JSSTEK
JURNAL STUDI SAINS DAN TEKNIK

E-ISSN: XXXX-XXXX
https://ojs-um.com/index.php/JSSTEK

PENGUJIAN KEAMANAN WEBSITE E-GOVERNMENT MENGGUNAKAN METODE GRAY BOX PENETRATION TESTING BERBASIS OWASP TOP 10:2025 DAN ISSAF

Chelvin Bintang Samudera Haryanto[1], Ahmad Wildan Razaqi[2], Ricky Widyadhana[3], Anindo Saka Fitri[4]
Universitas Pembangunan Nasional "Veteran" Jawa Timur

Korespondensi: 23082010193@student.upnjatim.ac.id

Abstract

This research focuses on testing the security of an e-government website managed by a provincial government agency. The application serves as a service portal for the Computer Security Incident Response Team, ensuring the integrity and confidentiality of its data are vital. The purpose of this research is to identify potential security vulnerabilities and develop technical mitigation recommendations that can be utilized by the agency. Testing was conducted proactively on a staging server using a Gray Box Penetration Testing approach with official authorization. The testing methodology integrates the Information Systems Security Assessment Framework (ISSAF) as a guideline for penetration testing and the Open Web Application Security Project (OWASP) Top 10:2025 as a reference for vulnerability classification. The test results demonstrate that the application's database architecture has a very good level of resilience against SQL Injection intrusions thanks to the implementation of the Object-Relational Mapping (ORM) system. Nevertheless, the testing successfully validated a number of vulnerability findings dominated by the categories Security Misconfiguration (A02:2025 with a Low to Medium risk level.

Keywords: *Penetration Testing, OWASP Top 10:2025, ISSAF, Gray Box, e-government website.*

Abstrak

Penelitian ini berfokus pada pengujian keamanan Web E-Government yang dikelola oleh Instansi Pemerintahan Tingkat Provinsi. Aplikasi tersebut berfungsi sebagai portal layanan tim tanggap insiden keamanan siber (Computer Security Incident Response Team), sehingga keutuhan dan kerahasiaan datanya menjadi aspek yang sangat vital untuk dijaga. Tujuan dari penelitian ini adalah mengidentifikasi potensi kerentanan keamanan serta menyusun rekomendasi mitigasi teknis yang dapat dimanfaatkan oleh pihak instansi. Pengujian dilakukan secara proaktif pada lingkungan pementasan (*staging server*) melalui pendekatan *Gray Box Penetration Testing* dengan otorisasi resmi. Metodologi pengujian mengintegrasikan kerangka *Information Systems Security Assessment Framework* (ISSAF) sebagai panduan alur penetrasi dan *Open Web Application Security Project* (OWASP) Top 10:2025 sebagai acuan klasifikasi kerentanan. Hasil pengujian membuktikan bahwa arsitektur basis data aplikasi memiliki tingkat ketahanan yang sangat baik terhadap intrusi *SQL Injection* berkat implementasi sistem *Object-Relational Mapping* (ORM). Meskipun demikian, pengujian berhasil memvalidasi sejumlah temuan kerentanan yang didominasi oleh kategori *Security Misconfiguration* (A02:2025), *Software and Data Integrity Failures Low* hingga *Medium*.

Kata kunci: *Penetration Testing, OWASP Top 10:2025, ISSAF, Gray Box, Web E-Government.*

Chelvin Bintang Samudera Haryanto, Ahmad Wildan Razaqi, Ricky Widyadhana, Anindo Saka Fitri
DOI: https://doi.org/10.3342/jsstek.v3i2.522

PENDAHULUAN

Perkembangan teknologi informasi dan komunikasi yang pesat telah mendorong transformasi digital di berbagai sektor, termasuk dalam penyelenggaraan pemerintahan. Implementasi Sistem Pemerintahan Berbasis Elektronik (SPBE) menjadikan aplikasi web sebagai media utama dalam penyampaian layanan publik dan tata kelola instansi[1]. Instansi Pemerintahan Tingkat Provinsi ini memiliki tim tanggap insiden keamanan siber atau *Computer Security Incident Response Team* (CSIRT) yang berfungsi melakukan pencegahan dan penanganan insiden di lingkungan pemerintah provinsi[2]. Sebagai sarana pendukung fungsi krusial tersebut, dikembangkanlah portal Web E-Government. Mengingat aplikasi ini berkaitan langsung dengan data insiden dan pelaporan keamanan siber, maka sistem tersebut wajib dipastikan memiliki tingkat resiliensi yang tinggi melalui pengujian keamanan yang sistematis dan terstandarisasi sebelum dirilis secara publik[3].

