PENGUJIAN KEAMANAN APLIKASI BERBASIS WEBSITE : SYSTEMATIC LITERATURE REVIEW

Naufal Daffa Fernaldy, Nurul Maharani Piranti, Catur Susaningsih
Politeknik Imigrasi
Jalan Satria-Sudirman, RT.001/RW.014, Tanah Tinggi, Kec. Tangerang, Kota Tangerang, Banten 15119
daffafernaldy2002@gmail.com

ABSTRAK

Peran keimigrasian sangat bermanfaat saat ini dimana lalu lintas orang asing merupakan hal yang lumrah terjadi di antar negara di seluruh dunia, dimana keimigrasian sendiri mengatur lalu lintas masuk dan keluarnya orang asing. Untuk mendukung sarana dan prasarana yang memadai, tidak lepas dari yang namanya teknologi informasi dan digitalisasi. Dimana sangat bermanfaat demi efisiensi baik sumber daya alam maupun sumber daya manusia yang digunakan. Kantor Imigrasi di Indonesia saat ini sudah menggunakan berbagai macam aplikasi dan website untuk mendukung berjalannya pelayanan publik dan penegakan hukum keimigrasian. Keamanan aplikasi dan website memiliki peran yang krusial dimana didalamnya mencakup data-data rahasia dan penting, serta berguna untuk pengembangan perangkat lunak modern. Studi ini menggunakan metodoe (OWASP) Open Web Application Security Project yang menyediakan berbagai metode dan panduan untuk mengidentifikasi dan mengatasi celah keamanan dan website. Penelitian ini bertujuan untuk menganalisis efektivitas penggunaan metode (OWASP) dengan teknik utama seperti OWASP top 10, OWASP Testing Guide, dan OWASP ZAP (Zed Attack Proxy). Metode penelitian ini melibatkan studi kasus pada sebuah aplikasi web untuk mengidentifikasi masalah dan celah keamanan serta kesalahan konfigurasi. Hasil pengujian menunjukkan bahwa metode OWASP mampu mengidentifikasi berbagai macam celah dan kesalahan konfigurasi yang ada pada website tersebut dengan tingkat akurasi yang tepat serta memberikan rekomendasi pencegahan. Pengujian keamanan ini menjadi solusi yang efektif bagi developer untuk memperbaiki dan meningkatkan ketahanan aplikasi terhadap serangan siber yang tidak diinginkan.

Kata kunci : *Pengujian Keamanan, OWASP, Mitigasi Kerentanan*

1. PENDAHULUAN

Perkembangan teknologi digital yang sangat cepat membuat meningkatnya pemanfaatan dan penggunaan aplikasi web dalam berbagai sektor. Tetapi, seiring dengan kemajuan tersebut ancaman yang dihadapi dalam penggunaan aplikasi semakin banyak dan kompleks. Serangan siber seperti injeksi SQL, cross-site scripting (XSS) dan phishing menjadi ancaman yang sangat serius yang dapat mengakibatkan kejahatan seperti pencurian data, gangguan layanan, serta kerugian materi dan finansial. Sehingga, pengujian keamanan aplikasi dan website menjadi indikator yang penting dalam pengembangan perangkat lunak.

Salah satu cara untuk mengidentifikasi celah keamanan adalah metode yang dikembangkan oleh Open Web Application Security Project (OWASP) yang berasal dari Amerika. OWASP menyediakan berbagai layanan untuk pengujian keamanan dan terbukti mengatasi celah yang dapat memicu kejahatan siber. Seperti OWASP top 10 yang berguna sebagai panduan pengujian keamanan yang menampilkan daftar 10 ancaman yang relevan dengan perkembangan saat ini. OWASP memiliki tools yang bernama OWASP Zed Attack Proxy (ZAP). Tools ini digunakan untuk mengidentifikasi potensi kerentanan dalam aplikasi secara otomatis.

