Brilliance
Research of Artificial Intelligence

E-ISSN : 2807-9035
Volume 5, **Number** 2, November 2025
https://doi.org/10.47709/brilliance.v5i2.6780

Database Vulnerability Analysis of North Aceh e-Kinerja Website Using SQL Injection

Fidyatun Nisa[1*], Muhammad Ikhwani[2], Nanda Sitti Nurfebruary[3], Siti Nayla Husna[4]
[1,2,3,4]Malikussaleh University, Aceh, Indonesia
[1]fidyatun.nisa@unimal.ac.id, [2]muhammad.ikhwani@unimal.ac.id, [3]nandasitti.nur@unimal.ac.id,
[4]siti.200180002@mhs.unimal.ac.id

open access

***Corresponding Author**

Article History:
Submitted: 08-12-2025
Accepted: 20-12-2025
Published: 29-12-2025

Keywords:
Information Security; SQL Injection; e-Kinerja; Blackbox Testing; ISSAF.

ABSTRACT

The rapid advancement of information technology has significantly increased the risk of cyber threats, particularly in web-based systems. One of the most common attack techniques used to exploit vulnerabilities in web applications is SQL injection, which can result in sensitive data leakage and system compromise. This study aims to evaluate the database security of the E-Kinerja website of North Aceh Regency against SQL injection attacks using a black-box penetration testing approach. The assessment is conducted based on the Information Systems Security Assessment Framework (ISSAF), which provides a structured and systematic methodology for comprehensive security evaluation. The testing process includes several stages, namely planning and preparation, information gathering, network mapping, vulnerability identification, and penetration testing, utilizing tools such as SQLMap and OWASP ZAP. The results indicate that the target website is not vulnerable to SQL injection attacks, as no exploitable parameters were identified during testing. This is largely due to the implementation of security mechanisms such as Web Application Firewall (WAF) and Intrusion Prevention System (IPS), which effectively detect and prevent unauthorized access attempts. This study highlights the importance of implementing layered security strategies and continuously updating security protocols to address emerging cyber threats. The findings contribute to improving database security awareness and provide practical recommendations for strengthening the resilience of information systems in the government sector.

INTRODUCTION

The rapid development of internet technology has transformed how information is accessed and managed, particularly in the public sector. Government institutions increasingly rely on web-based systems to enhance efficiency and transparency in managing administrative processes.

One such implementation is the E-Kinerja system used by the Human Resource Development and Personnel Agency (BKPSDM) of North Aceh Regency. This system plays a critical role in monitoring and evaluating civil servant performance(R, Gusty et al. 2020). However, the reliance on web applications introduces potential cybersecurity risks, particularly related to data confidentiality and integrity.

Web application security remains a critical issue due to the increasing number of cyberattacks targeting government systems(Abdul Gafur, 2023). Previous studies have shown that academic and institutional websites still contain various vulnerabilities, including medium and low-level risks that require continuous mitigation(Nisa et al., 2024). Web applications are frequent targets of cyberattacks, with SQL injection being one of the most critical vulnerabilities. SQL injection allows attackers to manipulate database queries and potentially access or alter sensitive information(Fitria, 2021). Therefore, evaluating the security of the E-Kinerja system is essential to ensure its resilience against such attacks.

This study aims to analyze database vulnerabilities using penetration testing based on the ISSAF framework to assess the system's resistance to SQL injection attacks.

LITERATURE REVIEW

Recent studies emphasize the increasing risks of web-based cyberattacks and the importance of penetration testing:

SQL injection remains one of the most common vulnerabilities in web applications (Alenezi et al., 2021). SQL injection represents a critical vulnerability that occurs when attackers are able to manipulate database queries through improperly validated user input. Previous research conducted at Universitas Malikussaleh identified multiple vulnerabilities in web systems using OWASP ZAP, indicating that continuous security evaluation is essential (Nisa et al., 2024).

Penetration testing is widely used to identify system weaknesses without accessing source code (Rahman et al., 2022).

Brilliance
Research of Artificial Intelligence

E-ISSN : 2807-9035
Volume 5, **Number** 2, November 2025
https://doi.org/10.47709/brilliance.v5i2.6780

ISSAF provides a comprehensive framework for structured security assessment (Umar et al., 2023). Penetration testing using the ISSAF framework has been widely applied to evaluate system security in various domains, including e-commerce and e-ticketing systems (Akhlia, 2025; Nazaruddin, 2024). ISSAF has three main phases: Planning and preparation phase; Assessment phase; and Reporting, clean up and destroy artifacts.

