


Security Testing of Personnel Management Information System (SIMPEG) Website Using the OWASP Web Security Testing (WSTG) Framework

Abrar Khalida^{1*}, Aulia Syarif Aziz²

Universitas Islam Negeri Ar-Raniry, Indonesia

E-mail: 190212028@student.ar-raniry.ac.id, 2aulia.aziz@ar-raniry.ac.id*

Article Info	ABSTRACT
Submitted: 09-04-2025 Final Revised: 22-04-2025 Accepted: 25-04-2025 Published: 26-04-2025	<p>This research examines the security of the Employee Management Information System (SIMPEG) at UIN Ar-Raniry Banda Aceh using the OWASP Web Security Testing Guide (WSTG) framework. The aim of this study is to identify and address potential security vulnerabilities within the system. The research is divided into three phases: identifying the issues, performing grey-box penetration testing with a focus on client-side testing as outlined in OWASP WSTG, and reporting the findings using the WSTG Checklist. The testing results revealed that out of the thirteen tests conducted, one vulnerability related to Cross Origin Resource Sharing (CORS) was discovered. This study concludes that the SIMPEG system at UIN Ar-Raniry Banda Aceh demonstrates a good level of security, though further improvements are necessary to address the identified issues. Recommendations for enhancing the security of SIMPEG include continuous testing and updates to address emerging threats.</p> <p>Keyword: Web Security; OWASP; Information System; Penetration Testing; Client-side testing</p> <p>Attribution-ShareAlike 4.0 International (CC BY-SA 4.0)</p>



Introduction

Along with the rapid development of information technology, websites now play an important role in various aspects such as information dissemination, business activities, and user interaction (Mishra & Agarwal, 2024). While it offers many benefits, websites are also vulnerable to attacks from hackers that can lead to personal data theft, reputational damage, or takeover of sensitive data (Maulana, 2021). Data from the State Cyber and Cryptography Agency (BSSN) recorded around

279.84 million cyberattacks in 2023, highlighting a sharp increase in attack incidents and the urgent need to maintain website security (Dataindonesia.id, 2023).

Website security is a vital component in information system management, especially for the Personnel Management Information System (SIMPEG) (de Rahu et al., 2023; Katresna et al., 2023). The system serves as an employee data management center that includes personal information, employment history, and other sensitive data. With this central role, the protection of SIMPEG from cyber threats is a must that cannot be ignored (Sudana, 2021).

In this context, SIMPEG is an important component in the operations of organizations that store and manage employee information (Chazar, 2015). The increasing trend of attacks on information systems such as SIMPEG, with various threats such as SQL injection and Cross-Site Scripting (XSS), underscores the need for in-depth security evaluations to protect data. The results of previous research on server security show that SIMPEG UIN Ar-Raniry has as many as 9 vulnerabilities that are categorized into medium level tread with a score of 6.4 (Bahtiar, 2024; Raazi, 2023).

To meet these challenges, a structured and proven effective approach is needed. The OWASP Web Security Testing Guide (WSTG) v4.2 framework is a widely recognized guide to web security testing (Foundation, 2019). This guide provides a comprehensive methodology for identifying and addressing vulnerabilities in website applications (Pratama, 2023). This test will cover various aspects of security, one of which is client-side testing. By implementing this framework, web managers can conduct a systematic and thorough evaluation of the security of their applications.

In addition, the WSTG Checklist v4.2 plays an important role in the preparation of vulnerability analysis reports. Using these various frameworks, the results of the analysis can provide practical recommendations for developers to strengthen the security of the system in the future. The focus of this test includes aspects on the client side. In addition, this study will also evaluate the extent of the effectiveness of the OWASP WSTG framework in detecting and addressing vulnerabilities in SIMPEG (Abdan, 2022).

