Full Paper

Identifikasi dan Analisis Kerentanan Keamanan pada Aplikasi Website Pemerintah Daerah Menggunakan Metodologi ISSAF dan OWASP Top 10 Tahun 2025

Ahmad Rifqi Abdurrahman[1], Raditya Bagus Pradana[2], Wisnu Hafid Firdaus Oktobrian[3], Eka Dyar Wahyuni[4], Siti Mukaromah[5]
[1,3]Program Studi Sistem Informasi, Universitas Pembangunan Nasional "Veteran" Jawa Timur, Indonesia

Informasi Artikel

Terbit: Juli 2026

Kata Kunci:

Penetration Testing
Keamanan Website
Kerentanan Keamanan
OWASP Top 10:2025
ISSAF

ABSTRAK

Perkembangan teknologi digital telah meningkatkan penggunaan *website* sebagai sarana pelayanan publik oleh instansi pemerintah daerah. Namun, pertumbuhan ini tidak diimbangi dengan keamanan yang memadai, sehingga meningkatkan risiko serangan siber terhadap aplikasi *website*. Penelitian ini bertujuan untuk menguji keamanan website pada aplikasi instansi pemerintah daerah menggunakan metodologi Information Systems Security Assessment Framework (ISSAF) dan standar Open Web Application Security Project (OWASP) Top 10:2025. Pengujian dilakukan pada *environment staging* menggunakan OWASP ZAP untuk *automated vulnerability scanning* yang dikombinasikan dengan verifikasi manual. Hasil penelitian mengidentifikasi 17 temuan kerentanan yang terdiri dari 8 temuan kategori *medium*, 5 temuan kategori *low*, dan 4 temuan kategori *informational*. Kerentanan terbanyak berada pada kategori *Security Misconfiguration* dengan 10 temuan, diikuti kategori *Broken Access Control*, *Injection*, *Insecure Design*, *Software and Data Integrity Failures*, dan *Mishandling of Exceptional Conditions* masing-masing dengan 1 temuan. Tidak ditemukan kerentanan dengan tingkat keparahan *high* atau *critical*. Penelitian ini membuktikan efektivitas penerapan ISSAF dan OWASP Top 10:2025 dalam mengidentifikasi kerentanan keamanan pada aplikasi web secara sistematis. Rekomendasi perbaikan disarankan untuk meningkatkan postur keamanan, khususnya pada konfigurasi *header*, Content Security Policy, dan mekanisme *input validation*.

Corresponding Author:

Ahmad Rifqi Abdurrahman
Email: ahmadrifqiabdurrahman@gmail.com

1. PENDAHULUAN

Di era kemajuan teknologi yang semakin cepat, masyarakat mengalami berbagai kemudahan. Kemajuan dalam teknologi digital telah mendorong kemudahan ini, yang telah mengubah cara organisasi memberikan layanan dan mengkomunikasikan data kepada masyarakat. *Website* yang digunakan oleh berbagai instansi untuk berkomunikasi dan menawarkan layanan kepada masyarakat adalah salah satu cara implementasinya [1]. Berdasarkan data yang dikumpulkan oleh Asosiasi Penyelenggara Jasa Internet Indonesia (APJII), jumlah orang yang menggunakan internet telah melampaui 210 juta pada tahun 2023 dan akan meningkat menjadi 221 juta pada tahun 2024 [2]. Karena itu, kemajuan ini sangat bermanfaat bagi masyarakat karena membuatnya lebih mudah untuk mendapatkan informasi dan layanan publik.

Meskipun memiliki banyak fitur, penggunaan situs *website* tersebut menimbulkan masalah keamanan yang signifikan. Serangan siber meningkat ketika jumlah pengguna dan data yang tersimpan di *website* meningkat. Perkembangan teknologi yang cepat tidak diimbangi dengan sumber daya manusia yang cukup, terutama dalam hal keamanan informasi, membuat ancaman ini semakin nyata. Kebocoran data pribadi dapat

terjadi, sistem menjadi tidak dapat diakses, dan kepercayaan institusi dapat hilang jika sistem keamanan tidak dijaga dengan baik [3].

