Analisis Kerentanan Cross Site Scripting (XSS): Metode Serangan, Dampak, dan Strategi Pengamanan

Nur Muhammad Kevin[*1], Ramadhan Renaldy [2]
[1, 2] Informatika, Universitas PGRI Semarang, Kota Semarang

Email: [1]nurmkevin532@gmail.com [2]ramadhanrenaldy@upgris.ac.id

Abstract

Cross Site Scripting (XSS) attacks pose a significant threat to web security, with the potential to disrupt web performance, steal sensitive user information, and even take full control of a website. This research aims to analyze various XSS attack methods, their impacts, and proposed security strategies. Among the 30 reviewed journals, the most frequently used method is the Open Web Application Security Project (OWASP), cited in 19 journals, with OWASP ZAP being the most commonly used tool, mentioned in 11 journals. The most recommended security strategy is Input Validation, suggested in 12 journals. XSS has a highly significant impact, not only compromising the integrity and confidentiality of user data but also disrupting the normal functionality and reputation of a website. This study reveals that despite efforts to mitigate XSS attacks, their success rates vary. It emphasizes the need for a comprehensive approach to address XSS attacks and protect websites from associated risks

Keywords: Cross Site Scripting (XSS); Web Security; Attack Methods; Impacts; Cybersecurity; System Literature Review (SLR);

Abstrak

Serangan Cross Site Scripting (XSS) merupakan ancaman yang sangat berbahaya terhadap keamanan web dengan potensi untuk merusak kinerja sebuah web, mencuri informasi sensitif pengguna, bahkan mengambil alih kendali penuh atas web tersebut. Penelitian ini bertujuan untuk menganalisis berbagai metode serangan XSS, dampaknya, dan strategi pengamanan yang diusulkan.Dari 30 jurnal yang direview, metode yang sering digunakan adalah Open Web Application Security Project (OWASP) sebanyak 19 jurnal,dengan tool yang sering digunakan yaitu OWASP ZAP sebanyak 11 jurnal, dan Strategi pengamanan yang paling banyak disarankan yaitu Validasi Input sebanyak 12 jurnal. XSS memiliki dampak sangat signifikan, tidak hanya merusak integritas dan kerahasiaan data pengguna, tetapi juga dapat mengganggu fungsi normal dan reputasi sebuah situs web. Penilitian ini menujukan meskipun telah dilakukan upaya untuk mengurangi serangan XSS, keberhasilannya bervariasi.

Kata Kunci: Skrip Lintas Situs (XSS); Keamanan Web; Metode Penyerangan; Dampak Penyerangan; Keamanan Siber; Sistem Literatur Review (SLR).

1. Pendahuluan

Website merupakan salah satu sarana untuk menyimpan dan menyebarkan informasi. Pengguna yang berhak dapat memperoleh data dan informasi yang ada didalamnya. Umumnya, data dan informasi tersimpan dalam sebuah database server[1][2]. Banyaknya data dan informasi yang tersebar di Internet mengundang pengguna internet yang tidak memiliki hak akses untuk mendapatkan data tersebut. Salah satunya dengan cara melakukan serangan Cross Site Scripting(XSS)[3].

Serangan Cross Site Scripting (XSS) adalah jenis serangan injeksi di mana penyerang menyisipkan skrip berbahaya, seperti JavaScript, ke dalam halaman web. Serangan ini dapat digunakan untuk berbagai tujuan jahat, termasuk mencuri data privasi pengguna, seperti informasi login dan data bisnis yang sensitif[4]. Serangan XSS sangat berbahaya karena dapat

dijalankan pada sisi klien, di browser pengguna, sehingga sering kali sulit untuk dideteksi dan dicegah[5].

Serangan Cross Site Scripting (XSS) dapat mengakibatkan berbagai macam masalah bagi pengguna, mulai dari ketidaknyamanan kecil hingga kompromi penuh terhadap akun mereka. Serangan XSS paling parah membuat data pengguna rentan, sehingga peretas tidak memiliki izin akses ke identitas dan akun pengguna[6][7]. Tindakan berbahaya mungkin berpotensi membahayakan file pengguna, penerapaan virus trojan yang akan mengarahkan pengguna ke situs web atau web lain halaman, dan mengubah cara data diterima oleh pengguna[8][9].

