Risk Analysis Of Accounting Information System Security Based On Vulnerability Data From OPENVAS, OWASP ZAP, And NMAP Tools: A Cybersecurity Perspective

Abdul Roup, Marwan Effendy
Institut Bisnis dan Informatika Kesatuan
*Email: abdulrouf.ci@*gmail.com

Submitted:
MAY 2025

Accepted:
JUNE 2025

ABSTRACT

Data security is a critical component of Accounting Information Systems (AIS), considering the sensitivity of financial information that must be safeguarded against cyber threats. This study aims to analyze security risks within an AIS platform by utilizing vulnerability scan data collected from the domain https://kiis.ibik.ac.id. Three open-source security tools—OpenVAS, OWASP ZAP, and NMAP—were used to detect potential system vulnerabilities. The research identifies and classifies these vulnerabilities based on severity levels and CVSS (Common Vulnerability Scoring System) scores. The findings reveal multiple medium and low-level vulnerabilities, including open TCP ports, missing anti-clickjacking headers, and improper content security policies, which could expose the system to threats such as cross-site scripting (XSS), clickjacking, and unauthorized access. The study recommends implementing essential security headers, closing unused ports, and conducting continuous system monitoring to enhance AIS resilience. These insights highlight the importance of proactive cybersecurity measures in protecting financial data integrity within modern accounting systems.

Keywords: accounting information system, data security, vulnerability analysis, CVSS, cybersecurity risk

INTRODUCTION

An Accounting Information System (AIS) is a structured set of procedures designed to collect, record, store, and process financial data generated from various business activities within an organization. This data is then used to produce relevant and accurate financial information for both internal and external users. In the digital era, the reliability and security of information systems are crucial to maintain the integrity of accounting data and protect organizational assets from potential threats. According to Wilkinson et al. (2020), AIS plays a key role in supporting managerial decision-making and ensuring accurate financial reporting.

As technology dependency increases, security threats to AIS are becoming more complex. Systems connected to the internet or other external networks are vulnerable to cyberattacks such as hacking, malware, and data breaches. This is exacerbated by the fact that many organizations often neglect proper oversight of their system security. Ghorbani et al. (2019) emphasize that organizations frequently struggle to secure their AIS effectively, especially in the face of evolving threats.

AIS security involves not only technical data protection but also compliance with regulatory and security standards. In Indonesia, data protection is governed by various regulations, including the recently enacted Personal Data Protection Law (PDP). This regulation emphasizes the importance of maintaining confidentiality and security of accounting data, particularly financial information. As Harsono (2021) highlights,

JIAKES

Jurnal Ilmiah Akuntansi Kesatuan
Vol. 13 No. 3, 2025
pg. 433 - 438
IBI Kesatuan
ISSN 2337 – 7852
E-ISSN 2721 – 3048
DOI: 10.37641/jiakes.v13i3.3590

organizations must adopt appropriate security policies, conduct regular audits, and implement strict security protocols to comply with such regulations.

A major portion of AIS security risks stems from system vulnerabilities. One common vulnerability is the presence of open ports that can be exploited by attackers. For instance, Chien et al. (2018) found that 70% of cyberattacks on corporate networks begin with the exploitation of unsecured ports. This underscores the need for effective network access monitoring to prevent exploitable entry points.

Other common vulnerabilities include misconfigured cross-domain settings and the absence of proper security headers. According to Joshi & Mukherjee (2017), improper configurations may result in cross-site scripting (XSS) or clickjacking attacks, allowing attackers to steal sensitive data from corporate accounting systems. Security measures such as implementing a Content Security Policy (CSP) are strongly recommended to safeguard systems against such attacks.

Rahman and Widjaja (2020) reveal that many small to medium-sized enterprises (SMEs) often overlook the importance of implementing security controls in their AIS. These organizations tend to assume that their size exempts them from being primary targets of cyberattacks. However, studies show that SMEs are often more vulnerable due to less robust security infrastructures compared to larger corporations.

In addition to external threats, AIS security is also challenged by internal risks. Wibisono (2019) notes that internal data breaches are often caused by inadequate oversight of user access rights. Employees with access to sensitive information may, either unintentionally or deliberately, leak data, potentially causing significant financial harm to the organization.