Penetration testing dapat dilakukan untuk mengurangi risiko tersebut. *Penetration testing* adalah simulasi serangan yang direncanakan dan terkendali yang digunakan untuk mengidentifikasi keamanan sistem sebelum orang yang tidak bertanggung jawab melakukannya [4]. Terdapat beberapa *framework* yang dapat digunakan untuk melakukan pengujian secara terukur dan sistematis seperti Information Systems Security Assessment Framework (ISSAF), National Institute of Standards and Technology (NIST), Open Web Application Security Project (OWASP), dan sebagainya [5]. Setiap *framework* menawarkan pendekatan dan pedoman yang berbeda untuk evaluasi keamanan.

Website milik instansi pemerintah daerah sangat penting untuk menyediakan layanan langsung kepada masyarakat. Data masyarakat yang dikelola oleh situs *website* ini biasanya termasuk informasi pribadi seperti data pribadi dan transaksi administratif. Apabila situs *website* diretas atau diserang siber, dampak langsung pada masyarakat termasuk kebocoran data pribadi dan penundaan akses ke layanan publik. Dengan mempertimbangkan pentingnya masalah ini, penelitian ini dilakukan untuk menguji keamanan website sebuah instansi pemerintah daerah dengan menggunakan *framework* ISSAF dan standar OWASP Top 10:2025. *Framework* ISSAF menyediakan struktur yang komprehensif untuk pelaksanaan *penetration testing*, sedangkan standar OWASP Top 10:2025 berfokus pada celah kerentanan yang paling umum dan berdampak besar pada aplikasi berbasis *website* [6]. Hasil penelitian ini diharapkan dapat menemukan kerentanan, mengukur risiko, dan menawarkan saran untuk meningkatkan keamanan sistem.

2. DASAR TEORI

Konsep dan dasar teori yang digunakan sebagai landasan analisis dalam penelitian ini dengan uraian sebagai berikut.

2.1. Analisis Keamanan Website

Analisis keamanan *website* adalah proses yang dilakukan secara sistematis untuk menilai, menguji, dan memeriksa sebuah situs web dengan tujuan menemukan celah keamanan, kerentanan, dan peluang keamanan siber. Tujuan dari proses ini adalah untuk mencegah peretasan, menjaga keamanan data pengguna, dan memastikan sistem beroperasi secara aman.

2.2. Metode ISSAF

ISSAF (Information Systems Security Assessment Framework) adalah adalah rangka kerja pengujian penetrasi yang digunakan untuk mengevaluasi ketahanan *website* terhadap berbagai ancaman keamanan [7]. *Framework* ini dipilih karena menyediakan proses evaluasi keamanan sistem informasi yang sistematis yang mencakup langkah-langkah perencanaan, pengumpulan data, analisis kerentanan, dan penyusunan laporan hasil pengujian.

2.3. Metode OWASP

OWASP merupakan *framework open source* yang mengumpulkan data tentang berbagai masalah keamanan pada layanan berbasis web dan menyarankan solusi untuk meningkatkan keamanan [8]. OWASP berusaha meningkatkan keamanan perangkat lunak dengan menyediakan berbagai alat, panduan, dan sumber daya kepada pengembang, praktisi keamanan, dan organisasi untuk menemukan dan mengatasi masalah keamanan pada aplikasi web [9].

2.4. OWASP Top 10:2025

OWASP Top 10 merupakan daftar sepuluh kerentanan keamanan aplikasi *website* yang paling umum ditemukan serta memiliki potensi risiko yang tinggi terhadap keamanan sistem [10]. OWASP maupun *penetration testing* dapat digunakan untuk mendeteksi dan menangani kerentanan keamanan sebelum kerentanan tersebut dimanfaatkan dalam serangan atau peretasan [11]. Beberapa standar dari OWASP Top 10 pada tahun 2025 mencakup *Broken Access Control* (A01), *Security Misconfiguration* (A02), *Software Supply Chain Failures* (A03), *Cryptographic Failures* (A04), *Injection* (A05), *Insecure Design* (A06), *Authentication Failures* (A07), *Software or Data Integrity Failures* (A08), *Security Logging and Alerting Failures* (A09), serta *Mishandling of Exceptional Conditions* (A10).

