Summative Assessment 1: Vulnerability Audit and Assessment - Baseline Analysis and Plan

Network Security June 2024

Word count: 586

Vulnerability Audit and Assessment
Baseline Analysis and Plan

0. Overview

This report provides a preliminary outline for a baseline analysis and plan for a vulnerability audit and assessment for an online **Zero Bank** website http://zero.webappsecurity.com/. The aim is to identify potential security weaknesses, evaluate their implications, and devise methods to mitigate risks.

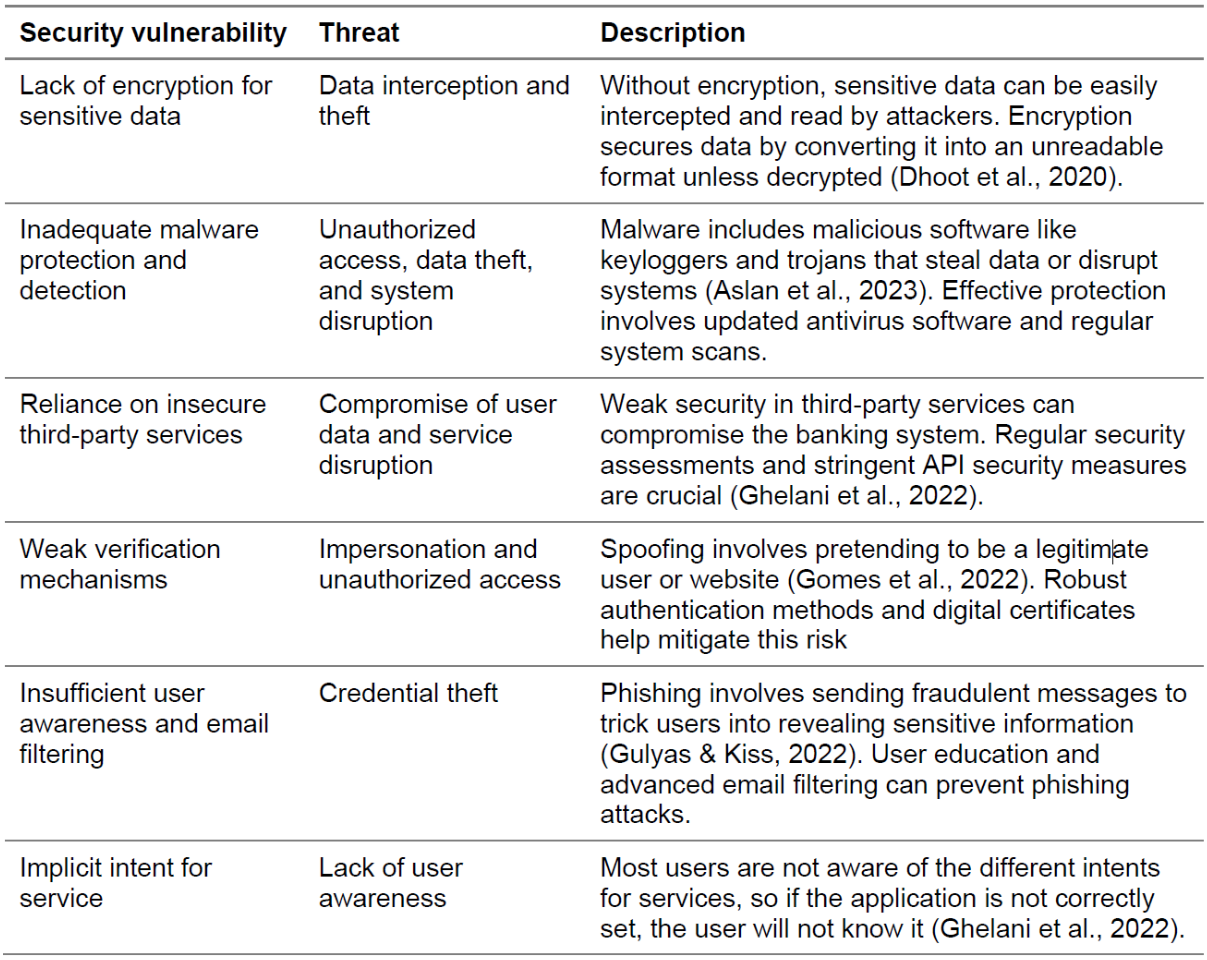
1. Introduction

As banks and financial institutions have increasingly adopted digital technologies, cybersecurity has become a critical concern (Oyewole et al. 2024). Robust measures must be implemented to safeguard sensitive data during digital transformations. The security of Personally Identifiable Information depends on effective cybersecurity defenses against breach and attack. The Banking, Financial Services, and Insurance industry is quickly increasing, with an average yearly growth rate of 22.4% expected to reach $195.5 billion by 2029. Given the substantial financial stakes involved, cybersecurity breaches could have severe economic consequences, leading to an increased demand for cybersecurity professionals and significant investment in security measures.

2. Security Challenges

Numerous studies have been conducted in this area, with researchers primarily focusing on various attacks on online applications including cross-site scripting, SQL injection, cross-site scripting (XSS), cross-site request forgery (CSRF), insecure direct object references, security misconfiguration and sensitive data exposure (Ahmad et al., 2024; Chaturvedi et al., 2021; Im et al., 2017). However, according to Shaji (2023), the biggest threats faced by online banks include unencrypted data, malware, third-party services, spoofing, and phishing. These attacks exploit vulnerabilities and can potentially lead to harm (Dawodu et al., 2023). Table 1 presents the threats that can exploit online banking applications, their vulnerabilities, and the descriptions of each.

