

Pelatihan Penerapan Enkripsi pada Source Code dan Database: Meningkatkan Keamanan dalam Pengelolaan Aplikasi Web

*Training on the Implementation of Encryption in Source Code and Databases: Enhancing
Security in Web Application Management*

Ahmad Sahal ^{1*}

Andre Kussuma Adiputra ²

Farida Nur Aini ¹

Indra Listiawan ¹

Rahagi Andhika ¹

¹Department of Information Technology, Faculty of Science and Technology, Respati University Yogyakarta, Indonesia

²Department of Accounting, Faculty of Social and Economic Sciences, Respati University, Yogyakarta, Indonesia

email: ihza_asm@respati.ac.id

Kata Kunci

Keamanan Aplikasi Web

Enkripsi

Pengabdian kepada Masyarakat

Keywords:

Web Application Security

Encryption

Community Service

Received: January 2026

Accepted: March 2026

Published: June 2026

Abstrak

Keamanan aplikasi *web* merupakan aspek penting dalam pengelolaan sistem informasi, terutama untuk melindungi data dari ancaman siber. Salah satu metode yang efektif untuk meningkatkan keamanan adalah penerapan enkripsi pada *source code* dan *database*. Kegiatan pengabdian kepada masyarakat ini bertujuan untuk meningkatkan pemahaman dan keterampilan guru serta siswa jurusan Rekayasa Perangkat Lunak di SMK Ibu Pawaiyatan Tamansiswa Yogyakarta dalam menerapkan teknik enkripsi pada pengembangan aplikasi *web*. Metode pelaksanaan meliputi pelatihan teori, praktik langsung, dan studi kasus yang mencakup penggunaan algoritma enkripsi AES, RSA, serta hashing SHA-256 dengan PHP CodeIgniter 3 dan MySQL. Pemilihan *framework* CodeIgniter 3 didasarkan pada kesesuaiannya dengan kurikulum pembelajaran di sekolah mitra serta kemudahan penggunaannya bagi peserta tingkat pemula. Hasil kegiatan menunjukkan peningkatan yang signifikan, di antaranya pemahaman konsep keamanan aplikasi *web* meningkat dari 45% menjadi 85%, pengetahuan tentang fungsi enkripsi dari 40% menjadi 90%, kemampuan menerapkan enkripsi pada *source code* dari 30% menjadi 80%, serta kemampuan enkripsi *database* dari 25% menjadi 75%. Selain itu, persepsi kesulitan peserta terhadap penerapan keamanan aplikasi *web* menurun dari 70% menjadi 25%. Kegiatan ini menghasilkan modul pelatihan dan dokumentasi teknis yang dapat digunakan sebagai bahan ajar berkelanjutan di lingkungan sekolah. Dengan demikian, pelatihan ini tidak hanya meningkatkan kompetensi peserta, tetapi juga mendukung integrasi praktik keamanan aplikasi *web* dalam proses pembelajaran yang berkelanjutan.

Abstract

Web application security is a critical aspect of information system management, particularly in protecting data from cyber threats. One effective approach to enhancing security is the implementation of encryption in both source code and databases. This community service program aims to improve the knowledge and skills of teachers and students from the Software Engineering department at SMK Ibu Pawaiyatan Tamansiswa Yogyakarta in applying encryption techniques in web application development. The implementation methods include theoretical training, hands-on practice, and case studies covering the use of encryption algorithms such as AES, RSA, and SHA-256 hashing, as well as PHP CodeIgniter 3 and MySQL. The selection of the CodeIgniter 3 framework is based on its alignment with the partner school's curriculum and its ease of use for beginner-level participants. The results of the program indicate significant improvements, including an increase in understanding of web application security concepts from 45% to 85%, knowledge of encryption functions from 40% to 90%, ability to implement encryption in source code from 30% to 80%, and database encryption skills from 25% to 75%. Additionally, participants' perceived difficulty in implementing web application security decreased from 70% to 25%. This program produced training modules and technical documentation that can be utilized as sustainable teaching materials within the school environment. Therefore, the training not only enhances participants' competencies but also supports the integration of web application security practices into a continuous learning process.