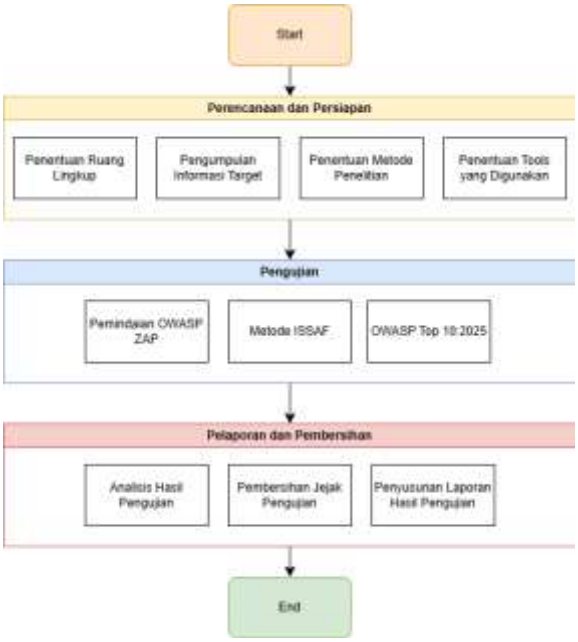
2.5. *Grey-Box Penetration Testing*

Grey box testing dalam *penetration testing* merupakan metode pengujian keamanan yang mengombinasikan pendekatan *black box*, di mana penguji tidak memiliki pengetahuan mengenai sistem, dengan pendekatan *white box*, di mana penguji mengetahui sebagian atau seluruh struktur internal sistem [12].

Penguji umumnya memiliki akses yang terbatas, misalnya hanya sebagai pengguna biasa, serta memahami alur kerja dan logika sistem, sehingga proses pengujian dapat dilakukan dengan lebih efisien dan menghasilkan analisis yang lebih mendalam.

3. METODOLOGI PENELITIAN

Penelitian ini menggunakan Information Systems Security Assessment Framework (ISSAF) sebagai sebagai acuan metodologis dan panduan utama untuk melakukan pengujian penetrasi pada *website* instansi pemerintah daerah. Seluruh tahapan pengujian keamanan dicover oleh ISSAF, yang merupakan alasan untuk memilihnya. Untuk menghindari dampak operasional secara langsung pada layanan publik yang digunakan oleh masyarakat dan instansi terkait, pengujian keamanan dilakukan pada staging lingkungan, yang merupakan replika dari sistem produksi. Staging lingkungan memastikan bahwa setiap aktivitas pengujian, termasuk simulasi eksploitasi, dapat dilakukan tanpa mengganggu sistem yang aktif melayani pengguna. Untuk menghasilkan evaluasi keamanan yang menyeluruh dan mendalam terhadap aplikasi target, tujuan penelitian ini dibagi menjadi tiga fase utama yang saling berhubungan. Fase-fase ini adalah sebagai berikut.



Gambar 1. Metodologi Pengujian

3.1. Perencanaan dan Persiapan

Perencanaan dan persiapan adalah tahap awal yang sangat penting dalam pelaksanaan pengujian penetrasi. Pada titik ini, ruang lingkup pengujian ditetapkan secara eksplisit untuk memastikan bahwa pengujian difokuskan pada topik yang terkait dengan keamanan. Sebelum pengujian dimulai, tujuan pengujian dijelaskan dengan rinci, batas-batas yang harus dipatuhi selama proses pengujian dijelaskan, dan izin resmi diurus oleh unit keamanan informasi instansi lokal. Selain itu, informasi rinci tentang aplikasi yang dimaksud dikumpulkan secara menyeluruh. Informasi ini mencakup teknologi yang digunakan, struktur halaman web, fitur aplikasi, dan karakteristik sistem lainnya. Untuk menemukan kerentanan keamanan, proses pengumpulan data ini sangat penting..

3.2. Pengujian

Seluruh proses identifikasi dan analisis kerentanan keamanan dilakukan secara sistematis di fase pengujian penetrasi. Pada titik ini, pemindaian keamanan OWASP ZAP digunakan untuk melakukan pemindaian keamanan otomatis terhadap aplikasi target. Selanjutnya, penguji melakukan validasi manual hasil pemindaian otomatis untuk memastikan bahwa semua temuan merupakan kerentanan asli dan bukan hasil positif palsu. Untuk memastikan bahwa celah keamanan yang ditemukan benar-benar dapat dimanfaatkan oleh penyerang tanpa mengganggu sistem atau operasional layanan publik, simulasi eksploitasi kemudian dilakukan secara terbatas dan terkendali pada staging lingkungan. Pengujian dapat menghasilkan hasil yang akurat dan dapat dipercaya sebagai basis untuk rekomendasi perbaikan melalui kombinasi pemindaian otomatis dan verifikasi manual ini.

