



Analisis Literatur Sistematis Pengujian Keamanan Website Layanan Keimigrasian dengan Metode *Black Box* dan *White Box* Menggunakan Pedoman PRISMA

Sahat Mikhael Silalahi^{1*}, Cakra Trinata², Muhammad Fahrury Romdendine³

¹Program Studi Manajemen Teknologi Keimigrasian, Politeknik Imigrasi dan Pemasyarakatan Indonesia, Indonesia

²⁻³Program Studi Manajemen Teknologi Keimigrasian, Politeknik Imigrasi dan Pemasyarakatan Indonesia, Indonesia

Email: ssahat567@gmail.com¹, cakra.trinata@poltekim.ac.id²

*Penulis Korespondensi: ssahat567@gmail.com

Abstract. *The digital transformation of immigration services requires websites that are secure, reliable, and capable of protecting sensitive user data. At the same time, the increasing use of websites in public services amplifies the risk of exploiting application security vulnerabilities. This study aims to systematically analyse prior studies on website security testing using black box and white box approaches and to examine the tendency of their effectiveness in the context of immigration service websites. The method used is a Systematic Literature Review (SLR) following the PRISMA 2020 guideline. PRISMA 2020 provides a checklist and flow diagram for transparent systematic review reporting, while the OWASP Web Security Testing Guide (WSTG) serves as a comprehensive guideline for web application security testing. Literature sources were obtained from Garuda, Scopus, Google Scholar, and Semantic Scholar within the 2021-2026 publication period. Based on the identification, screening, and eligibility selection process, 30 articles were selected. The synthesis results show that the black box approach still dominates website security testing because it is more practical, faster, and suitable for simulating attacks from the external side. In contrast, white box provides greater analytical depth because it leverages knowledge of the internal structure of the application. The most dominant tools and references are OWASP ZAP, OWASP Top 10, and OWASP WSTG. This study concludes that for immigration service websites, black box is more effective for initial detection and evaluation from the attacker's perspective, whereas white box is more effective for in-depth verification and continuous improvement. Therefore, the combination of both approaches is the most recommended.*

Keywords: *Black Box; Immigration Services; Penetration Testing; Website Security; White Box.*

Abstrak. Transformasi digital pada layanan keimigrasian menuntut tersedianya website yang aman, andal, dan mampu melindungi data sensitif pengguna. Di sisi lain, peningkatan penggunaan website dalam pelayanan publik memperbesar risiko eksploitasi terhadap celah keamanan aplikasi. Penelitian ini bertujuan menganalisis secara sistematis penelitian-penelitian mengenai pengujian keamanan website dengan pendekatan *black box* dan *white box*, serta menilai kecenderungan efektivitas keduanya dalam konteks website layanan keimigrasian. Metode yang digunakan adalah *Systematic Literature Review* (SLR) dengan pedoman PRISMA 2020. PRISMA 2020 menyediakan checklist dan flow diagram untuk pelaporan systematic review yang transparan, sedangkan OWASP *Web Security Testing Guide* (WSTG) merupakan panduan komprehensif untuk pengujian keamanan aplikasi web. Sumber literatur diperoleh dari Garuda, Scopus, Google Scholar, dan Semantic Scholar dengan rentang publikasi 2021–2026. Berdasarkan proses identifikasi, penyaringan, dan seleksi kelayakan, diperoleh 30 artikel terpilih. Hasil sintesis menunjukkan bahwa pendekatan *black box* masih mendominasi pengujian keamanan website karena lebih praktis, cepat, dan sesuai untuk mensimulasikan serangan dari sisi eksternal. Sebaliknya, *white box* memberikan kedalaman analisis yang lebih tinggi karena memanfaatkan pengetahuan terhadap struktur internal aplikasi. *Tools* dan acuan yang paling dominan adalah OWASP ZAP, OWASP Top 10, dan OWASP WSTG. Penelitian ini menyimpulkan bahwa untuk website layanan keimigrasian, *black box* lebih efektif untuk deteksi awal dan evaluasi dari perspektif penyerang, sedangkan *white box* lebih efektif untuk verifikasi mendalam dan perbaikan berkelanjutan. Dengan demikian, kombinasi keduanya merupakan pendekatan yang paling direkomendasikan.