Web Application Firewalls (WAF) are effective in mitigating injection-based attacks (Singh & Sharma, 2021). The implementation of Web Application Firewall (WAF) has proven effective in detecting and mitigating SQL injection and XSS attacks in real-time environments (Annas et al., 2024)

Intrusion Prevention Systems (IPS) enhance real-time attack detection and prevention (Kumar et al., 2022). Based on these studies, this research focuses on evaluating real-world implementation of web security mechanisms in government systems.

METHOD

This research uses a black-box penetration testing method, where the tester does not have access to the application source code. The research using ISSAF Framework that follows three main phases as shown in Figure 1:

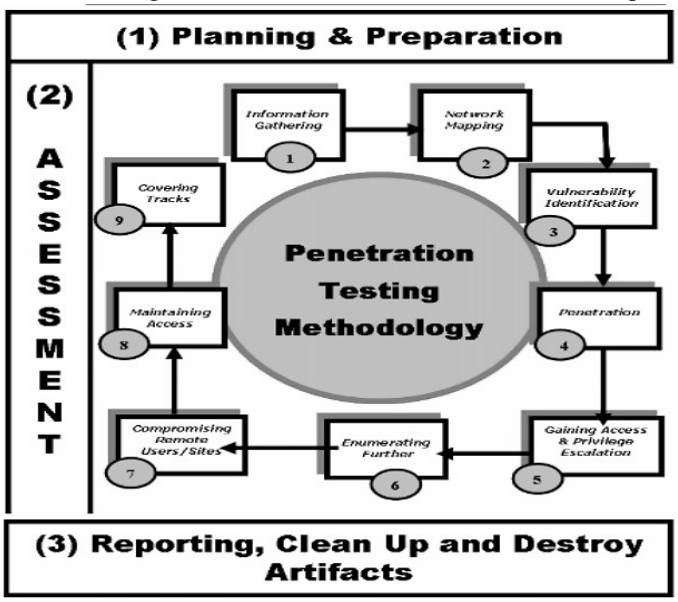

Fig. 1 ISSAF Methodology Framework

Planning And Preparation

This initial phase involves preparation and strategic planning prior to conducting penetration testing on the target web application. It includes defining the testing scope, objectives, and required tools to ensure a structured and effective assessment process.

Asesssment Phase

The assessment phase comprises several systematic steps to identify and evaluate potential vulnerabilities within the system:

- **Information Gathering:** This stage involves collecting preliminary information about the target system. The process includes identifying the Secure Socket Layer (SSL), domain information, and the Content Management System (CMS) used.
- **Network Mapping:** This step focuses on identifying the network structure and open ports by performing footprinting techniques to understand the system architecture.
- **Vulnerability Identification:** At this stage, various testing activities are conducted to detect common security vulnerabilities within the system.
- **Penetration Testing:** This phase involves simulating attacks by attempting to bypass security mechanisms in order to gain access to the system at various levels.
- **Gaining Access and Privilege Escalation:** In this step, the tester attempts to exploit identified vulnerabilities to obtain higher-level access privileges within the system.
- **Enumerating Further:** This stage aims to gather more detailed and specific information after initial access has been achieved, which helps in identifying deeper security weaknesses.
- **Compromise Remote User/Sites:** This phase involves exploiting vulnerabilities to gain broader access to the system remotely, enabling further exploration and control.

Brilliance
Research of Artificial Intelligence

E-ISSN : 2807-9035
Volume 5, **Number** 2, November 2025
https://doi.org/10.47709/brilliance.v5i2.6780

- **Maintaining Access:** At this stage, the tester attempts to maintain persistent access to the system, typically by deploying backdoors or similar mechanisms.
- **Covering the Track:** This final step in the assessment phase involves removing logs and traces of the testing activities to avoid detection.

Reporting, Clean Up, And Destroy Artifacts Phase

This final phase involves documenting the results of the penetration testing, including identified vulnerabilities and recommended mitigation strategies. Additionally, all testing artifacts, logs, and tools used during the assessment are removed to ensure system integrity.

