Research Article

International Journal of Information System and Technology (IJOINT)
Volume 02, Issue 01, PP. 10–17
e.ISSN: 3090-5672

Zero Entry Hacking and Common Vulnerability Scoring System (CVSS) Apisi Website

Subagja Wardaya [1]*

[1] Student, Science and Technology, UIN Syarif Hidayatullah, Jakarta – Indonesia
Email: ward_xmn@gmail.com[1]

*Corresponding Author Email: ward_xmn@gmail.com

Received: February 12, 2026; Revised: February 28, 2026; Accepted: March 07, 2026

Abstract

The current development of information technology encourages non-profit organizations to utilize web-based information systems to support their public services. However, along with this utilization, the issue of information system security has become crucial due to the high frequency of cyber-attacks. This study aims to identify vulnerabilities, conduct penetration testing, and measure the level of security risk on the main portal (http://apisi.org) and library information system (http://opac.apisi.org) belonging to the Indonesian School Information Professionals Association (APISI). This experimental study applies the Zero Entry Hacking (ZEH) methodology which includes four main phases: Reconnaissance, Scanning, Exploitation, and Post-Exploitation. The results of comprehensive testing using various security audit tools detected a total of 41 vulnerabilities in the APISI information system. Based on the measurement results using the Common Vulnerability Scoring System (CVSS) v3.1 calculator, 2 vulnerabilities were found to be categorized as Critical and 9 vulnerabilities to be categorized as High. Overall, the APISI website has an average vulnerability level of 6.6 on a scale of 10, which is included in the medium risk category. The exploit successfully demonstrated the execution of a Cross-Site Scripting (XSS) attack on the OPAC and the upload of a backdoor using Weevely, which granted full control over the server directory. Recommendations included establishing a security Standard Operating Procedure (SOP) and closing the security gap by regularly updating the software version.

Keyword: Information System Security, Association, Library, SLiMS, WordPress, Zero Entry Hacking.

1. Introduction

The current acceleration of global digitalization places information system security as a vital indicator for the sustainability of public services (Latupeirissa et al., 2024; Ribeiro et al., 2025). The urgency of data protection is based on empirical data showing a massive escalation of cyberattacks in Indonesia (Bhakti et al., 2024; Merlang & Siswanto, 2025; Solikhah, 2025). The National Cyber and Crypto Agency (BSSN), in collaboration with the Indonesian Honeynet Project (IHP), recorded a total of 12,895,554 cyberattacks and 513,863 malware attacks in Indonesia throughout 2018. The most common types of cyberattacks include

the distribution of malicious codes, viruses, worms, and Trojans. Amid this attack trend, hacking targets are no longer limited to government agencies or large financial institutions. Independent, non-profit social organizations, such as associations, are also easy targets because they often have relatively low awareness and configuration of information system security.

The Indonesian Association of School Information Professionals (APISI) is an independent, non-profit organization focused on developing school librarianship and librarian competency in Indonesia. To support the dissemination of information about its programs, APISI operates two web-based platforms: the main portal (http://apisi.org) and the Open Access Public Catalogue (OPAC) library online catalog system (http://opac.apisi.org). The main portal is used to promote activities such as seminars and training, while the OPAC platform facilitates circulation, borrowing, member registration, and access to the library's digital files. Infrastructure-wise, APISI's information system is built using the PHP programming language and a MySQL database. The main portal is based on the WordPress v4.7.13 Content Management System (CMS), while the OPAC portal utilizes the free, open-source platform Senayan Library Management System (SLiMS), also known as Senayan 7.

The implementation of information technology at APISI has been accompanied by a history of cybersecurity breaches that have disrupted service availability. Based on the digital hacking track record archive on the site http://zone-h.org, the main apisi.org portal was recorded as having experienced its first web defacement attack on October 6, 2013. A similar attack also hit the opac.apisi.org subdomain on April 22, 2016, carried out by a hacker named KingSkrupellos. In addition to the defacement, the APISI website was also hit by a massive bot registration attack characterized by a flood of random fake account registrations. These attacks caused the hosting file storage capacity to be full (overload) and resulted in the APISI hosting account being suspended by the hosting service provider, making the website completely inaccessible. So far, recovery efforts by the administrator have been limited to contacting the hosting provider to reactivate the account and perform a database restoration. These actions do not resolve the root of the problem because the actual security gap in the program code or server configuration has never been identified and closed. To mitigate the risk of further attacks that could compromise the confidentiality, integrity, and availability of APISI data, this study conducted systematic penetration testing. This study aimed to test the security of the APISI website, map all vulnerabilities in detail, and provide technical recommendations to close them. The practical benefit of this research is that it can serve as evaluation material for APISI IT managers to improve information system defenses against cyberattacks. For the academic world, this research provides scientific contributions and additional references regarding cybersecurity audit methodology in non-profit organizations.

