DAFTAR PUSTAKA

[1] V. Mantalean and D. Prabowo, "BSSN sebut ada 16 miliar serangan siber selama 2021.," Kompas.com. Accessed: Jul. 07, 2025. [Online]. Available: https://nasional.kompas.com/read/2022/03/07/20162321/bssn-sebut-ada-16-miliar-serangan-siber-selama-2021

[2] A. Risfil, "BSSN Catat Peretasan Situs Capai 1,6 Miliar Kasus," rri.co.id. Accessed: Jul. 07, 2025. [Online]. Available: https://www.rri.co.id/nasional/1521493/bssn-catat-peretasan-situs-capai-1-6-miliar-kasus

[3] F. Dianira, "Puluhan Mahasiswa Unud Diteror Spam, Diduga Data Bocor dari Situs Kampus," detik.com. Accessed: Jul. 07, 2025. [Online]. Available: https://www.detik.com/bali/hukum-dan-kriminal/d-7964624/puluhan-mahasiswa-unud-diteror-spam-diduga-data-bocor-dari-situs-kampus

[4] M. R. Kamal, "Implementasi Security Information and Event Management (SIEM) Dengan Splunk Untuk Analisis Tren Ancaman Siber Pada Jaringan UII," pp. 1–62, 2022, [Online]. Available: https://dspace.uii.ac.id/bitstream/handle/123456789/40786/17523098.pdf?sequence=1&isAllowed=y

[5] J. T. Santoso, *Teknologi Keamanan Siber (Cyber Security)*. 2023. [Online]. Available: https://penerbit.stekom.ac.id/index.php/yayasanpat/article/view/458%0Ahttps://penerbit.stekom.ac.id/index.php/yayasanpat/article/download/458/483

[6] A. Adebiyi, J. Arreymbi, and C. Imafidon, "Security Assessment of Software Design using Neural Network," *Int. J. Adv. Res. Artif. Intell.*, vol. 1, no. 4, pp. 1–7, 2012, doi: 10.14569/ijarai.2012.010401.

[7] Y. S. Kang, H. H. Cho, Y. Shin, and J. B. Kim, "A study on penetration testing methodology," *Int. J. Appl. Eng. Res.*, vol. 10, no. 18, pp. 39290–39293, 2015.

[8] Z. A. Khan, N. Safaat, M. Irsyad, and T. Darmizal, "Penetration Testing Information System Security Assessment Framework (ISSAF)," *Kaji. Ilm. Inform. dan Komput.*, vol. 4, no. 3, pp. 1593–1601, 2023, doi:

10.30865/klik.v4i3.1503.

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

[10] I. Cloudflare, “What is OWASP? What is the OWASP Top 10?,” cloudflare. Accessed: Jul. 07, 2025. [Online]. Available: https://www.cloudflare.com/learning/security/threats/owasp-top-10/

[11] A. Identifikasi Kerentanan Keamanan Pada Website Fakultas Ilmu Komputer Universitas Subang Menggunakan Metodologi Owasp Syafaat, “Identifikasi Kerentanan Keamanan Pada Website Fakultas Ilmu Komputer Universitas Subang Menggunakan Metodologi Owasp,” *E-Journal*, vol. 11, no. 1, pp. 84–99, 2024, [Online]. Available: http://ejournal.unsub.ac.id/index.php/Fasilkom

[12] G. Pramuja Inngam Fanani, Muhammad Amirul Mu’min, and N. Tristanti, “Analisis dan Pengujian Kerentanan Website Menggunakan OWASP ZAP,” *J. Ris. Sist. dan Teknol. Inf.*, vol. 3, no. 1, pp. 36–50, 2025, doi: 10.30787/restia.v3i1.1886.

[13] G. Guntoro, L. Costaner, and M. Musfawati, “Analisis Keamanan Web Server Open Journal System (Ojs) Menggunakan Metode Issaf Dan Owasp (Studi Kasus Ojs Universitas Lancang Kuning),” *JIPI (Jurnal Ilm. Penelit. dan Pembelajaran Inform.*, vol. 5, no. 1, p. 45, 2020, doi: 10.29100/jipi.v5i1.1565.

[14] K. T. Suli and N. Nirsal, “Rancang Bangun Sistem Informasi Desa Berbasis Website (Studi Kasus Desa Walenrang),” *D’computare J. Ilm. Teknol. Inf. dan Ilmu Komput.*, vol. 13, no. 1, pp. 24–32, 2023, doi: 10.30605/dcomputare.v13i1.57.