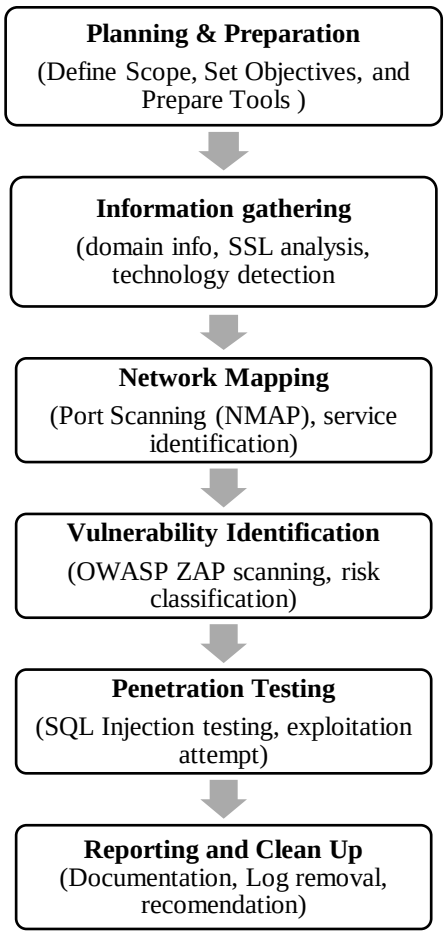

Fig. 2 Research stage using ISSAF Framework

RESULT

Planning And Preparation Phase

This phase involves defining the scope, objectives, and timeline of the security testing process. The primary objective of this study is to minimize potential risks arising from database security vulnerabilities in the E-Kinerja website of North Aceh Regency. The scope of this assessment focuses on the target website: https://ekin.acehutara.go.id/.

IP Modification (IP Spoofing):

The primary purpose of IP spoofing is to enhance anonymity during testing activities, avoid detection by the target system, bypass security restrictions, and simulate real-world attack scenarios. This approach allows the tester to evaluate how the system responds to potentially malicious traffic originating from unrecognized sources.

Brilliance
Research of Artificial Intelligence

E-ISSN : 2807-9035
Volume 5, **Number** 2, November 2025
https://doi.org/10.47709/brilliance.v5i2.6780

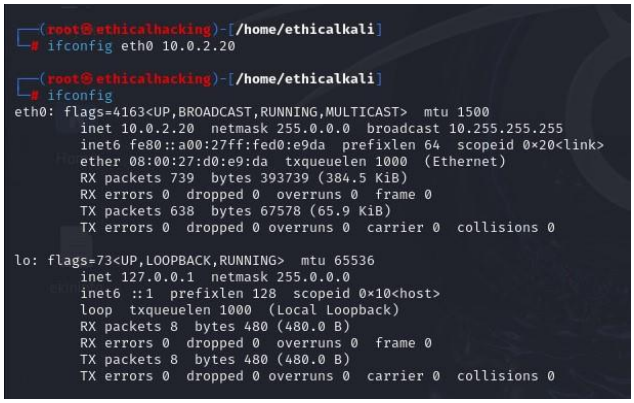

Fig. 3 IP Spoofing

MAC Address Modification:

The Media Access Control (MAC) address is a unique identifier assigned to network hardware devices, allowing each node within a network to be distinctly recognized. It plays a crucial role in facilitating communication and data exchange between devices. In this study, MAC address modification was performed to anonymize the tester's device within the network. This technique helps reduce the likelihood of detection by the target system during penetration testing, thereby enabling a more realistic simulation of attack scenarios.

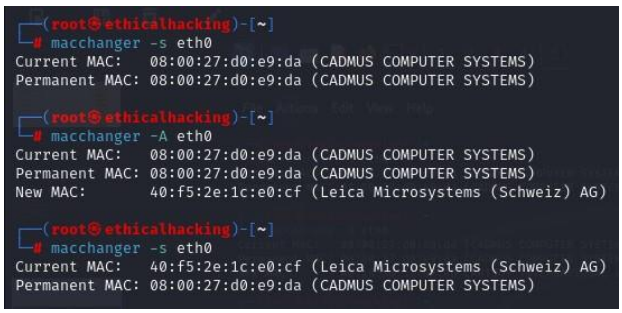

Fig. 4 MAC Address Modification

Assessment Phase

General Website Information Collection:

To obtain general information about the target website, the penetration tester utilized the *WhatWeb* tool. This tool was executed via the Kali Linux terminal using the following command:

whatweb ekin.acehutara.go.id -v

The results of this process provided key information about the target system, including its domain, server configuration, detected technologies, and HTTP headers.

Table 1. Information Gathering

Aspect	Information
URL	https://ekin.acehutara.go.id
IP Address	36.95.71.220
Country	Indonesia
Title	e-KINERJA - North Aceh Government
Detected Plugins	Apache, Bootstrap, HTML5, JQuery, Script
HTTP Headers	Server: Apache, X-Frame-Options: SAMEORIGIN

Brilliance
Research of Artificial Intelligence

E-ISSN : 2807-9035
Volume 5, **Number** 2, November 2025
https://doi.org/10.47709/brilliance.v5i2.6780

Secure Socket Layers (SSL) Analysis:

Fig. 5 SSL Scanning

Based on the SSL scanning results (see Figure 5), the E-Kinerja website utilizes TLS 1.2 and TLS 1.3 protocols, both of which are enabled. These protocols are cryptographic standards designed to secure communication between clients and web servers over the internet.