Table 1. Summary of Generic Security Challenges



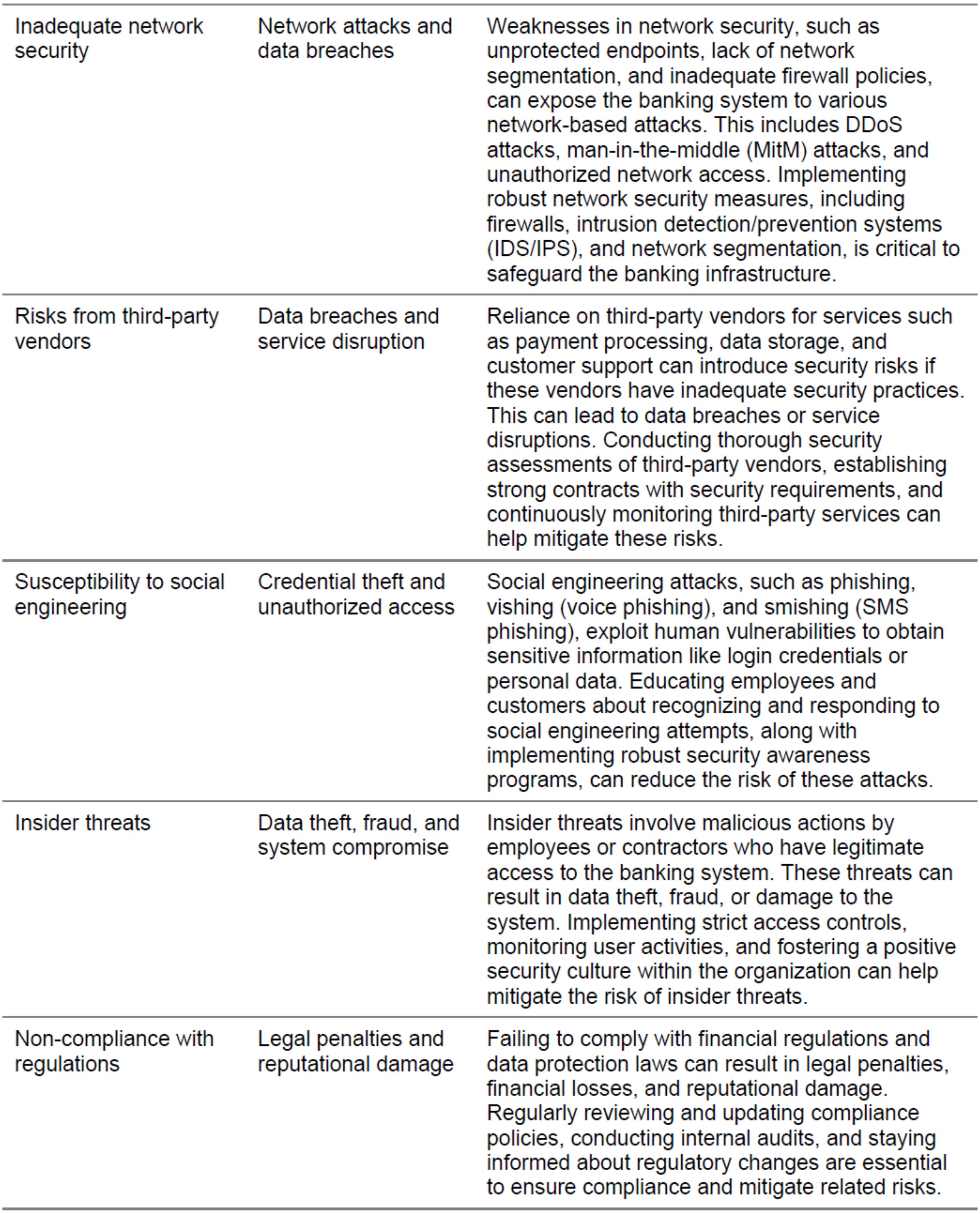
Security vulnerability	Threat	Description
Lack of encryption for sensitive data	Data interception and theft	Without encryption, sensitive data can be easily intercepted and read by attackers. Encryption secures data by converting it into an unreadable format unless decrypted (Dhoot et al., 2020).
Inadequate malware protection and detection	Unauthorized access, data theft, and system disruption	Malware includes malicious software like keyloggers and trojans that steal data or disrupt systems (Aslan et al., 2023). Effective protection involves updated antivirus software and regular system scans.
Reliance on insecure third-party services	Compromise of user data and service disruption	Weak security in third-party services can compromise the banking system. Regular security assessments and stringent API security measures are crucial (Ghelani et al., 2022).
Weak verification mechanisms	Impersonation and unauthorized access	Spoofing involves pretending to be a legitimate user or website (Gomes et al., 2022). Robust authentication methods and digital certificates help mitigate this risk
Insufficient user awareness and email filtering	Credential theft	Phishing involves sending fraudulent messages to trick users into revealing sensitive information (Gulyas & Kiss, 2022). User education and advanced email filtering can prevent phishing attacks.
Implicit intent for service	Lack of user awareness	Most users are not aware of the different intents for services, so if the application is not correctly set, the user will not know it (Ghelani et al., 2022).

Misconfiguration of intent-filters	Application malfunction	Without properly configuring the application, unexpected actions can occur (Mohanty et al., 2023).
Content Provider access from other apps on the device	Third-party application threat	There might be malicious applications on the device, and gaining access without permission could be harmful to the mobile banking application (Stanikzai & Shah, 2021).
