

BIBLIOGRAPHY

- [1] D. Rohmaniah, W. Miftahul Ashari, and A. Dwi Putra, “Enhancing Website Security Using Vulnerability Assessment and Penetration Testing (VAPT) Based on OWASP Top Ten,” 2025. [Online]. Available: <http://jurnal.polibatam.ac.id/index.php/JAIC>
- [2] S. Mushtaq and M. Shah, “Mitigating Cybercrimes in E-Government Services: A Systematic Review and Bibliometric Analysis,” *Digital*, vol. 5, no. 1, p. 3, Jan. 2025, doi: 10.3390/digital5010003.
- [3] A. Budiman, S. Ahdan, and M. Aziz, “Analisis Celah Keamanan Aplikasi Web E-Learning Universitas ABC dengan Vulnerability Assesment,” *Jurnal Komputasi*, vol. 9, no. 2, Oct. 2021, doi: 10.23960/komputasi.v9i2.2800.
- [4] Verizon Business, “2024 Data Breach Investigations Report,” 2024. Accessed: Dec. 01, 2025. [Online]. Available: <https://www.verizon.com/business/resources/reports/dbir/>
- [5] BSSN, “Lanskap Keamanan Siber Indonesia,” 2023. Accessed: Dec. 03, 2025. [Online]. Available: <https://www.bssn.go.id/laporan-kinerja-badan-siber-dan-sandi-negara-tahun-2023/>
- [6] Arizal, M. Hilal, and D. F. Priambodo, “Security Analysis of Indonesian Region Government Web Applications Based on NIST SP 800-115 and WSTG v4.2,” *Journal of Information Systems and Informatics*, vol. 8, no. 2, pp. 1776–1799, doi: 10.63158/journalisi.v8i2.1558.
- [7] Jatim Newsroom, “Kadiskominfo Jatim Buka Rapat Evaluasi Serangan Siber di Lingkungan Pemprov Jawa Timur,” Kominfo Jatim. Accessed: Dec. 04, 2025. [Online]. Available: <https://kominfo.jatimprov.go.id/berita/kadiskominfo-jatim-buka-rapat-evaluasi-serangan-siber-di-lingkungan-pemprov-jawa-timur>
- [8] Dinas Komunikasi dan Informatika Provinsi Jawa Timur, “Profil Diskominfo Provinsi Jawa Timur.” Accessed: Dec. 01, 2025. [Online]. Available: <https://kominfo.jatimprov.go.id/profil>
- [9] P. P. Indonesia, “Undang-undang (UU) Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi,” 2022
- [10] P. P. Indonesia, “Peraturan Presiden (Perpres) Nomor 95 Tahun 2018 tentang Sistem Pemerintahan Berbasis Elektronik,” 2025

- [11] J. Softić and Z. Vejzović, “Impact of Vulnerability Assessment and Penetration Testing (VAPT) on Operating System Security,” in *2023 22nd International Symposium INFOTEH-JAHORINA (INFOTEH)*, IEEE, Mar. 2023, pp. 1–6. doi: 10.1109/INFOTEH57020.2023.10094095.
- [12] A. Maliq Ibrahim, T. Defisa, H. Bayu Seta, and I. P. Wayan Widi, “Analisis Keamanan Sistem pada Website Perusahaan CV. Kazar Teknologi Indonesia dengan Metode Vulnerability Assessment and Penetration Testing (VAPT),” 2022.
- [13] B. Al-Sada, A. Sadighian, and G. Oligeri, “Analysis and Characterization of Cyber Threats Leveraging the MITRE ATT&CK Database,” *IEEE Access*, vol. 12, pp. 1217–1234, 2024, doi: 10.1109/ACCESS.2023.3344680.
- [14] V. Wahyudi, M. R. Arief, B. Santoso, and R. W. Nugroho, “Evaluasi Dasar Penetration Testing Menggunakan Framework MITRE ATT&CK,” *E-Link: Jurnal Teknik Elektro dan Informatika*, vol. 20, no. 1, p. 29, May 2025, doi: 10.30587/e-link.v20i1.9399.
- [15] A. B. Ajmal, S. Khan, M. Alam, A. Mehbodniya, J. Webber, and A. Waheed, “Toward Effective Evaluation of Cyber Defense: Threat Based Adversary Emulation Approach,” *IEEE Access*, vol. 11, pp. 70443–70458, 2023, doi: 10.1109/ACCESS.2023.3272629.
- [16] FIRST, “Common Vulnerability Scoring System v3.1: Specification Document,” Forum of Incident Response and Security Teams (FIRST). Accessed: Nov. 30, 2025. [Online]. Available: <https://www.first.org/cvss/v3-1/specification-document>
- [17] F. Gisma Putra and B. Soewito, “Measurement of Security System Performance on Websites of Personnel Information Systems in Government Using Common Vulnerability Scoring System,” *Jurnal Pendidikan Tambusai*, vol. 6, 2022, doi: <https://doi.org/10.31004/jptam.v6i1.3336>.
- [18] U. Ravindran and R. V. Potukuchi, “A Review on Web Application Vulnerability Assessment and Penetration Testing,” *Review of Computer Engineering Studies*, vol. 9, no. 1, pp. 1–22, Mar. 2022, doi: 10.18280/rces.090101.

