KERENTANAN KEAMANAN PORTAL E-GOVERNMENT DI INDONESIA: TINJAUAN LITERATUR SISTEMATIS BERDASARKAN OWASP TOP 10:2025 DAN IMPLIKASINYA BAGI KANTOR IMIGRASI KELAS I TPI PALEMBANG

Rayyan Rizqiki Kurniawan[1], Rasona Sunara Akbar[2], Okky Pratama Martadireja[3]
rayyankurniawan00@gmail.com[1], akbarrasona@gmail.com[2], okky.martadireja@gmail.com[3]
Politeknik Imigrasi dan Pemasyarakatan Indonesia

ABSTRAK

Transformasi digital pelayanan publik memperluas ketergantungan instansi pemerintah pada aplikasi berbasis web dan sekaligus meningkatkan kebutuhan pengendalian keamanan aplikasi. Penelitian ini bertujuan mengidentifikasi pola kerentanan, metode pengujian, dan strategi mitigasi pada portal e-government, kemudian merumuskan implikasinya bagi perencanaan audit keamanan website Kantor Imigrasi Kelas I TPI Palembang. Penelitian menggunakan Systematic Literature Review dan melaporkan proses seleksi berdasarkan PRISMA 2020. Sebanyak 32 dokumen akademik terbitan 2022 sampai 2026 dipilih dari Google Scholar, IEEE Xplore, Garuda, dan Semantic Scholar. Temuan yang semula menggunakan OWASP Top 10:2021 direklasifikasi secara semantik ke OWASP Top 10:2025 berdasarkan jenis kerentanan yang dilaporkan. Hasil sintesis menunjukkan bahwa kategori yang paling sering muncul adalah A05:2025 Injection pada 16 studi (50,00%), A02:2025 Security Misconfiguration pada 14 studi (43,75%), dan A01:2025 Broken Access Control pada 12 studi (37,50%). OWASP ZAP merupakan alat yang paling sering digunakan, yaitu pada 12 studi (37,50%), tetapi frekuensi penggunaan tidak diperlakukan sebagai bukti tunggal efektivitas. Temuan ini tidak membuktikan adanya kerentanan pada website Kantor Imigrasi Kelas I TPI Palembang, melainkan menyediakan dasar empiris untuk menyusun ruang lingkup pengujian langsung, prioritas mitigasi, dan tata kelola audit berkala.

Kata Kunci: Kerentanan Web, OWASP Top 10:2025, E-Government, Keamanan Siber, Systematic Literature Review.

ABSTRACT

The digital transformation of public services has increased government reliance on web applications and, at the same time, the need for stronger application security controls. This study identifies vulnerability patterns, testing methods, and mitigation strategies reported in e-government research and formulates their implications for planning a security audit of the Class I TPI Immigration Office of Palembang website. A Systematic Literature Review was conducted and reported using PRISMA 2020. Thirty-two academic documents published between 2022 and 2026 were selected from Google Scholar, IEEE Xplore, Garuda, and Semantic Scholar. Findings originally classified under OWASP Top 10:2021 were semantically recoded into OWASP Top 10:2025 according to the reported vulnerability type. The synthesis identified A05:2025 Injection in 16 studies (50.00%), A02:2025 Security Misconfiguration in 14 studies (43.75%), and A01:2025 Broken Access Control in 12 studies (37.50%). OWASP ZAP was the most frequently used tool, appearing in 12 studies (37.50%); however, frequency of use was not treated as stand-alone evidence of effectiveness. These results do not demonstrate that the Palembang immigration website is vulnerable. Instead, they provide an empirical basis for defining the scope of direct testing, prioritizing mitigation, and establishing periodic security audits.

Kata Kunci: *Web Vulnerability, OWASP Top 10:2025, E-Government, Cybersecurity, Systematic Literature Review.*

PENDAHULUAN

Digitalisasi layanan publik membuat portal e-government berperan sebagai kanal informasi, transaksi, dan interaksi antara instansi dengan masyarakat. Perluasan fungsi tersebut menambah permukaan serangan karena aplikasi web berhadapan dengan risiko pada kontrol akses, konfigurasi, komponen perangkat lunak, pengelolaan identitas, serta validasi masukan. OWASP Top 10 digunakan secara luas sebagai dokumen kesadaran keamanan aplikasi yang merangkum kategori risiko paling kritis. Versi 2025 memperbarui struktur kategori berdasarkan data pengujian dan masukan komunitas keamanan aplikasi (OWASP Foundation, 2025).

Konteks keimigrasian membutuhkan perhatian khusus karena layanan dan informasi yang dikelola berkaitan dengan identitas, dokumen perjalanan, status perizinan, serta komunikasi publik. Meskipun website kantor imigrasi daerah tidak selalu menyimpan seluruh data layanan inti, integrasi dengan layanan eksternal, penggunaan sistem manajemen konten, akun administrator, komponen pihak ketiga, dan konfigurasi server tetap dapat menimbulkan risiko. Risiko tersebut perlu diperiksa melalui pengujian yang memiliki ruang lingkup, izin tertulis, dan batasan non-destruktif.