Reflected XSS dapat terjadi kapan saja saat pengguna mengirimkan input ke aplikasi yang kemudian dipantulkan kembali ke pengguna yang sama[10]. Script diinjeksikan melalui koneksi, yang mengirimkan permintaan ke situs web rentan yang dapat mengeksekusi skrip berbahaya[11][12]. Biasanya, kerentanan ini dihasilkan dari permintaan yang tidak cukup disanitasi oleh sistem yang memiliki probabilitas untuk memanipulasi fungsi web dan mengeksekusi skrip berbahaya[13][14].

Stored XSS dapat terjadi pada saat pengguna melakukan input langsung disimpan di server yang ditargetkan. Skrip disimpan dan dieksekusi di server yang membuat pengguna memiliki hak istimewa untuk mengambil data yang disimpan, skrip berbahaya juga bisa jadi dikirim dari database dengan data yang diminta[13]. Jika data tidak dibuat aman sebelum direnderi di browser, itu kemungkinan pengguna diretas oleh penyusup tinggi dan data sensitif korban yang disimpan di server dapat disalahgunakan. Karena skrip disimpan di web server, kode berbahaya akan dieksekusi setiap saat ketika pengguna mengakses data itu[15][16].

DOM-Based XSS memungkinkan skrip untuk mengakses dan memperbarui konten dokumen secara dinamis, struktur, gaya, dan tampilan halaman[17]. Jenis kerentanan XSS ini dapat melakukannya idak perlu menyimpan data ke server tetapi mengeksekusi data DOM yang diperoleh klien secara lokal, dan memberikan effect seperti Reflected XSS[18][19].

Dari teknik serangan XSS yang sudah dijabarkan,studi ini akan mengevaluasi apa saja metode, tools, dan strategi pengamanan yang sering digunakan para penulis.Dengan metode paling efektif dari berbagai banyak penulis, tools yang paling banyak dipakai penulis maupun startegi pengamanan yang bervariasi yang paling banyak dipakai penulis untuk membantu mengurangi serangan XSS. Selain itu, serangan XSS juga memiliki dampak yang bervariasi tergantung bagaimana serangan itu dilancarakan.

Tujuan Studi Literatur ini untuk mengkaji pengetahuan tentang metode Cross Site Scripting (XSS), cara kerja serangan Cross Site Scripting (XSS) dan tools apa saja yang digunakan untuk mengatasi kerentanan[3][20]. Selain itu, studi ini juga akan mengeksplorasi dampak yang beragam dari serangan XSS terhadap keamanan dan kinerja website, serta upaya-upaya startegi pengamanan yang dapat diterapkan untuk mengurangi risiko serangan XSS yang terkait.

2. Metode

Pada penelitian ini, penulis menggunakan Systematic Literature Review (SLR). SLR merupakan metode penelitian yang bertujuan untuk melakukan tinjauan literatur secara sistematis dengan melalui langkah-langkah yang telah direncanakan dengan baik. SLR memiliki tiga fase utama yaitu Planning, Conducting dan Reporting. Berikut penjelasan dari masing masing langkah dalam SLR:

2.1 Planning

Penentuan tema merupakan langkah awal untuk memulai SLR. Dengan menentukan tema yang tepat maka pemilihan Research Question (RQ) dapat lebih mudah karena RQ yang akan kita tentukan dapat mengacu langsung pada tema yang telah ditentukan.

RQ dibutuhkan dalam pembuatan SLR karena RQ akan berfungsi untuk menjadi pedoman dalam proses pencarian dan ekstraksi literatur. Suatu RQ dapat dianggap baik apabila bermanfaat, dapat diukur, arahnya sesuai tema atau topik yang telah ditentukan diawal.

Langkah berikutnya penulis memilih lima penerbit untuk menjadi sumber dalam mencari jurnal yaitu Scholars(12), ResearchGate (11), IEEE (4), MDPI(1), IJCIS(1), IJITE(1). Jurnal yang dipilih berjumlah 30 jurnal.

2.2 Conducting

Tahapan conducting pada SLR merupakan tahapan yang berisi pemilihan jurnal sebagai refrensi untuk menelusuri RQ yang sudah didapatkan.

