Indonesian Journal of Multidisciplinary on Social and Technology
Homepage: https://journal.ilmudata.co.id/index.php/ijmst
Vol. 4 No. 3 (2026) pp: 1217-1223
P-ISSN: 2986-6790, e-ISSN: 2986-6782

Analisis Kerentanan Website MAN 2 Kebumen Terhadap Serangan Cross-site Scripting (XSS) Menggunakan Owasp ZAP

Ashfa Adlan Haqiqi[1], Fahmi Fachri[2]
[1,2] Program Studi Teknik Informatika, Fakultas Teknik, Universitas Ma'arif Nahdlatul Ulama
[1]ashfaadlan123@gmail.com , [2]fahmifachriumnu@gmail.com

Abstrak
School websites play an essential role in delivering information and academic services that are widely accessible through the internet. As the utilization of web applications continues to increase, security threats have become a major concern, particularly Cross-Site Scripting (XSS) attacks. This vulnerability occurs when a web application fails to properly validate and sanitize user input, allowing attackers to inject malicious scripts that are executed in users' browsers. This study aims to identify and analyze Cross-Site Scripting (XSS) vulnerabilities on the MAN 2 Kebumen website and to provide improvement recommendations based on web application security standards. The research employed a descriptive Vulnerability Assessment approach. Security testing was conducted using the OWASP Zed Attack Proxy (OWASP ZAP) as the vulnerability scanning tool, while the evaluation process referred to the OWASP Web Security Testing Guide (WSTG), particularly the Input Validation Testing category. The research stages consisted of problem identification, information gathering, tool configuration, website scanning, vulnerability analysis, evaluation, recommendation development, and conclusion. The results indicate that the MAN 2 Kebumen website still contains several security vulnerabilities, with the primary finding being a User Controllable HTML Element Attribute (Potential XSS) classified as a high-risk vulnerability. Verification using XSS payloads demonstrated that one of the payloads was successfully executed under specific conditions, indicating weaknesses in the website's input validation and input sanitization mechanisms. In addition, several weaknesses in the implementation of the Content Security Policy (CSP) were identified, potentially increasing the risk of successful XSS exploitation. Therefore, implementing input validation, output encoding, input sanitization, updating JavaScript libraries, and enforcing a stricter Content Security Policy are recommended to enhance the website's security against Cross-Site Scripting attacks.

Keywords: Cross-Site Scripting (XSS), Vulnerability Assessment, OWASP ZAP, OWASP WSTG, Web Security.

Abstrak
Website sekolah berperan sebagai media penyampaian informasi dan layanan akademik yang dapat diakses secara luas melalui internet. Seiring dengan meningkatnya pemanfaatan website, ancaman terhadap keamanan aplikasi web juga semakin meningkat, salah satunya adalah serangan *Cross-Site Scripting* (XSS). Kerentanan ini terjadi ketika aplikasi gagal melakukan validasi dan sanitasi input secara memadai sehingga penyerang dapat menyisipkan skrip berbahaya yang dieksekusi pada browser pengguna. Penelitian ini bertujuan untuk mengidentifikasi dan menganalisis kerentanan *Cross-Site Scripting (XSS)* pada website MAN 2 Kebumen serta memberikan rekomendasi perbaikan berdasarkan standar keamanan aplikasi web. Penelitian menggunakan metode *Vulnerability Assessment* dengan pendekatan deskriptif. Proses pengujian dilakukan menggunakan *OWASP Zed Attack Proxy (OWASP ZAP*) sebagai alat pemindaian, sedangkan evaluasi hasil mengacu pada *OWASP Web Security Testing Guide (WSTG),* khususnya kategori *Input Validation Testing*. Tahapan penelitian meliputi identifikasi masalah, *information gathering*, konfigurasi alat, pemindaian website, analisis kerentanan, evaluasi hasil, penyusunan rekomendasi perbaikan, dan penarikan kesimpulan. Hasil penelitian menunjukkan bahwa website MAN 2 Kebumen masih memiliki beberapa kerentanan keamanan, dengan temuan utama berupa *User Controllable HTML Element Attribute (Potential XSS)* yang dikategorikan berisiko tinggi. Verifikasi menggunakan payload XSS menunjukkan bahwa salah satu payload berhasil dieksekusi pada kondisi tertentu, sehingga mengindikasikan adanya kelemahan pada mekanisme validasi dan sanitasi input. Selain itu, ditemukan kelemahan konfigurasi *Content Security Policy* (CSP) yang berpotensi meningkatkan risiko eksploitasi XSS. Berdasarkan hasil tersebut, direkomendasikan penerapan validasi input, *output encoding*, sanitasi input, pembaruan pustaka JavaScript, serta konfigurasi CSP yang lebih ketat guna meningkatkan keamanan website terhadap serangan Cross-Site Scripting.