Salah satu metode yang paling komprehensif untuk mengevaluasi ketangguhan sebuah aplikasi web adalah *Penetration Testing* (Uji Penetrasi). Pengujian ini dilakukan dengan menyimulasikan teknik dan vektor serangan dari sudut pandang peretas guna mengidentifikasi celah kelemahan sebelum dieksploitasi oleh pihak yang tidak bertanggung jawab. Pengujian ini menggunakan pendekatan *Gray Box Penetration Testing*, di mana penguji diberikan otorisasi dan informasi secara parsial guna menyimulasikan skenario ancaman baik dari luar jaringan maupun dari dalam sistem sebagai pengguna yang terautentikasi.

Agar pengujian menghasilkan analisis yang mendalam, terstruktur, dan objektif, pendekatan ini mengintegrasikan dua kerangka kerja berstandar internasional. Kerangka *Information Systems Security Assessment Framework* (ISSAF) diaplikasikan sebagai panduan operasional alur kerja pengujian, sedangkan *Open Web Application Security Project* (OWASP) Top 10:2025 digunakan sebagai landasan klasifikasi kerentanan dan penilaian risiko. Berdasarkan urgensi tersebut, penelitian ini difokuskan pada pengujian dan evaluasi keamanan aplikasi web Web E-Government yang dilaksanakan secara terkontrol pada lingkungan pementasan (*staging server*) untuk memastikan bahwa audit mencakup lapisan aplikasi web hingga ketahanan basis data.

TINJAUAN PUSTAKA

Keamanan Informasi dan *E-Government*

Keamanan informasi (*information security*) merupakan suatu upaya proteksi menyeluruh untuk melindungi aset informasi dari berbagai potensi ancaman yang dapat merugikan keberlangsungan operasional organisasi[4]. Landasan utama dari keamanan informasi berpedoman pada konsep *CIA Triad*, yaitu *Confidentiality* (Kerahasiaan), *Integrity* (Keutuhan), dan *Availability* (Ketersediaan). Dalam konteks *e-government*, pelaksanaan pelindungan informasi sejalan dengan regulasi nasional[5], seperti Peraturan Presiden Nomor 95 Tahun 2018 tentang Sistem Pemerintahan Berbasis Elektronik (SPBE). Pembentukan tim pelindungan seperti *Computer Security Incident Response Team* (CSIRT)

Chelvin Bintang Samudera Haryanto, Ahmad Wildan Razaqi, Ricky Widyadhana, Anindo Saka Fitri
DOI: https://doi.org/10.3342/jsstek.v3i2.522

merupakan langkah konkret berdasarkan amanat Peraturan Badan Siber dan Sandi Negara (BSSN) Nomor 10 Tahun 2020 tentang Tim Tanggap Insiden Siber serta Peraturan BSSN Nomor 1 Tahun 2024 tentang Pengelolaan Insiden Siber untuk menanggulangi insiden keamanan siber dan memastikan hardening infrastruktur teknologi informasi pemerintahan tetap terjaga.

Penetration Testing

Penetration testing merupakan metode evaluasi keamanan yang dilakukan secara aktif dengan mensimulasikan taktik serangan siber nyata dari sudut pandang peretas (*attacker*) secara sah dan terencana. Pengujian ini memiliki tujuan utama untuk mengidentifikasi kelemahan teknis sebelum celah tersebut disalahgunakan oleh pihak luar. Dalam pelaksanaannya, salah satu pendekatan yang digunakan adalah *Gray Box Testing*, di mana penguji dibekali informasi parsial atau akses terbatas yang merepresentasikan pengguna biasa atau pengelola internal sistem[6]. Pendekatan ini sangat efisien untuk menguji ketahanan fungsionalitas internal *website*, menguji perimeter otorisasi, serta melakukan validasi logika dari dalam lingkungan *staging*.