3.2.1. Metode ISSAF

Information Systems Security Assessment Framework (ISSAF) kerangka kerja yang sistematis dan terorganisir untuk melaksanakan pengujian penetrasi pada sistem informasi. Semua aspek pengujian keamanan, dari perencanaan hingga pelaporan, diatur oleh *framework* ini, yang membuatnya menjadi pilihan yang tepat. Dalam penelitian ini, ISSAF diterapkan melalui tiga fase utama yang dimaksudkan untuk menjamin bahwa pengujian dilakukan secara menyeluruh dan metodis. Setiap fase memiliki tujuan dan tugas yang harus dilakukan untuk mencapai hasil pengujian terbaik. Tabel 1 menunjukkan bahwa langkah-langkah tersebut berhubungan dan saling mendukung untuk menghasilkan evaluasi keamanan yang menyeluruh terhadap aplikasi target.

Tabel 1. Tahapan Metode ISSAF

No.	Fase	Deskripsi
1	*Planning and Preparation*	Persiapan dan pengumpulan informasi tentang aplikasi target
2	*Assessment*	Identifikasi dan verifikasi kerentanan keamanan
3	*Reporting and Cleanup*	Dokumentasi temuan dan rekomendasi perbaikan

3.2.2. OWASP Top 10:2025

Open Web Application Security Project (OWASP) Top 10:2025 berfungsi sebagai referensi utama untuk mengklasifikasikan, mengkategorikan, dan memprioritaskan kerentanan keamanan yang ditemukan pada aplikasi *website*. OWASP Top 10:2025 adalah panduan yang diakui secara internasional yang dibuat berdasarkan analisis data kerentanan terbaru dari berbagai organisasi keamanan siber. Standar ini mencakup sepuluh jenis kerentanan paling penting yang berdampak besar pada keamanan aplikasi web, sehingga penggunaan standar ini memastikan bahwa pengujian difokuskan pada area yang paling rentan dan berpotensi menimbulkan risiko tinggi, seperti ditunjukkan pada Tabel 2.

Tabel 2. OWASP Top 10:2025

No.	Kode	Identitas Temuan
1	A01:2025	*Broken Access Control*
2	A02:2025	*Security Misconfiguration*
3	A03:2025	*Software and Data Integrity Failures*
4	A04:2025	*Cryptographic Failures*
5	A05:2025	*Injection*
6	A06:2025	*Insecure Design*
7	A07:2025	*Authentication Failures*
8	A08:2025	*Software and Data Integrity Failures*
9	A09:2025	*Security Logging and Monitoring Failures*
10	A10:2025	*Mishandling of Exceptional Conditions*

3.2.3. *Tools* dan Prosedur

OWASP Zed Attack Proxy (ZAP) dipilih sebagai perangkat utama untuk penetrasi uji untuk melakukan scanning kerentanan otomatis terhadap aplikasi target. OWASP ZAP dipilih karena merupakan alat open source yang kuat dan banyak digunakan dalam industri keamanan siber untuk menemukan kerentanan pada aplikasi *website*. Untuk menjamin akurasi dan validitas setiap temuan kerentanan, prosedur pengujian menggunakan kedua metode pemindaian otomatis dan verifikasi manual secara bersamaan. Pemindaian otomatis mendeteksi potensi kerentanan pada skala besar secara cepat, sementara verifikasi manual memastikan bahwa setiap hasil pemindaian benar-benar merupakan kerentanan yang sebenarnya, bukan hasil positif palsu yang dapat menyebabkan rekomendasi perbaikan yang tidak perlu. Metode hybrid ini menghasilkan hasil yang lebih akurat, konsisten, dan dapat digunakan sebagai dasar pengambilan keputusan untuk meningkatkan postur keamanan.

3.3. Pelaporan dan Pembersihan

Pelaporan dan pembersihan adalah langkah terakhir dalam pengujian penetrasi, dan mereka sama pentingnya dengan langkah-langkah sebelumnya. Pada titik ini, jejak pengujian dari staging lingkungan dibersihkan secara menyeluruh untuk memastikan tidak ada sisa atau bukti aktivitas pengujian yang tertinggal pada sistem. Selama proses pembersihan, log aktivitas pengujian, session data yang dibuat, file temporal, dan semua artifact lainnya yang dibuat selama proses pengujian dihapus. Setelah pembersihan selesai, laporan yang menyeluruh dibuat untuk mencatat setiap kerentanan yang ditemukan, mengevaluasi dampak potensial dari

setiap kerentanan, menentukan tingkat keparahan berdasarkan standar OWASP Top 10:2025, dan memberikan saran untuk perbaikan yang jelas dan dapat diterapkan. Dokumentasi laporan ini disusun berdasarkan hasil pemindaian OWASP ZAP dan verifikasi manual untuk memastikan akurasi informasi yang disajikan kepada stakeholder instansi.