Kata Kunci: Cross-Site Scripting (XSS), Vulnerability Assessment, OWASP ZAP, OWASP WSTG, Keamanan Website

1. Pendahuluan

Perkembangan teknologi informasi telah mendorong institusi pendidikan memanfaatkan website sebagai media penyampaian informasi, layanan akademik, dan komunikasi dengan masyarakat. Seiring meningkatnya pemanfaatan website, aspek keamanan menjadi sangat penting karena website yang terhubung dengan internet rentan terhadap berbagai ancaman siber, seperti pencurian data, penyisipan kode berbahaya, dan akses tidak sah. Salah satu kerentanan yang masih sering ditemukan pada aplikasi web adalah *Cross-Site Scripting* (XSS)**,** yaitu serangan yang memanfaatkan kelemahan validasi input untuk menyisipkan *script* berbahaya yang kemudian

dieksekusi oleh browser pengguna. Serangan ini dapat menyebabkan pencurian *session cookie*, pengambil alihan akun, maupun manipulasi tampilan website (Kuswara & Facrhi, 2025).
Website institusi pendidikan menjadi salah satu target serangan siber karena menyimpan berbagai informasi penting, seperti data siswa, guru, dan administrasi sekolah. Penelitian sebelumnya menunjukkan bahwa website sekolah masih memiliki berbagai kerentanan keamanan, seperti *Cross-Site Scripting* (XSS)**,** SQL Injection, dan *Security Misconfiguration*, yang berpotensi dimanfaatkan oleh penyerang untuk memperoleh akses ilegal terhadap sistem (Pahlawansah et al., 2025).Selain itu, XSS secara konsisten termasuk dalam daftar risiko keamanan aplikasi web yang dipublikasikan oleh *OWASP Top 10*, sehingga masih menjadi ancaman yang perlu mendapat perhatian. MAN 2 Kebumen sebagai salah satu institusi pendidikan yang memanfaatkan website sebagai media informasi juga memiliki potensi menghadapi ancaman tersebut. Berdasarkan observasi awal dan informasi dari pengelola website, ditemukan indikasi kerentanan *Cross-Site Scripting* (XSS) pada salah satu fitur website. Kondisi ini menunjukkan perlunya dilakukan analisis keamanan untuk mengidentifikasi kerentanan, mengetahui tingkat risikonya, serta memberikan rekomendasi perbaikan guna meningkatkan keamanan website.
Penelitian ini menggunakan metode *Vulnerability Assessment* dengan memanfaatkan OWASP Zed Attack Proxy (OWASP ZAP) sebagai alat pemindaian dan mengacu pada OWASP Web Security Testing Guide (WSTG) sebagai pedoman pengujian keamanan aplikasi web. Tujuan penelitian adalah mengidentifikasi dan menganalisis kerentanan *Cross-Site Scripting (XSS)* pada website MAN 2 Kebumen serta memberikan rekomendasi perbaikan sebagai upaya meningkatkan keamanan website terhadap potensi serangan siber.

2. Kajian Teori

2.1. Website

Website adalah kumpulan halaman web yang saling terhubung dan dapat diakses melalui internet menggunakan browser. Website berfungsi sebagai media untuk menyampaikan informasi, komunikasi, dan layanan digital kepada pengguna. Situs web sering dibangun menggunakan berbagai bahasa pemrograman, seperti HTML, CSS, JavaScript, dan PHP (Nurjannah & Abdul Muni, 2024).

2.2. Keamanan Website

Keamanan website merupakan suatu upaya untuk melindungi website dari berbagai ancaman, serangan, maupun akses tidak sah yang dapat mengganggu sistem dan merugikan pengguna. Keamanan website bertujuan untuk menjaga data, informasi, serta layanan yang terdapat pada website agar tetap aman, terjaga, dan dapat digunakan sebagaimana mestinya, dalam perkembangan teknologi informasi saat ini, keamanan website menjadi salah satu aspek yang sangat penting karena website telah digunakan sebagai media penyimpanan dan penyebaran berbagai informasi penting (Kuswara & Facrhi, 2025)

2.3. Kerentanan Website

Kerentanan website merupakan kelemahan atau celah keamanan pada aplikasi web yang dapat dimanfaatkan oleh pihak tidak bertanggung jawab untuk memperoleh akses ilegal, mencuri data, merusak sistem, maupun mengganggu layanan website, kerentanan aplikasi web adalah kelemahan yang muncul akibat kesalahan desain, konfigurasi, implementasi kode program, maupun manajemen keamanan sistem (Stallings et al., 2023).