Penelitian ini diharapkan dapat mengidentifikasi Tingkat keefektifan penggunaan metode OWASP ini untuk pengujian keamanan aplikasi website. Penelitian ini akan menelaah beberapa jurnal yang mengangkat topik pengujian keamanan menggunakan pendekatan berbasis OWASP serta membaca kesimpulan serta hasil yang kemudian akan dijabarkan pada jurnal ini, guna meningkatkan ketahanan aplikasi terhadap ancaman siber. Metode OWASP terbukti efektif dalam menangani kerentanan pada aplikasi berbasis web.[28]

2. TINJAUAN PUSTAKA

Pandemi covid-19 mendorong digitalisasi pada setiap aspek di pemerintahan, tak terkecuali di kantor imigrasi dimana pelayanan publik dan penegakan hukum memanfaatkan aplikasi berbasis website yang dilakukan secara daring. [1].

Setiap bulannya, Kantor Imigrasi menerima ribuan permohonan dari warga Negara Indonesia [2].

Keamanan jaringan sangat penting dimana didalamnya memuat data-data penting yang seharusnya menjadi prioritas organisasi dalam keamananannya.[3].

OWASP ZAP (Zed Attack Proxy) adalah sebuah aplikasi yang digunakan untuk penetration testing dalam menemukan celah keamanan (vulnerabilities) pada suatu aplikasi website yang menyediakan pemindai secara automatis.[4].

Celah keamanan yang dieksploitasi oleh penyerang ini disebebkan oleh kurangnya maintenance dan pemantauan dan perlindungan yang ada pada aplikasi tersebut, serta harus dilakukan langkah tepat untuk mitigasi dari serangan mendatang.[5]

Keamanan jaringan bergantung pada kecepatan jaringan untuk mengambil tindak lanjut pada sistem saat terjadi adanya gangguan.[6]

Aplikasi web merupakan salah satu platform yang saat ini lumrah digunakan dalam berbagai organisasi di pemerintahan karena kemudahannya dalam diakses yang juga menjadi sasaran populer dari berbagai ancaman siber.[7]

Pengujian ini menerapkan panduan OWASP WSTG untuk mengidentifikasi dan menguji celah keamanan pada sebuah website yang menyoroti efektivitas WSTG dalam mendeteksi celah keamanan serta memberikan rekomendasi perbaikan[8]

Penelitian ini menggabungkan metode penetration testing dan framework OWASP untuk mengidentifikasi kerentanan website yang diterapkan pada sebuah instansi.[9]

tudi ini membandingkan metode ISSAF dan OWASP yang menujukkan bahwa kedue metode tersebut efektif untuk mencari celah keamanan. Jika OWASP lebih fokus pada aplikasi web, sementara ISSAF memiliki cakupan yang lebih luas.[10]

Pentingnya pemilihan alat serta teknik yang sesuai untuk pengujian keamanan sistem.[11]

Pengujian keamanan adalah sebuah metode untuk mencari celah keamanan yang biasanya diterobos oleh oknum tidak bertanggungjawab, di Amerika sendiri penerobosan ini menyebabkan kerugian sebesar 9,44 juta dolar AS.[12]

Penetration test merupakan sebuah test yang diujicobakan ke sebuah website dengan cara simulasi penyerangan, dimana melalui teknik tersebut nantinya akan mengidentifikasi celah apa saja yang ada pada web tersebut serta menemukan solusinya.[13]

Pengujian keamanan sering disalahpahami. Pengujian keamanan membutuhkan pengalaman mendalam tentang mempelajari pola pikir dari penyerang, mempelajari manajemen resiko serta didasarkan pada realitas arsitektur sistem.[14]

Keamanan website bukan serta merta hanya diuji lalu ditemukan masalahnya. Lebih dari itu, keamanan website sendiri merupakan rangkaian yang saling berkaitan satu sama lain antara pengembangan chip dan perangkat sensor yang aman. Semua bersinergitas membentuk suatu rangkaian yang bersatu-padu membentuk sebuah keamanan.[15]

Serangkaian pedoman yang ada pada OWASP Top10 menjadi dasar rancangan keamanan aplikasi.[16]

Cross site scripting merupakan salah satu ancaman bahaya karena paling sering umum digunakan denga tujuan untuk memasukkan kode jahat atau digunakan sebagai bagian dari serangan phishing.[17]

