Journal of Artificial Intelligence and Engineering Applications

Website: https://ioinformatic.org/

15th October 2025. Vol. 5. No. 1; e-ISSN: 2808-4519

Security Analysis of the Silaturahmi UPN Jatim Website Based on the OWASP Top 10

Muhammad Rakha Naufal[1]*, Hilmi Arya Rafwa Muhammad[2], Muhammad Firza Pahlevi[3], Rafie Ahza Ghaisan[4], Agung Brastama Putra[5], Siti Mukaromah[6]

[1,2,3,4,5,6]Information Systems, Faculty of Computer Science, UPN "Veteran" Jawa Timur
22082010060@student.upnjatim.ac.id[1], 22082010061@student.upnjatim.ac.id[2], 22082010094@student.upnjatim.ac.id[3], 22082010192@student.upnjatim.ac.id[4], agungbp.si@upnjatim.ac.id[5], sitimukaromah.si@upnjatim.ac.id[6]*

Abstract

The Silaturahmi UPN Jatim website was developed to support academic services by facilitating course conversion for students involved in independent study and internship programs. However, as a web-based academic system, it faces potential cybersecurity threats such as SQL Injection, Cross-Site Scripting (XSS), and session hijacking—risks that continue to increase globally. This study aims to evaluate the website's security using the OWASP Top 10 framework to identify vulnerabilities and assess associated risks. A qualitative descriptive method was used, with data collected through manual inspection of the website's structure and behavior. Vulnerability classification and risk assessment were conducted based on OWASP Risk Rating and CVSS scores. The results identified 15 security issues, including a high-risk vulnerability related to cryptographic data exposure and several misconfigured security headers. The findings emphasize the need for improved security practices in academic systems. Recommendations are provided to enhance the site's protection, ensuring better compliance with modern security standards and strengthening digital trust within UPN Jatim's academic environment.

Keywords: *Web Security, OWASP Top 10, Vulnerability Assessment, Academic Information System, Cybersecurity*

1. Introduction

The rapid development of information technology has driven educational institutions to undergo digital transformation, including in facilitating communication and interaction among academic communities through online media. One such implementation is the Silaturahmi UPN Jatim website, which serves as a platform to assist students participating in independent study or internship programs in converting their academic credits based on related activities. However, the existence of institutional websites like this also poses security risks, especially with the increasing prevalence of cyberattacks such as SQL Injection, Cross-Site Scripting (XSS), and session hijacking, which continue to rise globally [1][2].

According to data from Indonesia's National Cyber and Crypto Agency (BSSN), there were more than 12 million incidents targeting web applications in Indonesia over the past year [1]. These attacks not only cause technical losses but also potentially undermine public trust in government institutions. The lack of skilled human resources in security testing and the absence of systematic risk assessment processes make many government websites vulnerable to attacks [2][3].

To address these challenges, a comprehensive and structured evaluation of information system security is essential. One effective approach is the Open Web Application Security Project (OWASP) methodology, which provides a list of the 10 most common web vulnerabilities (OWASP Top 10) [4]. This framework is particularly useful for identifying vulnerability types frequently found in modern web applications.

As part of the digital academic service system, the Silaturahmi UPN Jatim website plays a strategic role in supporting the "Kampus Merdeka" (Independent Campus) policy, particularly in the academic credit conversion process for independent studies and internships. This website stores and processes critical data related to students and other academic activities, thus requiring compliance with adequate security standards. However, until now, there has been no official or public report regarding penetration testing or vulnerability analysis on the website. Therefore, a security evaluation based on a structured and industry-standard approach is necessary to ensure the system is protected from potential cyber threats.

This study conducts a security analysis of the Silaturahmi UPN Jatim website using the OWASP Top 10 framework to identify potential vulnerabilities, assess risk levels, and provide necessary recommendations for improvement. The results of this research are expected to contribute significantly to enhancing the security and reliability of digital services at UPN Jatim.