2.4. Cross-Site Scripting

Cross Site Scripting (XSS) merupakan salah satu jenis kerentanan keamanan pada website yang terjadi ketika penyerang menyisipkan script berbahaya ke dalam halaman web yang kemudian dijalankan oleh browser pengguna. Serangan ini biasanya memanfaatkan kelemahan validasi input pada website sehingga script yang dimasukkan oleh penyerang dapat dieksekusi secara otomatis saat halaman diakses oleh pengguna lain.(OWASP Foundation, 2026b).

2.5. Owasp zap

OWASP ZAP merupakan tools open-source yang digunakan untuk melakukan pengujian keamanan aplikasi web secara otomatis maupun manual . Menurut OWASP, OWASP ZAP dirancang untuk membantu proses penetration testing dan vulnerability assessment pada aplikasi web dengan mendeteksi berbagai jenis kerentanan keamanan(Syahril Handaya, 2025)

2.6. Owasp Web Security Testing Guide

Owasp Top 10 merupakan daftar sepuluh jenis kerentanan keamanan aplikasi web yang paling berbahaya dan paling sering ditemukan berdasarkan data serta penelitian dari *Open Worldwide Application Security Project*, Owasp Top 10 digunakan sebagai st*and*ar internasional dalam proses pengujian keamanan *website* karena mampu membantu pengembang maupun administrator sistem dalam mengidentifikasi dan memahami berbagai ancaman keamanan aplikasi web (OWASP Foundation, 2026).

2.7. Vunerability Assessment

Vulnerability Assessment merupakan proses identifikasi, analisis, dan evaluasi terhadap kerentanan keamanan pada suatu sistem atau website. Tujuan utama dari Vulnerability Assessment adalah untuk mengetahui adanya celah keamanan yang dapat dimanfaatkan oleh pihak yang tidak bertanggung jawab sehingga dapat dilakukan tindakan pencegahan maupun perbaikan terhadap sistem. Dalam keamanan website, Vulnerability Assessment

DOI: https://doi.org/10.69693/ijmst.v4i2.12499

digunakan untuk mendeteksi berbagai jenis kerentanan seperti Cross Site Scripting (XSS), SQL Injection, Security Misconfiguration, dan kerentanan lainnya. Proses ini biasanya dilakukan menggunakan tools keamanan tertentu agar proses pengujian dapat dilakukan secara lebih efektif dan terstruktur (*National Institute of Standards and Technology*, 2026; Stallings et al., 2023).

3. Metode Penelitian

Penelitian ini menggunakan metode *Vulnerability Assessment* dengan pendekatan deskriptif untuk mengidentifikasi dan menganalisis kerentanan *Cross-Site Scripting* (XSS) pada website MAN 2 Kebumen. Proses pengujian mengacu pada *OWASP Web Security Testing Guide* (WSTG), khususnya kategori *Input Validation Testing*, serta menggunakan *OWASP Zed Attack Proxy* (OWASP ZAP) sebagai alat untuk melakukan pemindaian kerentanan. Pengujian dilakukan menggunakan pendekatan *Black Box Testing*, yaitu pengujian dari sisi pengguna tanpa mengakses kode sumber maupun konfigurasi internal sistem.

Data yang diperoleh berupa jenis kerentanan, lokasi kerentanan, tingkat risiko, dan bukti (*evidence*) hasil pemindaian. Analisis tingkat risiko mengacu pada *OWASP Risk Rating Methodology*, yang menyatakan bahwa tingkat risiko ditentukan berdasarkan dua komponen utama, yaitu *Likelihood* (kemungkinan kerentanan dapat dieksploitasi) dan *Impact* (besarnya dampak apabila eksploitasi berhasil dilakukan), dengan hubungan sebagai berikut:

$$\text{Risk} = \text{Likelihood} \times \text{Impact} \quad (1)$$

Namun, pada penelitian ini, peneliti tidak melakukan perhitungan nilai risiko secara mandiri, melainkan menggunakan *risk level* yang dihasilkan oleh OWASP ZAP**,** yaitu *High***,** *Medium***,** *Low***,** dan *Informational*, sebagai dasar analisis. Selanjutnya, setiap temuan dievaluasi berdasarkan pedoman OWASP WSTG untuk mengidentifikasi penyebab, potensi dampak, serta menyusun rekomendasi perbaikan sesuai dengan praktik keamanan aplikasi web guna meningkatkan keamanan website MAN 2 Kebumen terhadap serangan *Cross-Site Scripting* (XSS).