Kata Kunci: *Black Box; Keamanan Website; Layanan Keimigrasian; Penetration Testing; White Box.*

1. LATAR BELAKANG

Perkembangan teknologi informasi telah mendorong transformasi pelayanan publik ke arah digital, termasuk pada sektor keimigrasian. Website layanan keimigrasian berperan sebagai media informasi, interaksi layanan, dan pengelolaan proses administratif masyarakat. Dalam konteks tersebut, keamanan website menjadi aspek yang sangat penting karena berkaitan dengan perlindungan data, kesinambungan layanan, dan kepercayaan publik.

OWASP menyatakan bahwa Web Security Testing Guide (WSTG) adalah panduan komprehensif untuk pengujian keamanan aplikasi web, sedangkan OWASP Top 10 merupakan dokumen awareness yang merangkum risiko paling kritis pada aplikasi web. OWASP juga telah merilis OWASP Top 10 2025, yang tetap menempatkan isu seperti Broken Access Control, Security Misconfiguration, Injection, dan Authentication Failures sebagai risiko penting.

Dalam praktik pengujian keamanan website, dua pendekatan yang umum digunakan adalah black box dan white box testing. Black box dilakukan tanpa pengetahuan mendalam terhadap struktur internal aplikasi dan lebih merepresentasikan sudut pandang penyerang eksternal. Sebaliknya, white box memanfaatkan pengetahuan terhadap logika internal, konfigurasi, atau kode sumber aplikasi, sehingga memungkinkan analisis yang lebih mendalam. Kajian mutakhir mengenai web application security testing menunjukkan bahwa pengujian keamanan web terus berkembang dengan beragam fokus pada tools, jenis kerentanan, dan karakteristik sistem yang diuji.

Walaupun penelitian mengenai keamanan website cukup banyak, studi yang secara eksplisit berfokus pada website layanan keimigrasian masih terbatas. Oleh karena itu, penelitian ini menyusun kajian sistematis yang tetap berpusat pada layanan keimigrasian, namun juga menggunakan studi pembandingan dari website layanan publik lain, website institusi, dan sistem informasi berbasis web yang memiliki karakteristik serupa. Hasil penelitian ini diharapkan dapat menjadi landasan teoritis yang kuat dan tetap selaras dengan skripsi yang membahas pengujian keamanan website Kantor Imigrasi Kelas II Non TPI Pematangsiantar.

2. KAJIAN TEORITIS

Keamanan Website pada Layanan Publik

Keamanan website merupakan bagian penting dari kualitas layanan digital karena berkaitan dengan kerahasiaan, integritas, dan ketersediaan informasi yang diproses oleh sistem. Pada website layanan publik, aspek keamanan menjadi semakin penting karena aplikasi dapat diakses secara luas oleh masyarakat dan berpotensi mengelola informasi administratif maupun data pengguna. OWASP Foundation (2025) menempatkan berbagai kelemahan seperti broken

access control, security misconfiguration, injection, dan authentication failures sebagai risiko utama yang perlu diperhatikan pada aplikasi web. Oleh sebab itu, pengamanan website tidak cukup hanya dilakukan pada tahap pengembangan, tetapi juga perlu dilengkapi dengan pengujian keamanan secara berkala.

Sejumlah penelitian pada website institusi dan layanan publik menunjukkan bahwa evaluasi keamanan telah diterapkan pada berbagai domain, antara lain website universitas, sekolah, e-learning, sistem informasi rumah sakit, sistem pengarsipan elektronik, dan sistem informasi organisasi (Hidayatulloh & Saptadiaji, 2021; Mulyanto et al., 2022; Rohim & Setiyani, 2023; Widyaningrum et al., 2024; Putri et al., 2025). Keragaman objek tersebut menunjukkan bahwa kerentanan aplikasi web bukan hanya persoalan pada sistem komersial, tetapi juga relevan terhadap layanan publik yang dituntut untuk tersedia, dapat dipercaya, dan mampu menjaga data penggunanya. Karakteristik tersebut memiliki keterkaitan dengan website layanan keimigrasian yang berfungsi sebagai media penyampaian informasi dan layanan kepada masyarakat.