2. Research Methodology

2.1. Research Approach

This study employs a descriptive qualitative approach to describe the security condition of the UPNVJT Silaturahmi website based on actual findings from technical observations. This approach was selected to enable a comprehensive exploration of potential vulnerabilities without the need for active exploitation or full-scale attack simulation. A similar approach was used by Farismana & Pramadhana (2023) in their evaluation of information system security through a non-exploitative analysis [5], as well as by Cunong et al. (2020) in their risk assessment of government systems [6].

2.2. Data Collection Techniques

Data were collected through direct manual observation (manual inspection) of various pages on the UPNVJT Silaturahmi website. Observations were conducted using the inspect element feature in the browser to examine the HTML structure, HTTP headers, JavaScript scripts, and system interactions when users engage with the website. Elements observed included, but were not limited to:

1. Absence of security headers such as Content-Security-Policy, X-Frame-Options, and X-Content-Type-Options.
2. Presence of hashes, server information, or response timestamps.
3. Disclosure of code comments in client-side scripts.
4. Login structures and forms that lack additional protection.

Tools such as Google Dorks, Nmap, or automated scanners were not used. The data collection technique reflects widely accepted manual inspection methods, especially those outlined by Farismana & Pramadhana (2023) [5]. The literature used refers to OWASP Top 10 (2021) documentation, as well as prior studies relevant to the education and government sectors [5][6][7].

2.3. Vulnerability Analysis and Classification

The results from the observation process were mapped into the OWASP Top 10 categories, which represent the 10 most common and critical vulnerabilities found in web applications. Categories most frequently encountered in this study include, but are not limited to:

1. A02: Cryptographic Failures
2. A05: Security Misconfiguration
3. A06: Vulnerable and Outdated Components
4. A07: Identification and Authentication Failures

This classification approach follows the OWASP methodology and was also used in the study by Farismana & Pramadhana (2023) in the process of mapping vulnerabilities to OWASP standards [5].

2.4. Vulnerability Analysis and Classification

Each identified vulnerability was assessed for risk level using two main approaches:

1. **OWASP Risk Rating Methodology**, which evaluates risk based on the likelihood of exploitation and the potential impact of the vulnerability, producing risk classifications of low, medium, or high [6].
2. **CVSS (Common Vulnerability Scoring System)**, which provides numerical scores based on three aspects: exploitability, impact, and scope.

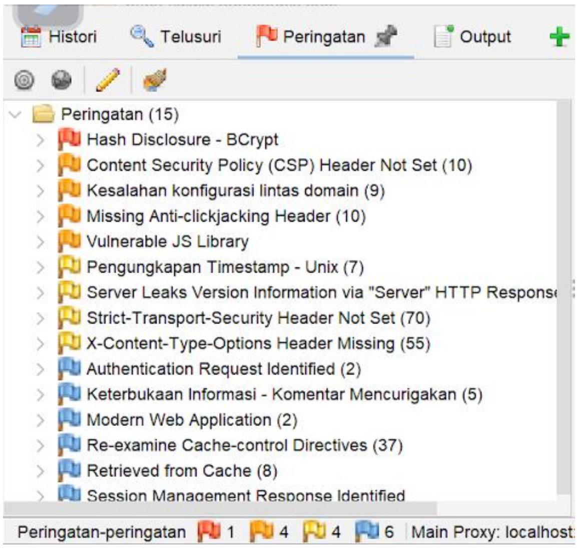
This approach allows for objective and quantitative risk assessments even without the use of automated tools.

2.5. Vulnerability Analysis and Classification

Following the classification and risk evaluation process, findings were compiled into tabular form containing information such as the vulnerability name, OWASP category, CVSS score, likelihood of threat occurrence, and finding status (found/not found). The findings were compiled manually to provide an in-depth overview of the website's security posture. This model of result compilation was also applied in the study by Farismana & Pramadhana (2023), which produced security findings tables in risk classification format to support recommendation formulation [5].