Pengujian menggunakan OWASP berhasil dan menemukan celah keamanan yang memanfaatkan kesalahan sistem dalam memvalidasi masukan pada formulir yang dapat dimanfaatkan oleh orang tidak bertanggungjawab.[18]

Berdasarkan data yang disajikan, Indonesia menjadi target rawan para hacker, maka dari itu perlu adanya peningkatan keamanan serta peningkatan kepedulian terhadap keamanan website.[19]

Tidak ada sistem yang benar-benar aman, aktivitas setiap jaringan perlu dipantau setiap saat.[20]

Pengujian penetrasi berhasil mengidentifikasi tingkat kerentanan dari rendah hingga sedang.[21]

Peengujian keamanan dengan metode OWASP terbukti efektif.[22]

Pengujian keamanan yang dilakukan menggunakan Webkiller, OWASP ZAP, Dirsearch dan Nuclei dengan hasil menunjukkan bahwa system access control pada sebuah website memiliki beberapa kerentanan yang dapat dieksploitasi[23]

OWASP Zap sebagai security testing tools memiliki fitur-fitur yang sangat membantu dalam proses pengujian sistem.[24]

Pengujian menggunakan OWASP ZAP menunjukkan 19 kerentanan yang perlu diatasi.[25]

OWASP merupakan metode untuk menguji aplikasi berbasis web yang dapat menunjukkan tentang seberapa baikkah manajemen otentifikasi, otorisasi, dan manajemen sesi sebuah website.[26]

Website merupakan sekumpulan halaman pada sebuah domain di internet yang memuat tentang hal-hal yang ditujukan dan dapat diakses secara luas melalui halaman depan menggunakan URL.[27]

Metode OWASP terbukti efektif dalam menangani kerentanan pada aplikasi berbasis web.[28]

Lembaga non-profit OWASP memiliki berbagai metode untuk pengujian keamanan yang terbukti efektif.[29]

Aplikasi berbasis website merupakan salah satu platform yang memiliki celah keamanan siber yang memiliki berbagai ancaman.[30]

OWASP ZAP mampu menemukan berbagai jenis kerentanan dan terbukti efektif sedangkan tools SQLMAP hanya berfokus kepada 1 serangan yaitu SQL Injection. [31]

3. METODE PENELITIAN

Penelitian ini menggunakan survey menyeluruh tentang metode pengujian keamanan apa yang cocok digunakan dan tepat untuk menguji suatu celah keamanan yang ada pada sebuah aplikasi website. Metode yang digunakan disini yaitu metode PRISMA (Preferred Reporting Items for Systematic Reviews and Meta-Analyses) Yaitu sebuah pedoman yang ada dalam penelitian transparansi dan meningkatkan kualitas pelaporan. Melalui proses identifikasi yaitu proses pencarian literatur yang jelas dan terstruktur dari berbagai database seperti google scholar serta menggunakan kata kunci yang relevan dan sistematis. Tahap selanjutnya yaitu screening atau penyaringan dengan menyeleksi artikel berdasal judul yang sesuai. Tidak lupa untuk mengecek kelayakan dari artikel tersebut apakah studi telah sesuai untuk dimasukkan dalam analisis. Kemudian artikel yang telah memenuhi kriteria akan dianalisis menjadi temuan bermakna.

Gambar 1. Flowchart Penelitian

3.1. Tahap 1 : Kriteria kelayakan artikel

Ditentukan oleh Inclusion Criteria, yaitu :

a. IC1 : artikel wajib merupakan penelitian asli yang sudah dipelajari dan ditulis dalam bahasa Inggris dan Indonesia
b. IC2 : artikel diterbitkan pada tahun 2004-2024.
c. IC3 : artikel bertujuan menganalisis metode dan perangkat peneliti lain untuk dikembangkan

Tabel 1. Hasil Seleksi Jurnal Penelitian

Sumber	Pengujian Keamanan Aplikasi Website	Pengujian Keamanan OWASP	Kandidat	Terpilih
Google Scholar	76.200	863	50	25
IEEE	5	5	5	4
ACM Digital Library	17.804	836	5	1