Given the wide range of threats, organizations must implement a layered approach to securing their AIS. One effective strategy is the use of vulnerability scanning tools such as OpenVAS, OWASP ZAP, and NMAP to identify potential system weaknesses. These tools can detect various vulnerabilities, from open ports to poor web security configurations. As Schaefer et al. (2018) state, regular use of vulnerability scanners is among the most effective methods for preventing cyberattacks.

Collaboration between IT teams and organizational management is essential in strengthening AIS security. IT professionals are responsible for the technical monitoring and updating of systems, while management must provide adequate resources and support for implementing necessary security solutions. Arifin (2020) asserts that the success of security implementations depends not only on the technology used but also on the commitment of all organizational stakeholders.

In conclusion, AIS security is a critical aspect that must not be overlooked. Organizations must proactively identify and manage existing risks using appropriate technologies and policies to safeguard their financial data from evolving threats.

METHOD

This study employed a qualitative-exploratory approach with a focus on technical vulnerability analysis using automated scanning tools. The primary objective was to identify potential security risks within an Accounting Information System (AIS) by examining a real-world web application, namely the domain https://kiis.ibik.ac.id. The research was conducted in several stages as follows:

1. **Target Identification and Scope Definition**
   The research object was defined as the domain https://kiis.ibik.ac.id, which functions as an AIS platform. The scope of testing included network services, open ports, and web application configurations accessible from the public internet.
2. **Tool Selection**
   Three widely recognized open-source security tools were utilized:
   - **OPENVAS** (Open Vulnerability Assessment System): for detecting network-level vulnerabilities.

- **OWASP ZAP** (Zed Attack Proxy): for scanning web application vulnerabilities, particularly those related to input validation, headers, and content security.
- **NMAP** (Network Mapper): for identifying open ports, service versions, and potential network exposure.

3. **Scanning and Data Collection**
   Each tool was configured using standard scanning profiles, and tests were conducted independently. The scanning process did not involve intrusive or destructive techniques, ensuring no disruption to the production environment. The results from each tool were exported and categorized by vulnerability type and severity level, following the Common Vulnerability Scoring System (CVSS) v3.1.
4. **Data Analysis**
   The collected vulnerability data were aggregated and analyzed to assess severity levels (Critical, High, Medium, Low) and potential impact on the AIS. The analysis emphasized how these vulnerabilities could affect confidentiality, integrity, and availability (CIA) of accounting data.
5. **Risk Interpretation**
   Identified vulnerabilities were mapped to specific AIS security risks such as data breaches, unauthorized access, or exposure to client-side attacks (e.g., clickjacking and cross-site scripting). The results were then used to formulate appropriate mitigation recommendations.
   This method allowed for a focused yet multidimensional evaluation of the AIS security posture, offering practical insights based on real-world vulnerability data.

RESULTS AND DISCUSSION

Table 1 Vulnerability Analysis by Tool

Tools	Total Vulnerabilities	CRITICAL	HIGH	MEDIUM	LOW	ACCEPTED
OPENVAS	1	0	0	1	0	0
OWASP ZAP	8	0	0	4	4	0
NMAP	13	0	0	11	2	0

B The combined scan results from OpenVAS, OWASP ZAP, and NMAP revealed several vulnerabilities requiring further analysis. Each tool focuses on different areas of security, offering a comprehensive overview of the security posture of the https://kiis.ibik.ac.id website.

OpenVAS identified one vulnerability—**TCP Timestamps Information Disclosure**—with a CVSS score of 2.6, categorized as low risk. Although this does not pose an immediate threat, it can be used to gather information (e.g., system boot time) that may assist attackers in crafting more sophisticated attacks. Even low-risk vulnerabilities should not be dismissed.

OWASP ZAP discovered eight vulnerabilities, four categorized as medium and four as low. These were primarily related to web application security misconfigurations, such as **Missing Anti-clickjacking Header** and **Content Security Policy (CSP) Header Not Set**. Such weaknesses can enable attacks like clickjacking or cross-site scripting (XSS), which may lead to information theft or interface manipulation. Implementing CSP and other protective headers is recommended to address these risks.