3. Results and Discussion

Based on the assessment results using OWASP ZAP, a total of 15 vulnerabilities were found on the Silaturahmi UPN Jatim website, each with varying severity levels. From these findings, 1 vulnerability was identified as high severity, 4 as medium severity, 4 as low severity, and 6 were classified as informational. These results indicate that the website still contains several security gaps that require attention, especially those with high severity levels. The types of threats detected can be seen in the image below:



Peringatan (15)

- Hash Disclosure - BCrypt
- Content Security Policy (CSP) Header Not Set (10)
- Kesalahan konfigurasi lintas domain (9)
- Missing Anti-clickjacking Header (10)
- Vulnerable JS Library
- Pengungkapan Timestamp - Unix (7)
- Server Leaks Version Information via "Server" HTTP Respons
- Strict-Transport-Security Header Not Set (70)
- X-Content-Type-Options Header Missing (55)
- Authentication Request Identified (2)
- Keterbukaan Informasi - Komentar Mencurigakan (5)
- Modern Web Application (2)
- Re-examine Cache-control Directives (37)
- Retrieved from Cache (8)
- Session Management Response Identified

Peringatan-peringatan 1 4 4 6 Main Proxy: localhost:

Fig. 1: OWASP ZAP Scan Result

Based on Figure 1, several security threats were detected and classified by OWASP ZAP. Each threat is marked with a colored flag icon indicating its severity or priority level. Red indicates high severity or critical vulnerabilities that need immediate attention, yellow for medium-risk vulnerabilities that should not be ignored, and blue for informational threats that carry low risk but still require monitoring. This classification helps in prioritizing mitigation efforts, ensuring that security management can be carried out more effectively. The classification according to the severity level of vulnerabilities can be seen in the table below:

Table 1: Results of Vulnerability Analysis Detected by OWASP ZAP

No	Vulnerability Name	Severity Level
1	Hash Disclosure - Bcrypt	High
2	Content Security Policy (CSP) Header Not Set	Medium
3	Cross-Domain Misconfiguration	Medium
4	Missing Anti-clickjacking Header	Medium
5	Vulnerable JavaScript Library	Medium
6	Unix Timestamp Disclosure	Low
7	Server Leaks Version Information via “Server” HTTP Header Field	Low
8	Strict-Transport-Security Header Not Set	Low
9	X-Content-Type-Options Header Missing	Low
10	Authentication Request Identified	Informational
11	Information Disclosure - Suspicious Comments	Informational
12	Modern Web Application Detected	Informational
13	Re-examine Cache-Control Directives	Informational
14	Retrieved from Cache	Informational
15	Session Management Response Identified	Informational

Based on the security analysis of the Silaturahmi UPN Jatim website, several potential threats were found and categorized according to the OWASP Top 10 standard, a list of the ten most common and dangerous web application security risks according to the Open Web Application Security Project (OWASP). The identification of these threats aims to provide a deeper understanding of system vulnerabilities and to provide recommendations that can be implemented to improve website security. The table above summarizes various detected threats along with their OWASP Top 10 category, explanations, and suggested mitigation steps.

Table 2: Threat Mapping Based on OWASP Top 10

No	Threat	OWASP Top 10 Category	Explanation	Recommendation
1	Hash Disclosure - Bcrypt	A02 - Cryptographic Failures	Hash of user password is exposed and at risk of brute-force attacks	Do not display password hashes on the web page or in public
2	Missing CSP Header	A05 - Security Misconfiguration	Missing Content-Security-Policy header; prone to XSS and unsafe content	Add a Content-Security-Policy header
3	Missing Anti-clickjacking Header	A05 - Security Misconfiguration	Missing X-Frame-Options header; prone to clickjacking attacks	Add X-Frame-Options: DENY or SAMEORIGIN
4	Server Leaks Version Info via HTTP Header	A05 - Security Misconfiguration	Reveals the type and version of server software	Hide or remove the server version header
5	X-Content-Type-Options Header Missing	A05 - Security Misconfiguration	MIME sniffing can occur if this header is not set	Add the header: X-Content-Type-Options: nosniff
6	Authentication Request Identified	A07 - Identification & Authentication Failures	Login endpoints detected; potentially vulnerable to brute-force attacks	User rate limiting, CAPTCHA, and HTTPS
7	Session Management Response Identified	A07 - Identification & Authentication Failures	Session ID was detected in the response	User secure tokens and encrypt them
8	Vulnerable JS Library	A06 - Vulnerable and Outdated Components	Outdated JavaScripts library is in use	Replace with the latest secure version

