DAFTAR PUSTAKA

[1] B. A. Mustafa and Fadhil. A. Al-Qirimli, "The Impact of Information Security Processes on Providing Secure Digital Systems," *Journal Port Science Research*, vol. 6, no. 4, pp. 344–347, Dec. 2023, doi: 10.36371/port.2023.4.4.

[2] Deputi Bidang Operasi Keamanan Siber dan Sandi BSSN, "Laporan Tahunan 2023 Honeynet Project BSSN," Jakarta Selatan, 2024.

[3] Deputi Bidang Operasi Keamanan Siber dan Sandi BSSN, "Laporan Tahunan 2022 Honeynet Project BSSN," Jakarta Selatan, 2023.

[4] Direktorat Operasi Keamanan Siber BSSN, "Lanskap Keamanan Siber Indonesia 2023," Jakarta Selatan, 2024.

[5] Direktorat Operasi Keamanan Siber BSSN, "Lanskap Keamanan Siber Indonesia 2022," Jakarta Selatan, 2023.

[6] Asosiasi Penyelenggara Jasa Internet Indonesia (APJII), "Survei Internet APJII 2024." Accessed: Mar. 07, 2024. [Online]. Available: https://survei.apjii.or.id/

[7] H. S. Abdullah, "Evaluation of Open Source Web Application Vulnerability Scanners," *Academic Journal of Nawroz University*, vol. 9, no. 1, pp. 47–52, Feb. 2020, doi: 10.25007/AJNU.V9N1A532.

[8] V. Appiah, M. Asante, I. K. Nti, and O. Nyarko-Boateng, "Survey of Websites and Web Application Security Threats Using Vulnerability Assessment," *Journal of Computer Science*, vol. 15, no. 10, pp. 1341–1354, Jan. 2019, doi: 10.3844/JCSSP.2019.1341.1354.

[9] "WSTG - Latest | OWASP Foundation." Accessed: Mar. 24, 2024. [Online]. Available: https://owasp.org/www-project-web-security-testing-guide/latest/3-The_OWASP_Testing_Framework/1-Penetration_Testing_Methodologies

[10] E. Zakia Darojat, E. Sediyono, and I. Sembiring, "Vulnerability Assessment Website E-Government dengan NIST SP 800-115 dan OWASP Menggunakan Web Vulnerability Scanner," *Jurnal Sistem*

Informasi Bisnis, vol. 12, no. 1, pp. 36–44, Sep. 2022, doi: 10.21456/VOL12ISS1PP36-44.

[11] R. Amankwah, J. Chen, P. K. Kudjo, B. K. Agyemang, and A. A. Amponsah, "An Automated Framework for Evaluating Open-Source Web Scanner Vulnerability Severity," *Service Oriented Computing and Applications*, vol. 14, no. 4, pp. 297–307, Dec. 2020, doi: 10.1007/S11761-020-00296-9/METRICS.

[12] M. Albahar, D. Alansari, and A. Jurcut, "An Empirical Comparison of Pen-Testing Tools for Detecting Web App Vulnerabilities," *Electronics 2022, Vol. 11, Page 2991*, vol. 11, no. 19, p. 2991, Sep. 2022, doi: 10.3390/ELECTRONICS11192991.

[13] R. Amankwah, J. Chen, P. K. Kudjo, and D. Towey, "An Empirical Comparison of Commercial and Open-Source Web Vulnerability Scanners," *Softw Pract Exp*, vol. 50, no. 9, pp. 1842–1857, Sep. 2020, doi: 10.1002/SPE.2870.

[14] P. Jarupunphol, S. Seatun, and W. Buathong, "Measuring Vulnerability Assessment Tools' Performance on the University Web Application," *Pertanika J Sci Technol*, vol. 31, no. 6, pp. 2973–2993, Oct. 2023, doi: 10.47836/pjst.31.6.19.

[15] A. Alanda, D. Satria, M. I. Ardhana, A. A. Dahlan, and H. A. Mooduto, "Web Application Penetration Testing Using SQL Injection Attack," *JOIV : International Journal on Informatics Visualization*, vol. 5, no. 3, p. 320, Sep. 2021, doi: 10.30630/joiv.5.3.470.

[16] A. Fadlil, I. Riadi, and M. A. Mu'Min, "Mitigation from SQL Injection Attacks on Web Server using Open Web Application Security Project Framework," *International Journal of Engineering*, vol. 37, no. 4, pp. 635–645, Apr. 2024, doi: 10.5829/IJE.2024.37.04A.06.

[17] A. Almaarif and M. Lubis, "Vulnerability Assessment and Penetration Testing (VAPT) Framework: Case Study of Government's Website," *Int J Adv Sci Eng Inf Technol*, vol. 10, no. 5, pp. 1874–1880, Oct. 2020, doi: 10.18517/IJASEIT.10.5.8862.