© 2026 Ahmad Sahal, Andre Kussuma Adiputra, Farida Nur Aini, Indra Listiawan, Rahagi Andhika. Published by Institute for Research and Community Services Universitas Muhammadiyah Palangkaraya. This is Open Access article under the CC-BY-SA License (<http://creativecommons.org/licenses/by-sa/4.0/>). DOI: <https://doi.org/10.33084/pengabdianmu.v11i6.12055>

PENDAHULUAN

Perkembangan teknologi informasi telah mendorong pemanfaatan aplikasi *web* secara luas di berbagai sektor, termasuk pendidikan, untuk mendukung proses administrasi, pembelajaran, dan pengelolaan data secara digital. Namun, peningkatan penggunaan aplikasi *web* juga diiringi oleh meningkatnya ancaman keamanan siber, khususnya yang berkaitan dengan perlindungan data dan autentikasi pengguna. Laporan OWASP Top 10 terbaru menunjukkan bahwa kerentanan aplikasi *web* masih didominasi oleh kelemahan pada mekanisme autentikasi, perlindungan data sensitif, serta kesalahan konfigurasi keamanan (OWASP Foundation, 2023). Penerapan enkripsi pada *source code* dan *database* merupakan salah satu pendekatan utama dalam meningkatkan keamanan aplikasi *web*. Enkripsi berfungsi untuk melindungi data dari akses tidak sah, baik saat penyimpanan maupun transmisi. Berbagai penelitian menunjukkan bahwa algoritma AES dan RSA mampu memberikan tingkat keamanan yang tinggi dengan dampak performa yang relatif rendah pada sistem berbasis *web* modern (Carvalho *et al.*, 2025; Rahman *et al.*, 2024). Selain itu, penggunaan *hashing* SHA-256 telah terbukti efektif dalam menjaga keamanan data autentikasi pengguna (Rabtsani, 2024). Dengan demikian, integrasi teknik kriptografi dalam pengembangan aplikasi *web* menjadi kebutuhan yang tidak dapat diabaikan. Meskipun demikian, praktik di lapangan menunjukkan bahwa pengembang pemula masih cenderung lebih memprioritaskan fungsionalitas aplikasi dibandingkan aspek keamanan. Kondisi ini juga terjadi di lingkungan pendidikan kejuruan, di mana pembelajaran keamanan aplikasi *web* belum menjadi fokus utama. Beberapa penelitian mengungkapkan bahwa rendahnya literasi keamanan siber di lingkungan pendidikan menyebabkan aplikasi yang dihasilkan rentan terhadap serangan dasar dan pelanggaran privasi data (Putra *et al.*, 2023; Watini *et al.*, 2024). SMK Ibu Pawiyatan Tamansiswa Yogyakarta sebagai salah satu sekolah kejuruan dengan program keahlian Rekayasa Perangkat Lunak telah mengintegrasikan pengembangan aplikasi *web* dalam proses pembelajaran. Namun, berdasarkan hasil observasi awal, pemahaman guru dan siswa terkait penerapan enkripsi pada *source code* dan *database* masih terbatas. Materi keamanan umumnya disampaikan secara teoritis tanpa diikuti praktik langsung, sehingga keterampilan teknis peserta dalam mengamankan aplikasi *web* belum berkembang secara optimal. Berbagai kegiatan pengabdian kepada masyarakat sebelumnya telah mengkaji penerapan kriptografi pada sistem berbasis *web*, seperti pengamanan *login*, dokumen digital, dan basis data. Namun, sebagian besar kegiatan tersebut belum mengintegrasikan pendekatan pembelajaran berbasis praktik secara sistematis dalam kurikulum pendidikan (Naimnule, 2025; Nugraha, 2025; Halimi, 2024). Padahal, pendekatan pelatihan berbasis praktik terbukti lebih efektif dalam meningkatkan kompetensi keamanan aplikasi *web* secara berkelanjutan (Almubarak *et al.*, 2023). Hal ini menunjukkan adanya kesenjangan antara kebutuhan pembelajaran keamanan yang aplikatif dengan implementasi pelatihan yang tersedia. Berdasarkan kesenjangan tersebut, kegiatan pengabdian kepada masyarakat ini bertujuan untuk meningkatkan pemahaman dan keterampilan guru serta siswa jurusan Rekayasa Perangkat Lunak dalam menerapkan teknik enkripsi pada pengembangan aplikasi *web*. Pelatihan difokuskan pada implementasi algoritma enkripsi dan *hashing* menggunakan PHP *CodeIgniter* 3 dan MySQL. Pemilihan *CodeIgniter* 3 didasarkan pada kesesuaiannya dengan kurikulum sekolah mitra, ketersediaan sumber belajar yang luas, serta kemudahan implementasi bagi peserta tingkat pemula, dibandingkan dengan *CodeIgniter* 4 yang memiliki konfigurasi lebih kompleks. Adapun kontribusi (kebaruan) dari kegiatan ini meliputi :

- 1) integrasi pelatihan keamanan aplikasi *web* berbasis praktik dalam lingkungan pendidikan kejuruan,
- 2) penerapan langsung teknik enkripsi pada *source code* dan *database* dalam skenario pembelajaran, serta
- 3) pengembangan modul pelatihan yang dapat digunakan sebagai bahan ajar berkelanjutan. Dengan demikian, kegiatan ini diharapkan tidak hanya meningkatkan kompetensi peserta, tetapi juga mendukung penerapan praktik pengembangan perangkat lunak yang aman secara berkelanjutan di lingkungan pendidikan.