Penelitian ini tidak melakukan pengujian langsung terhadap website Kantor Imigrasi Kelas I TPI Palembang. Fokus penelitian adalah sintesis literatur untuk mengidentifikasi pola kerentanan yang sering dilaporkan, metode pengujian yang digunakan, dan rekomendasi mitigasi yang dapat menjadi dasar penyusunan audit keamanan. Dengan batasan tersebut, hasil penelitian tidak boleh ditafsirkan sebagai bukti bahwa objek tersebut memiliki kerentanan tertentu.

Perubahan dari OWASP Top 10:2021 ke OWASP Top 10:2025 menuntut reklasifikasi temuan. Security Misconfiguration berpindah dari A05:2021 menjadi A02:2025. Vulnerable and Outdated Components diperluas menjadi A03:2025 Software Supply Chain Failures. Injection berpindah menjadi A05:2025, sedangkan Server-Side Request Forgery yang sebelumnya berdiri sebagai A10:2021 digabungkan ke A01:2025 Broken Access Control. Versi 2025 juga memperkenalkan A10:2025 Mishandling of Exceptional Conditions sebagai kategori baru (OWASP Foundation, 2025).

Berdasarkan latar belakang tersebut, penelitian ini menjawab tiga pertanyaan berikut.

Tabel 1 Pertanyaan Penelitian

Kode	Research Question	Tujuan
RQ1	Kategori kerentanan apa yang paling sering dilaporkan pada studi portal e-government setelah direklasifikasi ke OWASP Top 10:2025?	Mengidentifikasi pola kerentanan berdasarkan kategori OWASP Top 10:2025.
RQ2	Metode dan alat apa yang digunakan untuk mengevaluasi keamanan aplikasi web pada instansi pemerintah atau layanan publik?	Menggambarkan pendekatan pengujian yang digunakan dalam literatur.
RQ3	Rekomendasi mitigasi apa yang relevan untuk perencanaan audit keamanan website Kantor Imigrasi Kelas I TPI Palembang?	Merumuskan prioritas mitigasi berbasis sintesis literatur tanpa menyimpulkan kondisi keamanan objek secara langsung.

METODE PENELITIAN

Desain Penelitian

Penelitian menggunakan metode Systematic Literature Review untuk mengidentifikasi, menyeleksi, mengekstraksi, dan mensintesis penelitian yang relevan secara terstruktur. Pelaporan proses pencarian dan seleksi mengacu pada PRISMA 2020, sedangkan penyusunan strategi pencarian mempertimbangkan prinsip PRISMA-S agar sumber informasi dan kombinasi kata kunci dapat ditelusuri kembali (Page et al., 2021; Rethlefsen et al., 2021).

Sumber Informasi dan Strategi Pencarian

Penelusuran dilakukan pada Google Scholar, IEEE Xplore, Garuda, dan Semantic Scholar. Kombinasi istilah pencarian dibangun dari tiga kelompok konsep, yaitu keamanan aplikasi web, kerangka OWASP, dan konteks instansi publik. Bentuk umum strategi pencarian adalah: (vulnerability assessment OR penetration testing OR web security OR kerentanan website) AND (OWASP Top 10 OR OWASP) AND (e-government OR government portal OR sistem informasi pemerintah OR immigration). Sintaks disesuaikan dengan fasilitas pencarian pada setiap sumber.