Kerangka Kerja ISSAF dan OWASP Top 10:2025

Pelaksanaan pengujian keamanan yang komprehensif membutuhkan pedoman standar yang terstruktur guna menjamin konsistensi hasil pengujian. Metodologi pengujian ini mengadopsi kombinasi antara kerangka *Information Systems Security Assessment Framework* (ISSAF) sebagai panduan alur kerja dan metode *Open Web Application Security Project* (OWASP). Tahapan pengujian disinergikan ke dalam 5 (lima) fase utama, yaitu *Information Gathering & Planning*, *Network Mapping*, *Assessment & Vulnerability Identification*, *Exploitation & Penetration Testing*, dan *Reporting & Clean Up*. Sebagai landasan klasifikasi kerentanan dan penilaian tingkat risiko (*severity level*), standar OWASP Top 10 versi 2025 digunakan sebagai parameter ukur utama. Kategori risiko di dalamnya mencakup kelemahan seperti *Broken Access Control*, *Security Misconfiguration*, *Software Supply Chain Failures*, *Injection*, hingga *Mishandling of Exceptions[7]*.

Perangkat Lunak Pengujian

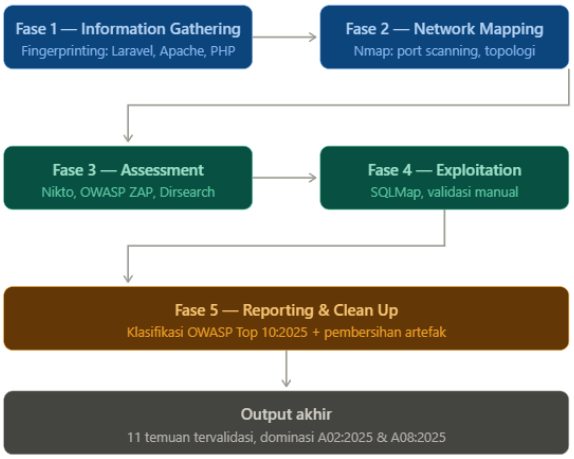
Pelaksanaan operasional *penetration testing* ini didukung oleh pemanfaatan berbagai perangkat lunak standar industri keamanan siber, yang dioperasikan di atas lingkungan sistem operasi Kali Linux. Alat yang digunakan meliputi *Nmap* untuk eksplorasi jaringan dan *port scanning*, *OWASP ZAP* (*Zed Attack Proxy*) untuk memindai potensi kerentanan aplikasi secara dinamis, serta *Dirsearch* untuk melakukan enumerasi jalur direktori[8]. Selain itu, alat *Nikto* digunakan untuk mendeteksi opsi server yang salah konfigurasi, *SQLMap* difokuskan untuk menguji ketahanan basis data dari kelemahan *SQL Injection*, dan utilitas baris perintah *curl* dimanfaatkan untuk memverifikasi perilaku respons HTTP secara manual.

Chelvin Bintang Samudera Haryanto, Ahmad Wildan Razaqi, Ricky Widyadhana, Anindo Saka Fitri
DOI: https://doi.org/10.3342/jsstek.v3i2.522

METODE

Penelitian ini menggunakan pendekatan Gray Box Penetration Testing, di mana pengujian dilakukan dengan bekal otorisasi parsial dan kredensial akses sebagai pengguna terautentikasi (Admin dan Superadmin). Objek pengujian difokuskan pada lingkungan pementasan (staging server) aplikasi web Web E-Government yang diakses melalui alamat IP internal http://[target]:[port]/ guna menjaga kerahasiaan infrastruktur instansi.

