Jurnal Komputer Antartika
Volume 4 Nomor 2 2026 Halaman 99-105
ISSN (Online) 2988-5272
DOI: https://doi.org/10.70052/jka.v4i2.1370

Analisis Kerentanan Keamanan Website Sekolah Menggunakan Metode Vulnerability Assessment Berbasis OWASP ZAP

Nur Fadhillatur Rahmadayanti[1], Muhlis Tahir[2], Ayu Sanusih[3]

[1,2,3] Universitas Trunojoyo Madura
Jl. Raya Telang, PO BOX 2, Kecamatan Kamal, Kabupaten Bangkalan, Madura, Indonesia

e-mail korespondensi: ayusanusih25@gmail.com

Submit: 22-05-2026 | Revisi: 10-06-2026 | Terima: 20-06-2026 | Terbit online: 10-07-2026

Abstrak
Perkembangan teknologi informasi yang pesat telah mendorong pemanfaatan website dalam berbagai sektor, termasuk pada lingkungan pendidikan sebagai media penyampaian informasi dan layanan akademik. Website sekolah berperan penting dalam pengelolaan data dan akses informasi secara daring, namun juga rentan terhadap berbagai ancaman keamanan siber. Oleh karena itu, diperlukan pengujian keamanan secara terstruktur untuk mengidentifikasi celah yang berpotensi disalahgunakan. Penelitian ini bertujuan untuk menganalisis tingkat kerentanan keamanan pada website sekolah menggunakan metode vulnerability assessment berbasis OWASP. Proses pengujian dilakukan dengan memanfaatkan tools OWASP ZAP sebagai vulnerability scanner melalui tahapan scanning, analisis kerentanan, dan pelaporan hasil berdasarkan standar OWASP Top 10. Hasil pengujian menunjukkan ditemukan 1 kerentanan kategori high, 8 kerentanan kategori medium, dan 6 kerentanan kategori low yang menunjukkan masih terdapat celah keamanan pada website yang perlu segera diperbaiki. Oleh karena itu, diperlukan tindakan mitigasi melalui validasi input, peningkatan kontrol akses, serta konfigurasi keamanan server guna meningkatkan keamanan sistem secara keseluruhan.

Kata Kunci : Keamanan website, Vulnerability assessment, OWASP ZAP, Kerentanan

Abstract
The rapid development of information technology has encouraged the utilization of websites in various sectors, including the educational environment as a medium for delivering information and academic services. School websites play an important role in managing data and providing online access to information; however, they are also vulnerable to various cybersecurity threats. Therefore, structured security testing is required to identify potential vulnerabilities that could be exploited. This study aims to analyze the level of security vulnerabilities in a school website using an OWASP-based vulnerability assessment method. The testing process was conducted using the OWASP ZAP tool as a vulnerability scanner through several stages, including scanning, vulnerability analysis, and reporting based on the OWASP Top 10 standard. The results of the testing showed that there was 1 high-risk vulnerability, 8 medium-risk vulnerabilities, and 6 low-risk vulnerabilities, indicating that the website still contains security gaps that need immediate attention. Therefore, mitigation efforts are required through input validation, improved access control, and proper server security configuration to enhance the overall security of the system.

Keywords : Website security, Vulnerability assessment, OWASP ZAP, Vulnerabilities

1. Pendahuluan

Perkembangan teknologi informasi yang sangat pesat telah membawa berbagai perubahan signifikan dalam kehidupan manusia, khususnya dalam bidang pendidikan. Salah satu bentuk pemanfaatan teknologi tersebut adalah penggunaan sistem informasi berbasis website sebagai media penyampaian informasi dan layanan digital. Website menjadi sarana yang efektif dalam mendukung aktivitas akademik, seperti penyampaian informasi sekolah, pengelolaan data siswa, serta layanan administrasi secara daring [1]. Website sekolah memiliki peran penting dalam meningkatkan efisiensi dan efektivitas penyebaran informasi kepada masyarakat luas. Dengan adanya sistem berbasis web, pengguna dapat mengakses informasi kapan saja dan di mana saja tanpa terbatas oleh ruang dan waktu [2]. Namun, di balik kemudahan tersebut, penggunaan website juga menimbulkan berbagai risiko, terutama yang berkaitan dengan aspek keamanan sistem informasi.