4. HASIL DAN ANALISIS

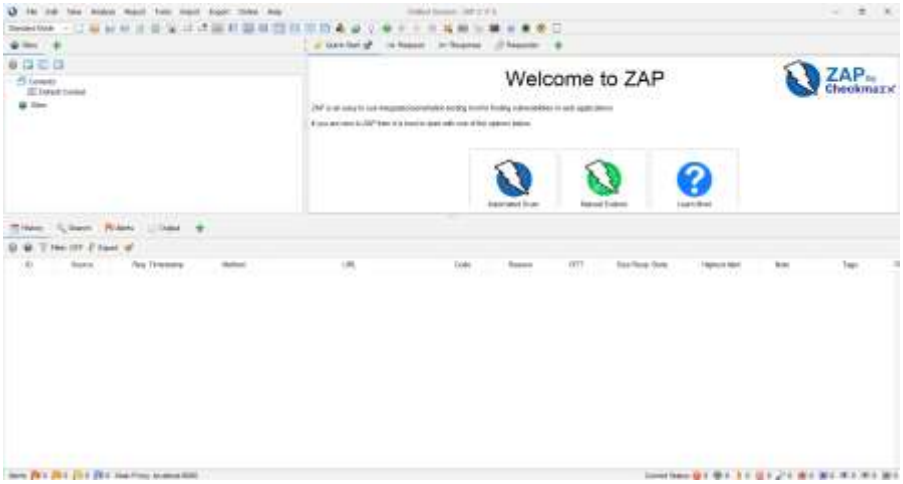
Hasil dari pengujian penetrasi yang dilakukan pada aplikasi web instansi pemerintah daerah. Pengujian dilakukan sesuai dengan metodologi ISSAF dan standar OWASP Top 10:2025. Tujuannya adalah untuk menemukan dan menganalisis kerentanan keamanan yang ada pada sistem. Penelitian mencakup temuan tentang kerentanan, tingkat keparahan, dan saran untuk perbaikan yang dapat meningkatkan keamanan postur aplikasi.

4.1. Perencanaan dan Persiapan

Untuk memastikan pengujian berjalan sesuai rencana, tahap perencanaan dan persiapan telah dilakukan secara sistematis. Pada tahap ini, ruang lingkup pengujian ditentukan dengan jelas, karakteristik aplikasi target diidentifikasi, dan alat yang diperlukan disiapkan. Proses perencanaan memastikan pengujian dilakukan dengan izin resmi dan mengikuti batasan yang telah disepakati untuk menjaga integritas sistem dan operasi layanan.

4.2. Pengujian

Kerentanan keamanan pada aplikasi web instansi pemerintah daerah ditemukan melalui proses pengujian. Pengujian menggunakan kombinasi pemindaian otomatis dengan OWASP ZAP dan verifikasi manual untuk memastikan setiap hasil akurat. Untuk memverifikasi celah keamanan yang ditemukan, simulasi eksploitasi dilakukan pada staging lingkungan. Ada sejumlah kerentanan yang ditemukan selama proses pengujian yang menyeluruh. Kerentanan kemudian dikategorikan menurut tingkat keparahan dan standar OWASP Top 10:2025.



Gambar 2. Tampilan Tools OWASP ZAP

4.2.1. Hasil Pengujian OWASP ZAP

Pemindaian menggunakan OWASP ZAP menghasilkan sejumlah temuan kerentanan dengan variasi tingkat keparahan. Temuan-temuan pada *website* ini mencakup kerentanan dengan kategori medium, low, dan informational. Setiap temuan kemudian diverifikasi secara manual untuk memastikan validitas dan menghindari temuan yang bersifat *false positive*. Total kerentanan yang ditemukan dan terverifikasi adalah 17 temuan, seperti ditampilkan pada Tabel 3.