Compared to TLS 1.2, TLS 1.3 provides enhanced security and improved performance, making it the preferred standard for modern web applications. Although SSL and TLS serve similar purposes, TLS is considered a more advanced and secure version.

Further analysis (Figure 6) revealed that the website holds a valid SSL certificate issued by cPanel, Inc. Certification Authority, with a validity period from July 16, 2024, to October 14, 2024. This certificate functions as a digital identity to ensure secure communication and verify the authenticity of the website.

Fig. 6 SSL Sertificate

Network Mapping:

The network mapping phase is essential for identifying open ports and active services within the target system. In this study, the tester used the *Nmap* tool with the following command:

nmap --top-ports 20 36.95.71.220

This process revealed several open ports and associated services, as shown in Table 2.

Table 2. Information Gathering

Port	Status	Service	Function
21	open	FTP	File transfer
22	open	SSH	Secure remote access
23	open	Telnet	Remote access (unencrypted)
25	open	SMTP	Email sending
80	open	HTTP	Web access (unencrypted)
110	open	POP3	Email retrieval
139	open	netbios-ssn	File sharing
443	open	HTTPS	Secure web access
445	open	microsoft-ds	Windows file sharing
3389	open	ms-wbt-server	Remote desktop access

Vulnerability Identification:

In this phase, vulnerability scanning was performed using OWASP Zed Attack Proxy (ZAP) version 2.15.0. The scan identified a total of 17 vulnerabilities, categorized into medium, low, and informational levels.

Brilliance
Research of Artificial Intelligence

E-ISSN : 2807-9035
Volume 5, **Number** 2, November 2025
https://doi.org/10.47709/brilliance.v5i2.6780

Table 3. Vulnerability Identification Results

No.	Vulnerability	Risk Level
1.	*Absence of Anti-CSRF Tokens*	*Medium*
2.	*Content Security Policy (CSP) Header Not Set*	*Medium*
3.	*Cross-Domain Misconfiguration*	*Medium*
4.	*Vulnerable JS Library*	*Medium*
5.	*Cookie No HttpOnly Flag*	*Low*
6.	*Cookie Without Secure Flag*	*Low*
7.	*Cookie Without SameSite Attribute*	*Low*
8.	*Cross-Domain JavaScript Source File Inclusion*	*Low*
9.	*Strict-Transport-Security Header Not Set*	*Low*
10.	*Timestamp Disclosure Unix*	*Low*
11.	*X-Content-Type-Options Header Missing*	*Low*
12.	*Authentication Request Identified*	*Informational*
13.	*Charset Mismatch (Header Versus Meta Content-Type Charset)*	*Informational*
14.	*Information Disclosure – Suspicious Comments*	*Informational*
15.	*Modern Web Application*	*Informational*
16.	*Re-example Cache-control Directives*	*Informational*
17.	*Session Management Response Identified*	*Informational*

Although no critical vulnerabilities were detected, the presence of medium and low-level issues indicates areas for improvement.

Penetration Testing:

The penetration testing phase focused specifically on SQL injection vulnerabilities using the SQLMap tool. The testing was conducted with the following command:

sqlmap -u https://ekin.acehutara.go.id/ --dbs

The results of the testing can be summarized as follows:

- **No Injectable Parameters Identified** : SQLMap did not detect any GET or POST parameters that could be tested for SQL injection. As a result, further exploitation could not be performed.
- **SQL Injection Attack Failed** : The failure of the attack indicates that the system is protected by security mechanisms such as: Web Application Firewall (WAF) and Intrusion Prevention System (IPS).

These technologies effectively monitor and filter malicious traffic, preventing unauthorized access attempts to the database.

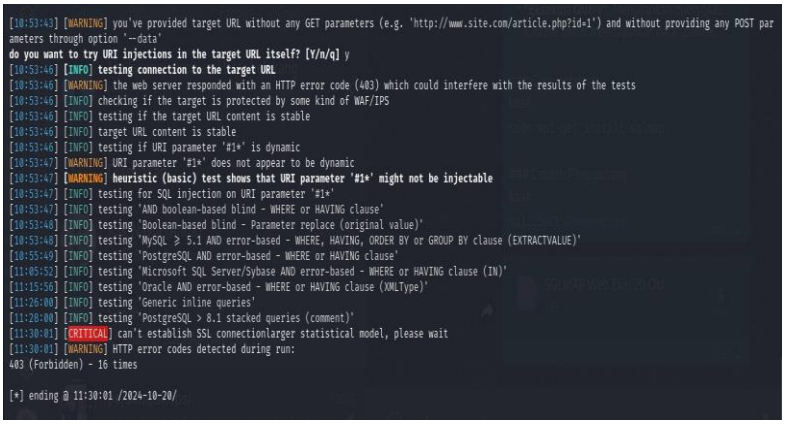

Fig. 7 Penetration Testing using SQL Map

Reporting, Clean Up, And Destroy Artifacts Phase

In the final phase, several files and logs generated during the testing process were identified. However, only relevant files used during the assessment were retained, including:

