Baseline Analysis of Zero Bank Website

This report provides a preliminary security assessment of the Zero Bank Website, a simulated online banking platform. The aim is to identify potential weaknesses based on visible elements and known vulnerabilities associated with financial web applications. The findings draw on recognised security standards and propose free, non-intrusive tools that could support a more in-depth audit.

Possible Security Vulnerabilities

A visual review of the website, along with browser-based inspection, suggests several common and business-specific vulnerabilities that might be present:

1. The site operates over unencrypted HTTP, leaving users vulnerable to data interception.
2. Missing security headers such as Content Security Policy (CSP) and X-Frame-Options.
3. Default user credentials: username/password
4. Input fields lack validation.
5. No sign of multi-factor authentication (MFA) on sign-in.
6. Sessions appear to lack timeout or inactivity expiry features.
7. No visible cookie consent banner or privacy notice, raising GDPR concerns.

Relevant Standards and Compliance Concerns

Although the site is a demo, if it were to represent a real financial service, it should adhere to the following industry and regulatory standards. The General Data Protection Regulation (GDPR) mandates data minimisation, transparency, and the lawful processing of personal data belonging to EU citizens (Intersoft Consulting, no date). The OWASP Top Ten outlines critical web application security risks that developers and auditors must address to protect against common threats (OWASP, 2021). Additionally, the Payment Card Industry Data Security Standard (PCI DSS) establishes strict security controls and validation processes to ensure the safe handling of payment card information (Barney, 2024).

Recommended Tools

For the future audit, the following free and open-source tools are appropriate, given the constraints of the environment:

1. OWASP ZAP – Used for passive analysis to highlight issues aligned with the OWASP Top Ten, without sending intrusive traffic.
2. SSL Labs (by Qualys) – Evaluates the SSL/TLS setup and assigns a security grade.
3. SecurityHeaders.com – Provides a quick review of HTTP response headers and identifies any missing protections.

Methodology

The future audit will adopt a black-box testing model, with no access to admin panels, source code, or credentials. It will be conducted remotely and use a manual, non-intrusive approach, involving visual inspection of elements, HTTP header analysis, and cookie evaluation via browser tools. No injection, scanning, or tampering will occur.

Business Impacts

Testing can impact website performance, especially during busy times. To avoid slowing down or disrupting the service, tests should be done during off-peak hours or maintenance periods. Coordinating with stakeholders helps ensure testing fits business needs and limits risks. Even for a demo site like Zero Bank, planning tests this way is important for real-world audits to protect service and user trust.

Tentative Timeline for Future Audit

Day	**Activities**
1	Set up tools, define scope, and prepare the testing environment.
2	Conduct manual inspection and document visible security elements.
3	Perform passive scans using the recommended tools.
4	Analyse scan results and map findings to relevant standards.
5	Compile and finalise the vulnerability report with recommendations.

Limitations and Assumptions

1. **Limitations:**
    a. No access to the website's source code or admin panel.
    b. Server-side issues cannot be verified.
    c. Logical flaws cannot be verified.
2. **Assumptions:**
    a. The website is designed to simulate a real banking website.
    b. Users are expected to interact as if it were a real service.
    c. Security and privacy should reflect normal banking expectations.

While the website is only a simulation, it has several vulnerabilities often seen in real-world banking sites, including weak session security, the absence of encryption, and limited compliance with data protection laws. Future audits can leverage open-source tools for passive, non-intrusive assessments to deepen this evaluation.

References

Barney, N. (2024) *What is PCI DSS (Payment Card Industry Data Security Standard)?*. Available at: https://www.techtarget.com/searchsecurity/definition/PCI-DSS-Payment-Card-Industry-Data-Security-Standard (Accessed: 16 May 2025).

Intersoft Consulting (no date) *GDPR*. Available at: https://gdpr-info.eu/ (Accessed: 16 May 2025).

OWASP (2021) *OWASP Top Ten*. Available at: https://owasp.org/www-project-top-ten/ (Accessed: 16 May 2025).