Previous studies have highlighted the vulnerability of government-based information systems, particularly SIMPEG, to a variety of cyber threats such as SQL Injection, Cross-Site Scripting (XSS), and unauthorized access due to poor input validation or insecure configurations (Ilias & Sukib, 2017; Priambodo et al., 2022; Safitri et al., 2020). The novelty of this research lies in its exclusive use of the OWASP Web Security Testing Guide (WSTG) v4.2 framework to conduct client-side penetration testing on the SIMPEG platform. Unlike general security audits, this study emphasizes practical, step-by-step identification of vulnerabilities using OWASP's structured testing methodology—specifically targeting the client-side attack surface which has often been neglected in SIMPEG-related penetration testing (Safriatullah, 2021). This research provides actionable insights by linking vulnerabilities to specific WSTG checklist items and offering tailored remediation recommendations (Hassanah, 2021; Supardi, 2024). Its contribution to information security management includes not only improving defense mechanisms in SIMPEG but also providing a model for other government institutions to enhance their web-based system security through structured penetration testing protocols. This research examines the security of the

Employee Management Information System (SIMPEG) at UIN Ar-Raniry Banda Aceh using the OWASP Web Security Testing Guide (WSTG) framework.

Materials and Methods

This study aims to test the security of the SIMPEG UIN Ar-Raniry Banda Aceh site which is in the testing stage using the OWASP WSTG version 4.2 guide, especially in the Client-side Testing aspect. This research process consists of three main phases, namely problem identification, penetration testing, and report results. Here is the test flow:

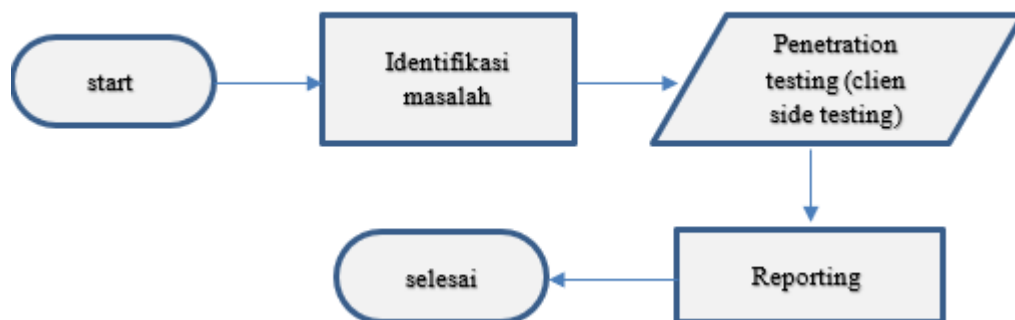


Figure 1. Research Flow

Results and Discussions

This study uses OWASP ZAP for vulnerability analysis, Chrome browser for manual exploration, and WSTG guidance as a framework. The steps to implement the research include accessing the target URL through OWASP ZAP to monitor network traffic, running various tests on the client-side, such as DOM-Based Cross Site Scripting, JavaScript Execution, HTML Injection, Client-side URL Redirect, CSS Injection, Client-side Resource Manipulation, Cross Origin Resource Sharing, Cross Site Flashing, Clickjacking, WebSockets, Web Messaging, Browser Storage, and Cross Site Script Inclusion, as well as recording all test results in a structured table.

Hasil WSTG Checklist

Based on the tests that have been carried out using various methods such as function identification, feature identification, code injection experiments, and testing with several types of tools, a table based on the following WSTG checklist is made:

Table 1. WSTG Checklist

Test ID	Test Name	Status	Note
WSTG-CLNT-01	Testing for DOM-Based Cross-Site Scripts	Not found	
WSTG-CLNT-02	Testing for JavaScript Execution	Not found	
WSTG-CLNT-03	Testing for HTML Injection	Not found	

WSTG-CLNT-04	Testing for Client-Side URL Redirects	Not found	
WSTG-CLNT-05	Testing for CSS Injection	Not found	
WSTG-CLNT-06	Testing for Client-Side Resource Manipulation	Not found	
WSTG-CLNT-07	Testing Cross-Origin Resource Sharing	Found	There is a vulnerability in the CORS configuration that can expose data to untrusted domains.
WSTG-CLNT-08	Testing for Cross-Site Flashing	Not found	
WSTG-CLNT-09	Testing for Clickjacking	Not found	
WSTG-CLNT-10	Testing WebSockets	Not found	
WSTG-CLNT-11	Testing Web Messages	Not found	
WSTG-CLNT-12	Testing Browser Storage	Not found	
WSTG-CLNT-13	Testing for Cross-Site Script Inclusion	Not found	

