RABIT : Jurnal Teknologi dan Sistem Informasi Univrab
Volume 9 No. 2 | Juli 2024 : Hal : 262-270
ISSN CETAK : 2477-2062
ISSN ONLINE : 2502-891X

PENERAPAN TEKNIK PENETRATION TESTING TERHADAP CROSS SITE SCRIPTING (XSS) DALAM PENGEMBANGAN WEBSITE

[1)] Ahmad Alfian Chandra, [2)] Ahmad Turmudi Zy, [3)] Agung Nugroho
[1,2,3)]Teknik Informatika, Fakultas Teknik, Universitas Pelita Bangsa
[1,2,3)] Jl. Inspeksi Kalimalang No.9, Cikarang Selatan,Kabupaten Bekasi, Jawa Barat - Indonesia
E-mail : chandra24@mhs.pelitabangsa.ac.id, turmudi@pelitabangsa.ac.id, agung@pelitabangsa.ac.id

ABSTRAK
Peningkatan penggunaan website dalam berbagai aspek kehidupan sehari-hari telah memunculkan kebutuhan mendesak untuk memastikan keamanan informasi yang disajikan. Salah satu ancaman signifikan dalam keamanan website adalah Cross-Site Scripting (XSS), dimana penyerang menyisipkan kode berbahaya ke dalam halaman web untuk dieksekusi oleh pengguna. Penelitian ini bertujuan untuk menerapkan teknik penetration testing sebagai metode untuk mendeteksi dan mengatasi kerentanan XSS dalam pengembangan website. Penelitian dilakukan melalui tiga tahapan: instalasi software untuk mendukung penetration testing, pelaksanaan penetration testing menggunakan OWASP ZAP untuk mengidentifikasi kerentanan, dan evaluasi serta implementasi solusi untuk mengatasi kerentanan yang ditemukan. Hasil penelitian menunjukkan bahwa penerapan fungsi htmlspecialchars dalam PHP efektif dalam mencegah eksekusi skrip berbahaya, sehingga mengurangi risiko serangan XSS. Selain itu, teknik penetration testing terbukti menjadi metode yang efektif dalam mengidentifikasi dan mengurangi risiko keamanan pada aplikasi web. Dengan demikian, penelitian ini menekankan pentingnya pengujian keamanan yang menyeluruh dan implementasi langkah-langkah pencegahan yang tepat untuk menjaga integritas dan kepercayaan pengguna terhadap aplikasi web.

Kata Kunci: Cross-Site Scripting (XSS), Penetration Testing, OWASP ZAP, Keamanan Website, htmlspecialchars.

ABSTRACT
The increasing use of websites in various aspects of daily life has led to an urgent need to ensure the security of the information presented. One of the significant threats in website security is Cross-Site Scripting (XSS), where an attacker inserts malicious code into a web page to be executed by the user. This research aims to apply penetration testing techniques as a method to detect and resolve XSS vulnerabilities in website development. The research was conducted through three stages: installation of software to support penetration testing, execution of penetration testing using OWASP ZAP to identify vulnerabilities, and evaluation and implementation of solutions to address the vulnerabilities found. The results show that the implementation of the htmlspecialchars function in PHP is effective in preventing the execution of malicious scripts, thereby reducing the risk of XSS attacks. In addition, penetration testing techniques proved to be an effective method in identifying and mitigating security risks in web applications. Thus, this research emphasizes the importance of thorough security testing and implementation of appropriate preventive measures to maintain the integrity and user trust of web applications.

Keyword: *Cross-Site Scripting (XSS), Penetration Testing, OWASP ZAP, Website Security, htmlspecialchars.*

PENDAHULUAN

Dalam era teknologi yang semakin berkembang ancaman siber semakin meningkat setiap hari, dan hampir seluruh dunia merasakan dampaknya. Ancaman siber adalah tindakan kriminal yang merusak, memanipulasi, dan mencuri data penting dari situs website, yang dapat menimbulkan masalah serius untuk keamanan jaringan, database, atau sistem komputer[1]. Website telah menjadi bagian penting dari kehidupan sehari-hari karena menawarkan platform untuk berbagai tugas, seperti bertransaksi dengan bank dan berinteraksi dengan jejaring social. Situs web dahulunya hanya digunakan untuk

