

DAFTAR PUSTAKA

- [1] G. Wawrzyniak and I. E. Fray, "New xml signature scheme that is resistant to some attacks," *IEEE Access*, vol. 8, pp. 35 815–35 831, 2020.
- [2] Wella, "Wawancara mengenai alur submisi dan keamanan dokumen skripsi di umn," *Komunikasi Pribadi (Surel)*, Juni 2025, diakses pada 23 Juni 2025.
- [3] IDEAPERS. (2024, 01) Diduga palsukan tanda tangan, wisuda salah satu mahasiswa afi terancam dibatalkan. Diakses 29 Juni 2025. [Online]. Available: <https://www.ideapers.com/2024/01/diiduga-palsukan-tanda-tangan-wisuda-salah%20Satu%20Mahasiswa-afi-terancam-dibatalkan.html>
- [4] Zoho Corporation, "Pades, cades, and xades — secure esign for eu businesses," <https://www.zoho.com/sign/pades-cades-xades.html>, 2024, diakses pada 23 Juni 2025.
- [5] Wella, "Wawancara mengenai kebutuhan badan standarisasi nasional terhadap pemanfaatan xml terhadap dokumen pdf," *Komunikasi Pribadi*, Juli 2025, diakses pada 1 Juli 2025.
- [6] Forum of Incident Response and Security Teams (FIRST), "Common vulnerability scoring system v4.0: Specification document," <https://www.first.org/cvss/v4-0/specification-document>, 2023, accessed on June 19, 2025.
- [7] F. P. Utama and R. M. H. Nurhadi, "Uncovering the risk of academic information system vulnerability through ptes and owasp method," *CommIT (Communication and Information Technology) Journal*, vol. 18, no. 1, pp. 39–51, April 2024. [Online]. Available: <https://journal.binus.ac.id/index.php/commit/article/view/9384>
- [8] Universitas Multimedia Nusantara, *Panduan Penulisan Tugas Akhir (Tesis)*, Tangerang, 2019.
- [9] Widjaja, Moeljono, "Wawancara mengenai alur submisi dan keamanan dokumen skripsi di umn," *Komunikasi Pribadi (Surel)*, Juni 2025, diakses pada 25 Juni 2025.
- [10] Universitas Multimedia Nusantara, IT Department, *User Guide - Academic - Student*, Universitas Multimedia Nusantara, Tangerang, Indonesia, nov 2023.
- [11] T. Otwell, "Laravel: A php framework for web artisans," Online; accessed 4 August 2025, 2011. [Online]. Available: <https://laravel.com>
- [12] Setasign, "Fpdi: Free pdf document importer," Online; accessed 4 August 2025. [Online]. Available: <https://www.setasign.com/products/fpdi/about/>

- [13] National Institute of Standards and Technology, *Secure Hash Standard (SHS)*, ser. Federal Information Processing Standards Publication. U.S. Department of Commerce, 2015, no. 180-4, standar yang mendefinisikan algoritma SHA, termasuk SHA-256.
- [14] ETSI, “Electronic signatures and infrastructures (esi); xades digital signatures; part 1: Building blocks and xades baseline signatures,” European Telecommunications Standards Institute, Tech. Rep. ETSI EN 319 132-1 V1.2.1, 2022.
- [15] R. S. Pressman, *Software Engineering: A Practitioner’s Approach*, 8th ed. New York, NY: McGraw-Hill Education, 2014.
- [16] Forum of Incident Response and Security Teams (FIRST), “Common vulnerability scoring system v4.0: User guide,” <https://www.first.org/cvss/v4-0/user-guide>, 2023, accessed on June 19, 2025.
- [17] OWASP Foundation, “Owasp top 10:2021,” <https://owasp.org/www-project-top-ten/>, 2021, diakses pada 4 Juli 2025.
- [18] —, “A01:2021 – broken access control,” https://owasp.org/Top10/A01-2021-Broken_Access_Control/, 2021, diakses pada 4 Juli 2025.
- [19] —, “A02:2021 – cryptographic failures,” https://owasp.org/Top10/A02-2021-Cryptographic_Failures/, 2021, diakses pada 4 Juli 2025.
- [20] —, “A03:2021 – injection,” <https://owasp.org/Top10/A03-2021-Injection/>, 2021, diakses pada 4 Juli 2025.
- [21] —, “A04:2021 – insecure design,” https://owasp.org/Top10/A04-2021-Insecure_Design/, 2021, diakses pada 4 Juli 2025.
- [22] —, “A05:2021 – security misconfiguration,” https://owasp.org/Top10/A05-2021-Security_Misconfiguration/, 2021, diakses pada 4 Juli 2025.
- [23] —, “A06:2021 – vulnerable and outdated components,” https://owasp.org/Top10/A06-2021-Vulnerable_and_Outdated_Components/, 2021, diakses pada 4 Juli 2025.
- [24] —, “A07:2021 – identification and authentication failures,” https://owasp.org/Top10/A07-2021-Identification_and_Authentication_Failures/, 2021, diakses pada 4 Juli 2025.
- [25] —, “A08:2021 – software and data integrity failures,” https://owasp.org/Top10/A08-2021-Software_and_Data_Integrity_Failures/, 2021, diakses pada 4 Juli 2025.

- [26] —, “A09:2021 – security logging and monitoring failures,” https://owasp.org/Top10/A09_2021-Security_Logging_and_Monitoring_Failures/, 2021, diakses pada 4 Juli 2025.
- [27] —, “A10:2021 – server-side request forgery (ssrf),” [https://owasp.org/Top10/A10_2021-Server-Side_Request_Forgery_\(SSRF\)/](https://owasp.org/Top10/A10_2021-Server-Side_Request_Forgery_(SSRF)/), 2021, diakses pada 4 Juli 2025.