9	Re-examine Cache-Control Directives	A05 -Security Misconfiguration	Headers not properly set; may cause data leakage	Add Cache-Control: no-store directives
10	Modern Web Application Detected (informational)	-	Indicator that the site uses a modern dynamic framework	No action required, informational only
11	Suspicious Comment Disclosure (suspected source)	A05 -Security Misconfiguration	Code comments contain internal info (usernames/API keys/etc)	Remove suspicious or sensitive code comments
12	Unix Timestamp Disclosure	A05 -Security Misconfiguration	Unix timestamps detected that could aid attackers in reconnaissance	Avoid disclosing timestamp information to the client-side

Based on the scanning results using OWASP ZAP on the Silaturahmi UPN Jatim website, several vulnerabilities were identified and categorized under the OWASP Top 10. The most dominant findings were Security Misconfiguration, Cryptographic Failures, Vulnerable Components, and Authentication Failures. These four categories occupy a crucial position in the OWASP list as they represent the main entry points for cyberattacks that threaten the integrity and confidentiality of information.

One common finding was the absence of important security headers such as Content-Security-Policy, X-Content-Type-Options, and X-Frame-Options, which indicate a Security Misconfiguration issue. The lack of these headers makes the application more vulnerable to Cross-site Scripting (XSS) and Clickjacking attacks. In addition, exposed information such as Bcrypt hashes and session IDs in HTTP responses also suggest Cryptographic Failures and Session Management Issues that must be addressed immediately.

Other findings include the use of vulnerable JavaScript libraries and suspicious comments in the code, both of which fall under the Vulnerable and Outdated Components category. These findings emphasize the importance of regular maintenance in digital assets, including periodic updates and the removal of sensitive information in public code. Some detected login endpoints indicate potential Authentication Weaknesses, particularly if they are not equipped with additional protections such as CAPTCHA or rate limiting.

To support this analysis, the security testing was conducted using the OWASP ZAP (Zed Attack Proxy) tool which maps threats based on OWASP Top 10 categories. This method is used to identify vulnerabilities that frequently occur on a website, based on severity (CVSS Score), frequency of occurrence, and system status. The results of this scan provide a clearer picture of the actual state of a website's security. The following is a summary of the detected security threats based on OWASP ZAP scanning:

Table 3: List of Security Threats Based on OWASP ZAP Method (Top 10)

No	Threat	CVSS Score	Frequency of Occurrence	Status
1	Broken Authentication	7.0	74%	Detected
2	Cryptographic Failures	7.4	28%	Detected
3	Injection (XXS, SQLi)	6.0	60%	Not Detected
4	Security Misonfiguration	6.0	73%	Detected
5	Vulnerable and Outdated Components	6.5	28%	Detected
6	Broken Access Control	6.0	55%	Not Detected
7	Identification & Authentication Failures	7.0	60%	Detected
8	Softwares and Data Integrity Failures	5.5	20%	Not Detected
9	Security Logging & Monitoring Failures	4.0	2%	Not Detected
10	Server-Side Request Forgery (SSRF)	4.5	2%	Not Detected

From the results of this scan, it can be concluded that several serious threats such as Broken Authentication and Security Misconfiguration were detected and carry a high CVSS score, thus requiring immediate attention. Meanwhile, some threats such as Injection and Broken Access Control were not detected in this study, but still need to be considered and periodically tested as they are generally classified as high-risk with fairly high occurrence rates. These findings are important considerations in formulating appropriate remediation steps and improving overall web application security.