Remote code execution	Unauthorized access	If remote code execution is allowed, an attacker can access the application remotely without authorization (Mohanty et al., 2023).
Getting IMEI and Device ID	Information leakage	Getting IMEI and device ID might lead to information leakage (Gomes et al., 2022).
Normal protection-level of permission	Third-party application threat	If the protection-level permission is not set, others can register and receive messages for the application (Stanikzai & Shah, 2021).
Local file system access	Malware (malicious code)	Malicious codes can be injected, thereby exploiting the system (Gulyas & Kiss, 2022).
Webview JavaScript enabled	Cross-site Scripting threat	It makes it prone to cross-site scripting attacks.
Not executing 'root' or system privilege checks	Platform manipulation	Sometimes users "root" or "jailbreak" devices to gain higher privileges. Unfortunately, this can leak sensitive information from the application, so it is important to check for 'root' in systems where the mobile banking apps are installed.
ADB backup	Improper disposal of the device	Improper device disposal with the installed application can lead to ADB backup falling into the wrong hands (Ahmad et al., 202).
File unsafe deleting	Improper disposal of devices	If the device is lost, sold, or stolen, the deleted sensitive information can be retrieved (Nilsson & Lehmann, (2020)..
Not checking Package signature code	Hacking	When hacking occurs, it cannot be detected by the application.
Allowing Screenshot capturing	Improper disposal of the device	If the mobile banking application gets into the wrong hand, the attacker can easily screenshot sensitive information out of the application (Ahmad et al., 202).
No APK installer sources checks	Phishing through fake applications	Criminals are fond of creating fake applications to deceive users into installing them, thereby stealing sensitive information from the user. Therefore, it is important to check the APK installer source to ascertain it is genuine (Yildirim & Varol, 2019)..