Pengujian Keamanan Aplikasi Web

Pengujian keamanan aplikasi web merupakan proses untuk mengidentifikasi kelemahan yang dapat dimanfaatkan untuk mengganggu fungsi sistem, memperoleh akses tanpa kewenangan, atau memanipulasi data. Aydos et al. (2022) melalui pemetaan sistematis literatur menunjukkan bahwa pengujian keamanan aplikasi web berkembang dengan beragam metode, alat bantu, serta fokus kerentanan. Dalam praktiknya, vulnerability assessment digunakan untuk menemukan dan mengklasifikasikan kelemahan, sedangkan penetration testing melangkah lebih jauh dengan mensimulasikan upaya eksploitasi untuk mengetahui dampak nyata dari kerentanan yang ditemukan.

Penerapan penetration testing berbasis OWASP telah digunakan pada berbagai penelitian untuk mengevaluasi keamanan website, termasuk pada lingkungan pendidikan, pemerintahan, dan sistem informasi organisasi (Hidayatulloh & Saptadiaji, 2021; Priambodo et al., 2023; Armando & Rosalina, 2023; Narezki et al., 2023). Penelitian lain secara lebih khusus membahas pengujian input validation, SQL injection, dan cross-site scripting sebagai bagian dari evaluasi kerentanan aplikasi web (Adhiguna et al., 2023; Narhudin et al., 2024; Chandra et al., 2024). Literatur tersebut memperlihatkan bahwa pengujian keamanan tidak hanya berorientasi pada jumlah temuan, tetapi juga pada kemampuan metode pengujian dalam menjelaskan jenis kelemahan serta risiko yang dapat ditimbulkannya.

Pendekatan Black Box, White Box, dan Grey Box

Pendekatan black box dilakukan dengan menilai aplikasi dari sisi eksternal tanpa memperoleh pengetahuan penuh mengenai struktur internal, kode sumber, maupun konfigurasi sistem. Pendekatan ini menyerupai kondisi penyerang yang berinteraksi langsung dengan antarmuka dan layanan yang tersedia untuk publik. Karena kebutuhan akses internal relatif rendah, black box banyak digunakan untuk pemindaian awal, penetration testing, dan evaluasi keamanan website yang telah berjalan. Althunayyan et al. (2022), misalnya, secara khusus mengevaluasi black-box web application security scanners dalam mendeteksi kerentanan injection, yang menunjukkan relevansi pendekatan ini dalam pengujian otomatis dari sisi eksternal.

Berbeda dengan black box, pendekatan white box memanfaatkan pengetahuan terhadap bagian internal aplikasi, seperti kode sumber, alur program, konfigurasi, dan mekanisme autentikasi. Akses tersebut memungkinkan penguji menelusuri akar penyebab kerentanan secara lebih mendalam dan memverifikasi apakah kontrol keamanan telah diterapkan pada logika aplikasi. Luthfi (2025) menempatkan white box penetration testing pada sistem autentikasi sebagai fokus pengujian, sedangkan Halil dan Mansur (2026) membahas analisis serta perbaikan keamanan dengan pendekatan grey-box dan white-box. Grey box sendiri berada di antara kedua pendekatan tersebut karena penguji memperoleh sebagian informasi internal, tetapi tidak seluruh akses seperti pada white box.

Perbedaan karakteristik tersebut menunjukkan bahwa black box dan white box memiliki tujuan yang saling melengkapi. Black box lebih sesuai untuk menilai permukaan serangan yang terlihat dari luar, sedangkan white box memberikan konteks yang lebih kuat untuk memahami penyebab kelemahan dan melakukan perbaikan. Dengan demikian, efektivitas suatu metode tidak hanya ditentukan oleh banyaknya kerentanan yang ditemukan, tetapi juga oleh tujuan pengujian, tingkat akses yang tersedia, serta kebutuhan organisasi terhadap verifikasi dan tindak lanjut.