DOI : https://doi.org/10.36341/rabit.v9i2.4822

menyebarkan informasi, tetapi sekarang menjadi alat yang dapat membantu masyarakat dalam pekerjaannya[2]. Website didefinisikan sebagai kumpulan informasi yang terdiri dari halaman web yang saling terhubung yang disediakan oleh individu, kelompok, atau pun organisasi. Situs web yang berkualitas tinggi memiliki tampilan visual yang menarik dan memenuhi kebutuhan pengguna[3]. Sebuah website juga dapat didefinisikan sebagai sebuah layanan di suatu domain internet yang terdiri dari satu atau lebih halaman yang dirancang khusus dan dapat diakses oleh orang di internet[4]. Namun, dengan kemajuan ini, pengembang website sering mengabaikan atau mengabaikan masalah baru terkait keamanan informasi. Kerentanan Cross Site Scripting (XSS) adalah salah satu ancaman keamanan yang paling sering digunakan.

Cross-site scripting (XSS) merupakan sebuah eksploitasi keamanan dimana penyerang menyisipkan kode berbahaya (biasanya Javascript) di sisi klien ke suatu halaman web. Ketika kode berbahaya ini bersama dengan halaman web asli akan ditampilkan dalam klien web (browser seperti IE, Mozilla dll), memungkinkan Hacker untuk mendapatkan akses yang lebih besar dari halaman tersebut[5]. Cross-website scripting (XSS) adalah salah satu kerentanan dalam keamanan komputer yang ditemukan dalam aplikasi web. XSS memberdayakan penyerang untuk menyuntikkan *script* pada sisi klien ke halaman situs web yang dilihat oleh pengguna. Kerentanan cross-site scripting dapat digunakan oleh musuh untuk melewati kontrol akses, misalnya, *same-origin policy*[6]. Cross-site scripting yang menargetkan sebuah website dapat membuat sebuah website menyimpan banyak string sebagai payload untuk serangan cross-site scripting. Metode web scraping, yang mengekstraksi dan mengumpulkan data dari sebuah website, dapat mengurangi risiko serangan cross-site scripting[7]. Cross Site Scripting terjadi karena kurangnya pengetahuan tim security dari ancaman terbaru maupun ancaman lama[8]. Oleh karena itu, sangat penting untuk memprioritaskan keamanan informasi, karena setiap akses yang tidak sah atau tidak bertanggung jawab terhadap informasi dapat menimbulkan keraguan terhadap keakuratannya dan berpotensi menyebabkan misinformasi. Di zaman yang serba digital seperti saat ini, sangat penting untuk memahami apa itu keamanan siber dan bagaimana mengguankannya dengan aman di dunia yang tidak dapat dihindari tanpa teknologi dan jaringan. Tanpa perlindungan yang memadai, file, data pribadi, dan aset virtual penting lainnya dapat berada dalam bahaya. Mempertahankan jaringan, perangkat lunak, dan data sensitif dari serangan siber dikenal sebagai keamanan siber. Serangan ini dapat dikategorikan sebagai ekspoitasi sumber daya, akses tidak sah ke sistem, atau serangan ransomware yang mencatat data dengan tujuan pemerasan[9]. Keamanan informasi adalah aset yang sangat berharga bagi organisasi karena merupakan salah satu aset strategis untuk menciptakan nilai bisnis[10]. Karena itu, penggunaan teknologi harus didukung oleh kesadaran akan pentingnya menjaga keamanan informasi agar masyarakat dapat menghindari efek negatif yang mungkin ditimbulkan oleh individu yang tidak bertanggung jawab saat menggunakan teknologi tersebut[11].

Serangan XSS ini dapat membahayakan aplikasi web. Kerentanan ini dapat merusak data pribadi pelanggan, data transaksi, data keuangan dll. Oleh sebab itu penting adanya keamanan pada website dimana nanti bisa diketahui celah yang dapat masuk ke dalam website tersebut[12]. Teknik pengujian penetrasi diperlukan untuk mengatasi masalah ini. Dengan melakukan penetration testing secara berkala, pengembang dapat memastikan