NMAP detected thirteen vulnerabilities, with eleven rated medium and two rated low. Most were related to open ports such as 443 (HTTPS), 80 (HTTP), and 8080 (alternate HTTP), which, if not properly monitored, could serve as entry points for brute force, scanning, or buffer overflow attacks. Proper port management, including closing unused ports and restricting access, is essential for network security.

Overall, the analysis emphasizes the importance of layered security approaches. Medium-level vulnerabilities, as found by OWASP ZAP and NMAP, indicate potential

risks that must be addressed promptly. Even low-risk findings, such as those from OpenVAS, could contribute to larger-scale attacks if left unmitigated. Security recommendations include reinforcing web policies, closing unnecessary ports, and maintaining continuous monitoring.

Vulnerability Types

- **Cross-Domain Misconfiguration**: Susceptible to attacks due to improper cross-domain settings.
- **Missing Anti-clickjacking Header**: Lacks protective headers against clickjacking attacks.
- **CSP: Wildcard Directive**: Use of wildcards in CSP policies that may weaken web security.
- **CSP Header Not Set**: Missing Content Security Policy headers increases exposure to XSS and other attacks.
- **Open TCP Ports**: Detection of open ports (443, 80, 8080) that pose security risks if unmanaged.

CVSS Scores

CVSS scores varied across vulnerabilities, providing insight into their severity. For instance, **TCP Timestamps Information Disclosure** has a CVSS score of 2.6, indicating minimal direct impact but potential as part of a broader exploit. Even low-scoring vulnerabilities should be considered within the context of layered attacks.

Risks to Accounting Information Systems

AIS exposed to networks with open ports or missing headers (such as anti-clickjacking or CSP) face risks including data theft, session hijacking, and XSS attacks. Given the sensitive nature of financial data, mitigating these risks is imperative.

CONCLUSION

This study highlights the critical importance of securing Accounting Information Systems (AIS) against a wide range of cybersecurity threats by conducting a vulnerability assessment using three open-source tools: OpenVAS, OWASP ZAP, and NMAP. The analysis of the https://kiis.ibik.ac.id domain identified multiple low to medium severity vulnerabilities, such as open TCP ports, missing anti-clickjacking headers, and absent or improperly configured Content Security Policy (CSP) headers. Although no high or critical vulnerabilities were detected, the presence of such issues still poses potential risks that may be exploited in multi-stage cyberattacks. These weaknesses, if left unmitigated, can lead to serious consequences including unauthorized access, data leakage, cross-site scripting (XSS), and session hijacking.

The study demonstrates the effectiveness of combining different vulnerability scanning tools to obtain a comprehensive security overview, each covering distinct aspects of AIS exposure—from network infrastructure to web application configurations. Furthermore, the use of CVSS scoring provides an objective measure to prioritize remediation efforts.

In conclusion, organizations must adopt a proactive and layered security strategy by routinely performing vulnerability assessments, implementing missing security headers, closing unused ports (e.g., 2082, 8080, 8880), Continuous Monitoring: Perform regular system scans to detect new vulnerabilities, and securing cross-domain configurations. Equally important is the collaboration between IT teams and management to ensure adequate resources, policy enforcement, and compliance with regulatory standards such as Indonesia's Personal Data Protection Law (PDP Law). By strengthening the security posture of their AIS, organizations can better protect sensitive financial data and maintain operational integrity in the face of evolving cyber threats.

Limitations

This study is subject to several limitations that should be acknowledged. First, the vulnerability analysis was conducted on a single domain, namely https://kiis.ibik.ac.id, which may not fully represent the broader landscape of accounting information systems across different organizations or industries. As a result, the generalizability of the findings

may be limited. Second, the study relied solely on automated scanning tools (OpenVAS, OWASP ZAP, and NMAP), without performing in-depth manual penetration testing or validation to confirm the exploitability of identified vulnerabilities. This may result in false positives or an incomplete picture of actual security risks. Third, the scan was performed at a single point in time, without longitudinal monitoring to assess the consistency or evolution of vulnerabilities. Future research should include multiple targets, integrate manual verification techniques, and adopt a time-based approach to gain a more comprehensive understanding of security posture dynamics in accounting information systems.

