E-ISSN : 2988-1986
https://ejournal.cahayailmubangsa.institute/index.php/kohesi

Kohesi: Jurnal Multidisiplin Saintek
Volume 11 No 2 Tahun 2026

PENGUJIAN SISTEM INFORMASI PELAYANAN PUBLIK PEMERINTAH DAERAH XYZ MENGGUNAKAN METODE PENETRATION TESTING BERDASARKAN OWASP TOP 10 2025

Salsa Bila Febrianti[1*], Farisa Dhonan Kaharani[2], Doddy Ridwandono[3]
Sistem Informasi, Universitas Pembangunan Nasional "Veteran" Jawa Timur
salsab.febrianti@gmail.com

ABSTRACT

The XYZ Local Government Public Service Information System serves as a crucial medium for delivering digital-based public services. As information technology systems grow increasingly complex, cybersecurity threats are also evolving, necessitating periodic security system evaluations. This study aims to identify security vulnerabilities within the Public Service Information System using a penetration testing method based on the OWASP Top 10:2025 standard. A "Gray Box Testing" approach was employed, wherein the tester possessed partial information about the system under test. Vulnerability identification was conducted using OWASP ZAP, followed by testing of the discovered vulnerabilities to verify their risk levels. The vulnerability scan revealed 17 findings. These results demonstrate that the OWASP Top 10:2025 standard effectively serves as a reference for penetration testing, enabling the identification of security vulnerabilities and the provision of remediation recommendations to enhance web application security.

Keywords: OWASP Top 10:2025, Penetration Testing, Public Service Information System, Security Testing, Web Security.

ABSTRAK

Sistem Informasi Pelayanan Publik Pemerintah Daerah XYZ merupakan media penting dalam penyelenggaraan layanan publik berbasis digital. Seiring meningkatnya kompleksitas teknologi informasi, ancaman keamanan siber juga semakin berkembang sehingga diperlukan evaluasi keamanan sistem secara berkala. Penelitian ini bertujuan mengidentifikasi dan mengevaluasi kerentanan keamanan pada Sistem Informasi Pelayanan Publik menggunakan metode Penetration Testing berdasarkan standar OWASP Top 10:2025. Pendekatan yang digunakan adalah Grey Box Testing, yaitu penguji memiliki sebagian informasi mengenai sistem yang diuji. Identifikasi kerentanan dilakukan menggunakan OWASP ZAP, kemudian dilakukan pengujian terhadap kerentanan yang ditemukan untuk memverifikasi tingkat risikonya. Hasil vulnerability scanning menunjukkan terdapat 17 temuan. Dari hasil ini OWASP Top 10:2025 efektif digunakan sebagai acuan dalam proses penetration testing untuk mengidentifikasi kerentanan keamanan sekaligus memberikan rekomendasi perbaikan guna meningkatkan keamanan aplikasi web.

Kata Kunci: Keamanan Sistem, OWASP Top 10:2025, Penetration Testing, Sistem Informasi Pelayanan Publik, Vulnerability Scanning

Article History
Received: Juli 2026
Reviewed:Juli 2026
Published: Juli 2026

Plagiarism Checker No 237.u873247.fh8374

Copyright : Author
Publish by : Kohesi

This work is licensed under a Creative Commons Attribution-NonCommercial 4.0 International License

PENDAHULUAN

Perkembangan teknologi informasi telah mendorong transformasi digital di berbagai sektor, termasuk pemerintahan. Salah satu implementasinya adalah pemanfaatan sistem informasi pelayanan publik berbasis web untuk meningkatkan efektivitas, efisiensi, transparansi, dan kualitas pelayanan kepada masyarakat. Sistem informasi pelayanan publik berperan sebagai media penyampaian informasi, pengelolaan data, pelaporan, serta koordinasi antarinstansi pemerintah. Oleh karena itu, sistem informasi menjadi aset penting yang harus menjaga aspek kerahasiaan (*confidentiality*), integritas (*integrity*), dan ketersediaan (*availability*) informasi. Keamanan sistem informasi menjadi aspek yang sangat penting karena sistem menghadapi berbagai ancaman yang dapat berasal dari dalam maupun luar organisasi. Ancaman tersebut dapat dilakukan oleh individu, kelompok, organisasi, maupun mekanisme tertentu yang berpotensi mengganggu stabilitas sistem. Apabila tidak ditangani dengan baik, ancaman tersebut dapat menyebabkan kerusakan, kebocoran, maupun gangguan terhadap informasi yang tersimpan di dalam sistem sehingga berdampak pada keberlangsungan layanan yang diberikan kepada Masyarakat (Pendahuluan, 2025).