Keamanan sistem informasi merupakan suatu upaya untuk melindungi data dan sistem dari ancaman yang dapat merusak, mencuri, atau memanipulasi informasi yang ada [3]. Seiring dengan meningkatnya perkembangan teknologi, ancaman terhadap keamanan sistem juga semakin kompleks dan beragam. Beberapa jenis serangan yang

sering terjadi pada website antara lain *Cross-Site Scripting (XSS)*, *SQL Injection*, serta kesalahan konfigurasi keamanan (*security misconfiguration*) [4].

Ancaman keamanan pada website menjadi permasalahan serius yang dapat berdampak pada kebocoran data, perubahan informasi, hingga terganggunya layanan sistem. Berdasarkan laporan keamanan siber di Indonesia, terjadi peningkatan jumlah serangan siber yang menargetkan sistem berbasis web, termasuk pada sektor pendidikan [5]. Hal ini menunjukkan bahwa masih banyak sistem yang memiliki celah keamanan akibat kurangnya pengujian dan evaluasi secara berkala. Oleh karena itu, diperlukan suatu metode yang dapat digunakan untuk mengidentifikasi dan menganalisis kerentanan pada sistem website. Salah satu pendekatan yang dapat digunakan adalah vulnerability assessment, yaitu proses sistematis untuk menemukan, mengklasifikasikan, dan mengevaluasi kerentanan dalam suatu sistem [6]. Beberapa penelitian sebelumnya menunjukkan bahwa metode vulnerability assessment berbasis OWASP ZAP efektif digunakan untuk mengidentifikasi celah keamanan pada website dan membantu proses mitigasi risiko keamanan [8], [9], [13]. Pendekatan ini memungkinkan pengelola sistem untuk mengetahui tingkat keamanan serta menentukan langkah mitigasi yang tepat.

Dalam penelitian ini, metode yang digunakan adalah pendekatan berbasis *Open Web Application Security Project* (OWASP), yang merupakan standar dalam pengujian keamanan aplikasi web. OWASP menyediakan panduan berupa *OWASP Top 10* yang berisi daftar kerentanan paling umum pada aplikasi web. Proses pengujian dilakukan menggunakan tools *OWASP Zed Attack Proxy (ZAP)* sebagai *vulnerability scanner* untuk mendeteksi celah keamanan pada website sekolah yang menjadi objek penelitian [7]. Penelitian yang dilakukan oleh Ariyanto [10] menunjukkan bahwa penggunaan OWASP ZAP dalam pengujian keamanan website mampu mengidentifikasi berbagai kerentanan yang berpotensi membahayakan sistem. Hasil penelitian Saputra dan Pratama [13] juga menunjukkan bahwa website sekolah masih rentan terhadap berbagai ancaman keamanan sehingga diperlukan evaluasi keamanan secara berkala. Berdasarkan permasalahan tersebut, penelitian ini bertujuan untuk menganalisis dan mengidentifikasi kerentanan keamanan pada website sekolah menggunakan metode *vulnerability assessment* berbasis OWASP, serta memberikan rekomendasi perbaikan guna meningkatkan keamanan sistem.

Berdasarkan permasalahan tersebut, penelitian ini bertujuan untuk menganalisis dan mengidentifikasi kerentanan keamanan pada website sekolah menggunakan metode *vulnerability assessment* berbasis OWASP, serta memberikan rekomendasi perbaikan guna meningkatkan keamanan sistem. Dengan adanya penelitian ini, diharapkan dapat membantu pengelola website dalam memahami tingkat keamanan sistem dan meminimalisir risiko serangan siber.