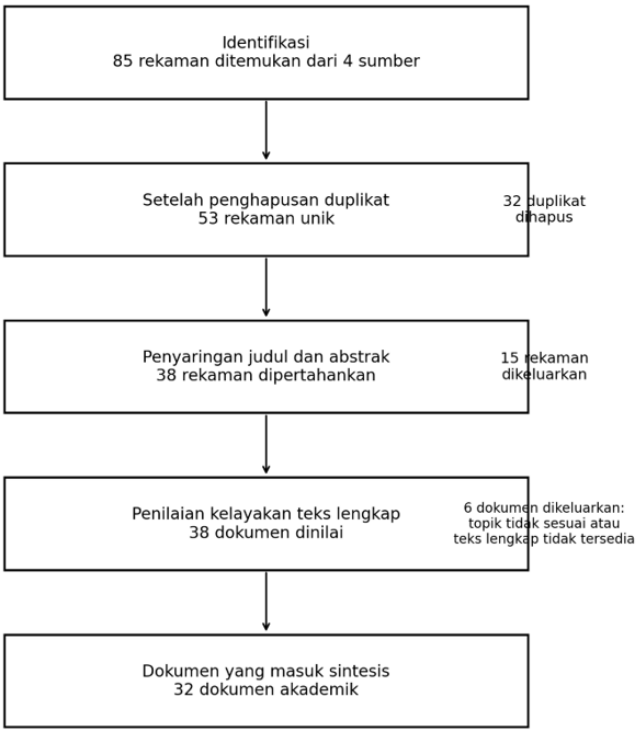
Kriteria Inklusi dan Eksklusi

Tabel 2 Kriteria Inklusi dan Eksklusi

Kriteria	Inklusi	Eksklusi
Tahun publikasi	2022 sampai 2026	Terbit sebelum 2022
Bahasa	Bahasa Indonesia atau Bahasa Inggris	Bahasa selain Indonesia dan Inggris
Topik	Keamanan aplikasi web, OWASP, penetration testing, vulnerability assessment, e-government, atau layanan publik	Tidak membahas keamanan aplikasi web
Jenis dokumen	Artikel jurnal, prosiding ilmiah, dan karya akademik yang menyediakan metode serta temuan	Blog, opini, berita, materi promosi, atau dokumen tanpa metode yang dapat diperiksa
Aksesibilitas	Teks lengkap tersedia	Hanya abstrak atau metadata
Relevansi	Memuat objek, metode, alat, kategori risiko, atau temuan yang dapat diekstraksi	Tidak menyediakan data yang dapat digunakan untuk menjawab RQ

Proses Seleksi Literatur

Pencarian awal menghasilkan 85 rekaman. Setelah 32 duplikat dihapus, tersisa 53 rekaman unik. Penyaringan judul dan abstrak mengeluarkan 15 rekaman sehingga 38 dokumen diperiksa dalam bentuk teks lengkap. Enam dokumen dikeluarkan karena topik tidak sesuai atau teks lengkap tidak tersedia. Tahap akhir menghasilkan 32 dokumen untuk sintesis. Alur tersebut ditampilkan pada Gambar 1.



Gambar 1 Alur Seleksi Literatur Berdasarkan PRISMA 2020

Ekstraksi, Reklasifikasi, dan Sintesis Data

Data yang diekstraksi mencakup penulis dan tahun, objek penelitian, metode atau alat, kategori OWASP yang digunakan pada publikasi asal, temuan utama, dan tingkat keparahan. Karena sebagian besar studi menggunakan OWASP Top 10:2021, setiap temuan direklasifikasi ke OWASP Top 10:2025 berdasarkan makna kerentanan yang dilaporkan, bukan sekadar mengganti nomor kategori. Reklasifikasi ini penting karena A03:2025 memperluas cakupan komponen rentan menjadi kegagalan rantai pasok perangkat lunak, A10:2021 SSRF digabungkan ke A01:2025, dan A10:2025 merupakan kategori baru untuk kesalahan penanganan kondisi luar biasa.

Frekuensi dihitung berdasarkan jumlah studi yang melaporkan sedikitnya satu temuan dalam suatu kategori. Satu studi dapat masuk ke lebih dari satu kategori sehingga total persentase tidak harus berjumlah 100 persen. Persentase dihitung dengan rumus jumlah studi pada kategori dibagi 32, kemudian dikalikan 100 persen.

Tabel 3 Pemetaan OWASP Top 10:2021 ke OWASP Top 10:2025

Kategori 2021	Kategori 2025	Prinsip reklasifikasi
A01 Broken Access Control	A01 Broken Access Control	Tetap pada A01; A10:2021 SSRF juga digabungkan ke A01:2025.
A05 Security Misconfiguration	A02 Security Misconfiguration	Perubahan peringkat dari A05 menjadi A02.
A06 Vulnerable and Outdated Components	A03 Software Supply Chain Failures	Cakupan diperluas ke dependensi, proses build, distribusi, dan pembaruan perangkat lunak.
A02 Cryptographic Failures	A04 Cryptographic Failures	Perubahan peringkat dari A02 menjadi A04.
A03 Injection	A05 Injection	Perubahan peringkat dari A03 menjadi A05.
A04 Insecure Design	A06 Insecure Design	Perubahan peringkat dari A04 menjadi A06.
A07 Identification and Authentication Failures	A07 Authentication Failures	Nama disederhanakan, substansi autentikasi dan sesi dipertahankan.
A08 Software and Data Integrity Failures	A08 Software or Data Integrity Failures	Perubahan kecil pada nama kategori.
A09 Security Logging and Monitoring Failures	A09 Security Logging and Alerting Failures	Penekanan ditambah pada fungsi peringatan.
Tidak ada kategori langsung	A10 Mishandling of Exceptional Conditions	Kategori baru untuk error handling, failing open, dan kondisi abnormal.

HASIL DAN PEMBAHASAN

1. Karakteristik Literatur Terpilih

Sebanyak 29 dari 32 dokumen (90,63%) terbit pada 2024 dan 2025. Masing-masing satu dokumen terbit pada 2022, 2023, dan 2026. Literatur mencakup portal pemerintah, layanan publik, aplikasi organisasi, aplikasi pendidikan, dan studi perbandingan alat

keamanan. Keragaman objek membantu mengidentifikasi pola umum, tetapi membatasi kemampuan generalisasi khusus terhadap website keimigrasian.