Tabel 2. Pertanyaan Penelitian. SLR ini memberikan jawaban atas Research Question berikut

ID	Pengujian Keamanan Aplikasi Website	Pengujian Keamanan OWASP
RQ 1	Metode apa yang pernah diusulkan peneliti sebelumnya untuk melakukan Pengujian Keamanan Aplikasi Website?	Mengidentifikasi dan menelaah metode dan platform yang telah digunakan peneliti sebelumnya untuk pengujian keamanan website.
RQ 2	Bagaimana metode OWASP membantu peneliti dalam pengujian keamanan aplikasi website?	Mengidentifikasi metode yang paling efektif dan mudah digunakan dalam pengujian keamanan website.
RQ 3	Seberapa efektif pengujian keamanan dengan metode OWASP dalam mencegah serangan siber?	Mengidentifikasi efektivitas metode yang digunakan dalam pengujian keamanan website.

3.2. Tahap 2 : Penetapan sumber literatur

a. Literatur dicari pada basis data daring dengan repositori signifikan untuk studi akademis menggunakan Harzing's Publish and Perrish dimana aplikasi tersebut bisa memua jurnal dari berbagai media seperti Google Scholar, Scopus dan serta melalui IEEE.
b. Pada artikel yang telah memenuhi syarat pada IC dilakukan juga pencarian artikel lain yang berhubungan dengan penelitian ini.

3.3. Tahap 3 : Pemilihan Literatur

a. Kata Kunci penentuan pertama adalah "Pengujian Keamanan Aplikasi Website" dan "Pengujian Keamanan OWASP".
b. Berguna untuk mengeksplorasi serta memilih judul abstrak dan artikel.
c. Kata kunci didapat dari hasil pencarian kelayakan kriterian yang sudah ditentukan.
d. Membaca artikel yang telah lolos pada tahap sebelumnya sesuai kriteria baik secara menyeluruh ataupun hanya sebagian untuk pertimbangan peninjauan lebih lanjut.
e. Artikel yang telah terpilih dinilai kembali untuk menemukan penelitian lain yang berkaitan

3.4. Tahap 4 : Pengumpulan Data

Data yang diperoleh dikumpulkan secara manual dengan membuat formulir ekstraksi data. Penelitian ini memfilter 200 jurnal berdasarkan kata kunci "Pengujian keamanan aplikasi website" dan 200 jurnal berdasarkan kata kunci "Pengujian Keamanan OWASP". Dari seluruh artikel, 30 jurnal ilmiah memenuhi syarat untuk dijadikan bahan penelitian, serta didapatkan kesimpulan yaitu dengan metode apakah yang paling banyak digunakan untuk pengujian keamanan website.

4. HASIL DAN PEMBAHASAN

Tabel 3. Hasil tinjauan literatur

NO	Judul	Tahun	Metode	Platform
1.	Analisis Kerentanan Keamanan Website Dengan Menggunakan Metode Penetration Testing dan Framework OWASP (Studi Kasus : Website Instansi XYZ)	2024	OWASP	Website