A major vulnerability was found in WSTG-CLNT-07 (Testing Cross-Origin Resource Sharing), where the Access-Control-Allow-Origin header allowed untrusted domains. This opens up the potential for exploitation of user data through cross-origin attacks.

The discovery of a misconfigured Access-Control-Allow-Origin header that allows untrusted domains aligns with the study by Zalewski (2011), which explained that insecure CORS settings can be exploited by attackers to perform Cross-Site Request Forgery (CSRF) and credential hijacking via malicious external domains. Furthermore, research by Altulaihan et al., (2023) found that approximately 36% of audited government web applications still apply overly permissive CORS configurations and fail to validate the origin strictly. This opens opportunities for the exploitation of sensitive user information, especially in token-based authentication systems.

In addition, Vulchi & Ackerman (2024) emphasized that CORS misconfigurations become even more dangerous when combined with session hijacking or malicious JavaScript injection, which are commonly introduced through third-party content such as untrusted ads or plugins. Therefore, the vulnerability found in WSTG-CLNT-07 (Testing Cross-Origin Resource Sharing) on the SIMPEG platform indicates that the system has not yet implemented best practices for security header configuration. This reinforces the urgency of tightening server-side validation for CORS headers and restricting allowed origins to a trusted whitelist only. Implementing these measures will significantly enhance the overall security posture of personnel information systems.

Conclusion

Based on the security audit results using the OWASP WSTG v4.2 framework, it can be concluded that most security aspects of the SIMPEG (Personnel Management Information System) at UIN Ar-Raniry Banda Aceh meet web security standards. However, a significant vulnerability was found in WSTG-CLNT-07 (Testing Cross-Origin Resource Sharing), where the system allowed untrusted domains through a misconfigured Access-Control-Allow-Origin header. This opens up potential threats such as cross-origin attacks, data exposure, and session hijacking. The findings reinforce the importance of using OWASP WSTG v4.2 as a reliable standard for security testing of web-based information systems, given its comprehensive and technology-adaptive testing structure. To strengthen the security posture of SIMPEG and similar systems

References

- Abdan, M. K. (2022). *Pengujian Keamanan Sistem Informasi Berbasis Web Berdasarkan Framework Owasp Wstg V4.2 (Studi Kasus: Sistem Sekawan VI Universitas Islam Indonesia)*. <https://dspace.uui.ac.id/handle/123456789/40225> AC - Aug. 06, 2024
- Altulaihan, E. A., Alismail, A., & Frikha, M. (2023). A survey on web application penetration testing. *Electronics*, 12(5), 1229.
- Bahtiar, D. E. N. and B. I. and A. (2024). Evaluasi Keamanan Website Menggunakan Metode Owasp: Penilaian Terhadap Serangan Injeksi Sql Dan Cross-Site Scripting (Xss). *JATI (Jurnal Mhs. Tek. Inform.)*, 8(1), 675–680. <https://doi.org/10.36040/jati.v8i1.8700>
- Chazar, C. (2015). Standar Manajemen Keamanan Informasi Berbasis ISO/IEC 27001: 2005. *J. Inf.*, VII(2), 48–57.
- Dataindonesia.id. (2023). *Data Jumlah Serangan Siber ke Indonesia hingga 2023*. <https://dataindonesia.id/internet/detail/data-jumlah-serangan-siber-ke-indonesia-hingga-2023> AC - Aug. 02, 2024
- de Rahu, K. Y., Neolaka, M. N. B. C., & Djaha, A. S. A. (2023). Personnel management information system in order to create up-to-date and integrated personel data and information in the personnel and human resources agency in malaka regency. *Journal of Multidisciplinary Academic and Practice Studies*, 1(1), 11–27.
- Foundation, O. (2019). *OWASP Web Security Testing Guide*. <https://owasp.org/www-project-web-security-testing-guide/> AC - Feb. 04, 2024
- Hassanah, S. E. P. and N. (2021). Analisis Keamanan Website Universitas Internasional Batam Menggunakan Metode Issaf. *J. Ilm. Inform.*, 9(02), 82–86. <https://doi.org/10.33884/jif.v9i02.3758>
- Ilias, A., & Sukib, N. (2017). Determinants of the Intention to Re-use Internet Business Reporting (IBR): The Structural Equation Modelling Approach. *International Conference on Accounting Studies (ICAS)*.
- Katresna, H. N., Khairina, E., & Salsabila, L. (2023). Enhancing Personnel Management: A Study on the Implementation of SIMPEG in the Batam City Staffing and Human Resources Development Agency. *Conference on Business, Social Sciences and Technology (CoNeSciNTech)*, 3(1), 176–181.
- Maulana, A. R. and R. R. S. and S. A. (2021). Analisis Keamanan Website dengan Information System Security Assessment Framework (Issaf) dan Open Web Application Security Project