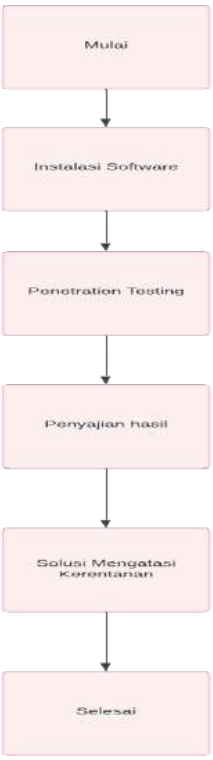
DOI : https://doi.org/10.36341/rabit.v9i2.4822 *Corresponding Author* : Ahmad Alfian Chandra

bahwa aplikasi mereka aman dari serangan XSS dan ancaman keamanan lainnya sebelum aplikasi dirilis ke publik. *Penetration testing* adalah serangkaian proses berisi prosedur dan teknik mengevaluasi keamanan terhadap sistem komputer atau jaringan dengan melakukan simulasi penyerangan untuk mengetahui letak celah-celah kerawanan pada sistem agar kemudian celah tersebut ditutup atau diperbaiki. *Penetration testing* dilakukan sebagai langkah *preventive* untuk mengatasi terjadinya peretasan pada suatu sistem[13]. Penetration testing atau pentesting juga bisa di sebut dengan Untuk menilai risiko yang terkait dengan pelanggaran keamanan yang mungkin terjadi, penguji tidak hanya menemukan kerentanan yang dapat digunakan oleh penyerang tetapi juga mengeksploitasi kerentanan untuk menilai apa yang mungkin didapat oleh penyerang setelah mengeksploitasi kerentanan dengan sukses[14]. Untuk menjamin validitas pengukuran dan penilaian, pengujian berkala secara sistematis diperlukan. OWASP Top 10 telah diuji dalam beberapa kelompok dan telah terbukti dapat mempercepat kategorisasi[15]. Organisasi OWASP telah mengembangkan alat pemindai kerentanan yang dikenal sebagai OWASP ZAP. Karena alat ini terus dikembangkan dan bersifat opensource, ini adalah proyek OWASP yang paling aktif[16]. OWASP memberikan peringkat sepuluh teratas berdasarkan eksploitasi, prevalensi, kemudahan untuk diidentifikasi, dan tingkat dampak kepada OWASP ZAP[17].

Dalam pengembangan website, ada berbagai solusi untuk mengatasi masalah XSS. Solusi untuk masalah XSS yang berasal dari penelitian sebelumnya. Seseorang dapat mencegah serangan cross-site scripting (XSS) dengan mengaktifkan filter XSS web browser dengan mengatur header respons HTTP X-XSSProtection[18]. Perbarui manajemen sesi untuk mencegah serangan Cross-Site Scripting (XSS). Gunakan teknik seperti penggunaan token keamanan, header HTTP yang sesuai, dan sanitasi input pengguna untuk mencegah injeksi skrip berbahaya[19]. Untuk mencegah Cross Site Scripting (XSS) juga bisa menggunakan htmlspecialchars. Fungsi htmlspecialchars() diberikan pada parameter inputan tersebut adalah untuk menghindari serangan xss yang berasal dari url yang menggunakan method $_GET seperti pada script data-index.php[20].

METODE

Pada penelitian ini menggunakan metode experimental dalam pengujiannya dengan menggunakan 4 tahapan, tahap pertama yang dilakukan yaitu persiapan lingkungan penelitian, kemudian melakukan pengujian penetration testing, yang terakhir yaitu implementasi dan evaluasi solusi dari pengujian penetration testing dari kerentanan website. Tahap penelitian yang dilakukan adalah sebagai berikut:



Gambar 1. Alur Metode penelitian

1. **Instalasi Software**

Tahap pertama penelitian adalah dengan melakukan instalasi software untuk menunjang kebutuhan penetration testing

2. **Penetration Testing**

Tahap ketiga penelitian ini adalah dengan melakukan uji penetration testing terhadap website testbed yang sudah di sediakan, dimana website tersebut seolah – olah di serang oleh attacker untuk mengetahui apakah terdapat kerentanan terhadap website tersebut.

3. **Penyajian Hasil**

Tahap ketiga penelitian adalah dengan melakukan Penyajian hasil dari penetration testing yang telah dilakukan, penyajian ini dilakukan untuk evaluasi terhadap developer segera melakukan perbaikan terhadap kerentanan yang telah di temukan.

4. **Solusi Mengatasi Kerentanan**

Tahap keempat penelitian adalah dengan memberikan Solusi untuk mengatasi kerentanan terhadap web supaya tidak terkena serang Cross Site Scripting (XSS).