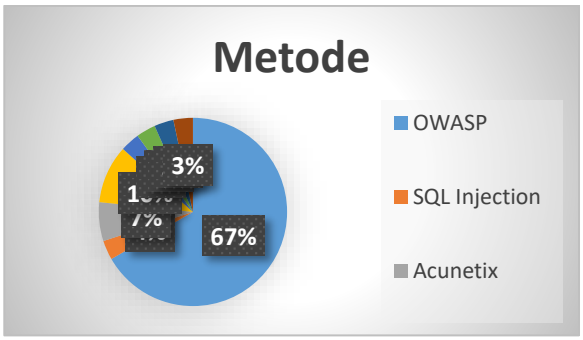
NO	Judul	Tahun	Metode	Platform
2.	Analisis Keamanan Web Server Open Journal System (OJS) Menggunakan Metode ISSAF dan OWASP (Studi Kasus OJS Universitas Lancang Kuning)	2020	ISSAF dan OWASP	Website
3.	Pengujian dan Analisis Keamanan Website Menggunakan Acunetix Vulnerability Scanner	2022	Acunetix Vulnerability Scanner	Website
4	Implementasi Vulnerability Assessment OWASP Pada Website Universitas Teknologi Mataram	2024	OWASP	Website
5	Pengujian Keamanan Fitur Upload File Pada Sistem Aplikasi Web	2022	Secure Coding	Aplikasi
6	Pengujian Kerentanan Celah Keamanan Website Menggunakan Threat Modelling Pada Website Prodi Teknologi Rekayasa Komputer Jaringan	2024	Threat Modelling	Website
7	Analisis Keamanan Sistem Website Menggunakan Metode Open Web Application Security Project Pada SIMANTEP.ID	2024	OWASP	Website
8	Analisis Keamanan Website Dengan ISSAF dan OWASP	2023	ISSAF dan OWASP	Website
9	Pengujian Celah Keamanan Menggunakan Metode OWASP Pada Website XYZ	2022	OWASP WSTG	Website
10	Penerapan Keamanan OWASP Terhadap Aplikasi GTFW Pada Website Universitas Battuta	2021	OWASP	Aplikasi
11	What is security testing? How to check the security strength of your application?	2023	Vulnerability Scanning, Penetration Testing	Website
12	What is network penetration testing?	2023	Penetration Testing	Website
13	Software security testing	2004	Blackbox Testing	Website
14	Exploring advanced techniques for security testing of sensor device chips	2024	Peningkatan keamanan perangkat keras serta memperkuat manajemen data	Web Programming
15	Evaluating Mobile Banking Security Posture Using the OWSP's MASVS Framework	2023	OWASP	Website
16	Pendeteksian keamanan website SMA Greenschool menggunakan metode OWASP dengan pengujian XSS	2022	OWASP	Website
17	Pengujian celah keamanan input validation pada aplikasi website menggunakan framework OWASP	2023	OWASP	Website
18	Analisis pengujian keamanan website pengelolaan internet Desa Kragan menggunakan metode penetration testing execution standard (PTES)	2024	Penetration Testing Execution Standard (PTES)	Website
19	Pengujian dan Analisa Keamanan Website Terhadap Serangan SQL Injection (Studi Kasus : Website UMK)	-	SQL Injection	Website
20	Pengujian keamanan website JDIH Kab.Tegal menggunakan Acunetix dengan standar ISO/IEC/27001:2013	2025	Acunetix	Website
21	Pengujian keamanan dengan metode OWASP Top 10 pada website eform helpdesk	2023	OWASP	Website
22	Analisis Keamanan dan Pengujian Access Control pada website pendidikan : Studi kasus di Universitas Hamzanwadi Lombok	2024	OWASP ZAP, Nuclei, Webkiller	Website
23	Pengujian keamanan sistem informasi berbasis web berdasarkan framework OWASP WSTG v4.2 (Studi kasus : Sistem Sekawan v1 Univesitas Islam Indonesia)	2022	OWASP WSTG	Website
24	Implementasi OWASP ZAP untuk pengujian keamanan sistem informasi akademik	2022	OWASP	Website
25	Penerapan pengujian keamanan web server menggunakan metode OWASP versi 4 (Studi Kasus Web Server Ujian Online)	2015	OWASP	Website
26	Pengujian celah keamanan website menggunakan teknik penetration testing dan metode OWASP Top 10 pada website SIM xxx	2021	OWASP	Website
27	Evaluasi Risikio celah keamanan pada aplikasi web dengan penilaian kerentanan dan pengujian penetrasi menggunakan metode OWASP dan NIST SP 800—revisi 1	2024	OWASP	Aplikasi Website
28	Implementasi OWASP Mobile Security Testing Guide (MSTG) untuk pengujian keamanan pada aplikasi berbasis android	2019	OWASP MSTG	Aplikasi Android
29	Pengujian keamanan web juice shop dengan metode	2023	OWASP	Website