Setelah mendapat 30 jurnal, selanjutnya adalah memilih berdasarkan Research Question. Untuk mempermudah proses direkomendasikan membuat kriteria yang akan membantu dalam pemilihan jurnal berdasarkan RQ1, RQ2, RQ3 dan akan menghasilkan 30 jurnal yang akan digunakan untuk di tinjau. Research Question pada penelitian ini adalah metode yang paling banyak digunakan, alat yang digunakan untuk mengetahui kerentanan, dan Startegi pengamanan yang akan dilakukan. Berikut merupakan tabel research question yang sudah dibuat:

Tabel 1. Tujuan dibentuk Research Question

ID	Research Question	Tujuan
RQ1	Metode apa saja yang paling banyak digunakan untuk mengidentifikasi kerentanan?	Mengetahui metode yang paling digunakan
RQ2	Tools/Alat apa saja yang paling banyak digunakan untuk mengidentifikasi kerentanan?	Mengetahui tools yang paling banyak digunakan untuk indentifikasi kerentanan
RQ3	Startegi pengamanan apa saja yang paling banyak digunakan?	Mengetahui startegi yang paling banyak digunakan

2.3 **Reporting**

Tahap terakhir dalam melakukan SLR adalah reporting atau pelaporan. Dalam tahap ini penulis mulai membuat laporan yang berisi Pendahuluan, Metode Penelitian, Hasil dan Pembahasan serta Kesimpulan. Selain itu, laporan juga dilengkapi dengan abstrak pada awal laporan.

Bagian abstrak berisi review dari laporan SLR yang telah dibuat. Abstrak berfungsi agar pembaca dapat mengetahui isi laporan secara singkat. Maka dari itu, abstrak harus sesuai dengan isi laporan serta menggunakan bahasa yang mudah dipahami dan singkat.

Pendahuluan akan berisi tentang tema yang telah ditentukan, Tema dapat berupa permasalahan, metode dan langkah apa yang diangkat. Selain itu, pendahuluan berisi alasan mengapa penulis memilih untuk mengangkat tema yang sebelumnya telah dipilih.

Metode Penelitian membahas tentang bagaimana langkah-langkah dari SLR yang dilakukan oleh penulis. Langkah yang dilakukan mulai menyusun tema, mencari jurnal, menentukan RQ, dan melakukan review terhadap jurnal yang ada sesuai dengan RQ yang ditentukan.

Untuk Hasil dan Pembahasan akan berisi tentang hasil dari jurnal yang telah didapatkan dan dilakukan filter. Pada hasil dan pembahasan juga akan dipaparkan bagaimana jawaban yang didapatkan dari jurnal terhadap RQ yang telah ditentukan. Bagian terakhir adalah kesimpulan yang merupakan penutup laporan.

Kesimpulan akan berisi rangkuman dari SLR yang telah dilakukan oleh penulis sesuai dengan RQ yang telah ditentukan sebelumnya.

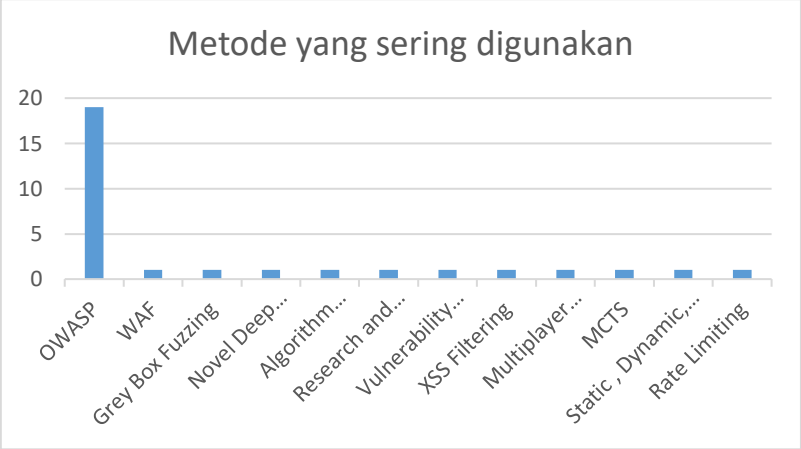
3. Hasil dan Pembahasan

Dengan menggunakan Systematic Literature Review (SLR), penulis dapat memaparkan hasil yang sudah dikaji dan disusun berdasarkan tiga Research Question (RQ) yang telah ditentukan.