2. Literature Review

2.1 Analysis of Relevant Research

A review of previous research was used to identify the position and novelty of this research. First, a study by Umar et al. (2024) conducted penetration testing on the IBM Bekasi AIS domain using the OWASP 10 standard and found a range of vulnerabilities, from mild to severe, on 10 faculty and directorate websites. Second, Yamin (2022) tested the security vulnerabilities of Udayana University's Personnel Information System using the Vulnerability Assessment and Penetration Testing (VAPT) framework and detected vulnerabilities in the form of Cross-Site Scripting (XSS) and Password Autocomplete. Third, a study by Bose

& Narayanan et al. (2023) analyzed cyberattacks on the CMSPY journal regarding the dangers of hacking based on the creation of fake websites (journal hijacking). Referring to this literature, this study focused on testing the WordPress and SLiMS CMS platforms specifically using the structured Zero Entry Hacking (ZEH) methodology.

2.2 Information Security Concept and the CIA Triad

The foundation of any well-designed information security program rests on three main pillars known as the "CIA Triad" (Althonayan & Andronache, 2018), i.e.:

1. Confidentiality aims to ensure that data and information can only be accessed by authorized parties. Failure of this pillar can occur due to interception attacks.
2. Integrity aims to ensure that data is not unauthorizedly altered by third parties during storage or transmission. Attacks that threaten this pillar include data modification and data fabrication.
3. Availability aims to ensure that systems and data are accessible to authorized users when needed. Attacks that consume bandwidth or storage capacity (such as DDoS) significantly threaten this availability.

2.3 Zero Entry Hacking (ZEH) Methodology

The methodology used in the penetration testing on the APISI website is Zero Entry Hacking (ZEH) (Anchugam, 2021; Aparicio-Navarro et al., 2019). This methodology was chosen because it is highly systematic in simulating attack tactics carried out by hackers from outside the network without initial authorization (zero credentials) (Sari & Pakaja; 2024; Utama et al., 2025). Based on the ZEH framework, the testing process is divided into four sequential stages: 1) Reconnaissance: The process of collecting as much data and information as possible about the target. 2) Scanning: The process of analyzing host activity status, open ports, system architecture, and scanning for vulnerabilities. 3) Exploitation: The attempt to prove the existence of a security vulnerability by injecting code or manipulating system parameters. Four) Post-Exploitation and Maintaining Access: The stage for testing whether the access gained can be maintained (for example, by installing a backdoor) and compiling reports on cybertest results.

2.4 Common Vulnerability Scoring System (CVSS)

The Common Vulnerability Scoring System (CVSS) is an open industry standard used to measure and map the level of software security vulnerabilities into a quantitative score (Elder et al., 2024; Mell et al., 2006). The CVSS divides assessment metrics into three main groups: Base Metrics (constant intrinsic characteristics of vulnerabilities), Temporal Metrics (measures the current state of exploitation activity), and Environmental Metrics (adjusts the score based on the organization's specific environment) (Feutrill et al., 2018; Milousi et al., 2024). The CVSS calculation formula calculates the functional value of various parameters (Petajasoja et al., 2011; Wang et al., 2022), for example: Attack Vector (AV), Attack Complexity (AC), Privileges Required (PR), User Interaction (UI), and their damage impact on the CIA Triad. The final calculation results are converted into qualitative ratings: Low (0.1 - 3.9), Medium (4.0 - 6.9), High (7.0 - 8.9), and Critical (9.0 - 10.0).

3. Method

3.1 Research Approach and Roadmap

This research uses an experimental hands-on penetration testing approach (Sarker et al., 2023). Testing is conducted externally (black-box testing perspective) to simulate real-world attacks from the internet (Salas

& Martins, 2015; Vats et al., 2020). The testing implementation blueprint is outlined in the ZEH Research Roadmap as follows:

- Phase 1: Reconnaissance: Verifying domain name information via Whois, email search using The Harvester, CMS/technology identification via WhatWeb, and vulnerability extraction via CXSecurity and Google Dorking.
- Phase 2: Scanning: Verifying target connectivity using Ping, mapping active ports using Nmap, and automatically scanning for security vulnerabilities using vulnerability scanners such as Uniscan, OWASP ZAP, and Acunetix.
- Phase 3: Exploitation: Validate the vulnerability using the Firefox browser, Java Script Damn Small Scanner (JSDS), and WPScan.
- Phase 4: Post-Exploitation: Install a web-based backdoor using Weevely to test the robustness of directory control and compile a final report.