- (Owasp) di Rumah Sakit Xyz. *J. Indones. Sos. Teknol.*, 2(4), 506–519. <https://doi.org/10.36418/JIST.V2I4.124>
- Mishra, R. K., & Agarwal, R. (2024). Impact of digital evolution on various facets of computer science and information technology. *Digital Evolution: Advances in Computer Science and Information Technology*, 17.
- Pratama, I. D. G. G. D. and G. M. A. S. and I. P. A. E. (2023). Penetration Testing Berbasis OWASP Testing Guide Versi 4.2 (Studi Kasus: X Website). *JITTER J. Ilm. Teknol. dan Komput.*, 4(1), 1613. <https://doi.org/10.24843/jtrti.2023.v04.i01.p06>
- Priambodo, D. F., Hasbi, M., & Malacca, M. S. (2022). Security Assessment Aplikasi Mobile Pemerintahan dengan Acuan OWASP Top 10 Mobile Risks. *JEPIN (Jurnal Edukasi dan Penelitian Informatika)*, 8(3), 560–571.
- Raazi, I. M. (2023). *Analisis Penilaian Keamanan Server Terhadap Sistem Informasi Manajemen Kepegawaian Dengan Metode NIST SP 800-115 Pada Universitas Islam Negeri Ar* <https://repository.ar-raniry.ac.id/id/eprint/29863/>
- Safitri, E. M., Larasati, A. S., & Hari, S. R. (2020). Analisis Keamanan Sistem Informasi E-Banking Di Era Industri 4.0: Studi Literatur. *Jurnal Ilmiah Teknologi Informasi dan Robotika*, 2(1). <https://doi.org/10.33005/jifti.v2i1.25>
- Safriatullah, A. S. A. and. (2021). Perancangan Dan Analisis Keamanan Pada Sistem Autentikasi Terpusat Freeradius. *J. Informatics Comput. Sci.*, 7(2), 106–112.
- Sudana, N. N. and A. T. and I. M. and S. P. and A. A. K. and O. (2021). Uji Fungsionalitas Sistem Informasi Manajemen Pegawai dengan Metode Black Box. *JITTER- J. Ilm. Teknol. dan Komput.*, 2(3).
- Supardi, D. A. U. and K. K. and R. (2024). Analisis Keamanan Website Menggunakan Ptes (Penetration Testing Execution And Standart). *J. Media Infotama*, 20(1), 106–112. <https://doi.org/https://jurnal.unived.ac.id/index.php/jmi/article/download/5367/4261>
- Vulchi, J. R., & Ackerman, E. (2024). *Integrating Web Security Headers into the Secure Software Development Lifecycle: Effective Strategies and Key Considerations*.
- Zalewski, M. (2011). *The tangled Web: A guide to securing modern web applications*. No Starch Press.