Perkembangan transformasi digital di sektor pemerintahan tidak hanya berfokus pada pemanfaatan teknologi untuk meningkatkan kualitas layanan publik, tetapi juga menuntut adanya strategi yang mampu mengantisipasi berbagai risiko yang menyertainya. Oleh karena itu, institusi pemerintah perlu mengembangkan strategi yang tidak hanya mengadopsi teknologi digital, tetapi juga memahami implikasi serta dampaknya dalam proses transformasi digital (Alfi, 2023). Sejalan dengan hal tersebut, Pemerintah Daerah XYZ memiliki Sistem Informasi Pelayanan Publik berbasis web untuk mendukung layanan penanganan insiden keamanan siber, penyampaian informasi keamanan, pelaporan insiden, serta koordinasi respons terhadap ancaman siber. Sebagai sistem yang mengelola informasi penting, keberadaan celah keamanan berpotensi menyebabkan kebocoran data, penyalahgunaan hak akses, gangguan layanan publik, serta menurunkan kepercayaan masyarakat. Oleh karena itu, diperlukan evaluasi keamanan untuk mengidentifikasi potensi kerentanan dan meningkatkan keamanan sistem.

Salah satu metode yang umum digunakan untuk mengevaluasi keamanan aplikasi web adalah *penetration testing*. *Penetration testing* merupakan subkategori dari *ethical hacking* yang bertujuan menguji dan melindungi keamanan informasi melalui simulasi serangan menggunakan metode yang umum digunakan oleh peretas (Jaelani & Khoirunnisa, 2023). Melalui simulasi tersebut, kerentanan dapat diidentifikasi sebelum dimanfaatkan oleh pihak yang tidak bertanggung jawab sehingga menjadi dasar penyusunan rekomendasi perbaikan. Penelitian ini menggunakan pendekatan *Grey Box Testing*, yaitu metode pengujian yang memberikan sebagian informasi mengenai sistem kepada penguji sehingga proses identifikasi kerentanan dapat dilakukan secara lebih efektif dibandingkan *black box testing* tanpa memerlukan akses penuh terhadap kode sumber sistem (Putri et al., 2025).

Sebagai acuan identifikasi kerentanan, penelitian ini menggunakan Open Worldwide Application Security Project (OWASP), yaitu organisasi nirlaba yang menyediakan berbagai standar dan panduan keamanan aplikasi secara *open source*. Salah satu kontribusi terpenting dari OWASP adalah OWASP Top 10, yaitu daftar yang disusun oleh komunitas OWASP yang mencakup sepuluh kerentanan keamanan aplikasi web yang paling sering ditemukan dan berpotensi mengancam keamanan situs web. Daftar tersebut diperbarui secara berkala untuk memberikan panduan mengenai kerentanan keamanan aplikasi web yang relevan dengan perkembangan ancaman siber (Khoirun & Tulodo, 2025). Oleh karena itu, penelitian ini menggunakan OWASP Top 10:2025 sebagai acuan karena telah memuat pembaruan kategori risiko keamanan yang lebih sesuai dengan kondisi aplikasi web saat ini.

Beberapa penelitian terdahulu menunjukkan bahwa penerapan OWASP dalam *penetration testing* mampu mengidentifikasi berbagai kerentanan pada aplikasi web. (Elanda & Buana, 2021) melakukan pengujian keamanan pada Sistem Informasi E-Office menggunakan OWASP Top 10 dan OWASP ZAP serta berhasil mengidentifikasi empat kategori kerentanan, yaitu *Sensitive Data Exposure, Security Misconfiguration, Cross-Site Scripting (XSS),* dan *Insecure Deserialization*. Penelitian tersebut menunjukkan bahwa OWASP Top 10 efektif digunakan sebagai acuan dalam mengidentifikasi serta mengevaluasi kerentanan keamanan sehingga dapat membantu pengembang menentukan langkah perbaikan sistem.