OWASP ZAP tercantum pada 12 dari 32 studi (37,50%) dan menjadi alat yang paling sering digunakan dalam matriks ekstraksi. Temuan ini menunjukkan tingkat adopsi yang tinggi, bukan bukti bahwa ZAP selalu paling akurat untuk semua kategori. Beberapa studi menggunakan pendekatan hibrida dengan SonarQube, Nmap, Burp Suite, Nuclei, Acunetix, Nikto, Vega Scanner, pemeriksaan manual, PTES, dan NIST SP 800-115.

2. RQ1: Distribusi Kategori OWASP Top 10:2025

Tabel 4 Frekuensi Kategori OWASP Top 10:2025 Pada 32 Dokumen

Kategori	Nama risiko	Frekuensi	Persentase	Keparahan yang dilaporkan
A05:2025	Injection	16 dari 32	50,00%	High sampai Critical
A02:2025	Security Misconfiguration	14 dari 32	43,75%	Medium sampai High
A01:2025	Broken Access Control	12 dari 32	37,50%	High
A07:2025	Authentication Failures	8 dari 32	25,00%	Medium sampai High
A03:2025	Software Supply Chain Failures	7 dari 32	21,88%	Medium sampai High
A06:2025	Insecure Design	4 dari 32	12,50%	Medium sampai High
A08:2025	Software or Data Integrity Failures	1 dari 32	3,13%	Medium sampai High
A10:2025	Mishandling of Exceptional Conditions	1 dari 32	3,13%	High
A04:2025	Cryptographic Failures	0 dari 32	0,00%	Tidak dapat disimpulkan
A09:2025	Security Logging and Alerting Failures	0 dari 32	0,00%	Tidak dapat disimpulkan

Hasil reklasifikasi menunjukkan bahwa Injection menempati posisi pertama. Temuan ini terutama berupa SQL Injection dan Cross-Site Scripting. Security Misconfiguration berada pada posisi kedua, antara lain berupa header keamanan yang tidak lengkap, layanan atau port yang tidak diperlukan, directory listing, dan konfigurasi server yang lemah. Broken Access Control berada pada posisi ketiga dan mencakup modifikasi hak akses, paparan data, CSRF, serta SSRF yang pada versi 2025 digabungkan ke A01.

Tidak ditemukannya A04 dan A09 dalam matriks tidak menunjukkan bahwa kedua risiko tersebut tidak ada pada portal e-government. Hasil tersebut hanya berarti bahwa ringkasan temuan pada dokumen terpilih tidak menyediakan bukti yang cukup untuk memasukkannya ke dua kategori tersebut. Security Logging and Alerting Failures juga sulit diidentifikasi melalui pemindaian eksternal karena memerlukan akses terhadap log, konfigurasi pemantauan, dan proses respons insiden.

3. RQ2: Metode dan Alat Evaluasi

Literatur memperlihatkan tiga pola evaluasi. Pertama, Dynamic Application Security Testing menggunakan OWASP ZAP, Acunetix, Vega Scanner, atau Burp Suite untuk menguji aplikasi yang sedang berjalan. Kedua, pemeriksaan jaringan dan konfigurasi menggunakan Nmap, Nikto, Nuclei, atau SSL Labs. Ketiga, pendekatan hibrida yang menggabungkan DAST, Static Application Security Testing seperti SonarQube, pemeriksaan manual, dan kerangka kerja PTES atau NIST SP 800-115.

Berdasarkan cakupan tersebut, OWASP ZAP layak digunakan sebagai salah satu alat dalam pengujian grey box karena dapat mendukung crawling, passive scan, active scan terbatas, dan pemeriksaan respons HTTP. Namun, hasil otomatis perlu diverifikasi secara manual untuk mengurangi false positive dan false negative. Kerentanan kontrol akses, logika bisnis, integritas dokumen, dan pengelolaan peran sering kali tidak dapat dinilai secara memadai hanya dengan pemindaian otomatis.

4. RQ3: Prioritas Mitigasi

Tabel 5 Prioritas Mitigasi Berdasarkan OWASP Top 10:2025

Kategori	Prioritas mitigasi	Contoh penerapan pada portal instansi
A01 Broken Access Control	Terapkan least privilege, validasi otorisasi pada server, RBAC, perlindungan CSRF, dan pembatasan akses direktori.	Uji setiap peran pengguna, cegah akses langsung ke berkas sensitif, dan gunakan token CSRF pada formulir yang mengubah data.
A02 Security Misconfiguration	Gunakan baseline hardening, matikan fitur atau port yang tidak diperlukan, hilangkan default account, dan lengkapi HTTP security headers.	Aktifkan HSTS, Content-Security-Policy, X-Content-Type-Options, serta kebijakan frame yang sesuai.
A03 Software Supply Chain Failures	Inventarisasi komponen, gunakan Software Bill of Materials, lakukan pemantauan CVE, dan perbarui dependensi melalui proses perubahan terkontrol.	Catat versi CMS, plugin, pustaka, server, dan komponen transitive; hapus komponen yang tidak didukung.
A05 Injection	Gunakan parameterized queries, validasi input sisi server, output encoding, dan Content Security Policy.	Larangan menyusun query SQL dari input pengguna dan pengujian khusus pada kolom pencarian, parameter URL, serta formulir.
A07 Authentication Failures	Terapkan MFA untuk administrator, rate limiting, kebijakan sesi, dan pencatatan kegagalan login.	Batasi percobaan login, rotasi kredensial administrator, dan akhiri sesi secara benar setelah logout atau tidak aktif.
A09 Logging and Alerting Failures	Catat peristiwa penting, lindungi integritas log, tetapkan ambang peringatan, dan uji proses eskalasi.	Pemindaian atau percobaan login berulang harus menghasilkan log dan peringatan yang ditinjau petugas.
A10 Mishandling of Exceptional Conditions	Terapkan exception handling yang konsisten, fail closed, rollback transaksi, dan hindari pesan kesalahan sensitif.	Pengguna menerima pesan umum, sedangkan rincian teknis disimpan dalam log internal yang terlindungi.