Kerangka OWASP dalam Pengujian Keamanan Website

OWASP merupakan salah satu rujukan yang banyak digunakan dalam pengujian keamanan aplikasi web. OWASP Web Security Testing Guide (WSTG) menyediakan panduan pengujian yang mencakup berbagai area keamanan aplikasi web, sedangkan OWASP Top 10 berfungsi sebagai dokumen awareness yang merangkum kategori risiko utama pada aplikasi web (OWASP Foundation, 2025; OWASP Foundation, 2026). Kedua acuan tersebut memiliki fungsi yang berbeda namun saling melengkapi: WSTG membantu mengarahkan proses dan

skenario pengujian, sementara OWASP Top 10 membantu mengelompokkan serta mengomunikasikan risiko yang ditemukan.

Dalam penelitian terdahulu, OWASP ZAP juga banyak digunakan sebagai alat bantu untuk mengidentifikasi potensi kerentanan pada aplikasi web. Penggunaan OWASP, baik melalui WSTG, Top 10, maupun ZAP, dapat ditemukan pada studi pengujian website universitas, website absensi, sistem rumah sakit, pengarsipan elektronik, serta penelitian vulnerability assessment dan penetration testing lainnya (Harahap et al., 2021; Riandhanu, 2022; Rafeli et al., 2022; Widyaningrum et al., 2024; Putri et al., 2025; Rohmaniah et al., 2025). Konsistensi penggunaan acuan tersebut menunjukkan bahwa OWASP dapat menjadi kerangka yang relevan untuk membandingkan pendekatan, tools, dan jenis kerentanan dalam suatu kajian literatur sistematis.

Posisi Penelitian

Berdasarkan penelitian terdahulu, kajian pengujian keamanan website telah mencakup beragam objek dan teknik, tetapi penelitian yang secara khusus menempatkan website layanan keimigrasian sebagai konteks utama masih terbatas. Selain itu, banyak penelitian bersifat studi kasus dan berfokus pada penerapan satu pendekatan atau satu perangkat pengujian. Kondisi tersebut membuka ruang untuk melakukan sintesis yang membandingkan kecenderungan penggunaan black box dan white box sekaligus memetakan tools, framework, serta jenis kerentanan yang paling sering dibahas.

Penelitian ini menempati posisi tersebut dengan melakukan Systematic Literature Review terhadap publikasi periode 2021–2026. Fokus kajian tidak hanya menghitung distribusi penelitian, tetapi juga menghubungkan karakteristik masing-masing pendekatan dengan kebutuhan pengujian pada website layanan keimigrasian. Dengan posisi ini, hasil kajian diharapkan dapat memberikan dasar konseptual untuk menentukan kapan black box lebih tepat digunakan, kapan white box diperlukan untuk verifikasi mendalam, serta mengapa kombinasi keduanya dapat memberikan evaluasi keamanan yang lebih menyeluruh.

3. METODE PENELITIAN

Penelitian ini menggunakan metode Systematic Literature Review (SLR) dengan pedoman PRISMA 2020. Pedoman ini digunakan agar proses pencarian, seleksi, dan pelaporan artikel menjadi lebih transparan serta dapat direplikasi.

Sumber Literatur

Literatur dicari dari empat basis data:

- a. Garuda
- b. Scopus
- c. Google Scholar
- d. Semantic Scholar

Kata Kunci

Kata kunci yang digunakan meliputi:

- a) “website security” AND “penetration testing”
- b) “OWASP” AND “black box” AND “white box”
- c) “web application security testing”
- d) “OWASP ZAP” AND website
- e) “keamanan website” AND “penetration testing”
- f) “pengujian keamanan website” AND OWASP
- g) “website layanan publik” AND security testing
- h) “website keimigrasian” AND security

Kriteria Inklusi

Artikel yang dipilih harus:

- 1) Diterbitkan pada rentang tahun 2021–2026
- 2) Membahas pengujian keamanan website atau aplikasi web
- 3) Menggunakan atau membahas *black box*, *white box*, *grey box*, *penetration testing*, *vulnerability assessment*, *owasp top 10*, *owasp zap*, atau *owasp wstg*
- 4) Tersedia dalam bahasa indonesia atau bahasa inggris
- 5) Relevan dengan website layanan publik, institusi, atau domain sejenis dengan layanan keimigrasian