3.1. Penyajian Hasil

Dalam bagian ini, hasil disajikan dengan representatif dari penelitian berdasarkan tiga Research Question (RQ) yang telah ditentukan. Hasil yang disajikan berbentuk tabel dan deskripsi untuk memudahkan pemahaman.

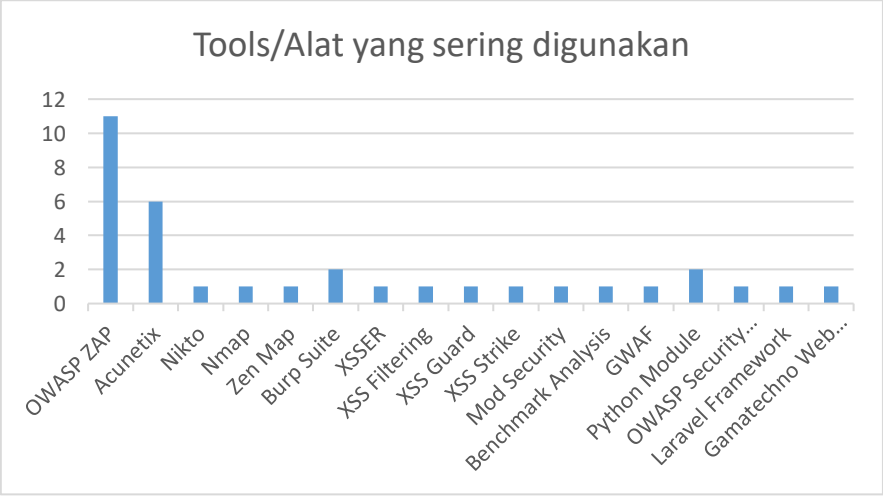
RQ1 (Metode apa saja yang paling digunakan untuk mengidentifikasi kerentanan?)



Gambar 1. Metode yang paling banyak digunakan

Pada Gambar 1 di perlihatkan bahwa metode yang paling banyak digunakan untuk mengidentifikasi kerentaanan yaitu OWASP sebanyak 19 jurnal sedangkan untuk metode lainnya hanya 1 Jurnal dengan metode yang berbeda. Hal ini membuktikan bahwa metode OWASP sangat efektif untuk menemukan kerentanan Cross Site Scripting (XSS) karena OWASP menyediakan pedoman dan alat yang komprehensif untuk mengidentifikasi kerentanan XSS[21]. sehingga memungkinkan deteksi yang lebih cepat dan akurat dibandingkan metode lainnya. Efektivitas OWASP dalam mendeteksi kerentanan XSS menjadikannya pilihan utama dalam studi ini.

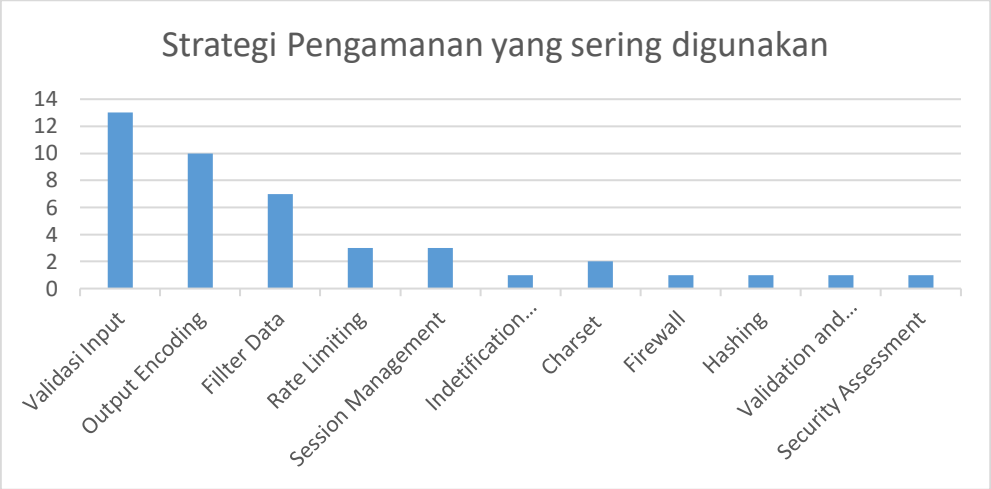
RQ(2) Tools/Alat apa saja yang paling banyak digunakan untuk mengidentifikasi kerentanan?