Prioritas mitigasi pada Tabel 5 perlu diterapkan melalui rencana tindakan yang memuat penanggung jawab, tingkat urgensi, target waktu, bukti perbaikan, dan pengujian ulang. Temuan berisiko tinggi harus ditangani lebih dahulu, tetapi kelemahan berisiko sedang yang muncul berulang juga tidak boleh dibiarkan karena dapat digabungkan dengan kelemahan lain dalam satu rangkaian serangan.

Matriks Sintesis Literatur

Tabel 6 menyajikan matriks sintesis yang telah direklasifikasi ke OWASP Top 10:2025. Reklasifikasi didasarkan pada kategori asal dan uraian temuan utama yang tersedia dalam dokumen kerja. Pemeriksaan ulang terhadap teks lengkap dan metadata bibliografis tetap diperlukan sebelum naskah diajukan ke jurnal.

Tabel 6 Matriks Sintesis 32 Dokumen Setelah Reklasifikasi ke OWASP Top 10:2025

No.	Penulis dan tahun	Objek	Metode dan alat	Kategori OWASP 2025	Temuan utama	Keparahan
1	Marbun (2025)	Web Kanim Kelas I TPI Jambi	OWASP ZAP, grey box	A01, A02, A03, A06	Header keamanan tidak lengkap, CSRF, paparan PII melalui integrasi, dan pustaka usang	High, Medium, Low
2	Ahmed (2025)	Web kementerian di Bangladesh	OWASP ZAP, Vega Scanner	A05	SQL Injection dan XSS	High
3	Firdaus & Widyawan (2025)	Web pemerintah kabupaten	PTES, OWASP Top 10	A05	SQL Injection dan XSS pada subdomain publik	High
4	Wisnu & Soewito (2026)	Aplikasi ekspor impor LNSW	SonarQube, OWASP ZAP	A03, A07	Kelemahan komponen dan autentikasi; pendekatan hibrida	Medium
5	Firnanda et al. (2025)	Web ERP PT XYZ	PTES, ISO 27005, OWASP ZAP	A01, A05, A07	CSRF, session hijacking, dan temuan injeksi	High, Medium
6	Madya et al. (2025)	Direktori PPID BNPB	NIST SP 800-115, ZAP, CVSS	A01, A05, A07	Directory listing, brute force, dan SQL Injection	High
7	Qadir et al. (2025)	Perbandingan alat pada aplikasi web	SAST dan DAST	A02, A03	Perbandingan deteksi misconfiguration dan komponen rentan	Medium
8	Ramadhan et al. (2025)	Tinjauan literatur	SLR, PRISMA	A02, A05	Dominasi standar OWASP dan tren deteksi XSS	Medium
9	Irvan et al. (2024)	Aplikasi inventori Kanim Langsa	OWASP Top 10	A01	Modifikasi hak akses tidak sah	High, Medium
10	Fatihah & Dinarto (2024)	CMS perusahaan daerah	ISSAF, ZAP	A05, A07	SQL Injection dan kelemahan autentikasi CMS	High, Medium
11	Anugraha & Alwi (2025)	Metodologi vulnerability assessment	OWASP ZAP	A01, A02, A03	Cookie tanpa perlindungan memadai dan pustaka JavaScript rentan	Medium
12	Hilda et al. (2024)	Website pemerintah desa	PTES, Nmap, Nikto, ZAP	A01, A02	Port tidak diperlukan dan direktori mengekspos dokumen	High, Medium
13	Yusuf et al. (2025)	Platform SINTA Kemdikbud	OWASP WSTG, TAM	A02, A07	Celah konfigurasi server, API, dan autentikasi	Medium
14	Sugara & Sriyasa (2024)	Pengujian website	Pemetaan risiko OWASP	A02, A03	Misconfiguration dan komponen usang	Medium
15	Dinata et al. (2025)	Website rumah sakit	Penetration testing, SSL Labs	A01, A05, A06	Kontrol akses, injeksi, dan kelemahan logika aplikasi	High, Medium
16	Mifthahuddin et al. (2025)	E-journal universitas	NIST SP 800-115, OWASP	A02, A03, A05	Kerentanan konfigurasi, komponen, dan injeksi pada OJS	High, Medium, Low
17	Rahmi et al. (2024)	Aplikasi web terintegrasi fakultas	Acunetix	A05, A10	Blind SQL Injection dan error message disclosure	High
18	Maniraj et al. (2024)	Deteksi kerentanan aplikasi web	OWASP ZAP	A02, A05	Temuan injeksi dan konfigurasi; simulasi mitigasi	High, Medium
19	Syarifudin et al. (2025)	Web distribusi zakat	Penetration testing OWASP	A01, A02, A07	CSRF serta kelemahan konfigurasi dan autentikasi	High, Medium
20	Adinugroho et al. (2022)	Sistem e-learning	Kerangka kerja OWASP	A07	Kelemahan manajemen sesi	High
21	Pramudia et al. (2025)	Simulasi aplikasi web	Eksploitasi OWASP Top 10	A05	Parameterized query menurunkan keberhasilan injeksi	High, Medium
22	Reonaldi et al. (2025)	Situs integrasi data kota	Footprinting, vulnerability scanning	A02	Kelemahan konfigurasi saat migrasi server	Medium
23	Wibowo et al. (2023)	Apache web server	Hardening server, NIST	A02	Pembatasan .htaccess dan banner grabbing	Medium, Low
24	Tahir & Risky (2024)	Web dinas pemerintah	PTES	A01, A05	Kontrol akses dan injeksi	High, Medium
25	Hilario et al. (2024)	Aplikasi Java web	Kajian kuantitatif OWASP	A01	Kelemahan kontrol akses akibat kesalahan pengkodean	High
26	Rahman et al. (2025)	Platform web	Nuclei, OWASP ZAP	A02, A03, A05	Temuan SSL atau network, komponen, XSS, dan header	Medium
27	Anisah (2025)	Analisis keamanan web	OWASP ZAP otomatis dan manual	A05	Pengujian injeksi melalui kombinasi crawling dan pemeriksaan manual	High, Medium