3.1. Tahapan Penelitian

Dalam penelitian ini, tahapan penelitian disusun berdasarkan metode Vulnerability Assessment dengan mengacu pada OWASP Web Security Testing Guide (WSTG) sebagai pedoman pengujian keamanan website. Penelitian difokuskan pada identifikasi dan analisis kerentanan Cross Site Scripting (XSS) pada website MAN 2 Kebumen menggunakan tools OWASP Zed Attack Proxy (OWASP ZAP).

Gambar 1. Tahapan Penelitian

Adapun penjelasan tahap-tahap sebagai berikut:

1. Identifikasi Masalah: Tahap pertama dalam penelitian ini adalah identifikasi masalah. Pada tahap ini dilakukan pengamatan awal terhadap website MAN 2 Kebumen untuk mengetahui kondisi keamanan website yang digunakan sebagai media informasi sekolah. Identifikasi masalah dilakukan karena website yang terhubung dengan internet memiliki potensi mengalami berbagai ancaman keamanan, salah satunya adalah serangan Cross Site Scripting (XSS).
2. *Information Gathering*: Tahap Information Gathering dilakukan untuk memperoleh informasi mengenai website yang menjadi objek penelitian (Natanael, 2024). Pada tahap ini dilakukan pengumpulan data terkait struktur website, halaman yang tersedia, formulir input, parameter URL, fitur yang dapat diakses pengguna, serta teknologi yang digunakan oleh website.
3. Konfigurasi tools: Sebelum proses pengujian dilakukan, peneliti melakukan konfigurasi terhadap tools OWASP ZAP yang akan digunakan dalam penelitian. Tahap ini meliputi instalasi perangkat lunak, pengaturan proxy, konfigurasi browser, serta pengaturan target website yang akan diuji.
4. Pemindaian Website dengan Owasp: Pemindaian keamanan website menggunakan OWASP ZAP. Pada tahap ini dilakukan proses crawling atau spidering untuk mengidentifikasi seluruh halaman dan fitur yang terdapat pada website. Setelah proses spidering selesai, dilakukan scanning untuk mendeteksi adanya kerentanan keamanan yang terdapat pada website. OWASP ZAP akan menganalisis berbagai komponen website dan memberikan informasi mengenai potensi kerentanan yang ditemukan.

DOI: https://doi.org/10.69693/ijmst.v4i2.12499

5. Analsis Kerentanan XSS: Hasil pemindaian yang diperoleh dari OWASP ZAP kemudian dianalisis untuk mengetahui jenis kerentanan yang ditemukan. Analisis dilakukan dengan memeriksa detail temuan yang berkaitan dengan Cross Site Scripting (XSS), termasuk lokasi kerentanan, parameter yang terpengaruh, serta tingkat risiko yang diberikan oleh OWASP ZAP. Pada tahap ini dilakukan pengelompokan temuan berdasarkan tingkat risiko keamanan yang meliputi kategori High, Medium, Low, dan Informational.
6. Evaluasi Berdasarkan WSTG: Tahap evaluasi dilakukan dengan mengacu pada OWASP Web Security Testing Guide (WSTG), khususnya kategori Input Validation Testing yang berkaitan dengan pengujian Cross Site Scripting (XSS). Evaluasi bertujuan untuk memastikan bahwa temuan yang diperoleh sesuai dengan standar pengujian keamanan aplikasi web.
7. Rekomendasi Perbaikan: Berdasarkan hasil analisis dan evaluasi yang telah dilakukan, peneliti menyusun rekomendasi perbaikan terhadap kerentanan yang ditemukan. Rekomendasi disusun dengan mempertimbangkan praktik keamanan website yang direkomendasikan oleh OWASP. Rekomendasi tersebut diharapkan dapat membantu pengelola website dalam meningkatkan keamanan sistem dan mengurangi risiko serangan Cross Site Scripting.
8. Penarikan Kesimpulan: Tahap terakhir dalam penelitian ini adalah penarikan kesimpulan berdasarkan seluruh proses yang telah dilakukan. Kesimpulan disusun berdasarkan hasil identifikasi kerentanan, analisis tingkat risiko, dan evaluasi keamanan website.

