

BIBLIOGRAPHY

- [1] K. C. Laudon and C. G. Traver, *E-Commerce 2021: Business, Technology, and Society*, 16th ed. New York, NY, USA: Pearson, 2021.
- [2] M. Rahman and D. Prasetyo, "Web security awareness and prevention," *J. Inf. Syst. Secur.*, vol. 10, no. 2, pp. 45–52, 2021.
- [3] International Telecommunication Union (ITU), *Global Cybersecurity Index 2020*. Geneva, Switzerland: ITU, 2021.
- [4] Badan Siber dan Sandi Negara (BSSN), *Laporan Tahunan Keamanan Siber Indonesia 2023*. Jakarta, Indonesia: BSSN, 2023.
- [5] R. Putra and A. Nugroho, "Analisis risiko keamanan website pemerintah daerah," *J. Teknol. Inf. Ilmu Komput.*, vol. 7, no. 3, pp. 211–220, 2020.
- [6] OWASP Foundation, *OWASP Top Ten Web Application Security Risks – 2021*. OWASP, 2021.
- [7] OWASP Foundation, *OWASP Application Security Verification Standard 4.0.3*. OWASP, 2021.
- [8] OWASP Foundation, *OWASP Testing Guide v4*, 2021.
- [9] K. Scarfone, M. Souppaya, A. Cody, and A. Orebaugh, *Technical Guide to Information Security Testing and Assessment*, NIST Special Publication 800-115. Gaithersburg, MD, USA: NIST, 2008.
- [10] Forum of Incident Response and Security Teams (FIRST), *Common Vulnerability Scoring System v3.1: Specification Document*, 2019.
- [11] X. Li and Y. Chen, "Hybrid grey-box penetration testing model for web applications," *IEEE Access*, vol. 7, pp. 115332–115341, 2019.
- [12] F. Yudhistira and R. Firmansyah, "Penguatan strategi pertahanan siber pada instansi pemerintahan daerah," *J. Keamanan Inf. Nas.*, vol. 5, no. 1, pp. 33–42, 2021.
- [13] Dinas Komunikasi dan Informatika Provinsi Jawa Timur, *Struktur Organisasi Dinas Komunikasi dan Informatika Provinsi Jawa Timur*, 2025.

- [14] K. Scarfone and M. Souppaya, Technical Guide to Information Security Testing and Assessment, NIST Special Publication 800-115. Gaithersburg, MD, USA: NIST, 2008.
- [15] H. Kaur and N. Kaur, "A review on penetration testing methodologies," *Int. J. Adv. Res. Comput. Sci.*, vol. 11, no. 2, 2020.
- [16] European Union Agency for Cybersecurity (ENISA), Penetration Testing Report 2022, 2022.
- [17] National Cybersecurity Center of Excellence (NCCoE), NIST Cybersecurity Practice Guides. Gaithersburg, MD, USA: NIST, 2023.
- [18] European Union Agency for Cybersecurity (ENISA), Threat Landscape Report 2022. Heraklion, Greece: ENISA, 2022.
- [19] TechTarget, "SQL injection (SQLi): Definition, examples and prevention," 2023.
- [20] L. Lundgren, "Understanding XSS attacks and defenses," *Cyber Secur. Rev.*, 2017.
- [21] ENISA, Threat Landscape Report 2022. European Union Agency for Cybersecurity, 2022.
- [22] MITRE, Common Weakness Enumeration (CWE), 2023.
- [23] A. Alqahtani and P. Zavorsky, "Comprehensive penetration testing framework aligned with organizational policies," in *Proc. IEEE*, 2020.
- [24] M. Chernyshev, S. Zeadally, and Z. Baig, "Healthcare data breaches: Implications for digital forensic readiness," *J. Med. Syst.*, vol. 43, no. 1, article 7, Jan. 2019.
- [25] A. Gueye and V. Marbukh, "A game-theoretic framework for network security vulnerability assessment and mitigation," in *Decision and Game Theory for Security*, J. Grossklags and J. Walrand, Eds. Berlin, Germany: Springer, 2012, pp. 186–200.
- [26] P. Shukla, R. Shah, and Y. Zala, "Web browser forensics: Mozilla Firefox," *Int. J. Electron. Secur. Digit. Forensics*, vol. 16, no. 4, pp. 391–411, 2024.
- [27] Wappalyzer, "Wappalyzer - Identify technology on websites," 2024. [Online]. Available: <https://www.wappalyzer.com/>
- [28] Oracle Corporation, "Oracle VM VirtualBox user guide for release 7.0," Oracle, Redwood City, CA, USA, 2024.