Alur pelaksanaan pengujian mengadopsi integrasi dua kerangka kerja, yaitu metodologi Information Systems Security Assessment Framework (ISSAF) untuk tahapan operasional dan standar Open Web Application Security Project (OWASP) Top 10:2025 untuk panduan klasifikasi kerentanan. Tahapan pengujian dibagi menjadi lima fase, yaitu: 1) Information Gathering & Planning, 2) Network Mapping, 3) Assessment & Vulnerability Identification, 4) Exploitation & Penetration Testing, dan 5) Reporting & Clean Up, sebagaimana diilustrasikan pada Gambar 1. Perangkat lunak pendukung yang dioperasikan pada sistem Kali Linux meliputi Nmap, OWASP ZAP, Nikto, Dirsearch, SQLMap, dan utilitas rekayasa manual curl.



Gambar 1. Alur Metodologi Pengujian

HASIL DAN PEMBAHASAN

Pelaksanaan evaluasi keamanan pada website tingkat provinsi ini dilakukan secara terkontrol pada lingkungan pementasan (*staging server*) guna memastikan bahwa seluruh simulasi serangan tidak mengganggu ketersediaan layanan pada *server* produksi (*production server*). Pengujian dieksekusi menggunakan pendekatan *Gray Box Penetration Testing*, di mana informasi awal jaringan dan otorisasi akses internal (kredensial uji) diberikan secara resmi oleh mentor dan pembimbing dari pihak instansi. Pengujian

Chelvin Bintang Samudera Haryanto, Ahmad Wildan Razaqi, Ricky Widyadhana, Anindo Saka Fitri
DOI: https://doi.org/10.3342/jsstek.v3i2.522

dilaksanakan dengan mengintegrasikan metodologi alur kerja ISSAF dan standar parameter OWASP Top 10:2025 yang dibagi ke dalam lima fase sistematis.

1. Information Gathering & Planning

Pada fase awal ini, pengumpulan informasi difokuskan pada pemetaan arsitektur perangkat lunak (technology fingerprinting) dan perimeter autentikasi target pada lingkungan pementasan dengan alamat server [target]. Menggunakan otorisasi akun internal tingkat Admin dan Superadmin, analisis dilakukan terhadap *HTTP Response Headers* dan mekanisme manajemen sesi server. Hasil ekstraksi data memvalidasi bahwa *website* target dibangun menggunakan kerangka kerja (*framework*) berbasis PHP, yang dibuktikan melalui keberadaan *cookie* sesi dan token perlindungan *Cross-Site Request Forgery* (anti-CSRF) bawaan sistem. Infrastruktur backend tersebut beroperasi menggunakan server web Apache dan mengeksekusi logika bahasa pemrograman PHP, di mana rincian versi spesifik perangkat lunak sengaja disamarkan untuk memitigasi risiko keamanan pengintaian.

2. Network Mapping

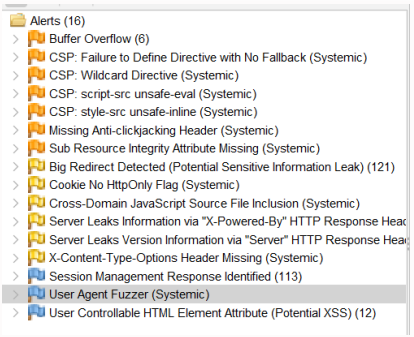
Fase pemetaan jaringan bertujuan untuk mengidentifikasi topologi dan layanan lalu lintas data yang berjalan pada infrastruktur target. Pemindaian komprehensif menggunakan utilitas Nmap menunjukkan bahwa server pementasan beroperasi secara terisolasi di dalam jaringan intranet lokal instansi. Hasil analisis porta (*port state*) mengonfirmasi bahwa lalu lintas HTTP untuk *website* target dilayani secara spesifik melalui porta [*port*] yang berstatus terbuka (open state), memberikan titik masuk (*entry point*) yang presisi untuk tahapan pengujian selanjutnya.