3.2. Alat dan Bahan

Alat dan bahan yang digunakan dalam penelitian ini terdiri atas perangkat keras, perangkat lunak, serta objek penelitian yang mendukung proses identifikasi dan analisis kerentanan Cross Site Scripting (XSS) pada website MAN 2 Kebumen.

Table 1. Software dan Hardware Pendukung

Hardware	Software
Laptop/komputer	Sistem Operasi
Koneksi Internet	Owasp Zap
	Browser

4. Hasil dan Pembahasan

4.1. *Information Gathering*

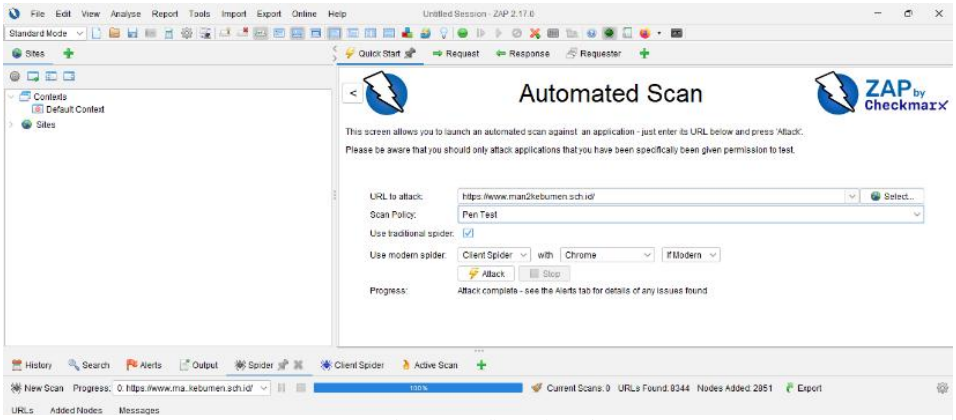
Information Gathering merupakan tahap awal yang dilakukan untuk memperoleh informasi mengenai karakteristik website sebelum proses pengujian keamanan dilakukan (Dewi, 2022). Pada tahap ini dilakukan identifikasi terhadap struktur website, halaman yang dapat diakses, parameter URL, formulir input, serta teknologi yang digunakan oleh website.

Table 2. Informasi Gathering

Informasi	Hasil
Domain	www.man2kebumen.sc.id
Bahasa Pemograman	PHP
Jumlah Url Ditemukan	8344
Form Input	Search, login, komentar

4.2. Konfigurasi Tools

Sebelum proses pemindaian dilakukan, dilakukan konfigurasi terhadap OWASP Zed Attack Proxy (OWASP ZAP) agar proses pengujian dapat berjalan dengan baik sesuai dengan target penelitian. Konfigurasi meliputi penentuan alamat website yang akan diuji, pengaturan ruang lingkup (scope) pengujian, serta pengaktifan fitur Spider dan



Gambar 2. Konfigurasi Tools

DOI: https://doi.org/10.69693/ijmst.v4i2.12499

Active Scan untuk mengidentifikasi halaman, parameter, dan potensi kerentanan pada website. Selain itu, browser dikonfigurasi agar terhubung dengan proxy OWASP ZAP sehingga seluruh permintaan (request) dan respons (response) antara browser dan website dapat dipantau serta dianalisis. Hasil konfigurasi tersebut ditunjukkan pada Gambar ini.