Gambar 2. Tools atau Alat yang sering digunakan

Pada Gambar 2 di perlihatkan bahwa Tools atau Alat yang paling banyak digunakan untuk mengidentifikasi kerentaanan yaitu OWASP ZAP sebanyak 11 jurnal, Acunetix sebanyak 6 Jurnal, Burp Suite sebanyak 2 Jurnal, dan Python Module sebanyak 2 Jurnal sedangkan untuk metode lainnya hanya 1 Jurnal dengan tools yang berbeda. Hal ini membuktikan bahwa tools OWASP ZAP banyak digunakan oleh penulis untuk menemukan kerentanan Cross Site Scripting (XSS).

RQ(3) Startegi pengamanan apa saja yang paling banyak digunakan?



Gambar 3. Strategi Pengamanan yang sering digunakan

Pada Gambar 3 di perlihatkan bahwa Strategi Pengaman yang paling banyak digunakan untuk mengatasi kerentaanan yaitu Validasi Input sebanyak 12 jurnal, Output Encoding sebanyak 10 Jurnal, Fillter Data sebanyak 7 Jurnal,Rate Limiting sebanyak 3 jurnal, Session Management sebanyak 3 jurnal, Charset sebanyak 2 jurnal, sedangkan untuk startegi pengamanan lainnya hanya 1 Jurnal dengan startegi pengamanan yang berbeda. Hal ini membuktikan bahwa Validasi Input menjadi salah satu strategi pengamanan yang paling banyak digunakan oleh penulis.

3.2. Pembahasan

RQ1: Metode Identifikasi Kerentanan

Temuan menunjukkan bahwa metode OWASP dominan dalam mengidentifikasi kerentanan XSS, digunakan dalam 19 dari 20 jurnal yang dianalisis. Ini menunjukkan bahwa OWASP menyediakan framework yang diakui luas dan efektif dalam mendeteksi kerentanan XSS[22]. Efektivitas OWASP mungkin karena pendekatannya yang komprehensif dan up-to-date dalam menyikapi berbagai jenis serangan XSS, sesuatu yang metode lain mungkin tidak mampu lakukan sebaik OWASP[23][24]. Selain itu, dukungan komunitas dan dokumentasi yang ekstensif menjadikan OWASP sebagai pilihan yang unggul[25].

RQ2: Tools/Alat Identifikasi Kerentanan

OWASP ZAP muncul sebagai alat yang paling banyak digunakan, yang mencerminkan kepercayaan komunitas keamanan pada alat ini. OWASP ZAP adalah alat open-source yang kuat untuk menemukan kerentanan, mudah digunakan, dan terus diperbarui dengan fitur baru[21][26]. Alat ini mendeteksi kerentanan XSS dengan efisiensi yang tinggi, mendukung analisis dinamis, dan menyediakan berbagai fungsionalitas yang mendalam untuk analisis keamanan aplikasi web[27][28]. Keunggulan OWASP ZAP dibandingkan dengan alat lain seperti Acunetix atau Burp

Suite mungkin terletak pada kemudahan penggunaan dan biaya yang lebih rendah[29][30].

RQ3: Strategi Pengamanan

Validasi input adalah strategi pengamanan yang paling sering digunakan untuk mencegah XSS. Ini masuk akal karena serangan XSS sering mengeksploitasi kelemahan dalam penanganan input oleh aplikasi web. Dengan memvalidasi semua input yang diterima aplikasi, resiko injeksi skrip berbahaya dapat diminimalkan. Output encoding dan filter data juga penting dalam memastikan bahwa data yang dikirim ke browser aman. Kombinasi strategi ini menunjukkan pendekatan berlapis untuk keamanan, yang sangat efektif dalam menghadapi ancaman XSS.