3.2 Data Collection Techniques

Population, operational, and system parameter data for this research were collected through three data collection methods: 1) Observation: Conducting a direct review of the research object at the APISI office in Tangerang, Banten, to record IP addresses and map the topology of running online services. 2) Interviews: Conducting a face-to-face Q&A with the APISI website manager, Achmad Sofyan, S.Fil., on November 20, 2018, to obtain a chronology of past cyberattacks and the mitigation measures taken. 3) Literature Review: Reviewing two thesis documents, three national journals, and three international journals on cybersecurity audits as comparative references.

3.3 Testing Hardware and Software

The penetration testing process was conducted in an isolated environment with the following system specifications: 1) Operating System: Kali Linux v2018.4 [67]. Two) Security Audit Tools: NMAP v7.25, Uniscan v6.2, wpscan v3.3.1, OWASP ZAP v2.5.0, Acunetix v11, Weevely, and JSDS. Three) Analysis Calculator: Web-based Common Vulnerability Scoring System (CVSS) v3.1 Calculator.

4. Result and Discussion

4.1 Reconnaissance Results

The initial reconnaissance phase provided valuable baseline information regarding APISI's information systems:

- WHOIS Domain apisi.org
  Indicates that the domain was first registered on July 16, 2010, and is managed by the Indonesian Reading Forum. The hosting server used is provided by MasterWeb (masterwebnet), supported by four servers (one main server and three backup servers).
- The Harvester (E-mail Harvesting)
  Successfully mapped the organization's official email accounts distributed on the Google search engine, including kotaksurat@apisi.org and hanna@apisi.org.
- WhatWeb (Technology Identification)
  Indicates that the main apisi.org portal uses the PHP programming language, the Apache web server, and the WordPress CMS v4.7.13. Meanwhile, the subdomain opac.apisi.org uses the Senayan 7 library automation platform (SLiMS).
- CXSecurity & Exploit-DB (Vulnerability Advisory)

A Google Hacking Database (GHDB) search detected 78 potential exploits for the WordPress CMS, while a search for the Senayan application yielded 0 (no public exploits found). The CXSecurity security advisory database identified WordPress 4.7.13 as having a Database Configuration File Download vulnerability, while SLiMS 7 had Arbitrary File Upload and Cross-Site Scripting vulnerabilities.

4.2 Scanning Results and Vulnerability Analysis

Port scanning using Nmap on the MasterWeb server IP (45.64.1.113) detected several important open ports, namely:

- Port 21 (FTP), Port 25 (SMTP), Port 80 (HTTP), Port 110 (POP3), Port 143 (IMAP), Port 443 (SSL/HTTPS), and Port 3306 (MySQL). Because APISI uses shared hosting, the management of these ports and services is under the full control of the file hosting provider, MasterWeb.
- An automated vulnerability scan was run using three vulnerability scanners to eliminate duplication. The combined scan results detected a total of 41 vulnerabilities on both APISI websites.
- These vulnerabilities ranged from critical structural vulnerabilities to secondary informational vulnerabilities such as Application Error Messages, Cookies without the Secure Flag Set, and WordPress installation documentation (readme.html) that had not been removed from the root directory.

4.3 Vulnerability Exploitation and Post-Exploitation

To validate the findings from the automated scanning tool, the following steps were performed directly on the system:

- Reflected Cross-Site Scripting (XSS) Exploit on opac.apisi.org: The exploit was carried out by injecting an XSS payload into the keywords parameter in the book search URL. When inserted with the payload: </script><script>alert(1);</script><script> and combined with the URL: http://opac.apisi.org/index.php?id=17&keywords=%3C%2Fscript%3E%3Cscript%3Ealert%281%29%3B%3C%2Fscript%3E%3Cscript%3E&p=show_detail
  the system failed to filter user input, resulting in the JavaScript code being successfully executed by the browser and displaying an alert box. This demonstrates a failure of the confidentiality and integrity pillars, as attackers could exploit this vulnerability to steal cookies or perform session hijacking.
- Arbitrary File Upload & Backdoor Installation Exploitation on opac.apisi.org: In SLiMS 7, an arbitrary file upload vulnerability was identified. Researchers attempted to upload a PHP-based backdoor file generated by the Weevely tool. After the upload was successful and the backdoor file was activated, researchers successfully gained full control over the APISI hosting operating system directory. Through the Weevely terminal, researchers were able to navigate files, download sensitive configuration files, and even manipulate databases. This represents the highest risk level (Critical) because it cripples all three pillars of the CIA Triad.
- Security Vulnerability Exploitation on apisi.org (WordPress): On the main portal, several vulnerabilities were detected in WordPress plugins used, such as WordPress NextGEN Gallery. Researchers successfully validated a Security Bypass vulnerability (CVSS score 7.0) that allows an outside user to reactivate the user registration feature previously disabled by the administrator. Additionally, a Remote Code Execution (RCE) vulnerability was discovered in the NextGEN Gallery plugin that allows attackers with low privileges (basic privileges) to inject a new PHP file (rce.php) by replacing the Default Styles parameter value.