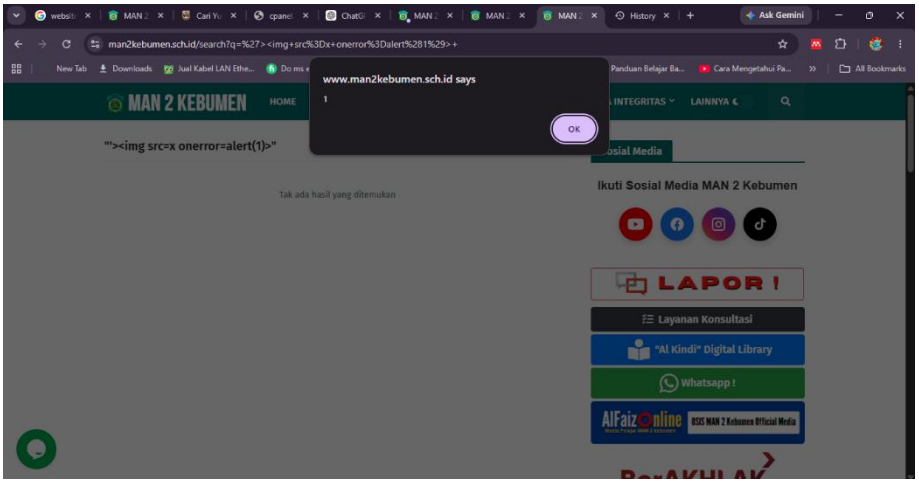
4.3. *Pemindaian dengan Owasp zap*

Tahap pemindaian dilakukan menggunakan OWASP Zed Attack Proxy (OWASP ZAP) untuk mengidentifikasi potensi kerentanan keamanan pada website MAN 2 Kebumen. Proses diawali dengan menjalankan fitur Spider untuk memetakan struktur website, mengidentifikasi halaman, parameter URL, dan formulir yang dapat diakses. Selanjutnya dilakukan Active Scan terhadap target yang telah teridentifikasi untuk mendeteksi kerentanan, khususnya Cross-Site Scripting (XSS). Setelah proses Spider dan Active Scan selesai dilakukan, OWASP ZAP menghasilkan beberapa temuan berupa alert yang menunjukkan adanya potensi kerentanan keamanan pada website MAN 2 Kebumen. Setiap alert disertai dengan informasi mengenai tingkat risiko (risk level), tingkat kepercayaan (confidence), lokasi temuan, serta bukti (evidence) yang digunakan sebagai dasar analisis. Hasil pemindaian menunjukkan bahwa selain ditemukan beberapa kelemahan konfigurasi keamanan, terdapat pula temuan yang berkaitan dengan potensi kerentanan Cross-Site Scripting (XSS) yang menjadi fokus penelitian.

Table 3. Temuan Kerentanan

No	Alert	Tingkat Resiko	Indikasi
1	User Controllable HTML Element Attribute (Potential XSS)	High	Mengindikasikan adanya input yang berpotensi mengeksekusi skrip berbahaya.
2	Content Security Policy (CSP) Header Not Set	Medium	Tidak adanya CSP meningkatkan risiko keberhasilan eksploitasi XSS.
3	CSP: Wildcard Directive	Medium	Penggunaan wildcard (*) dapat mengizinkan pemuatan skrip dari sumber yang tidak terpercaya.
4	CSP: script-src unsafe-inline	Medium	Mengizinkan eksekusi skrip inline yang dapat dimanfaatkan dalam serangan XSS.
5	Vulnerable JS Library	Medium	Library yang memiliki celah keamanan dapat dimanfaatkan untuk melakukan eksploitasi XSS.

Setelah pemindaian menggunakan OWASP ZAP, dilakukan verifikasi terhadap temuan User Controllable HTML Element Attribute (Potential XSS) dengan memberikan payload XSS pada parameter yang teridentifikasi. Pengujian menggunakan beberapa payload untuk dieksekusi namun dari beberapa payload yang digunakan "><img src=x onerror=alert(1)> menunjukkan bahwa payload tersebut berhasil dieksekusi pada kondisi tertentu sehingga memunculkan dialog alert(). Temuan ini mengindikasikan bahwa mekanisme validasi dan sanitasi input pada parameter tersebut belum berjalan secara optimal, sehingga berpotensi dimanfaatkan untuk melakukan serangan Cross-Site Scripting (XSS).



Gambar 3. Uji Payload

4.4. Evaluasi Berdasarkan Wstg

Evaluasi dilakukan dengan mengacu pada OWASP Web Security Testing Guide (WSTG), khususnya kategori Input Validation Testing yang berkaitan dengan pengujian Cross-Site Scripting (XSS). Berdasarkan hasil pemindaian menggunakan OWASP ZAP dan verifikasi menggunakan payload XSS, ditemukan bahwa aplikasi masih memberikan respons yang mengindikasikan adanya kelemahan pada mekanisme validasi dan sanitasi masukan pengguna. Kondisi tersebut menunjukkan bahwa pengendalian terhadap data yang diterima dari

DOI: https://doi.org/10.69693/ijmst.v4i2.12499

pengguna belum sepenuhnya sesuai dengan praktik keamanan yang direkomendasikan dalam OWASP WSTG. Selain itu, hasil pemindaian juga menunjukkan beberapa kelemahan konfigurasi Content Security Policy (CSP) yang berpotensi meningkatkan risiko keberhasilan eksploitasi XSS (Rodiansyah & Muttaqin, 2025). Oleh karena itu, website memerlukan penerapan validasi input, output encoding, sanitasi input, serta konfigurasi CSP yang lebih ketat untuk mengurangi risiko serangan Cross-Site Scripting.