2. Metode Penelitian

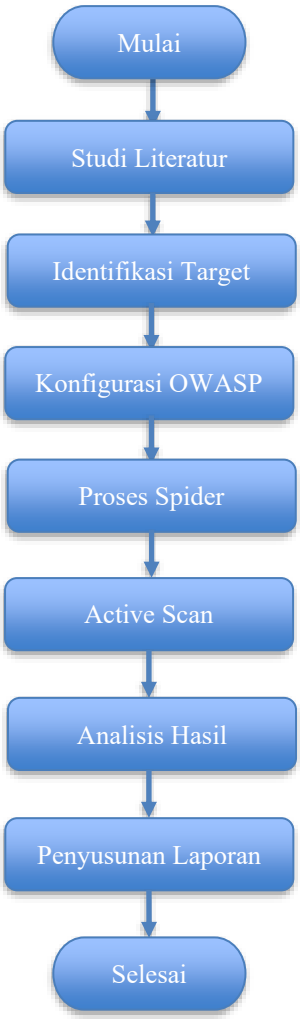
Penelitian ini menggunakan metode *Vulnerability Assessment* untuk mengidentifikasi tingkat keamanan website berdasarkan kerentanan yang ditemukan selama proses pengujian. Metode ini dilakukan dengan memanfaatkan tools OWASP ZAP sebagai alat bantu dalam mendeteksi celah keamanan pada aplikasi web. Penggunaan metode *Vulnerability Assessment* bertujuan untuk mengetahui jenis kerentanan yang terdapat pada website serta tingkat risiko yang ditimbulkan terhadap keamanan sistem.

Pada Gambar 1, proses penelitian dilakukan secara bertahap dimulai dari studi literatur, identifikasi website target, konfigurasi lingkungan pengujian, proses scanning menggunakan OWASP ZAP, hingga analisis hasil kerentanan yang ditemukan. Pengujian dilakukan menggunakan sistem operasi Debian yang dijalankan melalui VirtualBox dengan bantuan browser Mozilla Firefox untuk mengakses website target.

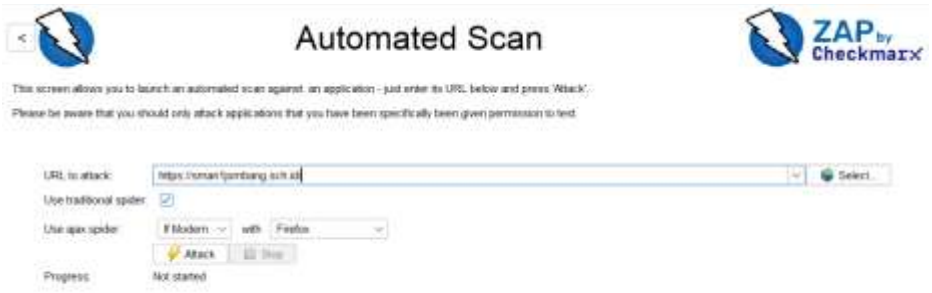
Tahap studi literatur dilakukan dengan mengumpulkan berbagai referensi yang berkaitan dengan keamanan website, *penetration testing*, *vulnerability assessment*, serta penggunaan OWASP ZAP dalam proses pengujian keamanan aplikasi web. Referensi diperoleh dari jurnal ilmiah, buku, artikel penelitian, dan sumber lainnya yang relevan dengan topik penelitian. Studi literatur bertujuan untuk memahami konsep dasar keamanan website, jenis-jenis kerentanan yang umum ditemukan pada aplikasi web, serta metode yang digunakan dalam proses identifikasi kerentanan. Selain itu, tahap ini juga digunakan sebagai dasar dalam menentukan alur penelitian dan teknik pengujian yang akan diterapkan. Selain itu, konsep rekayasa perangkat lunak dan pengembangan sistem yang aman juga mengacu pada prinsip-prinsip yang dijelaskan oleh Pressman [11]. Tahap kedua adalah identifikasi website target untuk mengetahui struktur halaman dan mengatur konfigurasi browser agar aktivitas *request* dan *response* terbaca oleh OWASP ZAP melalui mekanisme *proxy*. Tampilan awal target dapat dilihat pada gambar 2.