HASIL

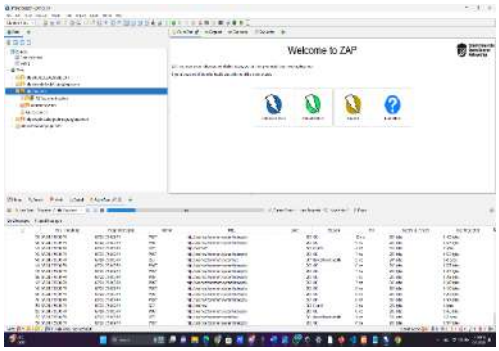
Dalam penelitian ini, peneliti menggunakan website yang memang sudah di sediakan untuk melakukan penetration testing. Penetration testing, atau pentesting, adalah proses yang dilakukan untuk mengevaluasi keamanan sistem komputer, jaringan, atau aplikasi web dengan cara mensimulasikan serangan dari pengguna yang tidak sah (malicious attacker). Penetration testing dilakukan dengan difokuskan terhadap celah keamanan cross site scripting(XSS). Seperti yang sudah di bahas pada metode penelitian peneliti menggunakan metode 3 tahapan pada penelitian penetration testing cross site scripting (XSS). Setelah mengetahui metode - metode apa saja yang digunakan, pada bagian hasil dan pemabahasan akan dijelaskan bagaimana hasil setiap prosesnya. Berikut tahapan hasil dan pembahasannya.

1. **Instalasi Software**

   Beberapa software yang harus di install oleh peneliti untuk melakukan penetration testing ialah menggunakan aplikasi OWASP ZAP dan XAMPP yang di gunakan sebagai tool pengujian Penetration Testing

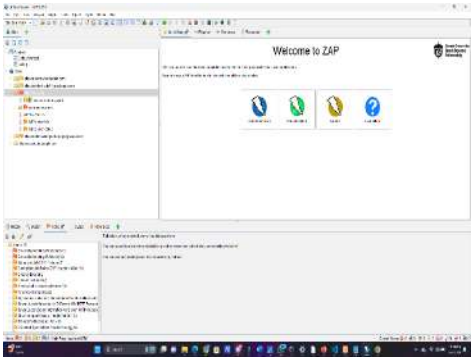
2. **Pelaksanan Penetration Testing**

   Proses Pelaksanaan penetration testing atau proses penguji kerentanan pada website yang telah di sediakan ini di lakukan menggunakan tool OWASP ZAP untuk melakukan scanning dan menemukan kerentanan pada website yang memiliki kerentanan. Berikut proses Penetration Testingnya.



Gambar 2 . Proses Scanning

Pada gambar di atas yaitu proses scanning terhadap website target



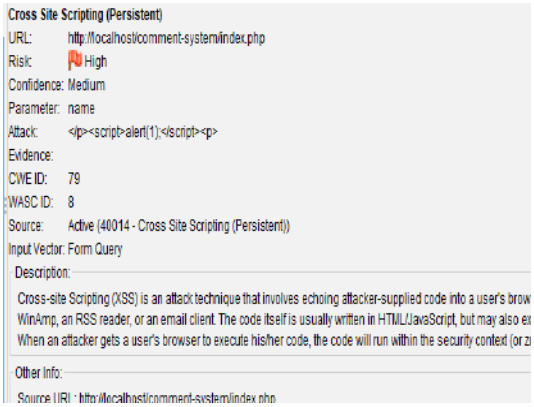
Gambar 3 . Kerentanan Yang Di Temukan

DOI : https://doi.org/10.36341/rabit.v9i2.4822 *Corresponding Author* : Ahmad Alfian Chandra

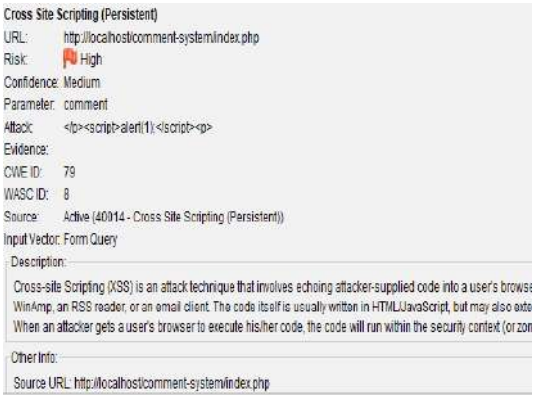
Pada gambar di atas menunjukan bahwa adanya kerentanan Cross Site Scripting di dalam website target yang telah di scanning.

