later.	63	1
Apache Tomcat 7.0.0 < 7.0.108 multiple vulnerabilities: Upgrade to Apache Tomcat version 7.0.108 or later.	32	1
JQuery 1.2 < 3.5.0 Multiple XSS: Upgrade to JQuery version 3.5.0 or later.	2	1

Scan Details

Policy:	Web Application Tests
Status:	Completed
Severity Base:	CVSS v3.0
Scanner:	Local Scanner
Start:	February 10 at 1:37 PM
End:	February 10 at 6:49 PM
Elapsed:	5 hours

Figure 7 : Remediation recommendations

(Tenable, 2026)

5. Key Vulnerability Findings

5.1. Outdated Software Components

Outdated software was found in multiple different components such as Apache Tomcat, OpenSSL, JQuery, and Apache HTTP Server (HTTPD) outdated components.

Impact:

Outdated Apache Tomcat, OpenSSL, Apache HTTP Server (HTTPD) version vulnerable to multiple critical security flaws.

Remediation Recommendations:

- Verify that the vulnerabilities found are not related to old libraries still exist on the system.

- Upgrade all components to the latest version using proper testing and change management process.

5.2. Cross-Site Scripting (XSS)

Multiple XSS was identified within few plugins.

Impact:

XSS vulnerabilities allow attackers to compromise browsers and execute scripts to progress to session hijacking, and privilege escalation, or steal credentials.

Remediation Recommendations:

- Apply strict input validation and output encoding.
- Restrict headers to script execution using Implementation Content Security Policy (CSP).

5.3. Web Application Potentially Vulnerable to Clickjacking

Remote server lacks X-Frame-Options or frame-ancestors, exposing them to clickjacking attacks that enable fraudulent user actions.

Impact:

Missed client-side defenses like frame-busting scripts leave systems vulnerable to clickjacking attacks, increasing the risk of unauthorized actions and security breaches.

Remediation Recommendations:

- Ensure the server includes X-Frame-Options or Content-Security-Policy in responses. These headers prevent page embedding.

5.4. HSTS Missing from HTTPS Server (RFC 6797)

Nessus scans identified that remote server lacks HSTS enforcement.

Impact:

Missing HSTS enforcement could enable downgrade, SSL-stripping, man-in-the-middle attacks, and weakening secure cookie protection over HTTPS connections.

Remediation Recommendations:

- Configure your web server to send the Strict-Transport-Security HTTP response header.
- Implement a Web Application Firewall or a Reverse proxy and HTTPs with at least TLS 1.2 encryption.

5.5. Authentication over Cleartext

Nessus vulnerability scans had identified that the web server uses authentication over HTTP and not HTTPS without encryption of data in transit.

Impact:

The server uses Basic authentication without encryption, exposing usernames and passwords to anyone intercepting the traffic.

Remediation Recommendations:

- Configure your web server to use the strict HTTPs of at least TLS 1.2.
- Implement an automated certificate management solution for all web servers

5.6. Identified Threats and Vulnerabilities

Threat Category	Description	Severity	CVSS	# Found
Outdated **Apache Tomcat** Components	Unpatched server software	Critical	10.0	48
Outdated **OpenSSL** Components	Unpatched server software	Critical	9.8	24
Outdated **Apache HTTPD Server** Components	Unpatched server software	Critical	10.0	36
CGI abuses: **XSS JQuery**	Stored script injection	Medium	6.1	2
Web Application Potentially Vulnerable to Clickjacking	Remote web server is not set with Frame-Options and response header	Medium	4.3*	20
HSTS Missing from HTTPS Server (RFC 6797)	HSTS allows downgrade attacks	Medium	6.5	12
authentication over cleartext	Web Server Uses HTTPS	Low	2.6*	2