- Macchanger.log: used for MAC address modification
- GVM (Greenbone Vulnerability Management): Vulnerability scanning management
- Notus Scanner: Vulnerability detection tool

E-ISSN : 2807-9035
Volume 5, **Number** 2, November 2025
https://doi.org/10.47709/brilliance.v5i2.6780

- Inetsim: Network service simulation tool
- OpenVPN: Secure network connection
- Apache2 Logs: Web server activity analysis

After completing the analysis, unnecessary files and logs were removed to ensure system cleanliness and prevent data accumulation.

DISCUSSION

The absence of SQL injection vulnerabilities indicates that the system has implemented adequate security controls. The use of WAF and IPS provides a layered security approach, which is consistent with modern cybersecurity practices. However, the presence of medium and low-level vulnerabilities suggests that further improvements are still necessary, particularly in security configuration.

CONCLUSION

Based on the conducted testing, it can be concluded that the database of the E-Kinerja website of North Aceh Regency is not vulnerable to SQL injection attacks. The penetration testing process could not proceed beyond the initial testing stage, as no exploitable entry points were identified. Consequently, advanced stages such as gaining access, privilege escalation, and covering tracks could not be performed.

This outcome is attributed to the effective implementation of security mechanisms, particularly the Web Application Firewall (WAF) and Intrusion Prevention System (IPS). These systems function synergistically to detect and block malicious activities, including SQL injection attempts, thereby preventing unauthorized access to the database.

Overall, the integration of WAF and IPS significantly enhances the security posture of the web application, ensuring data protection and system reliability against common cyber threats.

REFERENCES

Abdul Gafur, dan. (2023). PENERAPAN SISTEM KINERJA BERBASIS E-KINERJA PADA PEMERINTAHAN KOTA BEKASI IMPLEMENTATION OF E-KINERJA BASED PERFORMANCE SYSTEM ASSESSMENT IN BEKASI CITY GOVERNMENT. *Jurnal Administrasi Negara*, *29*(1).

Akhlia, Y. H. (2025). ISSAF-based penetration testing on e-commerce systems.

Alenezi, M., et al. (2021). Web application security vulnerabilities and prevention techniques. *Journal of Cyber Security Technology*, 5(2), 45–60.

Annas, M., Adek, R. T., & Afrillia, Y. (2024). Web application firewall design for cyber attack prevention.

Fitria, R. (2020). The Attacking Methods Involved in Current Trend Environment. *Jurnal Teknologi Terapan Sains 4.0*, 2(1)

Gusty, R. et al. (n.d.). Penerapan Sistem Informasi Sumber Daya Manusia Pada Program E. In *Jurnal Administrasi Politik dan Sosial* (Vol. 1). Retrieved from https://japs.ejournal.unri.ac.id/index.php/JAPS

Kumar, R., Singh, P., & Sharma, V. (2022). Intrusion prevention systems: A comprehensive study. International Journal of Network Security, 24(1), 12–25.

Nazaruddin, I. F. (2024). Security analysis of e-ticketing systems using ISSAF

Nisa, F., Nurfebruary, N. S., & Ikhwani, M. (2024). Analysis of academic portal website security using OWASP ZAP. *Jurnal Nasional Komputasi dan Teknologi Informasi*, 7(6)

Pratama, Y., et al. (2021). Cybersecurity awareness in government systems. *Journal of Digital Governance*, 3(1), 10–18.

Putra, R., et al. (2023). Penetration testing in public sector applications. *Indonesian Journal of Information Systems*, 8(2), 99–110.

Rahman, M., et al. (2022). Black-box penetration testing approach for web applications. IEEE Access, 10, 112233–112245.

Singh, A., & Sharma, K. (2021). Web application firewall effectiveness in cyber defense. Journal of Information Security, 12(3), 150–162.

Umar, R., Riadi, I., & Ihya, M. (2023). ISSAF framework for information system security assessment. Jurnal Teknologi Informasi, 12(1), 280–292.

Wibowo, A., et al. (2024). Security analysis of web applications using ISSAF. Journal of Information Systems Research, 15(1), 22–35.