Business-Specific Security Challenges:

Table 2. Summary of business-related security challenges.

Security vulnerability	Threat	Description
Weak authentication mechanisms	Unauthorized access and account takeover	Weak authentication mechanisms, such as simple passwords without multi-factor authentication (MFA), make it easier for attackers to gain unauthorized access to user accounts. This can lead to account takeover, unauthorized transactions, and identity theft. Strengthening authentication mechanisms with MFA and enforcing strong password policies are crucial to mitigate this threat.
Poor session management	Session hijacking and unauthorized access	Inadequate session management practices, such as not expiring sessions after a period of inactivity or using predictable session identifiers, can be exploited by attackers to hijack user sessions. This allows attackers to perform actions on behalf of legitimate users, potentially leading to unauthorized transactions and data breaches. Implementing secure session management practices, such as using secure cookies and session expiration policies, is essential to protect user sessions.
Insufficient data encryption	Data interception and theft	Without proper encryption, sensitive data (e.g., login credentials, personal information, transaction details) can be intercepted during transmission or compromised if stored in an unencrypted format. This can result in data theft and financial loss for customers. Ensuring that data is encrypted both in transit (using protocols like TLS) and at rest (using strong encryption algorithms) is vital for protecting sensitive information.
Inadequate security logging and monitoring	Undetected attacks and delayed incident response	Insufficient logging and monitoring capabilities hinder the detection of security incidents and anomalous activities. This can lead to prolonged exposure to attacks, as security breaches may go unnoticed for extended periods, increasing the potential damage. Implementing comprehensive logging and real-time monitoring solutions enables quick detection and response to security incidents, minimizing the impact of potential breaches.
Insecure configuration management	System compromise and unauthorized changes	Improperly configured systems, such as databases, web servers, and network devices, can expose vulnerabilities that attackers can exploit. This includes using default settings, weak configurations, and unpatched software. Ensuring secure configuration management by following best practices, regularly updating and patching systems, and conducting configuration audits can mitigate these risks.



Inadequate network security	Network attacks and data breaches	Weaknesses in network security, such as unprotected endpoints, lack of network segmentation, and inadequate firewall policies, can expose the banking system to various network-based attacks. This includes DDoS attacks, man-in-the-middle (MitM) attacks, and unauthorized network access. Implementing robust network security measures, including firewalls, intrusion detection/prevention systems (IDS/IPS), and network segmentation, is critical to safeguard the banking infrastructure.
Risks from third-party vendors	Data breaches and service disruption	Reliance on third-party vendors for services such as payment processing, data storage, and customer support can introduce security risks if these vendors have inadequate security practices. This can lead to data breaches or service disruptions. Conducting thorough security assessments of third-party vendors, establishing strong contracts with security requirements, and continuously monitoring third-party services can help mitigate these risks.
Susceptibility to social engineering	Credential theft and unauthorized access	Social engineering attacks, such as phishing, vishing (voice phishing), and smishing (SMS phishing), exploit human vulnerabilities to obtain sensitive information like login credentials or personal data. Educating employees and customers about recognizing and responding to social engineering attempts, along with implementing robust security awareness programs, can reduce the risk of these attacks.
Insider threats	Data theft, fraud, and system compromise	Insider threats involve malicious actions by employees or contractors who have legitimate access to the banking system. These threats can result in data theft, fraud, or damage to the system. Implementing strict access controls, monitoring user activities, and fostering a positive security culture within the organization can help mitigate the risk of insider threats.
Non-compliance with regulations	Legal penalties and reputational damage	Failing to comply with financial regulations and data protection laws can result in legal penalties, financial losses, and reputational damage. Regularly reviewing and updating compliance policies, conducting internal audits, and staying informed about regulatory changes are essential to ensure compliance and mitigate related risks.

