DAFTAR PUSTAKA

[1] bssn.go.id, “Publikasi,” https://www.bssn.go.id/publikasi/. Accessed: Dec. 12, 2025. [Online]. Available: https://www.bssn.go.id/publikasi/

[2] Md. A. Masum, Md. R. I. Sachcha, and A. Nayem, “Security Analysis of Government & Financial Websites of Bangladesh,” *I. J. Education and Management Engineering, ,* 2022.

[3] Haeruddin, G. Wijaya, H. Winata, S. Aji, and M. N. Faiz, “Website Security Analysis Using Vulnerability Assessment Method (Case Study: Universitas Internasional Batam),” *Journal of Innovation Information Technology and Application*, 2024.

[4] I. N. Laily, “Pengertian Website Menurut Para Ahli, Beserta Jenis dan Fungsinya,” Katadata. Accessed: Dec. 12, 2025. [Online]. Available: https://katadata.co.id/lifestyle/edukasi/6200a2a9697ec/pengertian-website-menurut-para-ahli-beserta-jenis-dan-fungsinya

[5] A. M. Ujung and M. I. P. Nasution, “Pentingnya Sistem Keamanan Database untuk melindungi data pribadi,” *JISKA: Jurnal Sistem Informasi Dan Informatika*, pp. 44–47, 2023, [Online]. Available: https://jurnal.unidha.ac.id/index.php/jiska/article/view/929/546

[6] R. Harahap, “Pengertian *Repository* Adalah: Tujuan, Fungsi dan Macam Repositori Perguruan Tinggi,” Jul. 15, 2023. [Online]. Available: https://www.kosngosan.com/2019/08/pengertian-*Repository*-adalah.html

[7] M. Akmal, “Analisis Dan Uji Coba Tingkat Keamanan Website UIN Ar-Raniry Menggunakan Acunetix Web Vulnerability Scanner,” 2023, [Online]. Available: https://*Repository*.ar-raniry.ac.id/id/eprint/32694/

[8] S. K. Khotimah, “Analisis Manajemen Risiko Keamanan Sistem Informasi Ujian CBT Online Pada Instansi XYX Menggunakan Metode Nist Sp 800-30,” UPN Veteran Jakarta, 2022. [Online]. Available: https://*Repository*.upnvj.ac.id/19811/

[9] N. V. I. Sugara and N. I. W. Sriyasa, “Analisis keamanan web menggunakan Open Web Application Security Web (OWASP),” *Indonesian Journal of Computer Science*, vol. 13, no. 2, 2024, doi: 10.33022/ijcs.v13i2.3736.

[10] owasp.org, “Pengenalan - OWASP Top 10:2021,” OWASP Top 10:2021. Accessed: Dec. 21, 2025. [Online]. Available: https://owasp.org/Top10/id/A00_2021_Introduction/

[11] Y. Taryana and N. Heryana, “Analisis Keamanan Website BPJS Kesehatan menggunakan Vulnerability Assessment dengan OWASP ZAP,” *Joutica – Jurnal Teknik Informatika*, 2025, doi: 10.30736/informatika.v8i1.951.

[12] A. Rajan and E. Erturk, “Web application security: Exploitation and countermeasures for SQL injection, XSS, and directory traversal. ,” *International Journal of Computer Applications*, 2017.

[13] ZAP, “Form security issues: insecure transitions and CSRF risks,” OWASP ZAP Documentation. Accessed: Dec. 23, 2025. [Online]. Available: https://www.zaproxy.org/docs/alerts/

[14] StackHawk, “Insecure form transitions between HTTP and HTTPS,” StackHawk Security Guides. Accessed: Dec. 19, 2025. [Online]. Available: https://docs.stackhawk.com/vulnerabilities/10041/

[15] A. Krishnan, “CSRF attacks and prevention techniques,” GeeksforGeeks. Accessed: Dec. 19, 2025. [Online]. Available: https://www.geeksforgeeks.org/computer-networks/what-is-cross-site-request-forgery-csrf/

[16] PortSwigger, “Cross-Site Request Forgery (CSRF): Prevention and token design,” PortSwigger Web Security Academy. Accessed: Dec. 19, 2025. [Online]. Available: https://docs.stackhawk.com/vulnerabilities/10042/

[17] StackHawk, “Secure form submission and HTTPS best practices,” StackHawk Security Guides. Accessed: Dec. 23, 2025. [Online]. Available: https://docs.stackhawk.com/vulnerabilities/10042/

[18] PortSwigger, “MIME sniffing and missing Content-Type vulnerabilities,” PortSwigger Web Security Academy. Accessed: Dec. 23, 2025. [Online]. Available: https://portswigger.net/web-security/csrf/preventing

[19] TuringSecure, “Understanding Content-Type vulnerabilities and secure header configuration,” TuringSecure Documentation. Accessed: Dec. 23, 2025. [Online]. Available: https://turingsecure.com/knowledge-base/issues/configuration-management/

[20] Invicti, “Content-Type header security and MIME sniffing risks,” Invicti Web Security Documentation. Accessed: Dec. 23, 2025. [Online]. Available: https://www.invicti.com/blog/web-security/how-bad-is-missing-content-type-header

[21] Beaglesecurity.com, “Understanding insecure form transitions and web security risks,” Beagle Security Blog. Accessed: Dec. 23, 2025. [Online]. Available: https://beaglesecurity.com/blog/vulnerability/insecure-https-to-http-form-transition.html

[22] A. R. Samosir, “Analisis Keamanan Website SIAKAD UPN ‘Veteran’ Jakarta Menggunakan Metode Vulnerability Assessment Berdasarkan Owasp Top Ten,” Universitas Pembangunan Nasional Veteran Jakarta., 2025. [Online]. Available: https://*Repository*.upnvj.ac.id/38297/

[23] G. Heyes, “Relative Path Confusion: Exploiting Web Browsers’ URL Resolution,” PortSwigger Web Security Research. Accessed: Dec. 23, 2025.

[Online]. Available: https://portswigger.net/research/detecting-and-exploiting-path-relative-stylesheet-import-prssi-vulnerabilities

[24] E. S. Alashwali, P. Szalachowski, and A. Martin, “Exploring HTTPS Security Inconsistencies: A Cross-Regional Perspective,” *ArXiv*, 2020.

[25] W. Stallings, *Data and Computer Communications* , 10th ed. Pearson, 2017.