NO	Judul	Tahun	Metode	Platform
	pentesting berbasis OWASP Top 10			
30	Pengujian penetrasi jaringan menggunakan OWASP ZAP dan SQLMAP untuk mengidentifikasi kerentanan keamanan website	2024	OWASP	Website

Tabel diatas menyimpulkan bahwa website menjadi platform pengujian keamanan yang lebih populer, karena kemudahannya dalam diakses, serta lebih populer. Website memberikan fleksibilitas kepada pengguna untuk diakses dimana saja dan kapan saja. Kedua, pengoperasian website cukup dengan membuka browser yang sudah ada pada masing-masing perangkat tanpa mengunduh aplikasi terlebih dahulu. Metode yang digunakan peneliti sebelumnya untuk menentukan metode yang digunakan dalam pengujian keamanan aplikasi dan website seperti metode OWASP, metode ISSAF, Acunetix Vulnerability Scanner, Secure Coding dan Threat Modelling. Terdapat dua metode yang sering digunakan dalam pengujian keamanan aplikasi website, yaitu Metode OWASP dan ISSAF. Dari kedua metode tersebut dilakukan pengembangan perangkat lunak melalui proses perencanaan, analisa, desain, serta implementasi pada sistem aplikasi website. Disimpulkan bahwa metode OWASP yang paling sering digunakan oleh peneliti untuk pengujian keamanan serta bisa digunakan secara gratis. Serta terbukti dari beberapa sumber literatur OWASP memiliki kemampuan untuk mengidentifikasi beberapa celah keamanan secara sistematis.

4.1. *Research Question*

Tahap pertama hasil pertanyaan tentang apa metode pengujian keamanan website yang paling sering digunakan dan efektif dilakukan oleh peneliti sebelumnya yaitu dengan grafik sebagai berikut.



Gambar 2. Grafik jumlah metode pengujian.

Berdasarkan Gambar 2, sebagian besar penelitian pengujian keamanan memanfaatkan metode OWASP. Peneliti terdahulu memanfaatkan metode OWASP karena OWASP digunakan secara luas dalam industri sebagai referensi utama untuk mengidentifikasi dan mengatasi celah keamanan, menyediakan daftar 10 besar resiko ancaman terbaru serta memastikan pengujian tetap relevan, mudah diakses dan open source dapat digunakan secara gratis.

5. KESIMPULAN DAN SARAN

Dari berbagai penelitian yang telah penulis baca, metode OWASP terbukti efektif dalam mengidentifikasi dan mengatasi celah keamanan website seperti SQL Injection, XSS, dan Broken Authentication. Alat bantu seperti OWASP ZAP, ASVS serta metode seperti ISSAF dan PTES sangat membantu dalam pengujian yang sistematis yang berguna untuk mencegah ancaman siber di kemudian hari. Namun pengujian keamanan bukan hanya bergantung kepada tools yang digunakan, tapi juga harus disertai pola pikir untuk pencegahan dari ancaman bahaya siber yang terus bekembang sesuai dengan perkembangan zaman dan teknologi. Namun perlu adanya pelatihan keamanan yang berlanjut bagi pengembang untuk melakukan pengujian keamanan secara berkelanjutan, menggunakan metode lain selain OWASP serta diharapkan di penelitian selanjutnya, peneliti dapat memperbanyak referensi literatur serta selalu mengikuti perkembangan pola serangan siber.

DAFTAR PUSTAKA

[1] A. Zirwan, “Pengujian dan Analisis Kemanan Website Menggunakan Acunetix Vulnerability Scanner,” *J. Inf. dan Teknol.*, vol. 4, no. 1, pp. 70–75, 2022, doi: 10.37034/jidt.v4i1.190.

[2] S. C. W. G. J. Priati Assiroj, “Analisis Efektivitas Aplikasi E-Arsip Pada Kantor Imigrasi Kelas I Tpi Cilacap,” 2023, [Online]. Available: https://www.mendeley.com/search/?query=priati+assiroj&dgcid=md_homepage

[3] M. Aqsa, M. Davi, J. B. Aceh, M. Km, and B. Indonesia, “Pengujian Kerentanan Celah Keamanan Website Menggunakan Threat Modelling Pada Website Prodi Teknologi Rekayasa Komputer Jaringan,” vol. 4, no. 2, pp. 198–208, 2024.