Tabel 3. Hasil Pengujian OWASP ZAP

No.	Kode	Identitas Temuan	Kategori Temuan
1	T01	*Buffer Overflow*	*Medium*
2	T02	*CSP: Failure to Define Directive with No Fallback*	*Medium*
3	T03	*CSP: Wildcard Directive*	*Medium*
4	T04	*CSP: script-src unsafe-eval*	*Medium*
5	T05	*CSP: style-src unsafe-inline*	*Medium*

6	T06	*Missing Anti-clickjacking Header*	*Medium*
7	T07	*Sub Resource Integrity Attribute Missing*	*Medium*
8	T08	*Improper Redirect Configuration*	*Low*
9	T09	*Cookie No HttpOnly Flag*	*Low*
10	T10	*Cross-Domain JavaScript Source File Inclusion*	*Low*
11	T11	*Verbose HTTP Header Information*	*Low*
12	T12	*Server Version Information Disclosure*	*Low*
13	T13	*X-Content-Type-Options Header Missing*	*Low*
14	T14	*Modern Web Application*	*Informational*
15	T15	*Session Management Response Identified*	*Informational*
16	T16	*Client-Side Input Validation*	*Informational*
17	T17	*User Controllable HTML Element Attribute (Potential XSS)*	*Informational*

4.2.2. Hasil Pemetaan OWASP Top 10:2025

Kerentanan yang ditemukan dikelompokkan dan dipetakan sesuai dengan kategori OWASP Top 10:2025 untuk memudahkan prioritisasi dan penanganan. Mapping ini membantu mengidentifikasi area-area kritis yang perlu mendapat perhatian khusus dalam perbaikan keamanan. Distribusi kerentanan berdasarkan kategori OWASP Top 10:2025 ditampilkan pada Tabel 4.

Tabel 4. Hasil Pemetaan Berdasarkan OWASP Top 10:2025

No.	Kode OWASP Top 10:2025	Identitas Temuan	Kategori Medium	Kategori Low	Kategori Informational	Total Jumlah Temuan
1	A01:2025	*Broken Access Control*	0	1	0	1
2	A02:2025	*Security Misconfiguration*	7	2	1	10
3	A03:2025	*Software and Data Integrity Failures*	0	0	0	0
4	A04:2025	*Cryptographic Failures*	0	0	0	0
5	A05:2025	*Injection*	0	0	1	1
6	A06:2025	*Insecure Design*	0	1	0	1
7	A07:2025	*Authentication Failures*	0	0	0	0
8	A08:2025	*Software and Data Integrity Failures*	0	1	0	1
9	A09:2025	*Security Logging and Monitoring Failures*	0	0	0	0
10	A10:2025	*Mishandling of Exceptional Conditions*	1	0	0	1
11	Tidak Terpetakan	-	0	0	2	2
Total			8	5	4	17

4.2.3. Analisis Hasil Pengujian

Hasil *penetration testing* yang telah dilaksanakan berhasil mengidentifikasi 17 temuan kerentanan yang tersebar pada berbagai kategori dalam standar OWASP Top 10:2025. Distribusi temuan menunjukkan dominasi yang signifikan pada kategori A02:2025 (*Security Misconfiguration*) dengan total 10 temuan, diikuti kategori A01:2025 (*Broken Access Control*), A05:2025 (*Injection*), A06:2025 (*Insecure Design*), A08:2025 (*Software and Data Integrity Failures*), dan A10:2025 (*Mishandling of Exceptional Conditions*) masing-masing dengan 1 temuan. Selain itu, terdapat 2 temuan yang tidak dapat dipetakan ke dalam kategori OWASP Top 10:2025 karena karakteristik spesifik dari temuan tersebut.

Berdasarkan analisis tingkat keparahan, distribusi temuan kerentanan adalah 8 temuan dalam kategori *medium*, 5 temuan dalam kategori *low*, dan 4 temuan dalam kategori *informational*. Tidak ditemukan kerentanan dengan tingkat keparahan *high* atau *critical* pada hasil pengujian ini. Dominasi kerentanan pada kategori medium menunjukkan bahwa sistem memiliki celah keamanan yang memerlukan penanganan prioritas menengah dan tidak boleh diabaikan. Kerentanan pada kategori A02 (*Security Misconfiguration*) mencakup berbagai masalah teknis seperti konfigurasi header yang tidak tepat, implementasi *Content Security Policy* (CSP) yang belum optimal, dan berbagai mekanisme keamanan aplikasi *website* lainnya yang belum dikonfigurasi secara sempurna sesuai dengan *best practices* di dunia industri.