Selanjutnya, (Hendita et al., 2022) mengimplementasikan OWASP ZAP versi 2.10.0 pada Website Sistem Informasi Akademik Universitas Pancasila. Hasil penelitian menunjukkan bahwa OWASP ZAP mampu mengidentifikasi 19 kerentanan dengan tingkat risiko sedang, rendah, dan informatif yang dipetakan ke dalam kategori *Broken Access Control, Security Misconfiguration, Vulnerable and Outdated Components,* serta *Software and Data Integrity Failures*. Hasil penelitian membuktikan bahwa OWASP ZAP efektif digunakan sebagai *vulnerability scanner* untuk membantu evaluasi keamanan aplikasi web.

Penelitian lainnya dilakukan oleh (Issaf & Koprawi, 2025) yang menerapkan *penetration testing* menggunakan framework ISSAF dan OWASP WSTG pada website Instansi XYZ. Pengujian dilakukan melalui tahapan *Gathering Publicly Available Information, Network Scanning, System Profiling, Service Profiling, Application Testing,* hingga *Vulnerability Identification/Assessment*. Hasil penelitian menunjukkan bahwa pendekatan *penetration testing* secara sistematis mampu membantu identifikasi dan evaluasi kerentanan keamanan website serta menghasilkan rekomendasi perbaikan.

Meskipun berbagai penelitian telah menerapkan OWASP Top 10 maupun OWASP ZAP, sebagian besar masih menggunakan acuan OWASP Top 10:2021 atau hanya berfokus pada proses *vulnerability scanning*. Penelitian yang menerapkan OWASP Top 10:2025 pada Sistem Informasi Pelayanan Publik di lingkungan pemerintah daerah masih relatif terbatas. Selain itu, penelitian ini mengombinasikan OWASP ZAP dengan *penetration testing* menggunakan pendekatan *Grey Box Testing* sehingga diharapkan mampu memberikan gambaran keamanan sistem yang lebih komprehensif sekaligus menghasilkan rekomendasi perbaikan sesuai standar keamanan aplikasi web terkini.

Berdasarkan uraian tersebut, penelitian ini bertujuan mengidentifikasi dan mengevaluasi kerentanan keamanan pada Sistem Informasi Pelayanan Publik Pemerintah Daerah XYZ menggunakan metode *Penetration Testing* berdasarkan standar OWASP Top 10:2025. Hasil penelitian diharapkan dapat memberikan informasi mengenai tingkat keamanan sistem, mengidentifikasi potensi kerentanan, serta menghasilkan rekomendasi perbaikan untuk meningkatkan keamanan layanan publik berbasis web.

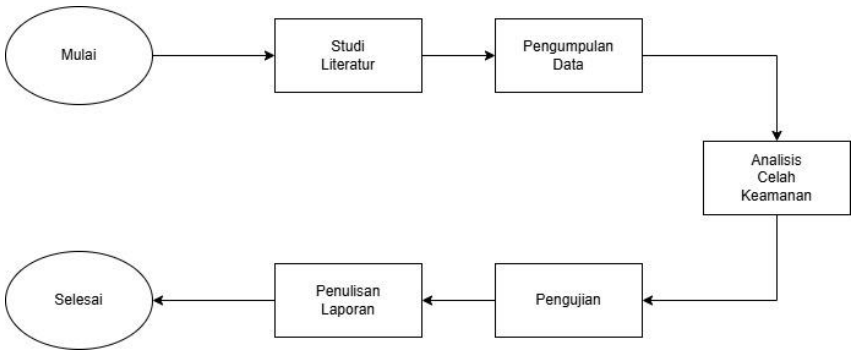
METODE PENELTIAN

Penelitian ini menggunakan pendekatan deskriptif dengan metode penetration testing untuk mengevaluasi tingkat keamanan website Sistem Informasi Pelayanan Publik Pemerintah Daerah XYZ. Pengujian dilakukan menggunakan pendekatan Grey Box Testing, yaitu metode yang memberikan sebagian informasi mengenai sistem kepada penguji sehingga proses identifikasi kerentanan dapat dilakukan secara lebih efektif tanpa memerlukan akses penuh terhadap kode sumber aplikasi. Proses penetration testing mengacu pada OWASP Web Security Testing Guide (WSTG) yang terdiri atas tahapan *planning, information gathering, vulnerability analysis, exploitation,* dan *reporting*. Analisis kerentanan dilakukan menggunakan OWASP ZAP dengan acuan OWASP Top 10:2025.

