

DAFTAR PUSTAKA

- [1] C. M. Annur, “Indonesia Masuk 3 Besar Negara dengan Kasus Kebocoran Data Terbanyak Dunia,” <https://databoks.katadata.co.id/teknologi-telekomunikasi/statistik/3f6a7dc0c5d0b7e/indonesia-masuk-3-besar-negara-dengan-kasus-kebocoran-data-terbanyak-dunia>. Accessed: Oct. 28, 2024. [Online]. Available: <https://databoks.katadata.co.id/teknologi-telekomunikasi/statistik/3f6a7dc0c5d0b7e/indonesia-masuk-3-besar-negara-dengan-kasus-kebocoran-data-terbanyak-dunia>
- [2] “LANSKAP KEAMANAN SIBER INDONESIA.”
- [3] Hartono and O. W. Purbo, *Membangun dan Menguji Keamanan Website*. Yogyakarta: ANDI, 2022.
- [4] R. Vallabhaneni, S. A. Vaddadi, S. E. Vadakkethil Somanathan Pillai, S. R. Addula, and B. Ananthan, “MobileNet based secured compliance through open web application security projects in cloud system,” *Indonesian Journal of Electrical Engineering and Computer Science*, vol. 35, no. 3, pp. 1661–1669, Sep. 2024, doi: 10.11591/ijeecs.v35.i3.pp1661-1669.
- [5] A. Choiriyah and N. Qomariasih, “Security Analysis on Websites Belonging to the Health Service Districts in Indonesia Based on the Open Web Application Security Project (OWASP) Top 10 2021,” in *Proceeding - International Conference on Information Technology and Computing 2023, ICITCOM 2023*, Institute of Electrical and Electronics Engineers Inc., 2023, pp. 267–272. doi: 10.1109/ICITCOM60176.2023.10442816.
- [6] “CWE Top 25 Most Dangerous Software Weaknesses,” <https://cwe.mitre.org/top25/>.
- [7] “About the OWASP Foundation,” <https://owasp.org/about/>. Accessed: Sep. 20, 2024. [Online]. Available: <https://owasp.org/about/>
- [8] “OWASP Top Ten,” <https://owasp.org/www-project-top-ten/>.
- [9] P. Vishwakarma, “OWASP Top 10 vs SANS/CWE Top 25: Complete Security Vulnerabilities Guide [2024],” <https://www.secopsolution.com/blog/owasp-top-10-vs-sans-25>.