Pembahasan

1. Perubahan Pola Setelah Reklasifikasi OWASP 2025

Reklasifikasi mengubah urutan risiko dibandingkan naskah awal. Injection menjadi kategori paling sering muncul karena SQL Injection dan XSS dilaporkan secara eksplisit pada banyak studi. Security Misconfiguration tetap menempati posisi tinggi, tetapi frekuensinya adalah 14 studi, bukan 26 studi sebagaimana tercantum pada naskah awal. Broken Access Control juga turun menjadi 12 studi setelah perhitungan diselaraskan dengan matriks ekstraksi. Perubahan ini menunjukkan pentingnya menjaga konsistensi antara tabel data, abstrak, hasil, dan kesimpulan.

Pada OWASP Top 10:2025, SSRF tidak lagi menjadi kategori tersendiri dan masuk ke Broken Access Control. Perubahan ini membuat analisis kontrol akses perlu mencakup pembatasan terhadap sumber daya internal, validasi tujuan permintaan server, serta segmentasi jaringan. Pada sisi lain, A03 Software Supply Chain Failures memperluas isu komponen usang menjadi persoalan pengelolaan dependensi, repositori, proses build, distribusi, dan pembaruan perangkat lunak.

2. Penggunaan OWASP ZAP dalam Pengujian Grey Box

OWASP ZAP paling sering digunakan dalam literatur terpilih karena bersifat terbuka dan mendukung pengujian aplikasi yang sedang berjalan. Namun, istilah paling efektif harus digunakan secara hati-hati. Efektivitas alat bergantung pada ruang lingkup, autentikasi, konfigurasi pemindai, kualitas crawling, jenis aplikasi, dan verifikasi manual. Dalam konteks grey box, peneliti dapat memperoleh akun uji dengan hak terbatas, daftar URL yang diizinkan, dan informasi teknologi umum tanpa meminta basis data, kode sumber, atau kredensial produksi.

Untuk website Kantor Imigrasi Kelas I TPI Palembang, pengujian sebaiknya memadukan passive scan, active scan non-destruktif pada ruang lingkup yang disetujui, pemeriksaan manual terhadap kontrol akses dan sesi, validasi header serta TLS, inventarisasi komponen, dan konfirmasi temuan bersama pengelola teknologi informasi. Seluruh aktivitas perlu didahului izin tertulis dan rencana pemulihan apabila pengujian memengaruhi layanan.

3. Implikasi Tata Kelola Keamanan

Temuan literatur menunjukkan bahwa audit keamanan tidak cukup dilakukan sekali pada saat serah terima aplikasi. Portal instansi memerlukan siklus inventarisasi aset, pembaruan komponen, peninjauan konfigurasi, pengelolaan akun administrator, pencatatan peristiwa, dan pengujian ulang setelah perubahan besar. Vendor pengembang dan pengelola internal perlu memiliki pembagian tanggung jawab yang jelas, termasuk batas waktu patch, prosedur eskalasi, pengendalian perubahan, serta penyimpanan bukti perbaikan.