Objek penelitian adalah website Sistem Informasi Pelayanan Publik Pemerintah Daerah XYZ yang berada pada lingkungan staging server. Pengujian dilaksanakan pada bulan Mei 2026.

Alur penelitian disusun secara sistematis untuk membantu memahami tahapan yang dilakukan dalam penelitian ini, mulai dari tahap awal hingga tahap akhir, sebagaimana ditunjukkan pada gambar dibawah ini.

Gambar 1. Alur Penelitian



1. Studi Literatur

Tahap awal berupa kajian terhadap referensi, standar, dan kerangka kerja yang relevan dengan penetration testing, meliputi OWASP Top 10, OWASP WSTG, sebagai dasar teori dan acuan metodologi penelitian.

2. Pengumpulan Data

Tahap penentuan ruang lingkup, tujuan, serta perolehan akses dan informasi sistem yang diperlukan melalui koordinasi dengan tim pengelola sistem, guna memastikan pengujian berjalan secara legal dan terstruktur.

3. Analisa Celah Keamanan

Tahap identifikasi dan analisis kerentanan menggunakan teknik *vulnerability scanning* dengan tools OWASP ZAP, untuk menemukan kelemahan konfigurasi keamanan dan memetakan temuan berdasarkan kategori OWASP Top 10:2025.

4. Pengujian

Tahap simulasi serangan (eksploitasi) terhadap kerentanan dengan level risiko *high* dan *medium* menggunakan tools CURL, guna membuktikan apakah kerentanan tersebut dapat dieksploitasi tanpa menimbulkan kerusakan pada sistem. Hasil detail pengujian tidak disertakan dalam laporan ini dikarenakan keterbatasan izin dari pihak Pemerintah Daerah XYZ terkait kerahasiaan data dan keamanan sistem.

5. Penulisan Laporan

Tahap penyusunan laporan akhir yang memuat hasil pengujian, tingkat risiko kerentanan, serta rekomendasi perbaikan sebagai acuan peningkatan keamanan sistem.

HASIL DAN PEMBAHASAN

Bab ini menyajikan hasil pengujian keamanan pada Sistem Informasi Pelayanan Publik Pemerintah Daerah XYZ menggunakan metode *penetration testing* berdasarkan acuan OWASP Top 10:2025. Tahapan pengujian meliputi *information gathering*, *vulnerability scanning*, verifikasi kerentanan, serta penyusunan rekomendasi perbaikan. Hasil pengujian selanjutnya dianalisis dan dibandingkan dengan penelitian terdahulu untuk mengetahui posisi penelitian yang dilakukan.

1. Hasil Information Gathering

Tahap *information gathering* bertujuan memperoleh informasi awal mengenai sistem target yang diperlukan sebelum proses pengujian dilakukan. Informasi diperoleh dari pihak Pemerintah Daerah XYZ sesuai ruang lingkup pengujian pada lingkungan *staging server*.

Tabel 1. Hasil Information Gathering

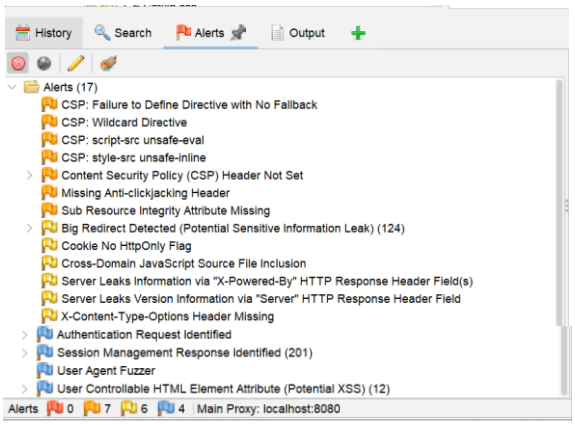
No.	Kategori	Hasil
1.	Target Utama	192.***.*.** — *****Pr**-*****
2.	Lingkup Pengujian	Staging Server (Internal Network 192.***.*.*)
3.	Aset yang Diuji	Port 8*** (*****)

Tahap ini menghasilkan informasi yang digunakan sebagai dasar pelaksanaan *vulnerability scanning* dan *penetration testing*. Penggunaan lingkungan *staging server* bertujuan meminimalkan risiko gangguan terhadap sistem produksi selama proses pengujian.