3. Assessment & Vulnerability Identification

Tahapan ini merupakan inti dari pencarian celah keamanan secara semi-otomatis sebelum tindakan eksploitasi aktif dilakukan. Pengujian lapis pertama menggunakan perangkat Nikto untuk memindai kelemahan konfigurasi server web menghasilkan lebih dari 60 log peringatan awal berskala tinggi (indikasi Shellshock). Bersamaan dengan itu, pemindaian dinamis berbasis arsitektur (dynamic scanning) menggunakan OWASP ZAP mendeteksi 16 indikasi kerentanan pada logika dan struktur kode aplikasi yang ditampilkan di Gambar 2. Zap Report. Selain itu, utilitas Dirsearch juga dikerahkan secara paralel untuk melakukan penelusuran direktori (path enumeration) guna mengidentifikasi berkas atau panel tersembunyi yang berisiko membocorkan data sensitif.

Chelvin Bintang Samudera Haryanto, Ahmad Wildan Razaqi, Ricky Widyadhana, Anindo Saka Fitri

DOI: https://doi.org/10.3342/jsstek.v3i2.522

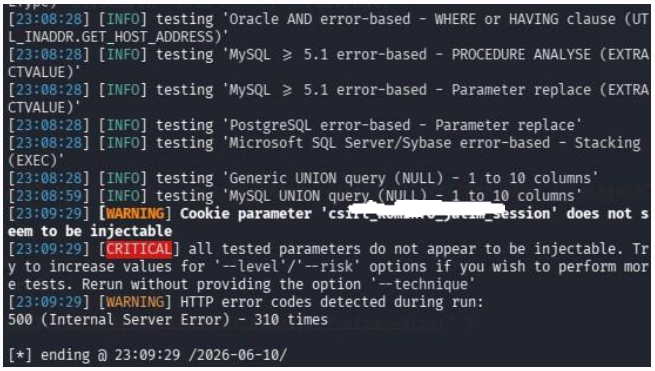


Gambar 2. Zap Report

4. Exploitation & Penetration Testing

Pada fase ini, seluruh data indikasi dari fase sebelumnya divalidasi secara analitis dan manual untuk mengeleminasi peringatan palsu (false positive) dan membuktikan dampak nyatanya.

Pengujian Penetrasi Berbasis ISSAF: Fokus pada evaluasi infrastruktur server dan basis data. Pengujian silang memvalidasi bahwa peringatan *Shellshock* dari *Nikto* merupakan *False Positive* karena sistem operasi server telah mendapatkan pembaruan keamanan (*patch*) terbaru. Pengujian agresi terhadap basis data menggunakan instrumen *SQLMap* mengembalikan status *True Negative* (*Not Injectable*) yang ditunjukkan pada Gambar 3. Hasil SQLMap. Arsitektur basis data terbukti sangat tangguh karena implementasi *Object-Relational Mapping* (ORM) pada Laravel berhasil menyanitasi kueri anomali. Selain itu, sistem manajemen kontrol akses terbukti bekerja optimal (*Directory Listing Disabled*) karena upaya *brute-force* pada struktur direktori menggunakan *Dirsearch* secara tegas ditolak dengan kode respons HTTP 403 *Forbidden* atau 404 *Not Found*.



Gambar 3. Hasil SQLMap

Chelvin Bintang Samudera Haryanto, Ahmad Wildan Razaqi, Ricky Widyadhana, Anindo Saka Fitri
DOI: https://doi.org/10.3342/jsstek.v3i2.522

Validasi Temuan OWASP Top 10:2025: Analisis ketat terhadap hasil pengerjaan proksi OWASP ZAP berhasil memvalidasi 11 temuan kerentanan riil yang direkapitulasi pada Tabel 1. Adapun 5 indikasi lainnya dari 16 temuan awal tereliminasi sebagai *false positive* setelah dilakukan verifikasi manual untuk membuktikan dampak nyatanya.