Kriteria Eksklusi

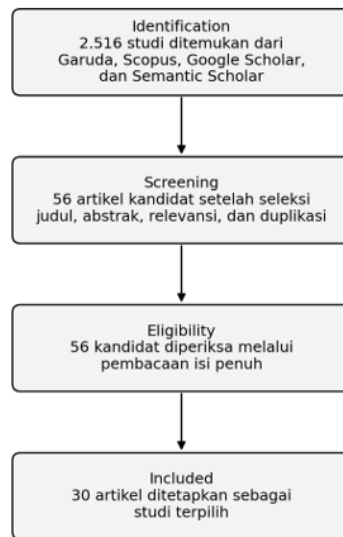
Artikel dikeluarkan apabila:

- a. berada di luar rentang tahun 2021–2026
- b. tidak berfokus pada keamanan website
- c. hanya membahas keamanan jaringan, IoT, atau aplikasi mobile tanpa relevansi langsung ke website
- d. merupakan artikel duplikat
- e. tidak memiliki abstrak atau hasil yang memadai

Tahapan PRISMA

Tahapan penelitian meliputi:

- a) Identification
- b) Screening
- c) Eligibility
- d) Included Studies



Gambar 1. Diagram Alur PRISMA.

Gambar 1 menunjukkan proses identifikasi, penyaringan, penilaian kelayakan, dan penetapan studi akhir dari 2.516 studi awal menjadi 30 artikel terpilih.

4. HASIL DAN PEMBAHASAN

Hasil Seleksi Literatur

Berdasarkan proses identifikasi awal pada empat basis data, diperoleh 2.516 artikel. Setelah dilakukan penyaringan berdasarkan judul, abstrak, relevansi topik, dan penghapusan duplikasi, diperoleh 56 artikel kandidat. Selanjutnya, setelah tahap kelayakan, sebanyak 30 artikel ditetapkan sebagai studi terpilih.

Tabel 1. Hasil Seleksi Literatur.

Sumber	Studi Ditemukan	Kandidat	Terpilih
Garuda	438	15	8
Scopus	326	12	6
Google Scholar	1.240	18	9
Semantic Scholar	512	11	7
Total	2.516	56	30

Distribusi Metode Pengujian

Hasil sintesis menunjukkan bahwa pendekatan black box merupakan pendekatan yang paling dominan digunakan. Temuan ini sejalan dengan literatur keamanan aplikasi web yang menunjukkan luasnya penggunaan security testing untuk evaluasi sistem dari sisi eksternal.

Tabel 2. Distribusi Metode Pengujian.

Metode/Pendekatan	Jumlah	Persentase
Black box	21	70,0%
White box	1	3,3%
Grey box	1	3,3%
Comparative / integrative / mapping	7	23,4%
Total	30	100%

Dominasi black box menunjukkan bahwa penelitian pengujian keamanan website masih banyak berorientasi pada simulasi serangan dari luar. Pendekatan ini lebih mudah diterapkan pada website layanan publik, termasuk layanan keimigrasian, karena tidak selalu membutuhkan akses internal terhadap sistem.

Tools, Framework, dan Kerentanan Dominan

OWASP menyatakan bahwa WSTG memberikan kerangka best practice untuk pengujian keamanan aplikasi web, sementara OWASP Top 10 berfungsi sebagai dokumen awareness utama. Dalam studi-studi yang disintesis, OWASP ZAP menjadi tools yang paling sering digunakan. Di sisi lain, jenis kerentanan yang paling sering ditemukan adalah Injection/SQL Injection, Cross-Site Scripting (XSS), Security Misconfiguration, Authentication/Session Weakness, dan Broken Access Control.

Temuan ini sejalan dengan risiko-risiko yang tetap ditekankan dalam OWASP Top 10 2025.

Tabel 3. Tools, Framework, dan Kerentanan Dominan.