Hasil SLR dapat digunakan untuk menentukan prioritas skenario uji, tetapi tidak dapat menggantikan pengujian langsung. Kesamaan fungsi atau teknologi dengan portal instansi lain juga tidak cukup untuk menyimpulkan bahwa kerentanannya sama. Setiap kesimpulan mengenai kondisi website Kantor Imigrasi Kelas I TPI Palembang harus didasarkan pada bukti pengujian yang diperoleh secara sah dan dapat direproduksi.

4. Keterbatasan Penelitian

Penelitian memiliki empat keterbatasan. Pertama, data berasal dari sumber sekunder dan tidak mencakup pengujian langsung pada objek yang menjadi konteks implikasi. Kedua, reklasifikasi OWASP Top 10:2025 dilakukan dari ringkasan temuan dalam matriks ekstraksi. Beberapa artikel tidak mencantumkan CWE sehingga pemetaan dapat mengandung perbedaan interpretasi. Ketiga, dokumen terpilih mencakup jenis publikasi dan objek yang beragam sehingga mutu bukti tidak seragam. Keempat, metadata bibliografis dan DOI seluruh sumber perlu diverifikasi kembali pada laman penerbit atau repositori resmi sebelum pengajuan naskah.

5. Arah Penelitian Lanjutan

Penelitian berikutnya perlu melakukan vulnerability assessment langsung pada website Kantor Imigrasi Kelas I TPI Palembang dengan izin tertulis dan pendekatan grey box. Pengujian dapat menggunakan OWASP ZAP sebagai salah satu alat, kemudian menggabungkannya dengan pemeriksaan manual, verifikasi komponen, dan penilaian risiko. Penelitian lanjutan juga dapat membandingkan beberapa kantor imigrasi dengan indikator yang sama serta menyusun pedoman audit keamanan khusus untuk portal layanan keimigrasian.

KESIMPULAN

Revisi berdasarkan OWASP Top 10:2025 menghasilkan pola yang berbeda dari naskah awal. Injection merupakan kategori yang paling sering dilaporkan pada 16 dari 32 studi (50,00%), diikuti Security Misconfiguration pada 14 studi (43,75%) dan Broken Access Control pada 12 studi (37,50%). OWASP ZAP menjadi alat yang paling sering digunakan, yaitu pada 12 studi, tetapi frekuensi tersebut tidak cukup untuk menyatakan bahwa ZAP selalu menjadi alat paling efektif.

Implikasi utama bagi Kantor Imigrasi Kelas I TPI Palembang adalah perlunya audit keamanan yang berizin, terukur, dan memadukan pengujian otomatis dengan verifikasi manual. Prioritas pemeriksaan meliputi kontrol akses, konfigurasi server dan header, dependensi perangkat lunak, injeksi, autentikasi, logging dan alerting, serta penanganan kondisi luar biasa. Hasil penelitian ini merupakan dasar penyusunan audit dan tidak membuktikan keberadaan kerentanan pada website yang bersangkutan.

DAFTAR PUSTAKA

Adinugroho, S., et al. (2022). Analisis keamanan sistem e-learning menggunakan kerangka kerja OWASP. Jurnal Informatika, 9(2), 115–123.

Ahmed, R. (2025). Web application security assessment of government portals in Bangladesh using OWASP ZAP. International Journal of Cybersecurity, 12(1), 45–58.

Anisah, N. (2025). Analisis keamanan sistem informasi web menggunakan penetration testing. Jurnal Keamanan Informasi, 8(1), 22–31.

Anugraha, D., & Alwi, M. (2025). Metodologi vulnerability assessment untuk keamanan aplikasi web. Jurnal Teknik Informatika, 14(2), 88–97.

Bagaskara, R., et al. (2025). Evaluasi keamanan website Dinas Sosial Surabaya menggunakan OWASP Top 10. Jurnal Sistem Informasi, 11(1), 34–43.

Dinata, P., et al. (2025). Penetration testing pada situs web rumah sakit: Paradoks keamanan HTTPS. Jurnal Keamanan Siber, 6(1), 11–20.

Fatihah, N., & Dinarto, A. (2024). Perbandingan keamanan CMS WordPress dan Drupal menggunakan framework ISSAF. Jurnal Teknologi Informasi, 15(3), 201–212.

Firdaus, A., & Widyawan. (2025). Evaluasi keamanan web pemerintah menggunakan OWASP dan PTES. Jurnal Informatika Pemerintahan, 4(1), 56–67.

Firnanda, T., et al. (2025). Vulnerability assessment web ERP menggunakan PTES dan ISO 27005. Jurnal Keamanan Informasi, 9(2), 78–91.

Hilario, C., et al. (2024). Quantitative assessment of access control vulnerabilities in Java web applications. Journal of Information Security, 15(4), 312–325.