Tabel 1. Rekapitulasi Owasp

No	Nama Kerentanan Keamanan Web	Tingkat Risiko	Kategori Kode OWASP 2025
1	CSP: *Failure to Define Directive with No Fallback*	Medium	A02:2025 *Security Misconfiguration*
2	CSP: *Wildcard Directive Detected*	Medium	A02:2025 *Security Misconfiguration*
3	CSP: *script-src unsafe-eval Permitted*	Medium	A02:2025 *Security Misconfiguration*
4	CSP: *style-src unsafe-inline Permitted*	Medium	A02:2025 *Security Misconfiguration*
5	*Missing Anti-clickjacking Header* (*X-Frame-Options*)	Medium	A02:2025 *Security Misconfiguration*
6	*Sub Resource Integrity* (SRI) *Attribute Missing*	Medium	A08:2025 *Software & Data Integrity Failures*
7	*Session Cookie No HttpOnly Flag*	Low	A02:2025 *Security Misconfiguration*
8	*Cross-Domain JavaScript Source File Inclusion*	Low	A08:2025 *Software & Data Integrity Failures*
9	*Server Leaks Information via HTTP Response Header*	Low	A02:2025 *Security Misconfiguration*

Chelvin Bintang Samudera Haryanto, Ahmad Wildan Razaqi, Ricky Widyadhana, Anindo Saka Fitri
DOI: https://doi.org/10.3342/jsstek.v3i2.522

10	*Server Leaks Version Information via HTTP Response Header*	Low	A02:2025 *Security Misconfiguration*
11	*X-Content-Type-Options Header Missing from Response*	Low	A02:2025 *Security Misconfiguration*

Berdasarkan Tabel 1, perimeter keamanan didominasi oleh Security Misconfiguration (A02:2025). Kegagalan sistem dalam menerapkan pelindungan Anti-clickjacking (X-Frame-Options) berisiko membuka celah UI Redressing, di mana aplikasi dapat dibingkai oleh pihak ketiga untuk mencuri kredensial pengguna. Konfigurasi Content Security Policy (CSP) yang terlalu permisif (unsafe-inline dan unsafe-eval) juga berpotensi memfasilitasi injeksi manipulasi antarmuka. Selain itu, ketiadaan atribut Subresource Integrity (SRI) pada pemuatan aset eksternal (A08:2025) sangat rentan memicu insiden Supply Chain Attack, sementara kebocoran identitas arsitektur perangkat lunak melalui header HTTP berisiko memberikan keuntungan pengintaian bagi peretas.

5. Reporting & Clean Up

Fase pelaporan (Reporting) disusun dengan mengklasifikasikan setiap kerentanan yang telah berhasil divalidasi berdasarkan standar parameter OWASP Top 10:2025. Sementara itu, sebagai tahapan penutup yang diwajibkan dalam metodologi ISSAF (Clean Up and Destroy Artifact), prosedur pembersihan jejak eksploitasi mutlak dilakukan. Seluruh sisa pengujian yang mencakup payload injeksi, akun uji sampah, maupun data buatan (dummy data) dibersihkan secara menyeluruh dari sistem target. Langkah mitigasi artefak ini merupakan prosedur krusial untuk memastikan bahwa seluruh rangkaian evaluasi keamanan tidak meninggalkan jejak yang dapat mengganggu stabilitas maupun layanan operasional server instansi pemerintahan tersebut.

Rekomendasi dan Mitigasi Teknis

Berdasarkan temuan yang divalidasi, upaya pengerasan server (server hardening) mutlak diperlukan. Mitigasi teknis yang direkomendasikan mencakup penerapan parameter *Subresource Integrity* (SRI) berserta atribut crossorigin pada aset pihak ketiga untuk mencegah Supply Chain Attack. Selain itu, perbaikan pada arsitektur *Content Security Policy* harus segera diterapkan dengan menghapus elemen *wildcard* dan mendefinisikan direktif secara eksplisit. Terakhir, pengungkapan versi dan teknologi pada konfigurasi inti server web perlu dinonaktifkan guna mencegah kebocoran jejak teknologi kepada peretas.