- [19] Kominfo Jatim, “Struktur Organisasi dan Wewenang DISKOMINFO Jawa Timur,” Kominfo Jatim. Accessed: Nov. 30, 2025. [Online]. Available: <https://kominfo.jatimprov.go.id/halaman/struktur-organisasi>
- [20] P. Poduk Hukum, “Peraturan Gubernur Jawa Timur Nomor 55 Tahun 2021 Tentang Pedoman Kerja Dan Pelaksanaan Tugas Pemerintah Provinsi Jawa Timur Tahun 2022,” 2021
- [21] Kementrian PANRB, “Laporan Hasil Evaluasi SPBE Tahun 2023,” 2023.
- [22] Kominfo Jatim, “Lkkip Diskominfo Jatim 2024,” 2024.
- [23] A. Adrian Audie Setiawan, H. Farisi, and A. Suharsono, “Analisis Keamanan Aplikasi Web silapetro.ub.ac.id Menggunakan Metode VAPT dan WSTG 4.2,” *Jurnal Pengembangan Teknologi Informasi dan Ilmu Komputer*, vol. 9, no. 6, pp. 2548–964, 2025, [Online]. Available: <http://j-ptiik.ub.ac.id>
- [24] M. B. Imtias, K. Umam, H. Mustofa, and M. H. Subowo, “Comparative Analysis of Penetration Testing Frameworks: OWASP, PTES, and NIST SP 800-115 for Detecting Web Application Vulnerabilities,” *Journal of Applied Informatics and Computing*, vol. 9, no. 6, pp. 3689–3696, Dec. 2025, doi: 10.30871/jaic.v9i6.9846.
- [25] C. Darmawan, J. P. P. Naibaho, and A. De Kweldju, “Penerapan Metode Vulnerability Assessment untuk Identifikasi Keamanan Website berdasarkan OWASP ID Tahun 2021,” *Edumatic: Jurnal Pendidikan Informatika*, vol. 8, no. 1, pp. 272–281, Jun. 2024, doi: 10.29408/edumatic.v8i1.25834.
- [26] M. Pandudinata and F. Ridho, “Analisis Keamanan Aplikasi Berbasis Web di Lingkungan BPS RI,” *Seminar Nasional Official Statistics*, vol. 2024, no. 1, pp. 549–558, Nov. 2024, doi: 10.34123/semnasoffstat.v2024i1.2109.
- [27] MITRE Corporation, “Enterprise Mitigations,” MITRE ATT&CK®. Accessed: Nov. 01, 2025. [Online]. Available: <https://attack.mitre.org/mitigations/enterprise/>
- [28] A. Hermawan, T. Hartati, and Y. A. Wijaya, “Analisa Keamanan Data Melalui Website Zahra Software Menggunakan Metode Keamanan Informasi CIA Triad,” *Jurnal Informatika: Jurnal Pengembangan IT*, vol. 7, no. 3, pp. 125–130, Sep. 2022, doi: 10.30591/jpit.v7i3.3428.
- [29] A. H. H. Harahap, C. D. Andani, A. Christie, D. Nurhaliza, and A. Fauzi, “Pentingnya Peranan CIA Triad Dalam Keamanan Informasi dan Data Untuk

- Pemangku Kepentingan atau Stakholder,” *Jurnal Manajemen dan Pemasaran Digital*, vol. 1, no. 2, pp. 73–83, Apr. 2023, doi: 10.38035/jmpd.v1i2.34.
- [30] Y. Raharja, “Implementasi Metode Osint untuk Mengidentifikasi Serangan Judi Online pada Website,” *Jurnal Informatika Polinema*, 2024, Accessed: Mar. 01, 2026. [Online]. Available: <https://api.semanticscholar.org/CorpusID:270188689>
- [31] OWASP Foundation, “OWASP Top 10_2021,” OWASP Foundation. Accessed: Nov. 30, 2025. [Online]. Available: <https://owasp.org/Top10/2021/>
- [32] OWASP Foundation, “OWASP Cheat Sheet Series,” OWASP. Accessed: Dec. 01, 2025. [Online]. Available: <https://cheatsheetseries.owasp.org/>
- [33] MITRE, “2024 CWE Top 25 Most Dangerous Software Weaknesses,” Common Weakness Enumeration. Accessed: Dec. 01, 2025. [Online]. Available: https://cwe.mitre.org/top25/archive/2024/2024_cwe_top25.html.
- [34] V. Vasilyev, A. Kirillova, A. Vulfin, and A. Nikonov, “Cybersecurity Risk Assessment Based on Cognitive Attack Vector Modeling with CVSS Score,” in *2021 International Conference on Information Technology and Nanotechnology (ITNT)*, 2021, pp. 1–6. doi: 10.1109/ITNT52450.2021.9649191.
- [35] K. Bennouk, N. Ait Aali, Y. El Bouzekri El Idrissi, B. Sebai, A. Z. Faroukhi, and D. Mahouachi, “A Comprehensive Review and Assessment of Cybersecurity Vulnerability Detection Methodologies,” *Journal of Cybersecurity and Privacy*, vol. 4, no. 4, pp. 853–908, Oct. 2024, doi: 10.3390/jcp4040040.
- [36] R. marta Dinata, M. Alzril, M. I. Yamin, H. Effendi, and M. Febriansyah, “Analisis Keamanan Situs Web Rumah Sakit Menggunakan Metode Penetration Testing OWASP,” *SAINSTECH: JURNAL PENELITIAN DAN PENGKAJIAN SAINS DAN TEKNOLOGI*, vol. 35, no. 2, pp. 99–100, Jun. 2025, doi: 10.37277/stch.v35i2.2383.
- [37] P. Mell *et al.*, “Measuring the Common Vulnerability Scoring System base score equation,” Nov. 2022. doi: 10.6028/NIST.IR.8409.
- [38] S. Gupta, M. Rohini, M. Manasa, S. Teja, and R. Sahana Lokesh, “Enhancing Web Application Security Using Penetration Testing and Vulnerability Scanning,” in *2025 International Conference on Knowledge Engineering and*