Hilda, R., et al. (2024). Penetration testing website pemerintahan desa menggunakan OWASP ZAP. Jurnal Sistem dan Teknologi Informasi, 12(3), 144–155.

Irvan, M., et al. (2024). Analisis keamanan aplikasi inventori kantor imigrasi menggunakan OWASP. Jurnal Teknik Komputer, 10(2), 67–76.

Madya, R., et al. (2025). Evaluasi kerentanan direktori PPID menggunakan NIST SP 800-115 dan OWASP ZAP. Jurnal Keamanan Siber Indonesia, 5(1), 23–34.

Maniraj, S., et al. (2024). Web application vulnerability detection using OWASP ZAP and threat mitigation simulation. International Journal of Security, 8(2), 89–101.

Marbun, J. I. N. S. (2025). Evaluasi kerentanan sistem informasi website Kantor Imigrasi Kelas I TPI Jambi menggunakan OWASP Top 10 [Skripsi].

Mifthahuddin, A., et al. (2025). Analisis kerentanan e-journal Universitas Mulawarman menggunakan NIST SP 800-115 dan OWASP. Jurnal Informatika Mulawarman, 20(1), 45–56.

Nawrocki, P., & Kolodziej, J. (2024). Best practices for web application vulnerability assessment using OWASP. Journal of Cybersecurity Research, 11(3), 234–248.

OWASP Foundation. (2025). OWASP Top 10:2025. https://owasp.org/Top10/2025/

Page, M. J., et al. (2021). The PRISMA 2020 statement: An updated guideline for reporting systematic reviews. BMJ, 372, n71. https://doi.org/10.1136/bmj.n71

Pramudia, R., et al. (2025). Simulasi eksploitasi kerentanan aplikasi web berbasis OWASP Top 10. Jurnal Keamanan Siber, 7(1), 34–45.

Pratiwi, D., & Sushanti, R. (2025). Evaluasi efektivitas dan keamanan portal imigrasi e-Visa MOLINA. Jurnal Administrasi Publik Digital, 3(1), 12–23.

Prayoga, A., et al. (2025). Deteksi persistent XSS pada sistem SIISTA Universitas Dhyana Pura menggunakan PTES. Jurnal Teknologi Informasi, 16(2), 167–178.

Qadir, A., et al. (2025). Comparative evaluation of approaches and tools for effective security testing of web applications. PeerJ Computer Science, 11, e2821. https://doi.org/10.7717/peerj-cs.2821

Rahman, F., et al. (2025). Komparasi Nuclei dan OWASP ZAP untuk evaluasi keamanan platform web. Jurnal Rekayasa Perangkat Lunak, 12(1), 56–67.

Rahmi, N., et al. (2024). Deteksi kerentanan aplikasi web terintegrasi menggunakan Acunetix. Jurnal Sistem Informasi, 10(2), 89–98.

Ramadhan, F., et al. (2025). Systematic literature review: Standar dan metodologi audit keamanan

aplikasi web. Jurnal Tinjauan Ilmu Komputer, 8(1), 1–15.
Reonaldi, B., et al. (2025). Analisis kerentanan situs web Pemerintah Kota Palu saat transisi server. Jurnal Informatika Palu, 6(1), 23–32.
Rethlefsen, M. L., Kirtley, S., Waffenschmidt, S., Ayala, A. P., Moher, D., Page, M. J., & Koffel, J. B. (2021). PRISMA-S: An extension to the PRISMA statement for reporting literature searches in systematic reviews. Systematic Reviews, 10, 39. https://doi.org/10.1186/s13643-020-01542-z
Sugara, D., & Sriyasa, I. (2024). Pemetaan risiko keamanan web menggunakan standar OWASP. Jurnal Ilmu Komputer, 17(3), 201–210.
Syarifudin, A., et al. (2025). Evaluasi keamanan web distribusi zakat menggunakan penetration testing OWASP. Jurnal Teknologi dan Sistem Informasi, 11(2), 78–89.
Tahir, M., & Risky, A. (2024). Analisis penetration testing web dinas pemerintahan menggunakan PTES. Jurnal e-Government, 9(2), 112–123.
Wibowo, A., et al. (2023). Apache web server security hardening menggunakan standar NIST. Jurnal Keamanan Jaringan, 7(1), 34–45.
Wisnu, A., & Soewito, B. (2026). Security assessment based on OWASP Top 10 using SonarQube and ZAP on export and import applications in the LNSW. INTENSIF: Jurnal Ilmiah Penelitian dan Penerapan Teknologi Sistem Informasi, 10(1), 36–53. https://doi.org/10.29407/intensif.v10i1.25294
Yusuf, R., et al. (2025). VAPT platform SINTA Kemdikbud menggunakan OWASP WSTG dan Technology Acceptance Model. Jurnal Pendidikan Digital, 4(1), 45–56.
Zairina, E., et al. (2025). Implementasi pengujian penetrasi pada sistem voting elektronik Indonesia menggunakan OWASP. Jurnal Sistem Pemilu Digital, 2(1), 12–23.