- [10] T. Petranovic and N. Zaric, "Effectiveness of Using OWASP TOP 10 as AppSec Standard," in *2023 27th International Conference on Information Technology, IT 2023*, Institute of Electrical and Electronics Engineers Inc., 2023. doi: 10.1109/IT57431.2023.10078626.
- [11] S. U. K. H. U. K. and M. I. R. A. Khan, "Systematic Literature Review on Security Risks and its Practices in Secure Software Development," *IEEE Access*, vol. 10, Jan. 2022.
- [12] B. Annie and F. Amber, "What is dynamic application security testing (DAST)?," <https://www.ibm.com/topics/dynamic-application-security-testing>.
- [13] "What is penetration testing?," <https://www.ibm.com/topics/penetration-testing>.
- [14] I. R. Dhaifullah, M. Muttanifudin, A. A. Salsabila, and M. A. Yakin, "Survei Teknik Pengujian Software," 2022.
- [15] M. G. and M. M.-T. D. Wang, "Information needs in bug reports for web applications," *J. Syst. Softw.*, vol. 219, Oct. 2024.
- [16] "Critical Applications," <https://www.sciencedirect.com/topics/computer-science/critical-application>.
- [17] M. A. Mohamed Mohideen *et al.*, "Behind the Code: Identifying Zero-Day Exploits in WordPress," *Future Internet*, vol. 16, no. 7, Jul. 2024, doi: 10.3390/fi16070256.
- [18] S. S. and R. R. P. S. L. Raju, "8 Use ModSecurity Web Application Firewall to Mitigate OWASP's Top 10 Web Application Vulnerabilities," *mplement. Enterprise. Cybersecurity with Open-source Software. Stand. Archi*, 2021.
- [19] O. C. M. K. H. H. and A. D. O. Ben Fredj, "An OWASP Top Ten Driven Survey on Web Application Protection Methods," *pringer International Publishing*, 2021.
- [20] A. P. S. P. and D. S. N. Chillur, "Deep Analysis of Attacks and Vulnerabilities of Web Security.".
- [21] N. Anantharaman and B. Wukkadada, "Identifying the Usage of Known Vulnerabilities Components Based on OWASP A9," *Iut. Infont. Conf. Emerg. Smart Comprmatcs*, 2020.
- [22] Z. Yin and S. U. J. Lee, "Security Analysis of Web Open-Source Projects Based on Java and PHP," 2023.
- [23] "OWASP WebGoat," <https://owasp.org/www-project-webgoat/>.
- [24] "Undang-undang (UU) Nomor 27 Tahun 2022 Pelindungan Data Pribadi," PeraturanBPK. Accessed: May 20, 2025. [Online]. Available: <https://peraturan.bpk.go.id/Details/229798/uu-no-27->
- [25] "Authorization Cheat Sheet," https://cheatsheetseries.owasp.org/cheatsheets/Authorization_Cheat_Sheet.html#ensure-lookup-ids-are-not-accessible-even-when-guessed-or-cannot-be-tampered-with. Accessed: May 20, 2025. [Online]. Available: https://cheatsheetseries.owasp.org/cheatsheets/Authorization_Cheat_Sheet.html#ensure-lookup-ids-are-not-accessible-even-when-guessed-or-cannot-be-tampered-with

- [26] “A01:2021 – Broken Access Control,” https://owasp.org/Top10/A01_2021-Broken_Access_Control/#how-to-prevent. Accessed: May 20, 2025. [Online]. Available: https://owasp.org/Top10/A01_2021-Broken_Access_Control/#how-to-prevent
- [27] “A02:2021 – Cryptographic Failures,” https://owasp.org/Top10/A02_2021-Cryptographic_Failures/#how-to-prevent. Accessed: May 20, 2025. [Online]. Available: https://owasp.org/Top10/A02_2021-Cryptographic_Failures/#how-to-prevent
- [28] “A04:2021 – Insecure Design.” Accessed: May 20, 2025. [Online]. Available: https://owasp.org/Top10/id/A04_2021-Insecure_Design/#cara-mencegah
- [29] “Error Handling Cheat Sheet,” https://cheatsheetseries.owasp.org/cheatsheets/Error_Handling_Cheat_Sheet.html#sources-of-the-prototype. Accessed: May 20, 2025. [Online]. Available: https://cheatsheetseries.owasp.org/cheatsheets/Error_Handling_Cheat_Sheet.html#sources-of-the-prototype
- [30] “A06:2021 – Vulnerable and Outdated Components,” https://owasp.org/Top10/A06_2021-Vulnerable_and_Outdated_Components/. Accessed: May 20, 2025. [Online]. Available: https://owasp.org/Top10/A06_2021-Vulnerable_and_Outdated_Components/
- [31] “A07:2021 – Identification and Authentication Failures,” https://owasp.org/Top10/A07_2021-Identification_and_Authentication_Failures/. Accessed: May 20, 2025. [Online]. Available: https://owasp.org/Top10/A07_2021-Identification_and_Authentication_Failures/
- [32] “Logging Cheat Sheet,” https://cheatsheetseries.owasp.org/cheatsheets/Logging_Cheat_Sheet.html#operational-use-cases. Accessed: May 20, 2025. [Online]. Available: https://cheatsheetseries.owasp.org/cheatsheets/Logging_Cheat_Sheet.html#operational-use-cases
- [33] Dr. J. Edwards, “Application Security,” in *Mastering Cybersecurity*, Berkeley, CA: Apress, 2024, pp. 139–171. doi: 10.1007/979-8-8688-0297-3_6.