Closing Remarks

Security in Accounting Information Systems is a critical responsibility for every organization, particularly amid the growing landscape of cyber threats. This study concludes that AIS vulnerabilities include open ports, misconfigured cross-domain settings, and the absence of essential security headers. Tools such as OpenVAS, OWASP ZAP, and NMAP identified several vulnerabilities rated medium and low—none immediately critical, but exploitable if ignored.

Preventive measures, such as closing unused ports, applying CSP policies, and activating headers like anti-clickjacking, should be prioritized. Additionally, cooperation between IT departments and management is crucial for effective security implementation. Previous research has also emphasized that AIS threats stem not only from external actors but also internal factors such as user error and access mismanagement.

Organizations should routinely perform security scans and adopt a multi-layered risk management approach. This includes ongoing vulnerability monitoring aligned with technological advancements and threat evolution. By enhancing security controls and promoting awareness, companies can better safeguard their accounting systems and financial data, ensuring compliance and operational integrity in the long term.

REFERENCE

[1] Arifin, M. (2020). **Implementasi Keamanan Sistem Informasi di Era Digital**. Jurnal Teknologi Informasi, 15(2), 123-136.

[2] Chien, W., Lee, J., & Chen, S. (2018). **A Study on the Vulnerability of Open Ports in Enterprise Networks**. International Journal of Network Security, 20(4), 569-579.

[3] Ghorbani, R., Rezaei, S., & Azimi, N. (2019). **Cybersecurity Challenges in Accounting Information Systems**. Journal of Information Systems, 24(3), 45-60.

[4] Harsono, T. (2021). **Perlindungan Data Pribadi dalam Sistem Informasi Akuntansi**. Jurnal Keamanan Siber, 8(1), 34-45.

[5] Hermawan, Y., Listari, S., Pematasari, I., & Adilah, R. N. (2021, December). Design Of Chatbot Helpdesk For Student Information Services At The United Mini Bank Laboratory IBI Kesatuan. In *International Conference on Global Optimization and Its Applications 2021* (Vol. 1, No. 1, pp. 234-234).

[6] Iriyadi, I., Meiryani, M. E. I. R. Y. A. N. I., Tiara, T. A. N. P. S., Purnomo, A. G. U. N. G., & Salim, G. A. Z. A. L. I. (2023). Blockchain utilization in actions to empower digitalization of accounting information systems for small and medium-sized entities in Indonesia. *Journal of Theoretical and Applied Information Technology*, *101*(17), 7033-7044.

[7] Joshi, R., & Mukherjee, D. (2017). **Preventing Cross-Site Scripting Attacks with Proper Web Security Configurations**. Journal of Web Security, 10(2), 150-164.

[8] Mulyana, A., & Rahmawati, R. (2024). Analysis of One Data Indonesia Portal User Satisfaction Using the Pieces Framework.

[9] Mulyana, M., Nurendah, Y., & Effendy, M. (2025). BUSINESS INTELLIGENCE. *Kesatuan Press*.

[10] Rahman, A., & Widjaja, P. (2020). **Analisis Risiko Keamanan pada Sistem Informasi Akuntansi di Perusahaan Kecil Menengah**. Jurnal Akuntansi dan Teknologi, 12(1), 75-89.
[11] Roup, A. (2024). MANAJEMEN TEKNOLOGI INFORMASI. *Kesatuan Press*.
[12] Schaefer, P., Kraus, S., & Angelini, J. (2018). **Effectiveness of Vulnerability Scanners in Detecting Network Vulnerabilities**. International Journal of Cybersecurity, 7(1), 101-110.
[13] Wilkinson, J., Cerullo, M., & Holt, D. (2020). **Accounting Information Systems: Understanding Risks and Controls**. McGraw-Hill Education.
[14] Wibisono, H. (2019). **Internal Threats in Accounting Information Systems: The Role of Access Control and User Awareness**. Journal of Information Security, 9(3), 200-213.