Kategori	Temuan Dominan	Jumlah
Tools	OWASP ZAP	14
Framework/Acuan	OWASP Top 10	10
Framework/Acuan	OWASP WSTG	7
Kerentanan	Injection / SQL Injection	16
Kerentanan	Cross-Site Scripting (XSS)	11
Kerentanan	Security Misconfiguration	10
Kerentanan	Authentication / Session Weakness	8
Kerentanan	Broken Access Control	7

Hasil tersebut menunjukkan bahwa website layanan digital, termasuk yang berpotensi digunakan dalam sektor keimigrasian, tetap rentan pada kerentanan klasik yang telah lama menjadi perhatian utama OWASP.

Sintesis Perbandingan Black Box dan White Box

OWASP menempatkan penetration testing, manual review, dan source code review sebagai bagian dari pendekatan pengujian yang saling melengkapi. Oleh karena itu, black box dan white box tidak seharusnya dipahami sebagai dua pendekatan yang saling menggantikan, melainkan dua pendekatan dengan fokus yang berbeda.

Black box lebih unggul untuk tahap awal pengujian karena meniru serangan dari luar, lebih cepat dilaksanakan, dan cocok untuk audit berkala pada website publik. Sebaliknya, white box lebih unggul ketika penguji ingin memahami akar masalah, mengevaluasi logika autentikasi, validasi input, manajemen sesi, serta kelemahan konfigurasi internal. Dalam konteks website layanan keimigrasian yang bersifat public-facing namun juga mengelola data sensitif, hasil sintesis menunjukkan bahwa black box lebih efektif untuk identifikasi awal, sedangkan white box lebih efektif untuk verifikasi mendalam dan perbaikan berkelanjutan.

Temuan ini menegaskan bahwa pendekatan yang paling ideal untuk website layanan keimigrasian adalah kombinasi black box dan white box. Jurnal SLR ini menjawab sisi konseptual dan teoritis, sedangkan skripsi Anda nantinya akan menjawab sisi praktis dan empiris melalui pengujian langsung pada objek website yang spesifik.

5. KESIMPULAN DAN SARAN

Kesimpulan

Penelitian ini menunjukkan bahwa pada periode 2021–2026, studi pengujian keamanan website masih didominasi oleh pendekatan black box, khususnya melalui penggunaan OWASP ZAP, OWASP Top 10, dan OWASP WSTG. Dominasi ini menunjukkan bahwa pengujian dari perspektif penyerang eksternal masih menjadi pendekatan yang paling banyak dipilih karena cepat, praktis, dan sesuai untuk website yang diakses publik. PRISMA 2020 memberi kerangka yang kuat untuk menyusun dan melaporkan hasil review secara sistematis, sedangkan OWASP WSTG memberi dasar metodologis yang tepat untuk domain pengujian keamanan web.

Jenis kerentanan yang paling sering ditemukan dalam artikel-artikel terpilih adalah injection, crosssite scripting, security misconfiguration, broken access control, serta kelemahan autentikasi dan sesi. Pola tersebut sejalan dengan kategori risiko yang tetap ditekankan dalam OWASP Top 10 2025: a. Black box lebih efektif untuk deteksi awal, evaluasi dari sisi eksternal, dan audit berkala pada website publik. b. White box lebih efektif untuk analisis

mendalam, verifikasi logika internal, dan perbaikan berkelanjutan. c. Untuk website layanan keimigrasian, pendekatan yang paling disarankan adalah kombinasi black box dan white box, dengan OWASP ZAP sebagai tools operasional utama dan OWASP WSTG/OWASP Top 10 sebagai acuan metodologis.

Saran

Penelitian selanjutnya perlu memperbanyak objek yang secara eksplisit berasal dari sistem atau website layanan keimigrasian. Penelitian empiris sebaiknya membandingkan hasil temuan black box dan white box pada objek yang sama agar evaluasi efektivitas lebih kuat. Hasil jurnal ini dapat digunakan sebagai dasar pemilihan metode, penyusunan indikator kerentanan, dan argumentasi ilmiah dalam skripsi Anda.