- Communication Systems (ICKECS)*, IEEE, Apr. 2025, pp. 1–5. doi: 10.1109/ICKECS65700.2025.11036050.
- [39] S. P. Maniraj, C. S. Ranganathan, and S. Sekar, “Securing Web Applications with OWASP ZAP For Comprehensive Security Testing,” *INTERNATIONAL JOURNAL OF ADVANCES IN SIGNAL AND IMAGE SCIENCES*, vol. 10, no. 2, pp. 12–23, Dec. 2024, doi: 10.29284/IJASIS.10.2.2024.12-23.
- [40] M. G. Abraham Danialdo, F. Andri Bakhtiar, and M. Data, “Penguujian Efektivitas OWASP ZAP dalam Menemukan Kerentanan dari Metasploitable,” *Jurnal Pengembangan Teknologi Informasi dan Ilmu Komputer*, vol. 7, no. 7, pp. 3431–3433, 2023, [Online]. Available: <https://j-ptiik.ub.ac.id/index.php/j-ptiik/article/view/13131>
- [41] S. Alazmi and D. C. De Leon, “A Systematic Literature Review on the Characteristics and Effectiveness of Web Application Vulnerability Scanners,” *IEEE Access*, vol. 10, pp. 33200–33219, 2022, doi: 10.1109/ACCESS.2022.3161522.
- [42] M. Baklizi, I. Atoum, N. Abdullah, O. A. Al-Wesabi, A. A. Otoom, and M. A.-S. Hasan, “A Technical Review of SQL Injection Tools and Methods: A Case Study of SQLMap,” *International Journal of Intelligent Systems and Applications in Engineering*, vol. 10, no. 3, pp. 75–85, Oct. 2022, [Online]. Available: <https://ijisae.org/index.php/IJISAE/article/view/2141>
- [43] Y. Muhyidin, M. H. Totohendarto, E. Undamayanti, and S. choerunnisa, “Perbandingan Tingkat Keamanan Website Menggunakan Nmap Dan Nikto Dengan Metode Ethical Hacking,” *Jurnal Teknologika*, vol. 12, no. 1, pp. 80–89, May 2022, doi: 10.51132/teknologika.v12i1.143.
- [44] Vanisa Dwi Agustina, Tamsir Ariyadi, Tari Syah Putra, and Ahmad Lega, “Teknik Penguujian Penetrasi HTTP Menggunakan Tools Burp Suite PADA KALI LINUX,” *STORAGE: Jurnal Ilmiah Teknik dan Ilmu Komputer*, vol. 4, no. 1, pp. 16–21, Feb. 2025, doi: 10.55123/storage.v4i1.4770.
- [45] IANA, “WHOIS Protocol Specification,” Internet Assigned Numbers .
- [46] Microsoft, “Nslookup,” Microsoft Learn. Accessed: Dec. 01, 2025. [Online]. Available: <https://learn.microsoft.com/en-us/windows-server/administration/windows-commands/nslookup>

- [47] F. Putra Utama and R. M. Hilmi Nurhadi, “Uncovering the Risk of Academic Information System Vulnerability through PTES and OWASP Method,” *CommIT (Communication and Information Technology) Journal*, vol. 18, no. 1, pp. 39–51, Apr. 2024, doi: 10.21512/commit.v18i1.9384.
- [48] D. Stenberg, “curl - Transfer a UR,” The cURL Project. Accessed: Dec. 01, 2025. [Online]. Available: <https://curl.se/docs/manpage.html>
- [49] PortSwigger, “Out-of-Band Application Security Testing (OAST).” Accessed: Dec. 01, 2025. [Online]. Available: <https://portswigger.net/burp/application-security-testing/oast>
- [50] K. Abdulghaffar, N. Elmrabbit, and M. Yousefi, “Enhancing Web Application Security through Automated Penetration Testing with Multiple Vulnerability Scanners,” *Computers*, vol. 12, no. 11, p. 235, Nov. 2023, doi: 10.3390/computers12110235.