3. Relevant Standards

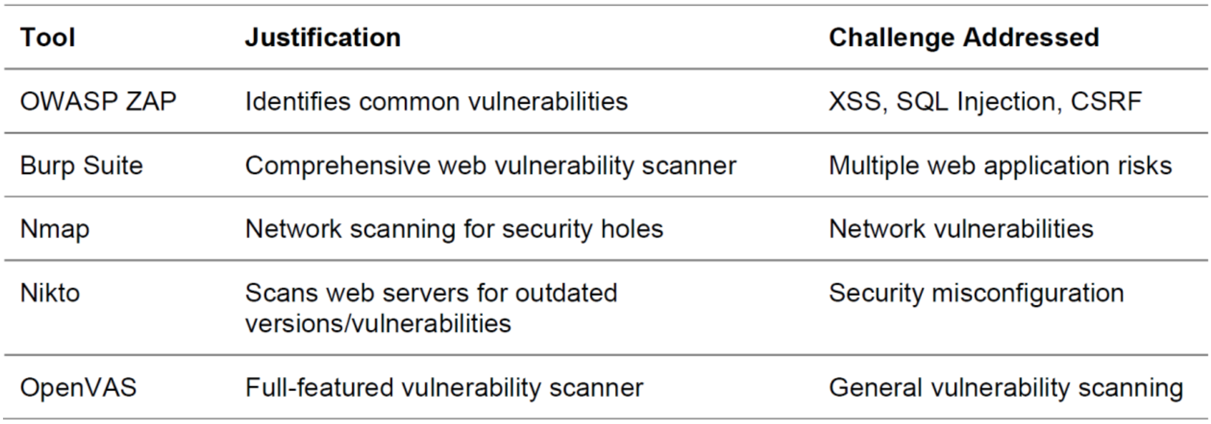
Security in financial institutions focuses on implementing security measures and technology to guard against unauthorized access, cyberattacks, and data breaches.

These include guidelines and methods aimed at protecting against computer viruses, malware, hacking, information theft, and unauthorized network access. Implementing cybersecurity measures in banking is primarily aimed at safeguarding customer assets, given the growing number of financial transactions being conducted online. Customers and business data are protected using conventional processes and organised documented standards:

- **GDPR** (General Data Protection Regulation) requires rigorous safety precautions, such as encryption and access limitations, to protect the personal information of EU citizens (Machado et al., 2023).
- **PCI DSS** (Payment Card Industry Data Security Standard) mandates strict security procedures for organisations processing credit card transactions to protect cardholder data (PCI, 2012).
- **ISO/IEC 27001** requires a systematic strategy to handling sensitive business data (Ewuga et al., 2024; Petranović & Žarić, 2023).
- **OWASP Top 10** highlights major security vulnerabilities for online applications, establishing a baseline for security solutions (Kumar & Gandhi, 2023).

4. Tools

Table 3. Tools and justifications.



Tool	Justification	Challenge Addressed
OWASP ZAP	Identifies common vulnerabilities	XSS, SQL Injection, CSRF
Burp Suite	Comprehensive web vulnerability scanner	Multiple web application risks
Nmap	Network scanning for security holes	Network vulnerabilities
Nikto	Scans web servers for outdated versions/vulnerabilities	Security misconfiguration
OpenVAS	Full-featured vulnerability scanner	General vulnerability scanning

5. Methodology

Approach:

- Remote and local assessments
- Combination of automated and manual testing

Models/Methodologies:

- OWASP Testing Guide: Standard for web application security testing.
- NIST SP 800-115: Technical guide for conducting assessments.