- [29] J. C. Jacob, "Enhancing virtualization security in Oracle VirtualBox: Investigating VM escape vulnerabilities and mitigations," M.S. thesis, Nat. College of Ireland, Dublin, Ireland, 2023.
- [30] S. V. N. Parasram et al., *Kali Linux 2018: Assuring Security by Penetration Testing*, 4th ed. Birmingham, UK: Packt Publishing, 2018.
- [31] N. Richardson, V. K. Yarlagadda, S. K. R. Anumandla, and S. C. R. Vennapusa, "Harnessing Kali Linux for advanced penetration testing and cybersecurity threat mitigation," *Am. Digits: J. Comput. Digit. Technol.*, vol. 2, no. 1, pp. 22–35, 2024.
- [32] V. N. Sankaran and J. B. Fernandes, "Advanced vulnerability detection and exploitation in web applications using Burp Suite," *Int. J. Mod. Comput. Inf. Commun. Technol.*, vol. 2, no. 11, pp. 1–10, Nov. 2024.
- [33] R. Patel and S. Sharma, "Comprehensive exploration of web application security testing with Burp Suite tools," *Int. J. Multidiscip. Res.*, vol. 5, no. 6, pp. 1–12, 2023.
- [34] S. K. Patel, V. R. Rathod, and J. B. Prajapati, "Nessus: Study of a tool to assess network vulnerabilities," *Int. J. Eng. Res. Technol.*, vol. 4, no. 10, pp. 688–691, Oct. 2021.
- [35] M. Baig, N. Gul, and A. Rehman, "Vulnerability scanning and analysis of network devices using Nessus," *J. Comput. Sci. Appl.*, vol. 8, no. 2, pp. 45–52, 2022.
- [36] G. F. Lyon, *Nmap Network Scanning: The Official Nmap Project Guide to Network Discovery and Security Scanning*. Sunnyvale, CA, USA: Insecure.Com LLC, 2009.
- [37] M. Rahman and S. Islam, "Web application reconnaissance using directory enumeration techniques," *Int. J. Inf. Secur. Res.*, vol. 9, no. 4, pp. 234–242, 2023.
- [38] ProjectDiscovery, "Nuclei - Fast and customizable vulnerability scanner," GitHub repository, 2024. [Online]. Available: <https://github.com/projectdiscovery/nuclei>
- [39] S. Dhawan and M. Singh, "Template-based vulnerability scanning with Nuclei: A modern approach," *J. Cybersecur. Res.*, vol. 5, no. 3, pp. 78–89, 2023.
- [40] M. Baklizi, I. Atoum, N. Abdullah, O. A. Al-Wesabi, A. A. Otoom, and M. A. Hasan, "A technical review of SQL injection tools and methods: A case study of SQLMap," *Int. J. Intell. Syst. Appl. Eng.*, vol. 10, no. 3, pp. 75–85, 2022.