Pada Gambar 2, alamat URL target dimasukkan ke dalam sistem. Pada tahap ini dilakukan pengamatan terhadap struktur halaman website, fitur yang tersedia, serta mekanisme akses yang digunakan oleh pengguna. Identifikasi dilakukan untuk mengetahui bagian-bagian website yang berpotensi memiliki kerentanan keamanan dan dapat dianalisis menggunakan OWASP ZAP. Selain itu, dilakukan juga pengaturan koneksi jaringan dan konfigurasi browser agar proses komunikasi antara browser dan website dapat dibaca oleh OWASP ZAP melalui mekanisme proxy. Proses ini bertujuan agar seluruh aktivitas request dan response yang terjadi pada website dapat dimonitor dan dianalisis selama proses scanning berlangsung. Sebelum proses scanning dilakukan, tahap awal yang perlu dilakukan yaitu melakukan konfigurasi OWASP ZAP sebagai proxy pada browser. Konfigurasi dilakukan dengan menghubungkan browser Mozilla Firefox ke alamat proxy OWASP ZAP agar seluruh aktivitas akses website dapat diteruskan melalui tools tersebut. Setelah konfigurasi berhasil dilakukan, browser akan terhubung langsung dengan OWASP ZAP sehingga setiap aktivitas request dan response pada website dapat direkam dan dianalisis. Tahap ini penting dilakukan untuk memastikan proses scanning dapat berjalan dengan

optimal serta seluruh halaman website dapat terdeteksi oleh sistem.

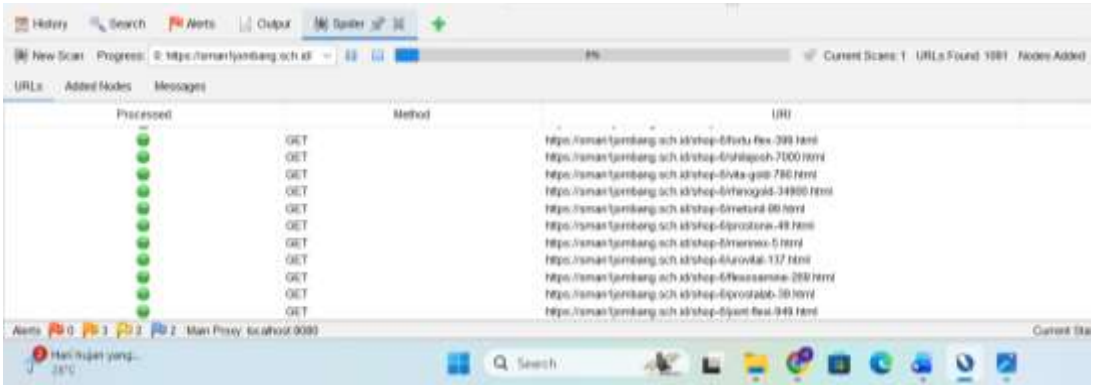


Gambar 1. Flowchart Penelitian

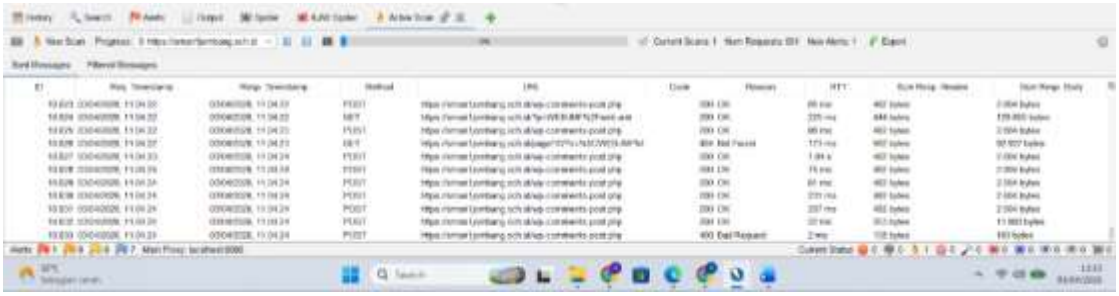


Gambar 2. Tampilan website Target

Setelah konfigurasi berhasil, dilakukan proses *scanning* menggunakan fitur *Spider* untuk memetakan seluruh tautan halaman web secara otomatis, yang dilanjutkan dengan proses *Active Scan* untuk mendeteksi celah keamanan spesifik seperti SQL Injection atau *Cross-Site Scripting* (XSS). Proses ini ditunjukkan pada Gambar 3 dan Gambar 4:



Gambar 3. Proses Spider Pada OWASP ZAP



Gambar 4. Proses Active Scan Menggunakan OWASP ZAP

Berdasarkan data pada Gambar 3 dan Gambar 4, tahap akhir yang dilakukan adalah Analisis KerentananProses scanning dilakukan menggunakan fitur *Spider* dan *Active Scan* yang tersedia pada OWASP ZAP. Tahap *Spider* digunakan untuk melakukan proses pencarian halaman website secara otomatis dengan tujuan mengidentifikasi seluruh halaman dan parameter yang dapat diakses oleh sistem. Setelah proses *Spider* selesai dilakukan, tahap selanjutnya yaitu melakukan *Active Scan* untuk mendeteksi berbagai jenis kerentanan keamanan pada website. Pada tahap *Active Scan*, OWASP ZAP akan melakukan pengujian terhadap parameter website untuk mendeteksi kemungkinan adanya celah keamanan seperti SQL Injection, Cross Site Scripting (XSS), *Security Misconfiguration*, dan kerentanan lainnya. Seluruh hasil scanning yang diperoleh kemudian direkam oleh sistem untuk dianalisis lebih lanjut pada tahap pembahasan.

Tahap analisis dilakukan dengan memeriksa hasil scanning yang diperoleh dari OWASP ZAP. Kerentanan yang ditemukan kemudian dikategorikan berdasarkan tingkat risiko yaitu *High*, *Medium*, *Low*, dan *Informational*. Proses analisis bertujuan untuk mengetahui tingkat keamanan website berdasarkan jumlah dan jenis kerentanan yang ditemukan selama proses pengujian. Analisis juga dilakukan untuk mengetahui penyebab munculnya kerentanan serta dampaknya terhadap keamanan website. Hasil analisis kemudian digunakan sebagai dasar dalam memberikan rekomendasi perbaikan terhadap sistem keamanan website.

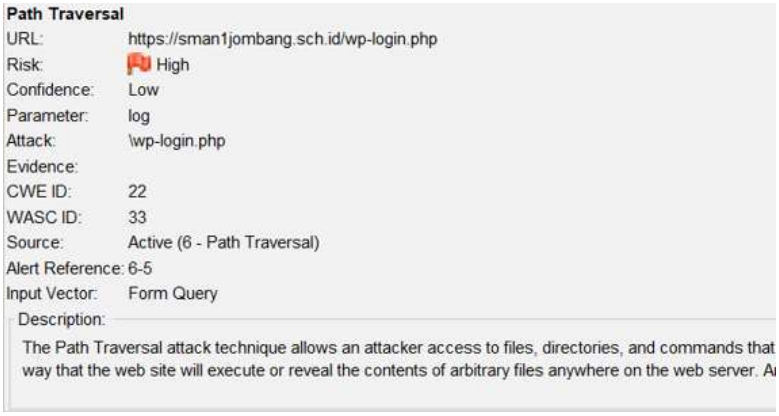
3. Hasil dan Pembahasan

3.1 Hasil Scanning Website

Proses pengujian keamanan website dilakukan menggunakan OWASP ZAP dengan metode *Vulnerability Assessment*. Pengujian dilakukan melalui proses *Spider* dan *Active Scan* untuk mendeteksi berbagai jenis kerentanan yang terdapat pada website target. Hasil scanning menunjukkan bahwa website masih memiliki beberapa kerentanan dengan tingkat risiko yang berbeda, yaitu *High*, *Medium*, dan *Low*. Kerentanan yang ditemukan menunjukkan bahwa sistem keamanan website masih memiliki beberapa celah yang dapat dimanfaatkan oleh pihak tidak bertanggung jawab apabila tidak segera dilakukan perbaikan. Hasil scanning yang diperoleh kemudian dikategorikan berdasarkan tingkat risiko kerentanan.