3. Penyajian Hasil

Setelah melakukan Penetration testing di atas, Langkah selanjutnya yaitu penyajian hasil yang telah di scanning menggunakan tool OWASP ZAP. Berikut hasil pengujian.



Gambar 4 . Hasil Scanning Parameter Name



Gambar 5 . Hasil Scanning Parameter Comment

Setelah melakukan penetration testing gambar di atas adalah menunjukan bahwa terdapat kerentanan cross site scripting pada parameter "name" dan "comment" atau kolom inputan name dan comment, tool OWASP ZAP juga melakukan attack injeksi code terhadap parameter "name" dan "comment", arti dari code tersebut yaitu untuk memunculkan sebuah notifikasi yang isi hanya sebuah angka satu.

No	URL	Parameter	Risk
1	http://localhost/comment-system/index.php	name	High
2	http://localhost/comment-system/index.php	comment	High

Tabel 1. Tabel Hasil Scanning

Pada table di atas merupakan penjelasan seberapa parah risiko yang mungkin terjadi pada website yang memiliki kerentan cross site scripting. Penelitian ini menemukaan dua kerentanan pada parameter "name" dan "comment". Untuk membuktikannya bisa di lihat pada gambar berikut.

Gambar 6 . Proses Pembuktian

Pada gambar di atas mencoba untuk memasukan code yang telah di berikan oleh tool OWASP ZAP di dalam kolom inputan name dan yang di bawah itu kolom komentar nya apakah benar bisa memunculkan notifikasi dan isinya angka satu.

DOI : https://doi.org/10.36341/rabit.v9i2.4822
Corresponding Author : Ahmad Alfian Chandra

Gambar 7 . Hasil Dari Pembuktian

Pada gambar di atas adalah sebuah notifikasi yang di eksekusi oleh kolom inputan name tadi setalah klik submit langsung memunculkan notifikasi yang isi notifikasi berikut hanya angka satu, berarti code yang di berikan oleh tool OWASP ZAP itu benar dan pada kolom name tersebut memiliki celah keamanan Cross Site Scripting.

4. Solusi Mengatasi Kerentaran

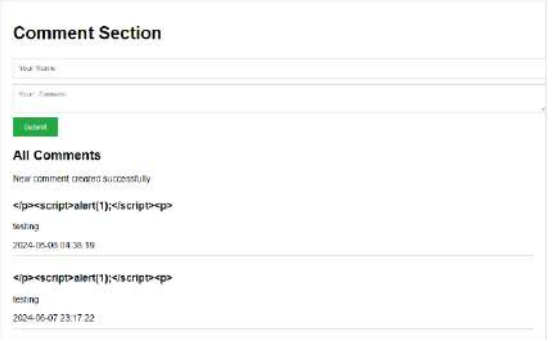
Solusi untuk mengatasi kerentanan cross site scripting yaitu menggunakan fungsi htmlspecialchars untuk mengonversi karakter khusus seperti <, >, &, dan " menjadi entitas HTML yang aman, supaya mencegah eksekusi skrip berbahaya yang disisipkan oleh orang yang tidak bertanggung jawab. Berikut gambar source code yang telah menggunakan htmlspecialchars dan pengujian ulang pada website setelah menggunakan htmlspecialchars.

Gambar 8 . Source Code Sebelum Perbaikan

Pada gambar di atas adalah sebuah code PHP yang sebelum menggunakan fungsi htmlspecialchars.

Gambar 9 . Source Code Setelah Perbaikan

Pada gambar di atas adalah sebuah code PHP yang sudah menggunakan fungsi htmlspecialchars, yang dimana penempatannya itu di baris code yang akan menghasilkan ouput pada kolom inputan name dan comment.