4. Conclusion

Based on the security analysis of the Silaturahmi UPN Jatim website using the OWASP Top 10 approach and the OWASP ZAP tool, several vulnerabilities with serious exploitation potential were identified. The main vulnerabilities identified include Hash Disclosure (A02: Cryptographic Failures), the absence of important security headers such as Content-Security-Policy and X-Frame-Options (A05: Security Misconfiguration), and weaknesses in authentication and session management mechanisms (A07: Identification & Authentication Failures). Several findings had high CVSS scores and fell into high-risk categories with frequent occurrences, such as Broken Authentication and Security Misconfiguration, indicating that the system has not yet met standard web application security requirements.

To mitigate risks and enhance system resilience against cyberattacks, several corrective actions must be implemented promptly. These include removing sensitive information such as hash and session IDs from responses, adding standard security headers, and applying more secure authentication mechanisms such as CAPTCHA and two-factor authentication. In addition, updating external components, implementing security by design principles, and conducting periodic audits and monitoring using tools such as OWASP ZAP are strongly recommended.

The implementation of these measures is expected to strengthen the security foundation of the Silaturahmi UPN Jatim website and increase user trust in the digital academic services provided.

References

[1] M. S. S. Wardaya, "Penetration Testing terhadap Website Asosiasi Pekerja Professional Informasi Sekolah Indonesia (APISI)," J. Kajian Pendidikan Ekonomi dan Ilmu Ekonomi, vol. 2, no. 1, pp. 1–19, 2019. [Online]. Available: https://www.scopus.com/inward/record.url?eid=2-s2.0-84886507390&partnerID=ZDt0x3y1

[2] Mabes TNI Angkatan Laut, "Keamanan Siber Indonesia Berada di 3 Posisi Terbawah di Antara Negara G20," Naval-CSIRT, 2022. [Online]. Available: https://naval-csirt.tnial.mil.id/keamanan-siber-indonesia-peringkat-ke-3-terbawah-di-antara-negara-negara-g20

[3] A. Bastian, H. Sujadi, and L. Abror, "Analisis Keamanan Aplikasi Data Pokok Pendidikan (Dapodik) Menggunakan Penetration Testing dan SQL Injection," INFOTECH J., vol. 6, no. 2, pp. 65–70, 2020.

[4] H. Setiawan, L. E. Erlangga, S. Siddiq, and Y. A. Gunawan, "Analisis Kerawanan pada Aplikasi Website Menggunakan Standar OWASP Top 10 untuk Penilaian Risk Rating," Info Kripto, vol. 17, no. 1, pp. 15–21, 2023, doi: 10.56706/ik.v17i1.64.

[5] R. Farismana and D. Pramadhana, "Perbandingan Vulnerability Assessment Menggunakan OWASP ZAP dan Acunetix pada Sistem Informasi Repository Politeknik Negeri Indramayu," J. Tek. Inform. dan Teknol. Informasi, vol. 3, no. 2, pp. 26–32, 2023.

[6] D. N. Cuong, M. Saputra, and W. Puspitasari, "Analisis Resiko Keamanan terhadap Website Dinas Penanaman Modal dan Pelayanan Terpadu Satu Pintu Pemerintahan XYZZY Menggunakan Standar Penetration Testing Execution Standard (PTES)," e-Proceeding Eng., vol. 7, no. 1, pp. 2090–2095, 2020.

[7] T. S. Revolino and D. J. Andri, "Analisis Perbandingan Metode Web Security PTES, ISSAF, dan OWASP di Dinas Komunikasi dan Informasi Kota Bandung," Prosiding SoBAT, vol. 1, no. 1, 2019.