3.1.1 Kerentanan Kategori High

Berdasarkan hasil scanning menggunakan OWASP ZAP ditemukan beberapa kerentanan dengan tingkat risiko *High*. Kerentanan kategori ini memiliki tingkat bahaya yang tinggi karena dapat memberikan dampak serius terhadap keamanan website, seperti pencurian data, manipulasi sistem, maupun akses tidak sah oleh pihak lain. Bukti temuan kerentanan ini ditunjukkan pada Gambar 5:



Gambar 5. Hasil Kerentanan Kategori High Pada OWASP ZAP

Berdasarkan Gambar 5, jenis kerentanan *High* yang terdeteksi adalah *Path Traversal* pada parameter login. Celah ini memerlukan tindakan perbaikan konfigurasi sistem segera agar penyerang tidak dapat mengakses direktori server secara ilegal.

3.1.2 Kerentanan Kategori Medium

Hasil scanning juga menunjukkan adanya beberapa kerentanan dengan tingkat risiko *Medium*. Kerentanan kategori ini memiliki dampak sedang terhadap keamanan website, namun tetap perlu diperhatikan karena dapat berkembang menjadi ancaman yang lebih serius apabila tidak dilakukan penanganan. Salah satu contoh rekaman kerentanan tersebut diperlihatkan pada Gambar 6.

Gambar 6. Hasil Kerentanan Kategori Medium Pada OWASP ZAP

Sebagaimana tertera pada Gambar 6, kerentanan yang muncul didominasi oleh belum dikonfigurasinya *Content Security Policy* (CSP) *Header* pada website target. Perbaikan celah ini dapat dilakukan dengan mengoptimalkan konfigurasi keamanan server.

3.1.3 Keterangan Kategori Low

Selain kerentanan kategori *High* dan *Medium*, hasil scanning juga menemukan beberapa kerentanan dengan tingkat risiko *Low*. Kerentanan ini memiliki tingkat ancaman yang relatif rendah, namun tetap perlu diperhatikan untuk meningkatkan kualitas keamanan website secara keseluruhan. Seperti yang di tujukan pada gambar 7:

Gambar 7. Hasil Kerentanan Kategori Low Pasa OWASP ZAP

Gambar 7 menunjukkan adanya kerentanan *HTTPS Content Available via HTTP*. Meskipun dampaknya relatif rendah, perbaikan tetap diperlukan demi menjaga enkripsi data pengguna secara menyeluruh.

3.2 Analisis Hasil Kerentanan

Hasil scanning yang diperoleh dari OWASP ZAP kemudian dianalisis berdasarkan tingkat risiko kerentanan yang ditemukan. Analisis dilakukan untuk mengetahui tingkat keamanan website serta menentukan prioritas perbaikan terhadap kerentanan yang memiliki risiko tinggi. Adapun hasil tingkat kerentanan website dapat dilihat pada Tabel 1.

Tabel 1. Hasil Tingkat Kerentanan Website

No	Tingkat Risiko	Jumlah Kerentanan	Persentase
1.	High	1	6,67%
2.	Medium	8	53,33%
3.	Low	6	40,00%
Total		**15**	**100%**

Berdasarkan data pada Tabel 1, ditemukan sebanyak 15 celah keamanan pada website sekolah yang diuji. Berdasarkan hasil pengujian tersebut, tingkat kerentanan keamanan didominasi oleh kategori *Medium* sebesar 53,33% (8 kerentanan), diikuti oleh kategori *Low* sebesar 40,00% (6 kerentanan), dan kategori *High* sebesar 6,67% (1 kerentanan).