Gambar 10 . Hasil Pengujian Ulang Parameter Name

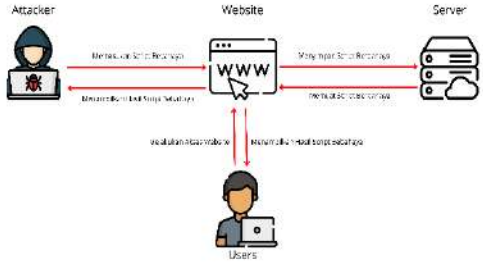
Pada gambar di atas adalah hasil pengujian ulang menggunakan code yang sama, yang dimana code tersebut seharusnya tidak bisa melakukan eksekusi untuk menampilkan notifikasi dan harus menjadi text biasa yang bisa di tampilkan di halaman web.

Gambar 11 . Pengujian Ulang Parameter Comment

DOI : https://doi.org/10.36341/rabit.v9i2.4822
Corresponding Author : Ahmad Alfian Chandra

Pada gambar di atas adalah hasil pengujian pada kolom inputan comment, yang dimana code tersebut menjelaskan untuk memindahkan halaman website ke website lain, contoh di atas yaitu untuk pindah ke website google.com. Hal ini akan bisa di gunakan oleh attacker untuk memindahkan ke halaman website yang memang sudah di sedikan oleh attacker.

5. Simulasi Kerentanan



Gambar 12 . Simulasi Kerentanan Yang Terjadi

Pada gambar di atas merupakan simulasi Ketika attacker menyerang website dan di akses oleh users. Berikut penjelasan dari keseluruhan simulasi diatas:

1. Attacker melakukan akses kepada website dan memasukan script berbahaya pada kolom inputan website yang sudah di targetkan.
2. Website melakukan penyimpanan script berbahaya kepada server.
3. Server memuat script kepada website target.
4. Website menampilkan hasil dari script berbahaya yang sudah di masukan oleh attacker, apabila ini terjadi tandanya attacker sudah berhasil dan bisa saja attacker menggunakan script yang Ketika users melakukan akses langsung pindah ke website clone yang sudah di buat oleh attacker.
5. Users melakukan akses website yang dimana users tersebut tidak mengetahui website tersebut terkena serangan.
6. Setelah di akses oleh users website akan menampilkan hasil script berbahaya yang dilakukan oleh attacker.

Setelah di akses oleh users website akan menampilkan hasil script berbahaya yang dilakukan oleh attacker.Setelah di akses oleh users website akan menampilkan hasil script berbahaya yang dilakukan oleh attacker.

KESIMPULAN

Kesimpulan dari penelitian ini adalah bahwa penerapan teknik penetration testing sangat efektif dalam mendeteksi dan mengatasi kerentanan Cross-Site Scripting (XSS) dalam pengembangan website. Penelitian ini menggunakan OWASP ZAP sebagai alat untuk melakukan scanning terhadap kerentanan XSS dan menemukan bahwa

DOI : https://doi.org/10.36341/rabit.v9i2.4822 *Corresponding Author* : Ahmad Alfian Chandra

parameter input seperti "name" dan "comment" pada website memiliki risiko tinggi terhadap serangan XSS. Solusi yang diberikan, yaitu penggunaan fungsi htmlspecialchars dalam PHP, terbukti mampu mencegah eksekusi skrip berbahaya, sehingga meningkatkan keamanan website secara signifikan. Dengan demikian, penelitian ini menekankan pentingnya pengujian keamanan yang menyeluruh dan implementasi langkah-langkah pencegahan yang tepat untuk menjaga integritas dan kepercayaan pengguna terhadap aplikasi web.

DAFTAR PUSTAKA

[1] S. Parulian, D. A. Pratiwi, and M. Cahya Yustina, "Ancaman dan Solusi Serangan Siber di Indonesia." [Online]. Available: http://ejournal.upi.edu/index.php/TELNECT/

[2] I. 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." [Online]. Available: https://www.zaproxy.org/download/.

[3] I. Rochmawati, "Analisis User Interface Situs Web Iwearup.Com," 2019. [Online]. Available: www.iwearup.com

[4] A. Sultan Hakim, T. Adi Cahyanto, and H. Azizah, "Serangan Cross-Site Scripting (Xss) Berdasarkan Base Metric CVSS V.2."