Techniques:

- Automated scanning for initial vulnerability identification.
- Manual testing for detailed analysis and verification.

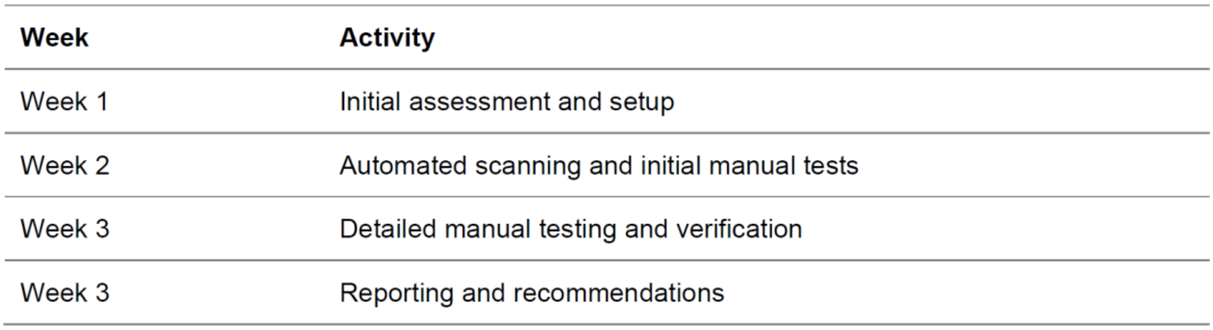
6. Business Impacts

Out-of-Hours Scanning: Conducting scans outside of peak business hours to minimize disruption.

Controlled Traffic Load: Ensuring scanning activities do not overwhelm network resources.

7. Timeline

Table 4. Timeline.



Week	Activity
Week 1	Initial assessment and setup
Week 2	Automated scanning and initial manual tests
Week 3	Detailed manual testing and verification
Week 3	Reporting and recommendations

8. Summary of Limitations and Assumptions

Limitations:

- Limited access to some internal systems.
- Potential for false positives/negatives in automated tools.

Assumptions:

- Full cooperation from the IT team.
- Access to necessary resources and documentation.

Summary

The vulnerability audit and assessment of the online banking platform http://zero.webappsecurity.com involves identifying potential vulnerabilities, ensuring compliance with relevant standards, and using a mix of automated and manual tools to assess and mitigate risks. The process is designed to minimize business disruption, follow a structured timeline, and acknowledge potential limitations and assumptions.

Reference list

Ahmad, I., Khan, S., & Iqbal, S. (2024). Guardians of the vault: Unmasking online threats and fortifying e-banking Security, a systematic review. Journal of Financial Crime. https://doi.org/10.1108/jfc-11-2023-0302

Aslan, Ö., Aktuğ, S. S., Ozkan-Okay, M., Yilmaz, A. A., & Akin, E. (2023). A comprehensive review of cyber security vulnerabilities, threats, attacks, and solutions. Electronics, 12(6), 1333. https://doi.org/10.3390/electronics12061333

Chaturvedi, M., Sharma, S., & Ahmed, G. (2021). Study of baseline cyber security for various application domains. IOP Conference Series: Materials Science and Engineering, 1099(1), 012051. https://doi.org/10.1088/1757-899x/1099/1/012051

Dawodu, S.O., Omotosho, A., Akindote, O.J., Adegbite, A.O., & Ewuga, S.K. (2023). Cybersecurity Risk Assessment in banking: Methodologies and best practices. Computer Science &amp; IT Research Journal, 4(3), 220–243. https://doi.org/10.51594/csitrj.v4i3.659

Dhoot, A., Nazarov, A. N., & Koupaei, A. N. (2020). A security risk model for online banking system. 2020 Systems of Signals Generating and Processing in the Field of on Board Communications. https://doi.org/10.1109/ieeeconf48371.2020.9078655

Ewuga, S.K., Egieya, Z.E., Omotosho, A. & Adegbite, A. (2024) ‘ISO 27001 in banking: An evaluation of its implementation and effectiveness in enhancing information security’, *Finance &amp; Accounting Research Journal*, 5(12), pp. 405–425. doi:10.51594/farj.v5i12.684.

