Task ‘Vulnerability Analysis – Literature Review Activity’ Unit 2

Baseline Vulnerability Audit of the Zero Bank Findings

A Literature-Informed Audit Using Software Security Sources and the National Vulnerabilities Database

Introduction

This document presents a baseline vulnerability audit of the Zero Bank web application; a deliberately vulnerable online banking simulation used for cybersecurity education. The purpose of this audit is to identify and classify common web application vulnerabilities by combining passive software site analysis, academic and professional literature, and pattern-based review of the National Vulnerabilities Database (NVD).

Rather than conducting intrusive penetration testing, this activity applies ethical, non-destructive methods to research and establish a baseline security posture. Common Weakness Enumeration (CWE) recognized vulnerability classes, as documented in the NVD, the Common Weakness Enumeration (CWE) can be used to assess potential risks and exercise support the development of auditing, analytical, and risk-assessment skills aligned with modern vulnerability management practices.

(Singla et al, 2023; MITRE, 2025; NIST, 2025).

1. Scope

The scope of this audit will focus on literature audit of the Zero Bank related to the web application (http://zero.webappsecurity.com) site. Web-based application vulnerabilities commonly affect such systems, in this case, using sources based on literature from passive discovery and analysis only, with no active scanning whatsoever, neither exploitation nor any service disruption. We will focus only on such approach that preserves the integrity and availability of the platform while maintaining ethical and legal boundaries.

(Ngowry, 2025; NCSC 2017)

1.1. Objectives

1. The objectives of this baseline audit are to
2. Identify literature about potential web application vulnerabilities in Zero Bank using passive literature research and documented behavior.
3. Mapping t identified weaknesses to recognized vulnerability classes (CWE) commonly recorded in the NVD.
4. Assess vulnerability impact, likelihood, and severity at a baseline level.
5. Provide remediation guidance based on industry and best academic practices.
6. Demonstrate how software vulnerability databases can inform real-world security audits without direct exploitation.
7. Reflecting any issues or challenges that have been encountered during literature research on the national vulnerabilities database. How these challenges have been resolved and how did this affect the final report.

(NCSC 2017; Knapp, 2024)

1.2. Methodology

This document follows a literature-based research methodology integrating the conceptual audit and vulnerability evaluation procedure, which was published and designed by recognized organizations that are experienced in assessment frameworks in combination with academic sources, the use of literature review and professional sources may include:

- Academic and peer-reviewed literature research.
- Security related articles and practitioner guides.
- Industry case studies of real-world cases.
- Government and professional security guidance.

This review emphasized vulnerabilities affecting this specific and similar web applications, threat actors’ behavior, and defensive strategies, drawing on kill-chain and threat-modelling perspectives.

(Kidd, 2024; Knapp, 2024).

1.3. Technology Identification

Passive reconnaissance must be used to assess the technology stack and application behavior of the Zero Bank platform. The application exhibits typical web-based banking architecture, including:

An HTTP-based communication (http://zero.webappsecurity.com).

A server-side session authentication.

Role-based functionality.

Server-side processing using Java code software and Apache Tomcat based components

According to literature sources, such architecture is oftentimes associated with authentication handling vulnerabilities and flaws related to access control, input validation, and session management.

(Ngowry, 2025; NCSC 2017).

1.4. National Vulnerabilities Database (NVD) Review

The National Vulnerabilities Database (NVD) was reviewed to identify common vulnerabilities and patterns weakness classes relevant to web applications like Zero Bank. Instead of mapping live CVEs directly to the platform, the audit will:

- Identify Common Weakness Enumerations (CWEs) frequently associated with browser-based protocols, containers and languages for instance, HTML, CSS, JAVA, Apache Tomcat and other relevant in the web system.
- Map the relevant weakness classes to the observed finding about the Zero Bank application literature.
- Use NVD trends to support severity and impact assessment.

This approach is consistent with ethical auditing practices where active scanning could cause disturbances and therefore is not ethical measure even when site is designed to be vulnerable.

(Ahlberg, 2014; NIST, 2025; MITRE, 2025)

1.5. Data Synthesis and Audit Classification

Findings from literature that used passive observation, NVD/CWE analysis were combined to create a baseline vulnerability profile. Vulnerabilities were classified as:

- Vulnerability class mapping (CWE) and mapping with NVD.
- Potential impact.
- Remediation.

(NIST, 2025; MITRE, 2025)

1.6. Overall Baseline Risk Posture

The Zero Bank web application demonstrates multiple high-severity vulnerabilities. These weaknesses are frequently exploited. These are documented in the NVD. Similar web-based systems are exposed. This would pose risks to confidentiality, integrity and availability.

(Ngowry, 2025; NIST, 2025; MITRE, 2025)

2. Detailed Vulnerability Findings

2.1. Exposed Administrative Interfaces and Weak Authentication

CWE-287 – Improper Authentication

- An access control interface which is publicly accessible and used also for administrative management was identified that had lacked adequate access controls. Those are some critical findings. There was also observable behavior that indicated insecure session management and credential handling using clear text data exposure.