Hasil pengujian menyeluruh menunjukkan bahwa aplikasi *website* masih memerlukan peningkatan besar dalam hal keamanan, terutama dalam hal konfigurasi keamanan, yang merupakan dasar keamanan aplikasi *website*. Mengingat efek yang dapat ditimbulkan oleh kerentanan jenis ini, penanganan serangan injeksi juga sangat penting. Untuk memastikan bahwa implementasi solusi yang dilakukan efektif, terukur, dan

sesuai dengan standar keamanan industri, rekomendasi perbaikan telah disusun secara menyeluruh dengan mempertimbangkan setiap hasil.

4.3. Pelaporan dan Pembersihan

Setelah fase pengujian keamanan selesai, seluruh jejak pengujian dibersihkan secara menyeluruh dan sistematis dari staging lingkungan untuk memastikan tidak ada sisa atau bukti aktivitas pengujian yang tertinggal pada sistem. Proses ini sangat penting untuk menjaga integritas lingkungan dan mencegah risiko keamanan yang mungkin ditimbulkan oleh artifact pengujian. Pembersihan mencakup penghapusan total dari log aktivitas pengujian, sesi data yang dibuat oleh alat pengujian, file cache dan temporal, dan setiap jejak teknis lainnya yang dibuat selama proses pengujian.

Setelah pembersihan selesai, laporan hasil pengujian disusun secara menyeluruh dan menyeluruh. Ini melibatkan dokumentasi dan analisis menyeluruh dari setiap temuan kerentanan, serta tingkat keparahan atau tingkat keparahan, kategori menurut standar OWASP Top 10:2025, deskripsi teknis kerentanan, analisis dampak yang mungkin terhadap keamanan sistem, dan saran untuk perbaikan yang spesifik. Laporan ini disusun dengan jelas dan terorganisir sehingga memberikan panduan yang lengkap bagi tim keamanan informasi dan manajemen risiko instansi untuk memperbaiki dan memperbaiki setiap masalah yang ditemukan dalam penelitian ini.

5. KESIMPULAN

Penetration testing yang telah dilakukan terhadap aplikasi *website* instansi pemerintah suatu daerah dengan menggunakan metodologi Information Systems Security Assessment Framework (ISSAF) dan standar Open Web Application Security Project (OWASP) Top 10:2025 berhasil mengidentifikasi 17 temuan kerentanan yang tersebar dengan distribusi 8 temuan dalam kategori *medium*, 5 temuan dalam kategori *low*, dan 4 temuan dalam kategori *informational*. Tidak ditemukan kerentanan dengan tingkat keparahan *high* maupun *critical* pada hasil pengujian ini, yang menunjukkan bahwa sistem memiliki tingkat keamanan dasar namun masih memerlukan perbaikan signifikan pada beberapa aspek kritis.

Hasil analisis mendalam menunjukkan bahwa kerentanan terbanyak terkonsentrasi pada kategori A02:2025 (*Security Misconfiguration*) dengan total 10 temuan, yang mencakup berbagai masalah konfigurasi *header*, implementasi *Content Security Policy* yang tidak optimal, dan mekanisme keamanan aplikasi *website* lainnya yang belum dikonfigurasi secara sempurna. Selain itu, terdapat temuan pada kategori *Injection* (A05:2025) yang juga memerlukan penanganan prioritas tinggi dalam melakukan *remediation*. Penelitian ini secara jelas membuktikan bahwa penerapan kombinasi metodologi ISSAF dan standar OWASP Top 10:2025 terbukti sangat efektif dalam mengidentifikasi kerentanan keamanan pada aplikasi web secara sistematis, terstruktur, dan terukur.

DAFTAR PUSTAKA

[1] S. R. Krisma Pertiwi, R. Tumanggor, K. A. Suripto, B. Odelia, K. Gracencia, dan G. T. Telaumbanua, “Hubungan Intensitas Penggunaan Media Sosial dengan Nasionalisme pada Generasi Muda di Era Digital,” *Riwayat Educ. J. Hist. Humanit.*, vol. 8, no. 4, hlm. 7393–7403, Okt 2025, doi: 10.24815/jr.v8i4.50322.