4.5. Rekomendasi Perbaikan

Berdasarkan hasil pemindaian menggunakan OWASP ZAP, verifikasi menggunakan *payload* XSS, serta evaluasi berdasarkan OWASP *Web Security Testing* Guide (WSTG), diketahui bahwa website MAN 2 Kebumen masih memiliki potensi kerentanan *Cross-Site Scripting* (XSS). Oleh karena itu, beberapa rekomendasi perbaikan dapat diterapkan untuk mengurangi risiko eksploitasi kerentanan tersebut.

Rekomendasi pertama adalah menerapkan validasi input (input validation) pada seluruh data yang diterima dari pengguna. Validasi dilakukan dengan membatasi jenis karakter dan format masukan sesuai kebutuhan aplikasi sehingga input yang tidak sesuai dapat ditolak sebelum diproses oleh sistem (Kristara & Adiguna, 2023).

Rekomendasi kedua adalah menerapkan output encoding sebelum data ditampilkan kembali pada halaman website. Teknik ini bertujuan untuk memastikan bahwa karakter khusus tidak dieksekusi sebagai kode oleh browser, melainkan ditampilkan sebagai teks biasa.

Selanjutnya, perlu dilakukan sanitasi input (*input sanitization*) untuk menghilangkan atau menonaktifkan tag HTML maupun kode JavaScript yang berpotensi digunakan dalam serangan XSS (Fadllan et al., 2026). Sanitasi dapat diterapkan pada seluruh formulir yang menerima masukan dari pengguna, seperti fitur pencarian maupun kolom komentar.

Selain itu, website disarankan untuk menerapkan *Content Security Policy* (CSP**)** yang lebih ketat. Berdasarkan hasil pemindaian ditemukan beberapa kelemahan konfigurasi CSP, seperti penggunaan unsafe-inline dan belum diterapkannya kebijakan CSP secara optimal. Penerapan CSP yang sesuai dapat membantu membatasi sumber skrip yang diizinkan sehingga mengurangi risiko eksekusi kode berbahaya (Trada et al., 2024).

Hasil *Information Gathering* juga menunjukkan penggunaan jQuery versi 2.2.4, sehingga disarankan untuk memperbarui pustaka JavaScript ke versi yang lebih baru dan masih memperoleh pembaruan keamanan. Pembaruan komponen perangkat lunak merupakan salah satu langkah penting untuk mengurangi potensi eksploitasi kerentanan yang telah diketahui (Pramuja Inngam Fanani et al., 2025).

5. Kesimpulan

Berdasarkan hasil penelitian yang telah dilakukan, dapat disimpulkan bahwa website MAN 2 Kebumen masih memiliki beberapa kerentanan keamanan yang teridentifikasi melalui proses Vulnerability Assessment menggunakan OWASP ZAP. Dari berbagai temuan yang diperoleh, penelitian ini memfokuskan analisis pada kerentanan Cross-Site Scripting (XSS). Hasil verifikasi menggunakan payload menunjukkan bahwa terdapat indikasi kerentanan XSS pada salah satu fitur website, yang mengindikasikan bahwa mekanisme validasi dan sanitasi input belum diterapkan secara optimal. Analisis tingkat risiko berdasarkan hasil OWASP ZAP serta evaluasi yang mengacu pada OWASP Web Security Testing Guide (WSTG) menunjukkan bahwa kondisi keamanan website masih memerlukan peningkatan, khususnya pada aspek validasi input, output encoding, dan penerapan Content Security Policy (CSP). Selain itu, ditemukan beberapa konfigurasi keamanan yang belum sesuai dengan praktik terbaik OWASP sehingga berpotensi meningkatkan risiko eksploitasi XSS. Berdasarkan temuan tersebut, penelitian ini berhasil mengidentifikasi potensi kerentanan Cross-Site Scripting (XSS) pada website MAN 2 Kebumen serta menghasilkan rekomendasi perbaikan yang dapat dijadikan acuan oleh pengelola website untuk meningkatkan keamanan aplikasi web dan meminimalkan risiko serangan di masa mendatang

Ucapan Terimakasih

Penulis mengucapkan terima kasih kepada seluruh pihak yang telah memberikan dukungan, bantuan, dan fasilitas selama proses penelitian ini berlangsung. Terima kasih disampaikan kepada pihak MAN 2 Kebumen yang telah memberikan izin serta menyediakan objek penelitian berupa website sekolah untuk keperluan analisis keamanan.

Penulis juga menyampaikan apresiasi kepada Program Studi Teknik Informatika, Fakultas Teknik, Universitas Ma'arif Nahdlatul Ulama atas dukungan akademik, fasilitas, serta arahan yang diberikan selama pelaksanaan penelitian.