Impact:

- Such findings by an adversary could enable account takeover. They could also lead to privilege escalation. There is also a risk of password spraying attacks. Authentication failures are among the most frequently exploited vulnerability classes recorded in the NVD.

(Ngowry, 2025; NIST, 2025, MITRE, 2025; Knapp, 2024).

Remediation:

- Enforcement of strict role-based access control.
- Implementation of multi-factor authentication.
- Secure credential storage using hashing and salting.
- Encryption of data-at-rest, in use, and in transit.
- Ensure session handling.

(Ngowry, 2025; NIST, 2025, MITRE, 2025; Knapp, 2024).

2.2. Sensitive Data Exposure and Transport Security

CWE-319 – Cleartext Transmission of Sensitive Information

- The web application was accessible via HTTP. This does not provide protection for sensitive data over that connection. The data is delivered in clear text form. It is exposed due to a lack of encryption which is designed to protect such data.

Impact:

- An unencrypted connection could be used to intercept data in transit, using sniffing an attacker can leverage attacks that can be used for credential, personal information and financial data theft. This is particularly dangerous in financial systems due to the value of the assets at stake.

(Ngowry, 2025; NIST, 2025, MITRE, 2025).

Remediation:

- Enforce encryption of data-in-transit, enforce HTTPS with strong TLS of at least version 1.2, a non-expired certificate from a trusted validated certificate authority, Better automated.
- Enable HSTS.
- Secure cookies using appropriate flags.

2.3. Broken Access Controls (IDOR)

CWE-284 – Improper Access Control

- Manipulation of object identifiers allowed access to other users’ data.

Impact:

- IDOR vulnerabilities are a prominent factor of data breaches in web applications.
- IDOR vulnerabilities are not represented as a standalone category in the NVD and are commonly mapped to the CWE-639 or, more broadly, CWE-284 (Improper Access Control) based on CVE analysis detail.

(Ngowry, 2025; NIST, 2025; CVE-2024-32166 Detail)

Remediation:

- Enforce server-side authorization checks.
- Use indirect object references or opaque identifiers.

(Ngowry, 2025; NIST, 2025, MITRE, 2025).

2.4. Cross-Site Scripting (XSS)

CWE-79 – Cross-Site Scripting

- Stored XSS was identified where unsensitized input was rendered in administrative interfaces.

(Ngowry, 2025; OWASP 2021).

Impact:

- XSS enables session hijacking and credential theft.

(Ngowry, 2025; OWASP 2021).

Remediation:

- Input validation and output encoding
- Content Security Policy (CSP) implementation

(Ngowry, 2025; Knapp 2024).

2.5. Missing CSRF Protections

CWE-352 – Cross-Site Request Forgery

- State-changing requests lacked anti-CSRF mechanisms malicious websites could trick legit users into unwanted or illegitimate action.

(Ngowry, 2025; OWASP 2021)

Impact:

- Attackers could trigger unauthorized financial transactions.

(Ngowry, 2025; OWASP 2021)

Remediation:

- Ensure CSRF tokens Implementation.
- Ensure request origins validation.
- Implement 2FA for high-risk actions.

(Ngowry, 2025; NIST, 2025, MITRE, 2025).

2.6. Outdated Server Components

CWE-1104 – Use of Unmaintained Software

- The server environment showed signs of outdated components with exposed directory listings.

(Ngowry, 2025)

Impact:

- Outdated software increases exposure to known, publicly documented CVEs.

(NIST, 2025).

Remediation:

- Upgrade and patch server components
- Disable directory browsing

(War, et al, 2025; Ngowry, 2025; NIST, 2025, MITRE, 2025).

Additional information:

- The NVD database does not list CWE-1104 as a standalone vulnerability. It is a set of related vulnerabilities that are recorded through CVEs and mapped to the broader CWE 2024-1199 classification, which is based on the impact of the flaw and the available analysis details of a set of third-party components that pose multiple vulnerabilities.

(War, et al, 2025)

2.7. Tools, Techniques, and Mitigation Approaches

The literature highlights the effectiveness of structured security practices such as:

- Threat modelling

- Kill-chain analysis
- Secure coding standards
- Regular vulnerability scanning
- Continuous patch management

(Knapp 2024)

National and professional guidance emphasizes ethical testing, defined scope, and responsible disclosure.

(NCSC 2017)

Critical Appraisal

This audit was designed to prioritize rigorous academic research over technical exploitation, and while it was limited to mapping frameworks designed for system-specific vulnerability artefacts, it ensures compliance with ethical, legal and institutional requirements by using vulnerabilities categories and classes, instead of exploiting individual vulnerabilities and their corresponding CVEs, this approach helps to retain a valid and plausible audit, in which the baseline is tested and that is align with NVD trend analysis and the requirements of this process.

(MITRE, 2025).

3. Reflection

3.1. Issues and Challenges Encountered

A key challenge was finding the right academic literature and aligning this finding with NVD data. Many NVD entries focus on real-world production systems, making direct CVE to-system mapping challenging without active scanning. in addition, some academic sources focus on enterprise-scale environments rather than simplified architecture.