4.4 Vulnerability Level Measurement Based on CVSS

Each vulnerability successfully validated through the exploitation phase is then assigned a risk score using the CVSS v3.1 calculator. Table 1 below summarizes the final overall vulnerability score for APISI's information system:

Table 1. Final Score of Vulnerability Level

No	Platform Name	Website Address	Confidentiality Value (C)	Integrity Value (I)
1	Main Portal	http://apisi.org	5.6	6.6
2	OPAC Catalog	http://opac.apisi.org	5.9	5.4
Total	System Average	APISI	5.8	6.0

The calculation results above indicate that the highest vulnerability is in the data availability pillar, with a score of 8.1. This is highly relevant to the historical fact that the APISI website was highly susceptible to total shutdown due to full hosting storage space triggered by bot exploit activity. The overall APISI system vulnerability score averaged 6.6, classified as a medium risk level.

4.5 Implications of the Findings for APISI System Security

The findings above have very serious technical and operational implications for APISI's operational continuity. The existence of the Arbitrary File Upload vulnerability in SLiMS and the RCE vulnerability in NextGEN Gallery WordPress open up significant opportunities for attackers to embed malicious shell files that could compromise the integrity of the entire seminar database and library book catalog. Furthermore, failing to disable the autocomplete feature on the civil service login form makes it easy for attackers to obtain administrator credentials when accessing the physical device previously used to manage the website. Without any fundamental improvements, the database restoration activities that APISI staff have relied on so far will only be temporary measures that will continue to be repeated when new attacks are launched by hackers.

5. Conclusion

This information system security audit study using a penetration testing approach successfully detected and mapped the security risk landscape on the APISI website in a measurable manner. Through the implementation of the Zero Entry Hacking (ZEH) methodology, a total of 41 security vulnerabilities were identified, including critical vulnerabilities such as Arbitrary File Upload in SLiMS and high-level vulnerabilities such as Remote Code Execution in WordPress plugins. Quantitative measurements using CVSS v3.1 parameters placed the APISI website's average vulnerability level at 6.6 (Medium). This research empirically proves that system recovery after a cyberattack requires more than just database restoration; it must also include identifying security vulnerabilities and closing vulnerable program code.

This cyber audit study has several limitations. The scope of the testing focused solely on technical testing of application-level vulnerabilities and APISI's web hosting server configuration. This study did not examine human error through social engineering techniques, which in the real world is often the primary entry point for many administrator credential data breaches.

Based on the findings and conclusions above, the researcher provides several strategic recommendations for the development of APISI's cyber defense in the future, including: One) Implementation of Technical

Recommendations needs to be expedited by updating the WordPress CMS version and the SLiMS platform to the latest stable version to close the RCE gap and unauthorized file uploads. Deleting sensitive installation files such as readme.html and setting important security headers such as X-Frame-Options: DENY and X-XSS-Protection: 1. Two) Developing a Standard Operating Procedure (SOP) for IT management that regulates the periodic password update cycle and limits on admin access rights. Three) Future research is expected to expand the scope of testing by including simulations of Social Engineering attacks to measure the readiness and cyber resilience of human resources managing information systems in the association environment.