[5] S. Suroto and A. Asman, "Ancaman Terhadap Keamanan Informasi Oleh Serangan Cross-Site Scripting (XSS) Dan Metode Pencegahannya," 2021. [Online]. Available: http://www.hackers.com?yid=

[6] P. Negeri, K. / Jurusan, T. Elektro, T. Komputer, and D. Jaringan, "Analisis Cross-Site Scripting (Xss) Injection-Reflected Xss And Stored Xss Mengggunakan Framework OWASP 10 Indah O. Laleb", [Online]. Available: http://attack.com/page.php?something=someth

[7] I. Y. Prabhaswara, I. Made, A. D. Suarjaya, N. Kadek, and D. Rusjayanthi, "Pengembangan Engine Web Crawler Sebagai Pencari Jejak Serangan Cyber Stored Cross-Site Scripting," 2023.

[8] M. I. Hany, A. Bhawiyuga, and A. Kusyanti, "Implementasi Cross Site Scripting Vulnerability Assessment Tools berdasarkan OWASP Code Review," 2021. [Online]. Available: http://j-ptiik.ub.ac.id

[9] A. Hidayat, Y. Samudra, P. Lely, and P. Andriyanto, "AMMA : Jurnal Pengabdian Masyarakat Sosialisasi Pengenalan Pentingnya Cyber Security Bagi Siswa Untuk Membangun Keamanan Informasi Dalam Era Digital," vol. 2, no. 5, 2023.

[10] E. Novianto *et al.*, "Some rights reserved BY-NC-SA 4.0 International License Keamanan Informasi (Information Security) Pada Aplikasi Sistem Informasi Manajemen Sumber Daya Manusia 1)," vol. 8, no. 1, pp. 10–15, 2023, doi: 10.36341/rabit.vx8i1.2966.

[11] E. W. Tyas Darmaningrat *et al.*, "Sosialisasi Bahaya dan Upaya Pencegahan Social Engineering untuk Meningkatkan Kesadaran Masyarakat tentang Keamanan Informasi," *Sewagati*, vol. 6, no. 2, Feb. 2022, doi: 10.12962/j26139960.v6i2.92.

[12] M. A. Z. Risky and Y. Yuhandri, "Optimalisasi dalam Penetrasi Testing Keamanan Website Menggunakan Teknik SQL Injection dan XSS," *Jurnal*

Sistim Informasi dan Teknologi, pp. 215–220, Aug. 2021, doi: 10.37034/jsisfotek.v3i4.68.

[13] S. Hidayatulloh and D. Saptadiaji, "Penetration Testing pada Website Universitas ARS Menggunakan Open Web Application Security Project (OWASP)." [Online]. Available: http://jurnal.itg.ac.id/

[14] M. Rozali and M. Dayan Sinaga, "Diagnosis Keamanan Web Menggunakan Metode Uji Penetrasi Website Sekolah Web Security Diagnosis Using School Website Penetration Test Method," 2024, [Online]. Available: http://kti.potensi-utama.ac.id/index.php/JID

[15] D. F. Priambodo, A. D. Rifansyah, and M. Hasbi, "Penetration Testing Web XYZ Berdasarkan OWASP Risk Rating," *Teknika*, vol. 12, no. 1, pp. 33–46, Feb. 2023, doi: 10.34148/teknika.v12i1.571.

[16] A. Elanda and R. Lintang Buana, "Analisis Kualitas Keamanan Sistem Informasi E-Office Berbasis Website Pada Stmik Rosma Dengan Menggunakan OWASP TOP 10," 2021.

[17] K. Nisa, A. Putra, R. A. Siregar, and M. Dedi Irawan, "Bulletin of Information Technology (BIT) Analisis Website Tapanuli Tengah Menggunakan Metode Open Web Application Security Project Zap (Owasp Zap)," vol. 3, no. 4, pp. 308–316, 2022, doi: 10.47065/bit.v3i1.

[18] I. Riadi, R. Umar, T. Lestari, S. Informasi, and U. Ahmad Dahlan, "Analisis Kerentanan Serangan Cross Site Scripting (XSS) pada Aplikasi Smart Payment Menggunakan Framework OWASP," 2020.

[19] D. E. Narhudin, B. Irawan, and A. Bahtiar, "Evaluasi Keamanan Website Menggunakan Metode Owasp: Penilaian Terhadap Serangan Injeksi Sql Dan Cross-Site Scripting (XSS)," 2024. [Online]. Available: https://rachmagroup.co.id

[20] A. Wira Utama and A. Senja Fitrani, "Techniques For Testing Website Security Using The Escaping Metacharacter Method Teknik Menguji Keamanan Website Dengan Menggunakan Metode Escaping Metacharacter," 2022.