(Şimşek, et al 2025).

3.2. How the Challenges Were Overcome

These challenges were addressed by:

- Focusing on CWE-level vulnerability classes rather than individual CVEs.
- Cross-referencing multiple literature sources to validate relevance.
- Application of a conceptual audit model rather than a running active or passive analysis by self but using an approach of logic and critical thinking to ensure consistency in the process.
- The analysis also used literature drawn from university literature and case studies to ensure relevancy. In addition, key concepts were distilled and examined from a practitioner perspective, in addition to the theoretical perspective.

This helped facilitate an audit that remained ethical and reasonable, at the same time, it was still grounded in recognized vulnerability data.

(Tiță, 2025)

3.3. Impact on the Final Report

As a result, the final report emphasizes baseline risk identification and classification rather than exploit execution, reducing technical specificity, strengthened the report’s academic validity and demonstrated how vulnerability databases can inform audits without active conducting testing.

(Tiță, 2025)

Use of Digital Tools

This report has been produced for educational purposes. All references, names, and trademarks remain the property of their respective owners. Monte Carlo simulations were conducted using Python, ensuring accuracy and reproducibility under given conditions and limitations, Grammarly was used for proofreading and language clarity, and ChatGPT was used for preliminary literature exploration and language refinement. All academic writing, analysis, argumentation, and conclusions represent the original work of the author.

Conclusion

This activity successfully demonstrates how software security literature and the National Vulnerabilities Database can be used to conduct a baseline vulnerability audit of different target architectures by relying on literature-based analysis and verified vulnerability frameworks. This audit supported the identification of risks and weaknesses commonly affecting organization’s assets across the globe on a daily basis, and although Zero Bank is a vulnerable educational platform, the findings identified highlight some real-world threats and flaws documented and observed by

many organization production environments. Thankfully, those are documented in the NVD database what helps practitioners to reinforce the importance of securing and using strong authentication, access control, encryption and secure coding practices. Ethical, literature-informed audits provide a valuable foundation for improving the security of web applications.

References

- Ahlberg, G., 2014. Generating web applications containing XSS and CSRF vulnerabilities.
- Eric D. Knapp & Joel Thomas Langill (2014) Industrial Network Security, 2nd Edition. Syngress. Available at: https://essex.primo.exlibrisgroup.com/permalink/44UOES_INST/o3t9un/cdi_safari_books_v2_9780124201149 . [Accessed: 5 February 2026].
- Kidd, C. (2024) Cyber Kill Chains: Strategies & Tactics. Splunk.
- MITRE (2025) Common Weakness Enumeration (CWE). Available at: https://cwe.mitre.org [Accessed: 2 February 2026].
- NCSC (2017) ‘Advice on how to get the most from penetration testing’. Available at: https://www.ncsc.gov.uk/guidance/penetration-testing [Accessed: 2 February 2026].
- Ngowry, (2025) Zero Bank (zero.webapsecurity.com) Vulnerability Assessment & Responsible Disclosure. Available at: https://medium.com/@ngowry12/zero-bank-zero-webappsecurity-com-

vulnerability-assessment-responsible-disclosure-7fd44b5aeee2 [Accessed: 2 February 2026].

- NIST (2025) CVE-2024-32166 Detail. National Vulnerability Database. Available at: https://nvd.nist.gov/vuln/detail/CVE-2024-32166 [Accessed: 5 February 2026].
- NIST (2025) National Vulnerability Database (NVD). Available at: https://nvd.nist.gov/vuln/categories 2 February 2026].
- Orzach, Y. & Khanna, D. (2022) Network Protocols for Security Professionals: *Probe and identify network-based vulnerabilities and safeguard against network protocol breaches*. 1st edition. Birmingham: Packet Publishing.
- OWASP Foundation, n.d. OWASP Top 10:(2021). Available at: https://owasp.org/Top10/en/ [Accessed: 7 February 2026]
- War, A., Nikiema, S.L., Samhi, J., Klein, J. and Bissyande, T.F., 2025. Security smells in infrastructure as code: a taxonomy update beyond the seven sins. arXiv preprint arXiv:2509.18761.
- Țiță I, Cujbă MC, Țăpuș N. Fractality and Percolation Sensitivity in Software Vulnerability Networks: A Study of CWE–CVE–CPE Relations. Applied Sciences. 2025 Oct 22;15(21):11336.
- Singla, R., Reddy, N., Bettati, R. and Alnuweiri, H., (2023). Toward a Multidimensional Analysis of the National Vulnerability Database. IEEE Access, 11, pp.93354-93367. [Accessed: 2 February 2026].
- Şimşek, Ş., Xia, H., Gluck, J., Medina, D.S. and Starobinski, D., 2025, July. Fixing Invalid CVE-CWE Mappings in Threat Databases. In 2025 IEEE 49th Annual Computers, Software, and Applications Conference (COMPSAC) (pp. 950-960). IEEE.