Acknowledgments

-

References

1. Althonayan, A., & Andronache, A. (2018, September). Shifting from information security towards a cybersecurity paradigm. In Proceedings of the 2018 10th International Conference on Information Management and Engineering (pp. 68-79).
2. Anchugam, C. V. (2021). Essential security elements and phases of hacking attacks. In Ethical hacking techniques and countermeasures for cybercrime prevention (pp. 114-143). IGI Global.
3. Aparicio-Navarro, F. J., Chadza, T. A., Kyriakopoulos, K. G., Ghafir, I., Lambotharan, S., & AsSadhan, B. (2019, February). Addressing multi-stage attacks using expert knowledge and contextual information. In 2019 22nd Conference on innovation in clouds, internet and networks and workshops (ICIN) (pp. 188-194). IEEE.
4. Bhakti, A., Sudirman, A., Sumadinata, R. W. S., & Bainus, A. (2024). State defense strategy in facing cyber threats after hacking incidents on government institutions: A case study in Indonesia. Journal of Human Security, 20(1), 109-117.
5. Bose, S., & Narayanan, A. K. (2023). Security Analysis of CMS based Websites through CMSPY. International Center For Research And Resources Development, 4(4)..
6. Elder, S., Rahman, M. R., Fringer, G., Kapoor, K., & Williams, L. (2024). A survey on software vulnerability exploitability assessment. ACM Computing Surveys, 56(8), 1-41.
7. Feutrill, A., Ranathunga, D., Yarom, Y., & Roughan, M. (2018, November). The effect of common vulnerability scoring system metrics on vulnerability exploit delay. In 2018 Sixth International Symposium on Computing and Networking (CANDAR) (pp. 1-10). IEEE.
8. Latupeirissa, J. J. P., Dewi, N. L. Y., Prayana, I. K. R., Srikandi, M. B., Ramadiansyah, S. A., & Pramana, I. B. G. A. Y. (2024). Transforming public service delivery: A comprehensive review of digitization initiatives. Sustainability, 16(7), 2818.
9. Merlang, R., & Siswanto, A. (2025). Penetration Testing System CERDAS With Brute Force Method. International Journal of Information Systems and Technology, 1(03), 104-114.
10. Mell, P., Scarfone, K., & Romanosky, S. (2006). Common vulnerability scoring system. IEEE Security & Privacy, 4(6), 85-89.
11. Milousi, K., Kiriakidis, P., Mengidis, N., Rizos, G., Mazi, M. S., Voulgaridis, A., ... & Tzovaras, D. (2024, July). Evaluating cybersecurity risk: A comprehensive comparison of vulnerability scoring methodologies. In Proceedings of the 19th international conference on availability, reliability and security (pp. 1-11).
12. Petajasoja, S., Kortti, H., Takanen, A., & Tirila, J. M. (2011, July). Ims threat and attack surface analysis using common vulnerability scoring system. In 2011 IEEE 35th annual computer software and applications conference workshops (pp. 68-73). IEEE.

13. Ribeiro, D., Fonte, V., Ramos, L. F., & Silva, J. M. (2025). Assessing the information security posture of online public services worldwide: Technical insights, trends, and policy implications. Government Information Quarterly, 42(2), 102031.
14. Salas, M. I. P., & Martins, E. (2015). A black-box approach to detect vulnerabilities in web services using penetration testing. IEEE Latin America Transactions, 13(3), 707-712.
15. Sari, D. P., & Pakaja, F. (2024). Carrying Out Website Security Analysis Using the Standard Penetration Testing Method. International Journal of Multidisciplinary Applied and Science Research, 1(01), 22-28.
16. Sarker, K. U., Yunus, F., & Deraman, A. (2023). Penetration taxonomy: A systematic review on the penetration process, framework, standards, tools, and scoring methods. Sustainability, 15(13), 10471.
17. Solikhah, M. A. (2025). Personal data protection in the era of digital transformation: Challenges and solutions in the indonesian cyber law framework. Indonesian Cyber Law Review, 2(1), 39-50.
18. Umar, R., Riadi, I., & Elfatiha, M. I. A. (2024). Security analysis of web-based academic information system using owasp framework. Kinetik: Game Technology, Information System, Computer Network, Computing, Electronics, and Control.
19. Utama, A., Khairil, K., & Supardi, R. (2025). Website Security Analysis Using Penetration Testing. International Journal of Information Systems and Technology, 1(02), 44-51.
20. Vats, P., Mandot, M., & Gosain, A. (2020, June). A comprehensive literature review of penetration testing & its applications. In 2020 8th International Conference on Reliability, Infocom Technologies and Optimization (Trends and Future Directions)(ICRITO) (pp. 674-680). IEEE.
21. Wang, Y., Yu, B., Yu, H., Xiao, L., Ji, H., & Zhao, Y. (2022). Automotive cybersecurity vulnerability assessment using the common vulnerability scoring system and Bayesian network model. IEEE Systems Journal, 17(2), 2880-2891.
22. Yamin, R. T. N., Suarjaya, I. M. A. D., & Pratama, I. P. A. E. (2022). Penetration Testing on the SISAKTI Application at Udayana University Using the OWASP Testing Guide Version 4. Jurnal Ilmiah Merpati (Menara Penelitian Akademika Teknologi Informasi), 10(3), 155.