[4] G. Guntoro, L. Costaner, and M. Musfawati, “Analisis Keamanan Web Server Open Journal System (Ojs) Menggunakan Metode Issaf Dan Owasp (Studi Kasus Ojs Universitas Lancang Kuning),” *JIPI (Jurnal Ilm. Penelit. dan Pembelajaran Inform.*, vol. 5, no. 1, p. 45, 2020, doi: 10.29100/jipi.v5i1.1565.

[5] D. Supriadi, E. Suryadi, R. Muslim, L. D. Samsumar, and U. T. Mataram, “IMPLEMENTASI VULNERABILITY ASSESSMENT OWASP (OPEN WEB APPLICATION SECURITY PROJECT) PADA WEBSITE,” vol. 1, no. 4, pp. 232–240, 2024.

[6] 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.

[7] M. A. Al Hilmi and R. K. Yunan, "Pengujian Keamanan Fitur Upload File pada Sistem Aplikasi Web," *J. Inform. J. Pengemb. IT*, vol. 7, no. 1, pp. 37–42, 2022, doi: 10.30591/jpit.v7i1.3336.

[8] A. I. Rafeli, H. B. Seta, and I. W. Widi, "Pengujian Celah Keamanan Menggunakan Metode OWASP Web Security Testing Guide (WSTG) pada Website XYZ," vol. 4221, pp. 97–103, 2022.

[9] G. Pramudya and A. Mukti, "Analisis Kerentanan Keamanan Website Dengan Menggunakan Metode Penetration Testing dan Framework OWASP (Studi Kasus : Website Instansi XYZ)," 2020.

[10] V. S. Nugroho and F. W. Christanto, "ANALISIS KEAMANAN WEBSITE DENGAN INFORMATION SYSTEM SECURITY ASSESSMENT FRAMEWORK (ISSAF) DAN OPEN WEB APPLICATION SECURITY PROJECT (OWASP) WEBSITE SECURITY ANALYSIS WITH INFORMATION SYSTEM SECURITY ASSESSMENT FRAMEWORK (ISSAF) AND OPEN WEB APPLICAT," vol. 8, no. 2, pp. 145–156, 2023.

[11] E. Nurelasari, D. Gumilang, and A. Farabi, "ANALISIS KEAMANAN SISTEM WEBSITE MENGGUNAKAN METODE OPEN WEB APPLICATION SECURITY PROJECT (OWASP) PADA SIMANTEP . ID," vol. 8, no. 3, pp. 3049–3054, 2024.

[12] A. Stead, "What is Security Testing? How to Check The Security Strength of Your Application," 2023, [Online]. Available: https://www.computer.org/publications/tech-news/trends/application-security-testing

[13] Gilad David Maayan, "What Is Network Penetration Testing?," 2023, [Online]. Available: https://www.computer.org/publications/tech-news/trends/network-penetration-testing-quick-guide

[14] C. Gary McGraw and B. Bruce Potter, "Software Security Testing," 2004, [Online]. Available: https://www.computer.org/csdl/magazine/sp/2004/05/j5081/13rRUygT7qP

[15] 250000 Suye Li, Jinan Vocational College, Jinan, China, "Exploring Advanced Techniques for Security Testing of Sensor Device Chips," pp. 665–669, 2024, [Online]. Available: https://www.computer.org/csdl/proceedings-article/icici/2024/732900a665/20l59MZWWGI

[16] A. G. Trevor Henry Chiboora, Lenah Chacha, Theoneste Byagutangaza, "Evaluating Mobile Banking Application Security Posture Using the OWASP's MASVS Framework," pp. 99–106, 2023, [Online]. Available: https://dl.acm.org/doi/10.1145/3588001.3609367

[17] P. Charly, K. E. Diatmika, I. M. P. Prayoga, and I. M. E. Listartha, "Pendeteksian Keamanan Website SMA Greenschool Menggunakan Metode Owasp dengan Pengujian XSS," *Format J. Ilm. Tek. Inform.*, vol. 11, no. 1, p. 77, 2022, doi: 10.22441/10.22441/format.2022.v11.i1.008.