[18] I. P. Agus, E. Pratama, A. A. Bagus, and A. Wiradarma, “Open Source Intelligence Testing Using the OWASP Version 4 Framework at the Information Gathering Stage (Case Study: X Company),” *International Journal of Computer Network and Information Security*, vol. 11, no. 7, p. 8, Jul. 2019, doi: 10.5815/IJCNIS.2019.07.02.

[19] “Vulnerabilities | OWASP Foundation.” Accessed: Mar. 19, 2024. [Online]. Available: https://owasp.org/www-community/vulnerabilities/

[20] “OWASP Risk Rating Methodology | OWASP Foundation.” Accessed: Mar. 19, 2024. [Online]. Available: https://owasp.org/www-community/OWASP_Risk_Rating_Methodology

[21] R. Nursyanti, R. Y. R. Alamsyah, and S. Perdana, “Perancangan Aplikasi Berbasis Web untuk Membantu Pengujian Kualitas Kain Tekstil Otomotif (Studi Kasus pada PT. Ateja Multi Industri),” *Explore: Jurnal Sistem Informasi dan Telematika (Telekomunikasi, Multimedia dan Informatika)*, vol. 10, no. 2, Oct. 2019, doi: 10.36448/JSIT.V10I2.1323.

[22] “Rekayasa Web - Janner Simarmata - Google Buku.” Accessed: Mar. 16, 2024. [Online]. Available: https://books.google.co.id/books?id=J8JpLoPUHGAC&printsec=frontcover#v=onepage&q&f=false

[23] G. Gunawan, A. Lawi, and A. Adnan, “Analisis Arsitektur Aplikasi Web Menggunakan Model View Controller (MVC) pada Framework Java Server Faces,” *Scientific Journal of Informatics*, vol. 3, no. 1, pp. 55–67, Jun. 2016, doi: 10.15294/SJI.V3I1.5958.

[24] A. Setiadi and F. Alfiah, “Sistem Penjualan Spare Part Toko AJM Motor Menggunakan CI Berbasis Arsitektur MVC,” *Simetris: Jurnal Teknik Mesin, Elektro dan Ilmu Komputer*, vol. 7, no. 2, pp. 575–586, Nov. 2016, doi: 10.24176/SIMET.V7I2.770.

[25] N. F. Saragih, R. Tamalawe, and I. M. Sarkis, “Analisis dan Implementasi Secure Code pada Pengembangan Sistem Keamanan Website fikom-methodist.com Menggunakan Penetration Testing dan OWASP ZAP,” Jurnal Times. Accessed: Mar. 16, 2024. [Online]. Available: https://ejournal.stmik-time.ac.id/index.php/jurnalTIMES/article/view/690

[26] D. A. K. Ningtyas, “Keefektifan Website Sekolah dalam Pemanfaatan sebagai Sumber Belajar,” 2019, Accessed: Mar. 28, 2024. [Online]. Available: https://repository.uksw.edu//handle/123456789/20179

[27] “Chapter 1: Introduction to School Websites.” Accessed: Mar. 20, 2024. [Online]. Available: https://fcit.usf.edu/websites/chap1/chap1.htm

[28] “Chapter 7: Other Issues.” Accessed: Mar. 20, 2024. [Online]. Available: https://fcit.usf.edu/websites/chap7/chap7.htm

[29] R. Ross, V. Pillitteri, R. Graubart, D. Bodeau, and R. McQuaid, “Developing Cyber-Resilient systems: A Systems Security Engineering Approach,” Dec. 2021. doi: 10.6028/NIST.SP.800-160v2r1.

[30] K. B. Schaffer, P. Mell, H. Trinh, and I. Van Wyk, “Recommendations for Federal Vulnerability Disclosure Guidelines,” May 2023. doi: 10.6028/NIST.SP.800-216.

[31] “Threat Modeling Process | OWASP Foundation.” Accessed: Apr. 04, 2024. [Online]. Available: https://owasp.org/www-community/Threat_Modeling_Process

[32] L. Kohnfelder and P. Garg, “The Threats to Our Products,” 1999.

[33] “Tentang OWASP - OWASP Top 10:2021.” Accessed: Mar. 11, 2024. [Online]. Available: https://owasp.org/Top10/id/A00-about-owasp/

[34] “OWASP Top Ten | OWASP Foundation.” Accessed: Mar. 16, 2024. [Online]. Available: https://owasp.org/www-project-top-ten/

[35] “OWASP Web Security Testing Guide | OWASP Foundation.” Accessed: Mar. 28, 2024. [Online]. Available: https://owasp.org/www-project-web-security-testing-guide/

[36] “WSTG - Latest | OWASP Foundation.” Accessed: Mar. 28, 2024. [Online]. Available: https://owasp.org/www-project-web-security-testing-guide/latest/4-Web_Application_Security_Testing/00-Introduction_and_Objectives/README