Dampak dari Serangan Cross Site Scripting (XSS)

Serangan Cross-Site Scripting (XSS) memiliki dampak serius terhadap keamanan dan integritas website serta data pengguna. Salah satu dampak utama adalah pencurian data sensitif, di mana penyerang mencuri informasi login, detail pribadi, atau data penting perusahaan untuk pencurian identitas, penipuan, atau aksi kriminal lainnya. Selain itu, serangan XSS dapat mengakibatkan pelanggaran data dengan mengubah konten halaman web atau merusak data yang tersimpan, yang merusak reputasi situs web dan mengurangi kepercayaan pengguna.

Phishing juga merupakan dampak serius lainnya, di mana penyerang menyisipkan dan menjalankan kode berbahaya di browser pengguna untuk memasang malware atau mencuri informasi sensitif. Serangan XSS juga dapat mengganggu operasi normal situs web, menyebabkan kesalahan skrip atau crash yang mengakibatkan downtime dan kerugian bisnis. Oleh karena itu, penting untuk melindungi situs web dari serangan XSS guna menjaga keamanan data pengguna dan integritas situs.

4. Kesimpulan

Berdasarkan hasil penelitian, dapat disimpulkan yaitu metode OWASP terbukti paling banyak digunakan untuk mendeteksi kerentanan XSS, dengan 19 jurnal mendukung efektivitasnya. OWASP menyediakan panduan dan alat yang komprehensif, seperti OWASP ZAP adalah alat yang paling banyak digunakan, diikuti oleh modul Acunetix, Burp Suite, dan Python. Alat-alat ini membantu peneliti dan profesional keamanan mendeteksi dan memperbaiki kerentanan XSS dengan sangat efektif. Strategi keamanan yang disarankan dan paling umum digunakan adalah validasi input, pengkodean keluaran, dan filter data.

Selain itu, penelitian ini juga menunjukkan dampak signifikan dari serangan XSS, yang meliputi pencurian data sensitif, kerusakan integritas data, phising, malfungsi. Kombinasi metode deteksi yang efektif, alat yang andal, dan strategi pertahanan yang komprehensif adalah kunci untuk melindungi situs web dari ancaman serangan XSS. Pendekatan ini diharapkan dapat mengurangi risiko dan dampak serangan XSS serta meningkatkan keamanan dan kepercayaan pengguna terhadap situs web.

5. Referensi

[1] B. Harahap, “Penerapan Keamanan Owasp Terhadap Aplikasi GTFW Pada Website Universitas Battuta,” *J. Inform. dan Teknol. Pendidik.*, vol. 1, no. 2, pp. 80–86, 2021, doi: 10.25008/jitp.v1i2.15.

[2] X. Zhang, Y. Zhou, S. Pei, J. Zhuge, and J. Chen, “Adversarial Examples Detection for XSS Attacks Based on Generative Adversarial Networks,” *IEEE Access*, vol. 8, pp. 10989–10996, 2020, doi: 10.1109/ACCESS.2020.2965184.

[3] S. Suroto and A. Asman, “Ancaman Terhadap Keamanan Informasi Oleh Serangan Cross-Site Scripting (XSS) Dan Metode Pencegahannya,” *Zo. Komput.*, vol. 11, no. 1,

pp. 11–19, 2021, [Online]. Available: http://ejurnal.univbatam.ac.id/index.php/komputer/article/view/658

[4] B. Ghozali, K. Kusrini, and S. Sudarmawan, "Mendeteksi Kerentanan Keamanan Aplikasi Website Menggunakan Metode Owasp (Open Web Application Security Project) Untuk Penilaian Risk Rating," *Creat. Inf. Technol. J.*, vol. 4, no. 4, p. 264, 2019, doi: 10.24076/citec.2017v4i4.119.

[5] I. Riadi, R. Umar, and T. Lestari, "Analisis Kerentanan Serangan Cross Site Scripting (XSS) pada Aplikasi Smart Payment Menggunakan Framework OWASP," *JISKA (Jurnal Inform. Sunan Kalijaga)*, vol. 5, no. 3, pp. 146–152, 2020, doi: 10.14421/jiska.2020.53-02.