[18] U. Pamulang, "PENGUJIAN CELAH KEAMANAN INPUT VALIDATION PADA," vol. 1, no. 4, pp. 50–55, 2023.

[19] L. F. Burhani and D. Priyawati, "Analisis pengujian keamanan website pengelolaan internet desa kragan menggunakan metode penetration testing execution standard (ptes)," vol. 9, no. 1, pp. 307–319, 2024.

[20] M. Dahlan, A. Latubessy, M. Nurkamid, and L. H. Anggraini, "Pengujian Dan Analisa Keamanan Website Terhadap Serangan SQL Injection (Studi Kasus : Website UMK)," vol. 7, pp. 13–19, 2015.

[21] M. Ainurrohman and Y. Nurasri, "Pengujian Keamanan Website JDIH Kab . Tegal Menggunakan Acunetix dengan Standar ISO / IEC / 27001 : 2013," vol. 2, no. 3, pp. 3320–3323, 2025.

[22] R. R. Yusuf and T. N. Suharsono, "PENGUJIAN KEAMANAN DENGAN METODE OWASP TOP 10 PADA WEBSITE EFORM HELPDESK," pp. 402–413, 2023.

[23] P. Gymnastiar, "Analisis Keamanan dan Pengujian Access Control pada Website Pendidikan : Studi Kasus di Universitas Hamzanwadi Lombok," pp. 951–959, 2024.

[24] Muhammad Kemal Abdan, "PENGUJIAN KEAMANAN SISTEM INFORMASI BERBASIS WEB BERDASARKAN FRAMEWORK OWASP WSTG v4 . 2 (STUDI KASUS : SISTEM SEKAWAN v1 UNIVERSITAS ISLAM INDONESIA) PENGUJIAN KEAMANAN SISTEM INFORMASI BERBASIS WEB BERDASARKAN FRAMEWORK OWASP WSTG v4 . 2 (STUDI KASUS," vol. 2, 2022.

[25] G. Kusuma, "Implementasi Owasp Zap Untuk Pengujian Keamanan Sistem Informasi Akademik," *J. Teknol. Inf. J. Keilmuan dan Apl. Bid. Tek. Inform.*, vol. 16, no. 2, pp. 178–186, 2022, doi: 10.47111/jti.v16i2.3995.

[26] A. F. Mohmmad Muhsin, "Penerapan Pengujian Keamanan Web Server Menggunakan Metode OWASP versi 4 (Studi Kasus Web Server Ujian Online)," vol. 9, no. 1, pp. 31–42, 2015.

[27] Y. Thurfah, A. Rosaliah, and B. Hananto, "Pengujian Celah Keamanan Website Menggunakan Teknik Penetration Testing dan Metode OWASP TOP 10 pada Website SIM xxx," no. September, pp. 752–761, 2021.

[28] S. D. Raihan, S. Prabowo, and D. Oktaria, "Evaluasi Risiko Celah Keamanan Pada Aplikasi Web Dengan Penilaian Kerentanan dan Pengujian Penetrasi Menggunakan Metode OWASP dan NIST SP 800-30 Revisi 1," vol. 2, no. 2, pp. 27–34, 2024.

[29] L. H. Yumnun, A. Kusyanti, and D. P. Kartikasari, "Implementasi OWASP Mobile Security Testing Guide (MSTG) Untuk Pengujian Keamanan Pada Aplikasi Berbasis Android," vol. 3, no. 11, pp. 10579–10585, 2019.
[30] M. Dzaki, A. Vriano, and I. Komputer, "PENGUJIAN KEAMANAN WEB JUICE SHOP DENGAN METODE," vol. 01, no. 06, pp. 81–90, 2023.
[31] R. Rahman *et al.*, "PENGUJIAN PENETRASI JARINGAN MENGGUNAKAN OWASP ZAP DAN SQLMAP UNTUK," vol. 1, no. 4, pp. 9–12, 2024.