Meskipun kategori *High* memiliki persentase terkecil, hasil tersebut menunjukkan bahwa tetap terdapat celah keamanan dengan tingkat risiko tinggi yang sangat kritis sehingga perlu dilakukan tindakan perbaikan dan mitigasi secara segera guna menghindari eksploitasi server.

3.3 Pembahasan

Berdasarkan hasil pengujian keamanan website menggunakan OWASP ZAP, ditemukan beberapa kerentanan dengan tingkat risiko yang berbeda yaitu *High*, *Medium*, dan *Low*. Hasil tersebut menunjukkan bahwa website masih memiliki beberapa celah keamanan yang perlu diperhatikan agar tidak dimanfaatkan oleh pihak yang tidak bertanggung jawab. Temuan ini sejalan dengan penelitian Munadi [8], Yasin dan Fauzan [9], serta Saputra dan Pratama [13] yang menemukan bahwa website masih memiliki berbagai kerentanan yang dapat dimanfaatkan oleh penyerang apabila tidak dilakukan pengamanan secara berkala.

Kerentanan dengan tingkat risiko *High* ditemukan sebanyak 1 kerentanan. Kerentanan kategori ini memiliki tingkat ancaman yang tinggi karena dapat memberikan dampak serius terhadap keamanan website, seperti kebocoran data, akses tidak sah, maupun gangguan terhadap sistem website. Oleh karena itu, kerentanan kategori *High* perlu segera dilakukan perbaikan untuk meminimalkan risiko serangan siber. Menurut Whitman dan Mattord [15], keamanan informasi tidak hanya bergantung pada teknologi yang digunakan, tetapi juga pada penerapan kebijakan keamanan dan proses pemeliharaan sistem yang berkelanjutan.

Selain itu, ditemukan juga 8 kerentanan dengan tingkat risiko *Medium*. Kerentanan kategori *Medium* menunjukkan adanya kelemahan pada sistem keamanan website yang dapat memengaruhi keamanan sistem apabila tidak segera ditangani. Kerentanan ini umumnya disebabkan oleh konfigurasi keamanan yang kurang optimal, kurangnya validasi input, maupun pengaturan keamanan server yang belum maksimal.

Hasil scanning juga menunjukkan adanya 6 kerentanan dengan tingkat risiko *Low*. Meskipun memiliki tingkat ancaman yang relatif rendah, kerentanan kategori *Low* tetap perlu diperhatikan karena dapat menjadi celah tambahan yang dimanfaatkan oleh penyerang apabila digabungkan dengan kerentanan lainnya. Oleh sebab itu, perbaikan terhadap kerentanan kategori *Low* tetap diperlukan untuk meningkatkan kualitas keamanan website secara keseluruhan. Proses identifikasi ancaman dan aktivitas mencurigakan juga menjadi bagian penting dalam menjaga keamanan sistem sebagaimana dijelaskan oleh Provos dan Honeyman [12] serta Scarfone dan Mell [14] dalam penelitian terkait deteksi dan pencegahan intrusi.

Penggunaan OWASP ZAP dalam penelitian ini mampu membantu proses identifikasi kerentanan website secara otomatis dan lebih efisien. Melalui proses scanning yang dilakukan, sistem dapat memberikan informasi terkait tingkat risiko kerentanan sehingga memudahkan proses analisis keamanan website.

Berdasarkan hasil pengujian yang telah dilakukan, diperlukan beberapa upaya perbaikan untuk meningkatkan keamanan website, seperti memperbaiki konfigurasi server, meningkatkan validasi input pengguna, menggunakan protokol keamanan yang lebih baik, serta melakukan pembaruan sistem keamanan secara berkala. Dengan adanya perbaikan tersebut, diharapkan keamanan website dapat meningkat dan risiko serangan terhadap sistem dapat diminimalkan.