2. Hasil Vulnerability Scanning

Proses *vulnerability scanning* dilakukan menggunakan OWASP ZAP untuk mengidentifikasi potensi kerentanan pada website. Pemindaian dilakukan menggunakan fitur *Automated Scan* dan hasilnya diklasifikasikan berdasarkan tingkat risiko menggunakan OWASP Risk Rating Methodology.

Gambar 2. Hasil Vulnerability Scanning



Hasil pemindaian menunjukkan terdapat 17 temuan kerentanan, yang terdiri atas 7 kerentanan tingkat Medium, 6 kerentanan tingkat Low, dan 4 temuan Informational. Dari seluruh temuan tersebut, 13 kerentanan berhasil dipetakan ke dalam kategori OWASP Top 10:2025, yaitu Broken Access Control, Security Misconfiguration, Insecure Design, dan Software and Data Integrity Failures.

Temuan ini menunjukkan bahwa sebagian besar kerentanan berasal dari konfigurasi keamanan yang belum optimal, terutama pada penerapan *HTTP Security Header* dan *Content Security Policy*. Kondisi tersebut berpotensi meningkatkan risiko serangan seperti *Cross-Site Scripting (XSS)*, *clickjacking*, kebocoran informasi server, serta penyalahgunaan konfigurasi aplikasi apabila tidak segera dilakukan perbaikan.

Hasil penelitian ini sejalan dengan penelitian Elanda dan Buana (2021) yang menemukan kerentanan pada kategori Security Misconfiguration, serta penelitian Hendita et al. (2022) yang juga mengidentifikasi Security Misconfiguration dan Software and Data Integrity Failures menggunakan OWASP ZAP. Perbedaannya, penelitian ini menggunakan OWASP Top 10:2025 sebagai acuan sehingga klasifikasi kerentanan mengikuti pembaruan standar keamanan aplikasi web terbaru.

3. Rekomendasi Perbaikan

Berdasarkan hasil *vulnerability scanning* dan proses verifikasi, disusun rekomendasi perbaikan terhadap seluruh kerentanan yang ditemukan. Rekomendasi tersebut bertujuan meningkatkan keamanan aplikasi serta mengurangi kemungkinan eksploitasi oleh pihak yang tidak berwenang. Rekomendasi yang diberikan meliputi:

Tabel 2. Rekomendasi Perbaikan

No	Kerentanan	Resiko	Rekomendasi
1.	CSP: Failure to Define Directive with No Fallback	Medium	Menambahkan *fallback directive* seperti default-src pada konfigurasi Content Security Policy (CSP).
2.	CSP: Wildcard Directive	Medium	Menghindari penggunaan wildcard (*) dan menentukan domain yang diizinkan secara spesifik.
3.	CSP: script-src unsafe-eval	Medium	Menghapus penggunaan unsafe-eval dan menghindari fungsi eval() atau sejenisnya.
4.	CSP: style-src unsafe-inline	Medium	Menghilangkan unsafe-inline dengan menggunakan file CSS terpisah atau *nonce/hash*.
5.	Content Security Policy (CSP) Header Not Set	Medium	Mengimplementasikan header Content Security Policy (CSP) pada server web.
6.	Missing Anti-clickjacking Header	Medium	Menambahkan header X-Frame-Options atau frame-ancestors pada CSP.
7.	Sub Resource Integrity Attribute Missing	Medium	Menambahkan atribut integrity dan crossorigin pada resource eksternal (SRI).
8.	Big Redirect Detected	Low	Membatasi mekanisme *redirect* hanya ke domain terpercaya dan menghindari informasi sensitif pada URL.