Ghelani, D., Hua, T. K., & Koduru, S. K. (2022). Cyber Security Threats, Vulnerabilities, and Security Solutions Models in Banking. https://doi.org/10.22541/au.166385206.63311335/v1

Gomes, L., Deshmukh, A., & Anute, N. (2022). Cyber security and internet banking: Issues and preventive measures. Journal of Information Technology and Sciences, 8(2), 31–42. https://doi.org/10.46610/joits.2022.v08i02.005

Gulyas, O., & Kiss, G. (2022). Cybersecurity threats in the banking sector. 2022 8th International Conference on Control, Decision and Information Technologies (CoDIT). https://doi.org/10.1109/codit55151.2022.9804140

Im, J., Yoon, J. & Jin, M. (2017) ‘Interaction platform for improving detection capability of Dynamic Application Security Testing’, *Proceedings of the 14th International Joint Conference on e-Business and Telecommunications* [Preprint]. doi:10.5220/0006437104740479.

Kumar, A. and Gandhi, A. (2023) ‘A study using OWASP on Secure Open Banking Architecture’, *2023 3rd International Conference on Advance Computing and Innovative Technologies in Engineering (ICACITE)* [Preprint]. doi:10.1109/icacite57410.2023.10182656.

Machado, P., Vilela, J., Peixoto, M. & Silva C. (2023) ‘A systematic study on the impact of GDPR compliance on organizations’, Proceedings of the XIX Brazilian Symposium on Information Systems [Preprint]. doi:10.1145/3592813.3592935.

Maximize Market Research (2023) *Cyber security in BFSI market: Global Market Size, dynamics, regional insights and market segment analysis (by component, Deployment Model, enterprise size)*, *Maximize Market Research*. Available at: https://www.maximizemarketresearch.com/market-report/cyber-security-in-bfsi-market-global-market/169820/?utm_source=Globenewslwire&utm_medium=PR [Accessed: 20 June 2024].

Mohanty, S., Sharma, S., Pattnaik, P. K., & Hol, A. (2023). A comprehensive review on cyber security and online banking security frameworks. Advances in Information Security, Privacy, and Ethics, 1–22. https://doi.org/10.4018/978-1-6684-9317-5.ch001

Nilsson, A., & Lehmann, S. (2020). Make Banking Simple Again. 1–57.

Oyewole, A. T., Okoye, C. C., Ofodile, O. C., & Ugochukwu, C. E. (2024) ‘Cybersecurity risks in online banking: A detailed review and Preventive Strategies applicatio’, *World Journal of Advanced Research and Reviews*, 21(3), pp. 625–643. doi:10.30574/wjarr.2024.21.3.0707.

PCI (2012) *Payment card industry data security standard handbook* [Preprint]. doi:10.1002/9781119197218.

Petranović, T. and Žarić, N. (2023) ‘Effectiveness of using OWASP top 10 as AppSec standard’, *2023 27th International Conference on Information Technology (IT)* [Preprint]. doi:10.1109/it57431.2023.10078626.

Shaji, A.M. (2023) *Cybersecurity in Digital Banking: Threats, Challenges & Solution*, *Enterslice*. Available at: https://enterslice.com/learning/cybersecurity-in-digital-banking-threats-challenges-and-solution/ [Accessed: 24 June 2024].

Stanikzai, A. Q., & Shah, M. A. (2021). Evaluation of cyber security threats in banking systems. 2021 IEEE Symposium Series on Computational Intelligence (SSCI). https://doi.org/10.1109/ssci50451.2021.9659862

Yildirim, N., & Varol, A. (2019). A research on security vulnerabilities in online and Mobile Banking Systems. 2019 7th International Symposium on Digital Forensics and Security (ISDFS). https://doi.org/10.1109/isdfs.2019.8757495