Ucapan terima kasih juga disampaikan kepada dosen pembimbing dan seluruh pihak yang telah memberikan masukan, motivasi, serta bantuan teknis sehingga penelitian mengenai analisis kerentanan website terhadap serangan Cross-Site Scripting (XSS) menggunakan OWASP ZAP ini dapat diselesaikan dengan baik.

Reference

Dewi, B. T. K. & M. A. S. (2022). Kajian Literatur: Metode Dan Tools Pengujian Celah Keamanan Aplikasi Berbasis Web. *Automata*, *3*(1), 1–8. Https://Journal.Uii.Ac.Id/AUTOMATA/Article/View/21883/12030

Fadllan, M. F., Isnaini, K. N., & Ikhsan, A. N. (2026). Evaluasi Celah Keamanan Cross-Site Scripting (XSS) Pada Website Menggunakan Black-Box Penetration Testing. *Jurnal Algoritma*, *23*(1), 105–114. Https://Doi.Org/10.33364/Algoritma/V.23-1.3122

DOI: https://doi.org/10.69693/ijmst.v4i2.12499

Kristara, F. S., & Adiguna, M. A. (2023). Pengujian Celah Keamanan Input Validation Pada. *Jurnal Penelitian Ilmu Komputer*, *1*(4), 50–55.

Kuswara, R., & Facrhi, F. (2025). Analisis Keamanan Website Di Smk Wongsorejo Gombong Terhadap Serangan Cross-Site Scripting (Xss) Menggunakan Penetration Testing. *JATI (Jurnal Mahasiswa Teknik Informatika)*, *9*(2), 2700–2707. Https://Doi.Org/10.36040/Jati.V9i2.13158

Natanael, N. (2024). Web Penetration Testing Dalam Mencari Kerentanan Sql Injection. *JATI (Jurnal Mahasiswa Teknik Informatika)*, *7*(6), 3135–3138. Https://Doi.Org/10.36040/Jati.V7i6.7992

National Institute Of Standards And Technology. (2026). Https://Www.Nist.Gov/

Nurjannah, & Abdul Muni. (2024). Analisis Keamanan Website Sekolah Sman 1 Tempuling Dengan Menggunakan Open Web Application Security Project (Owasp). *Jurnal Perangkat Lunak*, *6*(2), 351–361. Https://Doi.Org/10.32520/Jupel.V6i2.3442

OWASP Foundation. (2026a). *Metodologi Peringkat Risiko OWASP*. Https://Owasp.Org/Www-Community/OWASP_Risk_Rating_Methodology

OWASP Foundation. (2026b). *OWASP Foundation, The Open Source Foundation For Application Security*. Https://Owasp.Org/

Pahlawansah, H., Basmar, M. F., & Yusuf, M. (2025). *Analisis Kerentanan Website SMK Muhammadiyah 2 Bontoala Makassar Menggunakan Metode OWASP (Open Web Application Security Project)*. *6*(2), 92–100.

Pramuja Inngam Fanani, G., Muhammad Amirul Mu'min, & Tristanti, N. (2025). Analisis Dan Pengujian Kerentanan Website Menggunakan OWASP ZAP. *Jurnal Riset Sistem Dan Teknologi Informasi*, *3*(1), 36–50. Https://Doi.Org/10.30787/Restia.V3i1.1886

Rodiansyah, H., & Muttaqin, H. F. (2025). Studi Analisis Celah Keamanan Website Spin Laboratorium Kalibrasi Menggunakan Metode Pemindaian Owasp Zap, Burp Suite, Dan Nessus. *Syntax Literate ; Jurnal Ilmiah Indonesia*, *10*(7), 1058–1074. Https://Doi.Org/10.36418/Syntax-Literate.V10i7.60738

Stallings, W., Brown, L., Bauer, M. D., & Howard, M. (2023). *Computer Security : Principles And Practice (5th Edition)*.

Syahril Handaya, R. I. (2025). *Implementasi Penetration Testing Pada Aplikasi Web Sistem Evaluasi Data Bidang TIK Polda Aceh - Hendri,+Syahril+(2)*. *115*, 1–15.

Trada, M., Teknik, J., & Polbitrada, E. (2024). Analisis Metode OWASP V4 . 2 Dalam Pengujian Keamanan Sistem Informasi Rumah Sakit. *Medika Trada : Jurnal Teknik Elektromedik Polbitrada*, *5*(2), 87–97.

DOI: https://doi.org/10.69693/ijmst.v4i2.12499