[37] “OWASP Mobile Application Security | OWASP Foundation.” Accessed: Mar. 28, 2024. [Online]. Available: https://owasp.org/www-project-mobile-app-security/

[38] “scriptingxss/owasp-fstm: The Firmware Security Testing Methodology (FSTM) is composed of nine stages tailored to enable security researchers, software developers, consultants, and Information Security professionals with conducting firmware security assessments.” Accessed: Mar. 28, 2024. [Online]. Available: https://github.com/scriptingxss/owasp-fstm

[39] “Kali Linux | Penetration Testing and Ethical Hacking Linux Distribution.” Accessed: May 08, 2024. [Online]. Available: https://www.kali.org/

[40] “Kali Tools | Kali Linux Tools.” Accessed: May 08, 2024. [Online]. Available: https://www.kali.org/tools/

[41] “Get Kali | Kali Linux.” Accessed: May 08, 2024. [Online]. Available: https://www.kali.org/get-kali/#kali-platforms

[42] “whois/README at next · rfc1036/whois · GitHub.” Accessed: May 09, 2024. [Online]. Available: https://github.com/rfc1036/whois/blob/next/README

[43] “whois | Kali Linux Tools.” Accessed: May 09, 2024. [Online]. Available: https://www.kali.org/tools/whois/

[44] “theHarvester/README.md at master · laramies/theHarvester · GitHub.” Accessed: May 09, 2024. [Online]. Available: https://github.com/laramies/theHarvester/blob/master/README.md

[45] “Find out what websites are built with - Wappalyzer.” Accessed: May 10, 2024. [Online]. Available: https://www.wappalyzer.com/

[46] “Technologies - Wappalyzer.” Accessed: May 10, 2024. [Online]. Available: https://www.wappalyzer.com/technologies/

[47] “APIs - Wappalyzer.” Accessed: May 10, 2024. [Online]. Available: https://www.wappalyzer.com/api/

[48] “nmap | Kali Linux Tools.” Accessed: May 10, 2024. [Online]. Available: https://www.kali.org/tools/nmap/

[49] “Nmap: the Network Mapper - Free Security Scanner.” Accessed: May 10, 2024. [Online]. Available: https://nmap.org/

[50] “zaproxy | Kali Linux Tools.” Accessed: May 10, 2024. [Online]. Available: https://www.kali.org/tools/zaproxy/

[51] “zaproxy/README.md at main · zaproxy/zaproxy · GitHub.” Accessed: May 10, 2024. [Online]. Available: https://github.com/zaproxy/zaproxy/blob/main/README.md

[52] “burpsuite | Kali Linux Tools.” Accessed: May 10, 2024. [Online]. Available: https://www.kali.org/tools/burpsuite/

[53] “Download Burp Suite Community Edition - PortSwigger.” Accessed: May 10, 2024. [Online]. Available: https://portswigger.net/burp/communitydownload

[54] “Burp Scanner - Web Vulnerability Scanner from PortSwigger.” Accessed: May 10, 2024. [Online]. Available: https://portswigger.net/burp/vulnerability-scanner

[55] “sqlmap: automatic SQL injection and database takeover tool.” Accessed: May 09, 2024. [Online]. Available: https://sqlmap.org/

[56] “sqlmap | Kali Linux Tools.” Accessed: May 09, 2024. [Online]. Available: https://www.kali.org/tools/sqlmap/

[57] Z. Bin Akhtar and A. T. Rawol, “Uncovering Cybersecurity Vulnerabilities: A Kali Linux Investigative Exploration Perspective,” *International Journal of Advanced Network, Monitoring and Controls*, vol. 9, no. 2, pp. 11–22, Jun. 2024, doi: 10.2478/IJANMC-2024-0012.

[58] J. Shahid, M. K. Hameed, I. T. Javed, K. N. Qureshi, M. Ali, and N. Crespi, “A Comparative Study of Web Application Security Parameters: Current Trends and Future Directions,” *Applied Sciences 2022, Vol. 12, Page 4077*, vol. 12, no. 8, p. 4077, Apr. 2022, doi: 10.3390/APP12084077.

[59] W. Mazurczyk and L. Caviglione, “Cyber reconnaissance techniques,” *Commun ACM*, vol. 64, no. 3, pp. 86–95, Mar. 2021, doi: 10.1145/3418293/SUPPL_FILE/3418293-VOR.PDF.

[60] S. N. Hidayah Zulkiffli, M. N. Ahmad Zawawi, and F. A. Rahim, “Passive and Active Reconnaissance: A Social Engineering Case Study,” *2020 8th International Conference on Information Technology and Multimedia, ICIMU 2020*, pp. 138–143, Aug. 2020, doi: 10.1109/ICIMU49871.2020.9243402.