Table 1: Tenable Nessus Essentials Plus findings

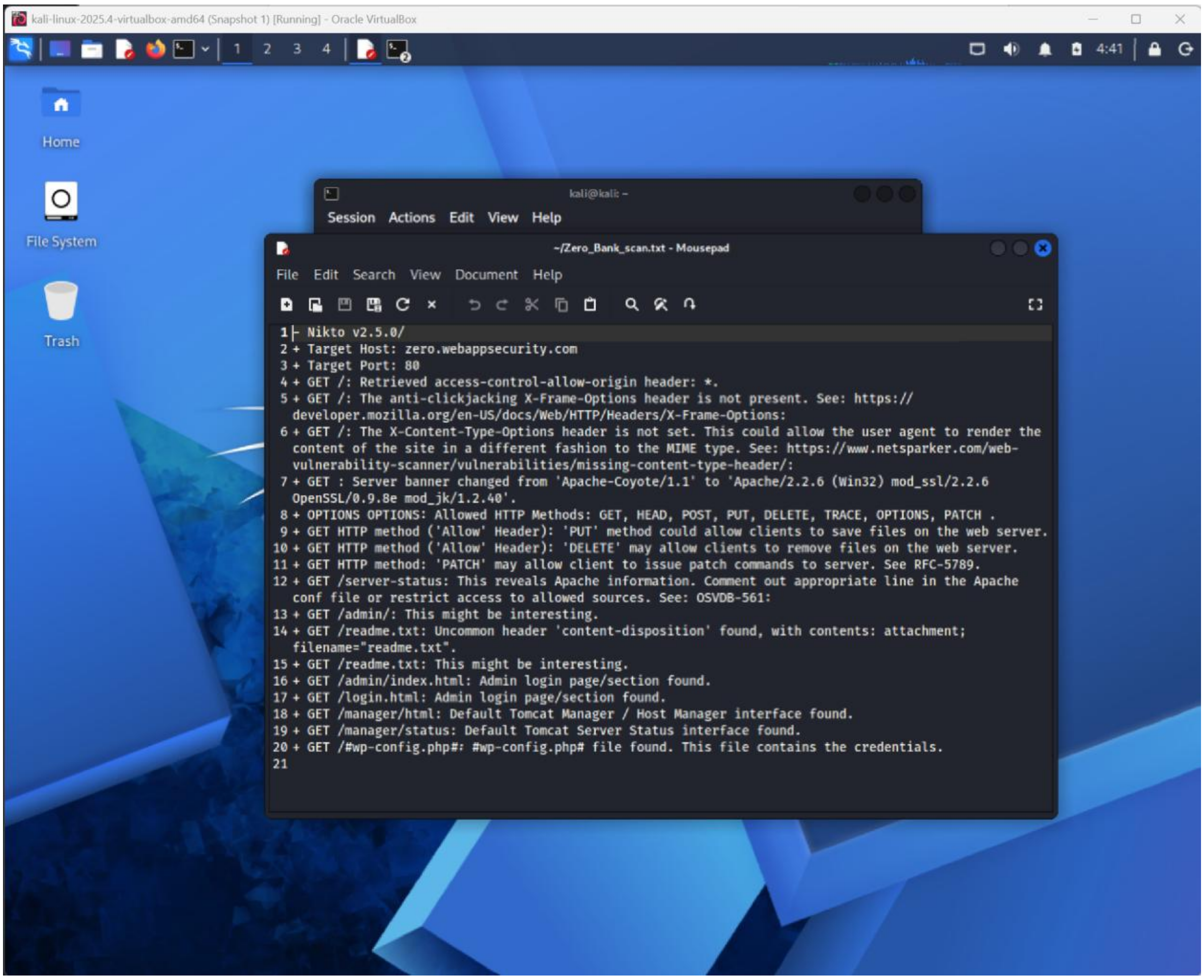
(Tenable, 2026, MITRE, 2024)

5.1. Link to Scanning Report Logs

https://am25251.github.io/uoe-eportfolio/files/03-Network_Security_January/Unit_3/Ethical_non_intrusive_scan_of_Zero_Bank_wl4sr1.pdf

6. Tools Used and Operational Impact

- Nessus (free): Comprehensive vulnerability detection; potential performance overhead.
- Nessus was accessed via Kali's web server from Windows 11 browser: https://192.168.1.140:8834/#/.
- Nikto assessments showed similar results with minor variations; due to document limits, findings are out of scope, with only illustration included.


kali-linux-2025.4-virtualbox-amd64 (Snapshot 1) [Running] - Oracle VirtualBox
Home
File System
Trash
4:41
kali@kali: ~
Session Actions Edit View Help
~/Zero_Bank_scan.txt - Mousepad
File Edit Search View Document Help

```
- Nikto v2.5.0/
+ Target Host: zero.webappsecurity.com
+ Target Port: 80
+ GET /: Retrieved access-control-allow-origin header: *.
+ GET /: The anti-clickjacking X-Frame-Options header is not present. See: https://
  developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Frame-Options:
+ GET /: The X-Content-Type-Options header is not set. This could allow the user agent to render the
  content of the site in a different fashion to the MIME type. See: https://www.netsparker.com/web-
  vulnerability-scanner/vulnerabilities/missing-content-type-header/:
+ GET : Server banner changed from 'Apache-Coyote/1.1' to 'Apache/2.2.6 (Win32) mod_ssl/2.2.6
  OpenSSL/0.9.8e mod_jk/1.2.40'.
+ OPTIONS OPTIONS: Allowed HTTP Methods: GET, HEAD, POST, PUT, DELETE, TRACE, OPTIONS, PATCH .
+ GET HTTP method ('Allow' Header): 'PUT' method could allow clients to save files on the web server.
+ GET HTTP method ('Allow' Header): 'DELETE' may allow clients to remove files on the web server.
+ GET HTTP method: 'PATCH' may allow client to issue patch commands to server. See RFC-5789.
+ GET /server-status: This reveals Apache information. Comment out appropriate line in the Apache
  conf file or restrict access to allowed sources. See: OSVDB-561:
+ GET /admin/: This might be interesting.
+ GET /readme.txt: Uncommon header 'content-disposition' found, with contents: attachment;
  filename="readme.txt".
+ GET /readme.txt: This might be interesting.
+ GET /admin/index.html: Admin login page/section found.
+ GET /login.html: Admin login page/section found.
+ GET /manager/html: Default Tomcat Manager / Host Manager interface found.
+ GET /manager/status: Default Tomcat Server Status interface found.
+ GET /#wp-config.php#: #wp-config.php# file found. This file contains the credentials.
```

Figure 8: Nikto Scan Results

7. Assumptions and Limitations

- Given this closed system, architecture is assumed.
- Automated scanning using Nessus may generate false positives.
- Static assessment is Out-of-Scope.
- Testing was limited to publicly exposed interfaces.