[6] J. R. Tadhani, V. Vekariya, V. Sorathiya, S. Alshathri, and W. El-Shafai, "Securing web applications against XSS and SQLi attacks using a novel deep learning approach," *Sci. Rep.*, vol. 14, no. 1, pp. 1–18, 2024, doi: 10.1038/s41598-023-48845-4.

[7] R. M. Wibowo and A. Sulaksono, "Web Vulnerability Through Cross Site Scripting (XSS) Detection with OWASP Security Shepherd," *Indones. J. Inf. Syst.*, vol. 3, no. 2, pp. 149–159, 2021, doi: 10.24002/ijis.v3i2.4192.

[8] E. Diatmika, P. Charly, I. M. P. Prayoga, I. M. E. Listartha, T. Informatika, and U. P. Ganesha, "Pendeteksian Keamanan Website SMA Greenschool Menggunakan Metode Owasp dengan Pengujian XSS," vol. 11, pp. 77–82, 2022.

[9] N. Kshetri, D. Kumar, J. Hutson, N. Kaur, and O. F. Osama, "AlgoXSSF: Detection and Analysis of Cross-Site Request Forgery (XSRF) and Cross-Site Scripting (XSS) Attacks via Machine Learning Algorithms," pp. 1–8, 2024, doi: 10.1109/isdfs60797.2024.10527278.

[10] Y. Nugraha, A. Widjajarto, and M. Fathinuddin, "Implementasi dan Analisis Attack Tree pada Aplikasi DVWA Berdasar Metrik Time dan Skill Level," *J. Sains Komput. Inform. (J-SAKTI*, vol. 7, no. 2, pp. 838–850, 2023.

[11] M. Alsaffar, S. Aljaloud, and B. A. Mohammed, "Detection of Web Cross-Site Scripting (XSS) Attacks," pp. 1–13, 2022.

[12] D. Demhi, J. R. Batmetan, and O. E. . Liando, "Cross-site Scripting Reflected as A Risk High-Level Attack on University Website," *Int. J. Inf. Technol. Educ.*, vol. 1, no. 3, pp. 103–111, 2022, doi: 10.62711/ijite.v1i3.65.

[13] I. Laleb, "Analisis Cross-Site Scripting (Xss) Injection – Reflected Xss and Stored Xss Mengggunakan Framework Owasp 10," *J. Ilm. Flash*, vol. 8, no. 1, p. 36, 2023, doi: 10.32511/flash.v8i1.952.

[14] K. F. Alenzi and O. A. Bashir Abbas, "A Defensive Framework for Reflected XSS in Client-Side Applications," *J. Web Eng.*, vol. 21, no. 7, pp. 2209–2230, 2022, doi: 10.13052/jwe1540-9589.2179.

[15] H. Dilshan Jayawardana *et al.*, "An Analysis of XSS Vulnerabilities and Prevention of XSS Attacks in Web Applications," no. June, 2023, doi: 10.13140/RG.2.2.21854.00321.

[16] M. Liu, B. Zhang, W. Chen, and X. Zhang, "A Survey of Exploitation and Detection Methods of XSS Vulnerabilities," *IEEE Access*, vol. 7, pp. 182004–182016, 2019, doi: 10.1109/ACCESS.2019.2960449.

[17] F. M. M. Mokbal, W. Dan, A. Imran, L. Jiuchuan, F. Akhtar, and W. Xiaoxi, "MLPXSS: An Integrated XSS-Based Attack Detection Scheme in Web Applications Using Multilayer Perceptron Technique," *IEEE Access*, vol. 7, pp. 100567–100580, 2019, doi: 10.1109/ACCESS.2019.2927417.

[18] X. Song, R. Zhang, Q. Dong, and B. Cui, "Grey-Box Fuzzing Based on Reinforcement Learning for XSS Vulnerabilities," *Appl. Sci.*, vol. 13, no. 4, 2023, doi: 10.3390/app13042482.

[19] K. Joylin Bala, E. Babu Raj, and A. M. Anusha Bamini, "XSS attack prevention over code injection vulnerabilities in web applications," *Int. J. Innov. Technol. Explor. Eng.*, vol. 8, no. 8, pp. 882–886, 2019.