9.	Cookie No HttpOnly Flag	Low	Menambahkan atribut HttpOnly pada seluruh cookie sesi aplikasi.
10.	Cross-Domain JavaScript Source File Inclusion	Low	Membatasi penggunaan JavaScript dari domain eksternal dan menerapkan HTTPS serta SRI.
11.	Server Leaks Information via X-Powered-By	Low	Menghapus atau menyembunyikan header X-Powered-By.
12.	Server Leaks Version Information via Server Header	Low	Menyembunyikan informasi versi server pada header HTTP Server.
13.	X-Content-Type-Options Header Missing	Low	Menambahkan header X-Content-Type-Options: nosniff.

KESIMPULAN DAN SARAN

Berdasarkan hasil penelitian, metode penetration testing dengan pendekatan Grey Box Testing berdasarkan standar OWASP Top 10:2025 berhasil mengidentifikasi dan mengevaluasi kerentanan keamanan pada Sistem Informasi Pelayanan Publik Pemerintah Daerah XYZ. Pengujian menggunakan OWASP ZAP menghasilkan 17 temuan kerentanan dengan 13 temuan berhasil dipetakan ke dalam kategori OWASP Top 10:2025. Hasil tersebut menunjukkan bahwa sebagian besar kerentanan disebabkan oleh konfigurasi keamanan yang belum optimal, sehingga penerapan OWASP Top 10:2025 terbukti efektif sebagai acuan dalam mengidentifikasi kerentanan dan menyusun rekomendasi perbaikan untuk meningkatkan keamanan aplikasi web. Oleh karena itu, pengelola sistem disarankan untuk segera mengimplementasikan rekomendasi perbaikan yang telah diusulkan, khususnya pada konfigurasi Content Security Policy (CSP), HTTP Security Header, pengamanan cookie, dan konfigurasi server, serta melakukan pengujian keamanan secara berkala agar keamanan sistem tetap terjaga dan mampu mengantisipasi munculnya kerentanan baru.

DAFTAR PUSTAKA

Alfi, M. (2023). *Jurnal Kajian Stratejik Ketahanan Nasional Analisis Risiko Keamanan Siber dalam Transformasi Digital Pelayanan Publik di Indonesia Analisis Risiko Keamanan Siber Dalam Transformasi Digital Pelayanan Publik di Indonesia*. *6*(2). https://doi.org/10.7454/jkskn.v6i2.10082

Elanda, A., & Buana, R. L. (2021). *ANALISIS KUALITAS KEAMANAN SISTEM INFORMASI E-OFFICE BERBASIS WEBSITE PADA STMIK ROSMA DENGAN MENGGUNAKAN OWASP TOP 10*. *6*(2), 185–191.

Hendita, G., Kusuma, A., Informatika, P. T., Teknik, F., Pancasila, U., & Selatan, J. (2022). *IMPLEMENTASI OWASP ZAP UNTUK PENGUJIAN KEAMANAN SISTEM INFORMASI AKADEMIK*. *16*(2), 178–186.

Issaf, M. F., & Koprawi, M. (2025). *Analisis Keamanan Website Pada Instansi XYZ Melalui Penetration Testing*. *5*(1), 547–555.

Jaelani, W. L., & Khoirunnisa, F. (2023). *PENETRATION TESTING WEBSITE DENGAN METODE BLACK BOX TESTING UNTUK MENINGKATKAN KEAMANAN WEBSITE PADA INSTANSI (REDACTED)*. *05*(01), 1–8.

Khoirun, M. F., & Tulodo, R. P. (2025). *Analisis Kerentanan Website Menggunakan Metode Penetration Testing Dengan Standar Keamanan OWASP Top 10 : 2021 Studi Kasus Website Sistem Informasi Manajemen Laboratorium Dinas Kesehatan Kabupaten Tegal*. *02*(06), 762–773.

Pendahuluan, I. (2025). *Analisis Keamanan Sistem Informasi Menggunakan Metode Vulnerability Assesment pada Aplikasi Web Karangasem . go . id*. *9*(2), 466–473.

Putri, D. A., Wahanani, H. E., & Nurlaili, A. L. (2025). *Penerapan teknik*. *10*(3), 2366–2377.