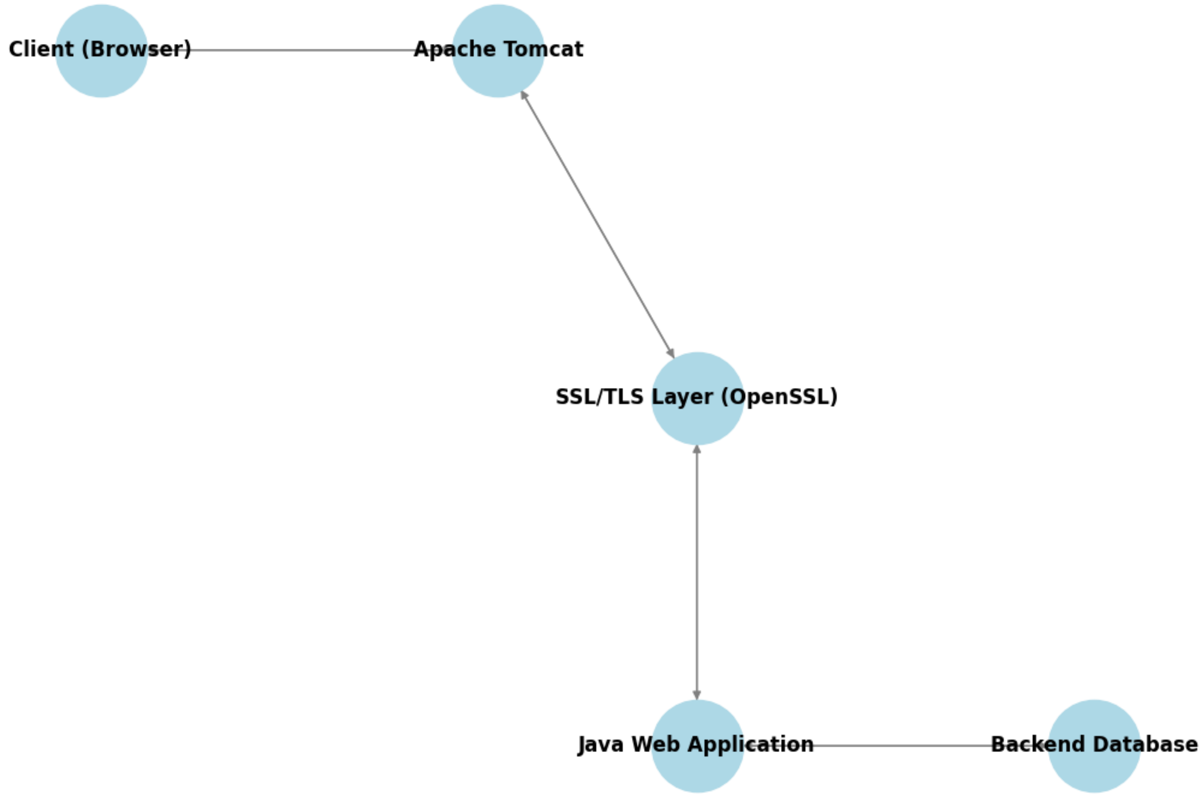


Figure 9: Simplified architecture

Phase	Duration
VM Setup and Configuration	1 day
Reconnaissance and Scanning	2 days
Manual Validation	2 days
Analysis and Reporting	2 days

Table 2: Assessment Timeline

Conclusion

This analysis of Zero Bank web-application had identified multiple high-risk security vulnerabilities from outdated software, XSS, Clickjacking, downgrade attacks and unencrypted connections. Zero Bank is an intentionally vulnerable platform, yet these weaknesses reflect real-world security flaws in many Fintech production systems. Designing and implementing effective patch and change management practices, strong encryption, robust access control mechanism with continuous security testing, is essential for properly managing these risks. Ethical security assessments using structured methodologies and industry-leading Nessus were selected to provide valuable results in improving overall security posture.

References

- NIST (2021) Technical guide to information security testing and assessment, NIST SP 800-115. National Institute of Standards and Technology. Gaithersburg, MD: NIST.
- NCSC (2022) ‘Advice on how to get the most from penetration testing’. Available at: https://www.ncsc.gov.uk/guidance/penetration-testing [Accessed: 6 February 2026].
- MITRE (2024) Common Vulnerabilities and Exposures (CVE) Program. Available at: https://cve.mitre.org [Accessed: 12 February 2026].

- MXToolbox (2021) *MXToolbox SuperTool*. Available at: https://mxtoolbox.com [Accessed: 15 February 2026].
- Tenable (2026) Nessus Essentials Plus. Available at: https://www.tenable.com/products/nessus/nessus-essentials [Accessed: 11 February 2026].