[15] E. Saad and R. Mitchell, *OWASP Web Security Testing guide Version 4.2*. owasp, 2020. [Online]. Available: https://owasp.org/www-project-web-security-testing-guide/

[16] OISSG, *Information Systems Security Assessment Framework (ISSAF)*. 2006. [Online]. Available: https://kr-labs.com.ua/books/oissg-pentest.pdf

[17] A. Fauzi *et al.*, “Peran CIA (Confidentiality, Integrity, Availability) pada

Layanan Internet Banking di Perbankan," *J. Ilmu Multidisplin*, vol. 2, no. 1, pp. 99–105, 2023, doi: 10.38035/jim.v2i1.230.

[18] Heru Wijayanto Aripradono, Haeruddin, and Kurnia Cantra, "Evaluation of Two-Factor Authentication (2FA) TOTP in Higher Education Using Vulnerability Assessment and CIA Triad," *J. E-Komtek*, vol. 8, no. 2, pp. 245–254, 2024, doi: 10.37339/e-komtek.v8i2.2113.

[19] OWASP, "Content Security Policy (CSP) Header Not Set." Accessed: Nov. 25, 2025. [Online]. Available: https://www.zaproxy.org/docs/alerts/10038-1/

[20] tenable, "Missing 'X-Frame-Options' Header." Accessed: Nov. 25, 2025. [Online]. Available: https://www.tenable.com/plugins/was/98060

[21] OWASP, "X-Content-Type-Options Header Missing," X-Content-Type-Options Header Missing. Accessed: Nov. 25, 2025. [Online]. Available: https://www.zaproxy.org/docs/alerts/10021/

[22] OWASP, "Strict-Transport-Security Multiple Header Entries (Non-compliant with Spec)." Accessed: Nov. 25, 2025. [Online]. Available: https://www.zaproxy.org/docs/alerts/10035-3/

[23] Tenable, "Missing HTTP Strict Transport Security Policy." Accessed: Nov. 25, 2025. [Online]. Available: https://www.tenable.com/plugins/was/98056

[24] OWASP, "HttpOnly cookies." Accessed: Nov. 28, 2025. [Online]. Available: https://owasp.org/www-community/HttpOnly

[25] OWASP, "Cookie Without Secure Flag." Accessed: Nov. 25, 2025. [Online]. Available: https://www.zaproxy.org/docs/alerts/10011/

[26] Tenable, "Cookie Without Secure Flag Detected." Accessed: Nov. 25, 2025. [Online]. Available: https://www.tenable.com/plugins/was/98064

[27] OWASP, "Testing for Cookies Attributes." Accessed: Nov. 28, 2025. [Online]. Available: https://owasp.org/www-project-web-security-testing-guide/v41/4-Web_Application_Security_Testing/06-Session_Management_Testing/02-Testing_for_Cookies_Attributes.html

[28] OWASP, ."htaccess Information Leak." Accessed: Nov. 28, 2025. [Online]. Available: https://www.zaproxy.org/docs/alerts/40032/

[29] MDN, "Apache Configuration: .htaccess." Accessed: Nov. 28, 2025.

[Online]. Available: https://developer.mozilla.org/en-US/docs/Learn_web_development/Extensions/Server-side/Apache_Configuration_htaccess

[30] OWASP, “HTTP Server Response Header.” Accessed: Nov. 28, 2025. [Online]. Available: https://www.zaproxy.org/docs/alerts/10036/

[31] APACHE, “Server.” Accessed: Nov. 28, 2025. [Online]. Available: https://httpd.apache.org/docs/current/mod/core.html#servertokens

[32] Microsoft, “Masking Content Headers (Banners).” Accessed: Nov. 28, 2025. [Online]. Available: https://learn.microsoft.com/en-us/previous-versions/msp-n-p/ff648552(v=pandp.10)

[33] OWASP, “How do I handle a False Positive?” Accessed: Nov. 26, 2025. [Online]. Available: https://www.zaproxy.org/faq/how-do-i-handle-a-false-positive/

[34] OWASP, “Highest False Positives Last Month.” Accessed: Nov. 26, 2025. [Online]. Available: https://www.zaproxy.org/docs/statistics/highest-false-positives-last-month/

[35] S. Jain, “Understanding TLS 1.2 and TLS 1.3.” Accessed: Nov. 26, 2025. [Online]. Available: https://www.encryptionconsulting.com/tls-1-2-and-tls-1-3/