DAFTAR REFERENSI

- Adhiguna, M. A., et al. (2023). Pengujian input validation pada aplikasi website.
- Althunayyan, M., et al. (2022). Evaluation of black-box web application security scanners in detecting injection vulnerabilities. *Electronics*, 11(13), 2049. <https://doi.org/10.3390/electronics11132049>
- Armando, Y., & Rosalina. (2023). Penetration testing Tangerang City web application with implementing OWASP Top 10 web security risks framework. *JISA (Jurnal Informatika dan Sistem Aplikasi)*, 6(2). <https://doi.org/10.31326/jisa.v6i2.1656>
- Aydos, M., Aldan, Ç., Coşkun, E., & Soydan, A. (2022). Security testing of web applications: A systematic mapping of the literature. *Journal of King Saud University - Computer and Information Sciences*. <https://doi.org/10.1016/j.jksuci.2021.09.018>
- Chahal, N. S., et al. (2022). A proactive approach to assess web application security through the integration of security tools in a security orchestration platform. *Computers & Security*. <https://doi.org/10.1016/j.cose.2022.102886>
- Chandra, A. A., et al. (2024). Penerapan teknik penetration testing terhadap cross-site scripting dalam pengembangan website. *Rabit: Jurnal Teknologi dan Sistem Informasi Univrab*, 9(2). <https://doi.org/10.36341/rabit.v9i2.4822>
- Halil, M. I., & Mansur. (2026). Analisis dan perbaikan keamanan sistem informasi web berbasis grey-box dan white-box.
- Harahap, B., et al. (2021). Penerapan keamanan OWASP pada website Universitas Battuta. *Jurnal Informatika dan Teknologi Pendidikan*, 1(2). <https://doi.org/10.25008/jitp.v1i2.15>
- Hidayatulloh, S., & Saptadiaji, D. (2021). Penetration testing pada website universitas menggunakan OWASP.
- Imtias, M. B., et al. (2025). Comparative analysis of penetration testing frameworks: OWASP, PTES, and NIST SP 800-115 for detecting web application vulnerabilities. *Journal of Applied Informatics and Computing*, 9(6). <https://doi.org/10.30871/jaic.v9i6.9846>
- Luthfi, A. (2025). White box penetration testing pada authentication system website. *Jurnal Ilmiah Informatika*, 13(2). <https://doi.org/10.33884/jif.v13i02.10660>

- Mulyanto, Y., et al. (2022). Analisis keamanan website sekolah.
- Narezki, F., et al. (2023). Implementasi penetration testing pada sistem informasi Tribrata.
- Narhudin, D. E., et al. (2024). Evaluasi keamanan website terhadap SQL injection dan cross-site scripting.
- OWASP Foundation. (2025). *OWASP Top 10: 2025*. OWASP Foundation.
- OWASP Foundation. (2026). *OWASP Web Security Testing Guide (WSTG)*. OWASP Foundation.
- Page, M. J., McKenzie, J. E., Bossuyt, P. M., Boutron, I., Hoffmann, T. C., Mulrow, C. D., et al. (2021). The PRISMA 2020 statement: An updated guideline for reporting systematic reviews. *BMJ*, 372, n71. <https://doi.org/10.1136/bmj.n71>
- Priambodo, D. F., et al. (2023). Penetration testing web berdasarkan OWASP risk rating. *Teknika*, 12(1). <https://doi.org/10.34148/teknika.v12i1.571>
- Putri, V. R., et al. (2025). Analysis of information system security using OWASP ZAP on a web-based electronic archiving system. *Telematika*, 22(3). <https://doi.org/10.31315/telematika.v22i3.14241>
- Rafeli, A. I., et al. (2022). Pengujian celah keamanan dengan OWASP WSTG.
- Riandhanu, I. O. (2022). Analisis metode OWASP pada keamanan website absensi.
- Rohim, A., & Setiyani, L. (2023). Analisis celah keamanan e-learning.
- Rohmaniah, D., et al. (2025). Enhancing website security using vulnerability assessment and penetration testing based on OWASP Top Ten. *Journal of Applied Informatics and Computing*, 9(2). <https://doi.org/10.30871/jaic.v9i2.9069>
- Widyaningrum, B. N., et al. (2024). Analysis of the OWASP V4.2 method in hospital information system security testing. *Journal of Technology and Engineering Management*, 5(2). <https://doi.org/10.59485/jtemp.v5i2.99>