Chelvin Bintang Samudera Haryanto, Ahmad Wildan Razaqi, Ricky Widyadhana, Anindo Saka Fitri
DOI: https://doi.org/10.3342/jsstek.v3i2.522

PENUTUP

Kesimpulan

Pengujian keamanan pada Web E-Government telah berhasil dilaksanakan menggunakan metode *Gray Box Penetration Testing* yang mengacu pada kerangka kerja ISSAF dan standar OWASP Top 10:2025. Hasil pengujian menyimpulkan bahwa arsitektur basis data aplikasi memiliki tingkat ketahanan yang sangat baik dan terbukti aman dari ancaman eksploitasi *SQL Injection*. Meskipun demikian, pengujian berhasil mengidentifikasi sejumlah temuan kerentanan dengan tingkat risiko *Low* hingga *Medium* yang didominasi oleh kategori *Security Misconfiguration* (A02:2025) dan *Software and Data Integrity Failures* (A08:2025). Kerentanan tersebut berakar dari kelemahan konfigurasi server, seperti ketidaklengkapan aturan *Content Security Policy* (CSP), absennya beberapa atribut *HTTP Security Headers*, serta ketiadaan validasi integritas (*Subresource Integrity*) pada pemuatan aset pihak ketiga.

Saran dan Ucapan Terimakasih

Bagi pihak pengelola *website*, disarankan untuk segera menindaklanjuti temuan pada kategori *Security Misconfiguration* dengan melakukan pengerasan server (*server hardening*), khususnya menyempurnakan konfigurasi *Content Security Policy* dan melengkapi *header* keamanan. Selain itu, disarankan untuk melakukan pengujian keamanan secara berkala agar kerentanan baru dapat dideteksi sedini mungkin. Penulis mengucapkan terima kasih yang sebesar-besarnya kepada pengelola layanan E-Government dan tim tanggap insiden siber pada instansi pemerintahan tingkat provinsi terkait, serta segenap civitas akademika Fakultas Ilmu Komputer Universitas Pembangunan Nasional “Veteran” Jawa Timur atas bimbingan, fasilitas, dan dukungan yang telah diberikan selama pelaksanaan evaluasi dan penelitian ini.

DAFTAR PUSTAKA

[1] D. Andriani, A. Haris, and A. History, “Strategi Keamanan Transaksi Elektronik dalam Pelayanan Publik Berbasis E-Government Electronic Transaction Security Strategies in E-Government-Based Public Services ARTICLE INFO ABSTRACT,” vol. 1, no. 2, pp. 3109–3973, 2025, doi: 10.69616/pb.v1i2.563.

[2] Mochamad Azhar, “BSSN luncurkan tim tanggap insiden siber (CSIRT) pemerintah daerah,” GOVINSIDER. Accessed: Jun. 23, 2026. [Online]. Available: https://govinsider.asia/indo-en/article/bssn-luncurkan-tim-tanggap-insiden-siber-csirt-pemerintah-daerah

[3] A. B. Setiawan, “Kajian Kesiapan Keamanan Informasi Instansi Pemerintah Dalam Penerapan E-Government STUDY OF GOVERNMENT INFORMATION SECURITY READINESS IN IMPLEMENTING OF E-GOVERNMENT.”

[4] D. Budiyanto and M. Mabruri, “PENTINGNYA KEAMANAN SIBER DALAM ERA DIGITAL: TINJAUAN GLOBAL DAN KONDISI DI INDONESIA,” *Prosiding Seminar Nasional Sains dan Teknologi Seri III Fakultas Sains dan Teknologi*, vol. 2, no. 1, 2025.

[5] Tri Ginanjar Laksana, "Peran Pemerintah Dalam Membangun Kebijakan Keamanan Siber Untuk Meningkatkan Kepercayaan Pengguna E-Commerce Di Indonesia," 2025.

[6] N. Pirsa and Sumijan, "Meningkatkan Keamanan Sistem Informasi Puskesmas Terpadu dengan Metode Gray-Box Penetration Test Menggunakan Computer Assisted Audit Techniques," *Jurnal Informasi dan Teknologi*, Sep. 2020, doi: 10.37034/jidt.v2i4.79.

[7] A. Kennedy, W. H. Surya, and F. X. Wartoyo, "Tantangan dan Solusi Penerapan E-Government di Indonesia," *JURNAL TERAPAN PEMERINTAHAN MINANGKABAU*, vol. 4, no. 2, pp. 134–147, Dec. 2024, doi: 10.33701/jtpm.v4i2.4459.

[8] D. Lee, "Analisis Kerentanan Aplikasi Akademik Berbasis Website XYZ Menggunakan OWASP," vol. 11, no. 2, 2023.