- [41] SQLMap Development Team, "sqlmap: Automatic SQL injection and database takeover tool," 2024. [Online]. Available: <https://sqlmap.org/>
- [42] OJ Reeves, "Gobuster - Directory/File, DNS and VHost busting tool," GitHub repository, 2024. [Online]. Available: <https://github.com/OJ/gobuster>
- [43] D. Stenberg, Everything curl: The Complete Guide to Using curl and libcurl, 2024. [Online]. Available: <https://ec.haxx.se/>
- [44] S. P. Maniraj, C. S. Ranganathan, and S. Sekar, "Securing web applications with OWASP ZAP for comprehensive security testing," *Int. J. Adv. Signal Image Sci.*, vol. 10, no. 2, pp. 12–23, Dec. 2024.
- [45] F. P. Putra, U. Ubaidi, A. Hamzah, W. A. Pramadi, and A. Nuraini, "Systematic literature review: Security gap detection on websites using OWASP ZAP," *Brilliance Res. Artif. Intell.*, vol. 4, no. 1, pp. 348–355, 2024.
- [46] N. A. Syarifudin and L. Setiyani, "Analysis of higher education SIAKAD website security gaps using the vulnerability assessment method," *Int. J. Multidiscip. Approach Res. Sci.*, vol. 1, no. 3, pp. 332–344, 2024.
- [47] Hahwul, "Dalfox: Powerful XSS scanning and parameter analysis tool," GitHub repository, 2024. [Online]. Available: <https://github.com/hahwul/dalfox>
- [48] K. Lee and J. Park, "Advanced XSS detection using context-aware scanning techniques," *J. Web Appl. Secur.*, vol. 7, no. 3, pp. 112–125, 2024.
- [49] D. Patel, "Parameter mining for web application security testing," *J. Web Secur.*, vol. 3, no. 4, pp. 89–98, 2023.
- [50] L. Martinez, "Leveraging web archives for security reconnaissance," *Int. J. Penetration Test.*, vol. 6, no. 2, pp. 45–56, 2024.
- [51] R. Johnson, "Attack surface discovery through parameter enumeration," *Bug Bounty J.*, vol. 2, no. 3, pp. 67–78, 2023.
- [52] M. Tewari and N. Datt, "Assessing browser security: A detailed study based on CVE metrics," *Future Internet*, vol. 17, no. 3, article 104, Feb. 2025.
- [53] H. Chen, "Advanced techniques for web path discovery in penetration testing," *J. Ethical Hacking*, vol. 4, no. 2, pp. 56–67, 2022.

- [54] A. Gupta and R. Sharma, "Automated security testing using ProjectDiscovery tools in CI/CD pipelines," in Proc. Int. Conf. Cybersecur. Privacy, 2024, pp. 145–152.
- [55] Y. Alkhurayyif and Y. S. Almarshdy, "Adopting automated penetration testing tools: A cost-effective approach to enhancing cybersecurity in small organizations," J. Inf. Secur. Cybercrimes Res., vol. 6, no. 2, pp. 89–102, 2023.
- [56] J. Doe and A. Smith, "Effective Filter for Common Injection Attacks in Online Web Applications," Int. J. Web Appl. Secur., vol. 5, no. 2, pp. 55–68, 2022.
- [57] F. Rahman and L. Prasetyo, "Uji Penetrasi Server Universitas PQR Menggunakan Metode NIST SP 800-115," J. Inf. Syst. Secur., vol. 4, no. 1, pp. 25–34, 2023.
- [58] S. Brown and K. Miller, "Structuring a Comprehensive Software Security Course Around the OWASP ASVS," IEEE Trans. Educ., vol. 66, no. 4, pp. 421–430, 2022.
- [59] H. Zhang, Y. Liu, and P. Chen, "Cybersecurity Risk Assessment Based on Cognitive Attack Vector Modeling with CVSS Score," Int. J. Cyber Secur. Digit. Forensics, vol. 11, no. 3, pp. 145–160, 2022.
- [60] M. Safwan and R. Hidayat, "Security Testing of XYZ Website Application Using ISSAF and OWASP WSTG v4.2 Methods," J. Web Eng. Secur., vol. 7, no. 1, pp. 75–90, 2023.