[2] Andana Adytia Kusuma, Sadu Wasistiono, dan Andi Pitono, “PENERAPAN E-GOVERNMENT DALAM MENINGKATKAN KUALITAS PELAYANAN PUBLIK DI DINAS PENANAMAN MODAL DAN PELAYANAN TERPADU SATU PINTU KOTA BANDUNG PROVINSI JAWA BARAT,” *VISIONER J. Pemerintah. Drh. Indones.*, vol. 13, no. 2, hlm. 145–158, Agu 2021, doi: 10.54783/jv.v13i2.422.

[3] M. L. B. Hikam, F. Dewi, dan D. Praditya, “ANALISIS MANAJEMEN RISIKO INFORMASI MENGGUNAKAN ISO/IEC 27005:2018 (STUDI KASUS: PT.XYZ),” *JIPI J. Ilm. Penelit. Dan Pembelajaran Inform.*, vol. 9, no. 2, hlm. 728–734, Mei 2024, doi: 10.29100/jipi.v9i2.4709.

[4] A. Abdullah dan M. Koprawi, “Analisis Keamanan Website Pada Instansi XYZ Melalui Penetration Testing Menggunakan Framework ISSAF & OWASP,” *Digit. Transform. Technol.*, vol. 5, no. 1, hlm. 547–555, Agu 2025, doi: 10.47709/digitech.v5i1.6881.

[5] K. U. Sarker, F. Yunus, dan A. Deraman, “Penetration Taxonomy: A Systematic Review on the Penetration Process, Framework, Standards, Tools, and Scoring Methods,” *Sustainability*, vol. 15, no. 13, hlm. 10471, Jul 2023, doi: 10.3390/su151310471.

[6] V. S. Nugroho dan F. W. Christanto, “ANALISIS KEAMANAN WEBSITE DENGAN INFORMATION SYSTEM SECURITY ASSESSMENT FRAMEWORK (ISSAF) DAN OPEN WEB APPLICATION SECURITY PROJECT (OWASP),” *Netw. Eng. Res. Oper.*, vol. 8, no. 2, hlm. 145–156, Jan 2024, doi: 10.21107/nero.v8i2.19712.

[7] I. E. Cahyo, J. D. Santoso, dan H. Utama, “Analisis Hasil Uji Penetrasi Menggunakan Metode Information Systems Security Assessment Framework (ISSAF) Pada Website,” *J. MULTIDISIPLIN BHATARA*, vol. 3, no. 1, hlm. 24–31, Feb 2026, doi: 10.59095/jmb.v3i1.262.

[8] H. Hermanto dan H. Haeruddin, "Peningkatan Sistem Keamanan Website Menggunakan Metode OWASP," *J. Ilmu Komput. Dan Bisnis*, vol. 13, no. 1, hlm. 94–104, Mei 2022, doi: 10.47927/jikb.v13i1.277.

[9] E. Nurelasari dan D. Gumilang Al Farabi, "ANALISIS KEAMANAN SISTEM WEBSITE MENGGUNAKAN METODE OPEN WEB APPLICATION SECURITY PROJECT (OWASP) PADA SIMANTEP.ID," *JATI J. Mhs. Tek. Inform.*, vol. 8, no. 3, hlm. 3049–3054, Mei 2024, doi: 10.36040/jati.v8i3.9314.

[10] Nur Romadhoni Hidayat dan Muhammad Faishol Amrulloh, "Analisis Keamanan Website Universitas XYZ Menggunakan Pendekatan Penetration Testing Berdasarkan OWASP Top 10," *Indexia*, vol. 8, no. 1, hlm. 1–10, Mei 2026, doi: 10.30587/indexia.v8i1.10432.

[11] Z. Zairina, R. B. Huwae, dan A. H. Jatmika, "IMPLEMENTASI OWASP TOP 10 DALAM PENGUJIAN PENETRASI WEBSITE : MENGIDENTIFIKASI CELAH KEAMANAN DALAM SISTEM PENGELOLAAN VOTING INDONESIA," *J. Teknol. Inf. Komput. Dan Apl. JTIKA*, vol. 7, no. 1, hlm. 98–108, Mar 2025, doi: 10.29303/jtika.v7i1.456.

[12] M. I. Halil dan M. Mansur, "Analysis and Improvement of an Agribusiness Web Information System Security using Grey-Box and White-Box Testing," *SISTEMASI*, vol. 15, no. 2, hlm. 628, Feb 2026, doi: 10.32520/stmsi.v15i2.5939.