[20] D. Ending Narhudin, B. Irawan, and A. Bahtiar, "Evaluasi Keamanan Website Menggunakan Metode Owasp: Penilaian Terhadap Serangan Injeksi Sql Dan Cross-

Site Scripting (Xss)," *JATI (Jurnal Mhs. Tek. Inform.*, vol. 8, no. 1, pp. 675–680, 2024, doi: 10.36040/jati.v8i1.8700.

[21] B. I. Dewangkara, K. S. Santi, V. A. Putri, and I. M. E. Listartha, "Penerapan Analisis Kerentanan XSS dan Rate Limiting pada Situs Web MTsN 3 Negara Menggunakan OWASP ZAP," *J. Inform. Upgris*, vol. 8, no. 1, pp. 1–6, 2022, doi: 10.26877/jiu.v8i1.10266.

[22] D. Dwi Cahyani, L. P. Windy Puspita Dewi, K. D. Rama Suryadi, and I. M. Edy Listartha, "Analisis Kerentanan Website Smp Negeri 3 Semarapura Menggunakan Metode Pengujian Rate Limiting Dan Owasp," *Inser. Inf. Syst. Emerg. Technol. J.*, vol. 2, no. 2, p. 106, 2022, doi: 10.23887/insert.v2i2.42936.

[23] I. O. Riandhanu, "Analisis Metode Open Web Application Security Project (OWASP) Menggunakan Penetration Testing pada Keamanan Website Absensi," *J. Inf. dan Teknol.*, vol. 4, no. 3, pp. 160–165, 2022, doi: 10.37034/jidt.v4i3.236.

[24] I. M. A. J. Januraga, G. B. P. Wijaya, L. Patrick, and I. M. E. Listartha, "Mendeteksi Keamanan Website SMP Negeri 1 Blahbatuh Menggunakan Metode Open Web Application Security Project (OWASP) Versi 2.11 XSS & Rate Limiting," *Format J. Ilm. Tek. Inform.*, vol. 11, no. 2, p. 137, 2023, doi: 10.22441/format.2022.v11.i2.005.

[25] D. Priyawati, S. Rokhmah, and I. C. Utomo, "Website Vulnerability Testing and Analysis of Internet Management Information System Using OWASP," *Int. J. Comput. Inf. Syst. Peer Rev. J.*, vol. 3, no. 3, pp. 143–147, 2022, doi: 10.29040/ijcis.v3i3.90.

[26] S. A. Hafsari, "Analisis Keamanan Website Pendaftaran Mahasiswa Baru Dengan Munggunakan Metode Vulnerability Assessment TIN : Terapan Informatika Nusantara," vol. 4, no. 11, pp. 698–708, 2024, doi: 10.47065/tin.v4i11.5060.

[27] R. R. Yusuf and T. N. Suharsono, "Pengujian Keamanan Dengan Metode Owasp Top 10 Pada Website Eform Helpdesk," *Pros. Semin. Sos. Polit. Bisnis, Akunt. dan Tek.*, vol. 5, p. 402, 2023, doi: 10.32897/sobat.2023.5.0.3132.

[28] M. Mahdi Maulana Lubis, D. Handoko, and N. Wulan, "Analisis Implementasi Laravel 9 Pada Website E-Book Dalam Mengatasi N+1 Problem Serta Penyerangan Csrf dan Xss," *Januari*, vol. 2023, no. 2, pp. 173–187, 2022, [Online]. Available: https://jurnal.unity-academy.sch.id/index.php/jirsi/index%0Ahttp://creativecommons.org/licenses/by-sa/4.0/

[29] G. Angga Septiawan, K. W. S. Irawan, I. Mayasari, and I. M. E. Listartha, "Analisis Kerentanan XSS dan Rate Limiting Pada Website SMAN 8 Denpasar Menggunakan Framework OWASP ZAP," *J. Inform. Upgris*, vol. 8, no. 1, pp. 6–8, 2022, doi: 10.26877/jiu.v8i1.10271.

[30] J. R. B. Higuera, J. B. Higuera, J. A. S. Montalvo, J. C. Villalba, and J. J. N. Pérez, "Benchmarking approach to compare web applications static analysis tools detecting OWASP top ten security vulnerabilities," *Comput. Mater. Contin.*, vol. 64, no. 3, pp. 1555–1577, 2020, doi: 10.32604/cmc.2020.010885.