4. Kesimpulan

Berdasarkan hasil penelitian yang telah dilakukan menggunakan OWASP ZAP, dapat disimpulkan bahwa website yang diuji masih memiliki beberapa kerentanan keamanan dengan tingkat risiko yang berbeda, yaitu *High*, *Medium*, dan *Low*. Hasil scanning menunjukkan terdapat 1 kerentanan kategori *High*, 8 kerentanan kategori *Medium*, dan 6 kerentanan kategori *Low*. Kerentanan kategori *High* menjadi prioritas utama yang perlu segera diperbaiki karena memiliki tingkat ancaman yang tinggi terhadap keamanan website, sedangkan kerentanan kategori *Medium* dan *Low* juga perlu diperhatikan untuk meningkatkan kualitas keamanan sistem secara keseluruhan. Penggunaan OWASP ZAP dalam penelitian ini mampu membantu proses identifikasi kerentanan website secara otomatis dan efisien sehingga proses analisis keamanan website dapat dilakukan dengan lebih mudah. Oleh karena itu, diperlukan peningkatan keamanan website melalui perbaikan konfigurasi server, validasi input pengguna, penggunaan protokol keamanan yang lebih baik, serta pembaruan sistem keamanan secara berkala agar risiko serangan terhadap website dapat diminimalkan.

Referensi

[1] A. S. Rosa dan M. Shalahuddin, Rekayasa Perangkat Lunak Terstruktur dan Berorientasi Objek. Bandung: Informatika, 2018.
[2] B. Raharjo, Keamanan Sistem Informasi Berbasis Internet. Bandung: Informatika, 2019.
[3] W. Stallings, Network Security Essentials: Applications and Standards, 6th ed. Boston: Pearson, 2017.
[4] OWASP Foundation, "OWASP Top 10 Web Application Security Risks," 2021. [Online]. Available: https://owasp.org/www-project-top-ten/. [Accessed: 20-May-2026].
[5] Badan Siber dan Sandi Negara, "Laporan Tahunan Keamanan Siber Indonesia," BSSN, Jakarta, 2023.
[6] D. Stuttard dan M. Pinto, The Web Application Hacker's Handbook: Finding and Exploiting Security Flaws, 2nd ed. Indianapolis: Wiley Publishing, 2011.
[7] OWASP Foundation, "OWASP Zed Attack Proxy (ZAP)," 2024. [Online]. Available: https://www.zaproxy.org/. [Accessed: 20-May-2026].
[8] R. Munadi, "Analisis Keamanan Website Menggunakan OWASP ZAP," Jurnal Teknologi Informasi dan Komunikasi, vol. 10, no. 2, hal. 45–52, 2022. DOI: https://doi.org/10.35870/jti.v10i2.124
[9] A. Yasin dan M. Fauzan, "Implementasi Vulnerability Assessment pada Website Menggunakan OWASP," Jurnal Informatika, vol. 8, no. 1, hal. 12–20, 2021. DOI: https://doi.org/10.31311/ji.v8i1.9211
[10] S. Ariyanto, "Pengujian Keamanan Website dengan Metode Penetration Testing dan OWASP," Jurnal Ilmiah Komputer, vol. 5, no. 3, hal. 88–95, 2020. DOI: https://doi.org/10.33322/jik.v5i3.1012
[11] R. Pressman, Software Engineering: A Practitioner's Approach, 8th ed. New York: McGraw-Hill, 2015.
[12] N. Provos dan P. Honeyman, "Detecting Stealthy Portscans," in Proceedings of the 10th USENIX Security Symposium, Washington DC, USA, 2001, pp. 1–13. Available: https://www.usenix.org/conference/10th-usenix-security-symposium/detecting-stealthy-portscans
[13] A. Saputra dan E. Pratama, "Analisis Kerentanan Website Sekolah Menggunakan OWASP ZAP," Jurnal Sistem Informasi dan Teknologi, vol. 4, no. 2, hal. 101–109, 2023. DOI: https://doi.org/10.35134/jsisfotek.v4i2.210
[14] K. Scarfone dan P. Mell, "Guide to Intrusion Detection and Prevention Systems," NIST Special Publication 800-94, 2012. DOI: https://doi.org/10.6028/NIST.SP.800-94
[15] M. Whitman dan H. Mattord, Principles of Information Security, 7th ed. Boston: Cengage Learning, 2021.