METODE

Waktu, Lokasi, dan Subjek Kegiatan

Kegiatan pengabdian kepada masyarakat ini dilaksanakan pada bulan Oktober hingga November 2025 di SMK Ibu Pawiyatan Tamansiswa Yogyakarta. Pelaksanaan kegiatan dilakukan dalam enam pertemuan terjadwal setiap hari Sabtu,

yaitu pada tanggal 18 Oktober 2025, 25 Oktober 2025, 1 November 2025, 8 November 2025, 15 November 2025, dan 22 November 2025. Setiap pertemuan dilaksanakan dalam dua sesi, yaitu pukul 08.00–10.00 WIB dan 10.30–12.30 WIB, yang mencakup penyampaian materi teori dan praktik secara bertahap dan berkelanjutan. Materi pelatihan disusun secara sistematis mulai dari pengantar keamanan *web*, identifikasi ancaman dan serangan, pemahaman OWASP Top 10, hingga implementasi keamanan lanjutan seperti enkripsi, keamanan API, dan *penetration testing* sederhana. Subjek kegiatan terdiri dari 25 peserta yang meliputi 5 guru dan 20 siswa jurusan Rekayasa Perangkat Lunak. Pemilihan subjek didasarkan pada kebutuhan peningkatan kompetensi keamanan aplikasi *web* di lingkungan pendidikan kejuruan yang berorientasi pada praktik pengembangan perangkat lunak.

Tabel I. Jadwal Pelaksanaan Kegiatan Pelatihan.

No Hari/Tanggal	Waktu	Materi
1 Sabtu, 18 Okt 2025	08.00–10.00	Pengantar Keamanan <i>Web</i>
	10.30–12.30	Jenis Ancaman dan Serangan
2 Sabtu, 25 Okt 2025	08.00–10.00	OWASP Top 10
	10.30–12.30	SQL Injection
3 Sabtu, 1 Nov 2025	08.00–10.00	Cross-Site Scripting (XSS)
	10.30–12.30	Session dan MFA
4 Sabtu, 8 Nov 2025	08.00–10.00	Keamanan <i>Database</i> dan Enkripsi
	10.30–12.30	HTTPS dan Validasi Input
5 Sabtu, 15 Nov 2025	08.00–10.00	Keamanan API dan OAuth 2.0
	10.30–12.30	Eksplorasi API
6 Sabtu, 22 Nov 2025	08.00–10.00	Penetration Testing
	10.30–12.30	Evaluasi dan Studi Kasus

Alat dan Bahan

Pelaksanaan kegiatan memanfaatkan perangkat keras dan perangkat lunak yang mendukung penerapan keamanan aplikasi *web* secara praktis. Perangkat keras yang digunakan meliputi komputer atau *laptop* dengan spesifikasi minimal prosesor *Intel Core i3* atau setara, RAM 8 GB, serta sistem operasi *Windows 10* atau versi yang lebih baru. Spesifikasi ini dipilih untuk memastikan kelancaran proses pengembangan dan pengujian aplikasi *web* terenkripsi, sebagaimana direkomendasikan dalam implementasi keamanan berbasis enkripsi modern (Rahman *et al.*, 2024). Perangkat lunak yang digunakan meliputi *framework PHP CodeIgniter 3* sebagai *platform* pengembangan aplikasi *web*, sistem manajemen basis data MySQL versi 8.x untuk pengelolaan data, serta *web browser* modern untuk pengujian fungsionalitas dan keamanan aplikasi. Bahan pendukung kegiatan berupa modul pelatihan keamanan aplikasi *web*, contoh *source code*, dan dataset uji yang dirancang untuk mendukung proses pembelajaran berbasis praktik. Penerapan keamanan difokuskan pada algoritma *Advanced Encryption Standard* (AES) dengan panjang kunci 256-bit, RSA sebagai mekanisme enkripsi asimetris, serta algoritma *hashing* SHA-256 untuk pengamanan data autentikasi. Ketiga algoritma ini dipilih karena memiliki tingkat keamanan yang tinggi dan telah direkomendasikan dalam praktik pengembangan aplikasi *web* modern (Carvalho *et al.*, 2025; Almubarak *et al.*, 2023).

Metode Pelaksanaan

Metode pelaksanaan kegiatan pengabdian ini dirancang dalam bentuk pelatihan terpadu yang mengombinasikan pendekatan teori dan praktik langsung. Pendekatan ini dipilih karena terbukti efektif dalam meningkatkan kompetensi keamanan aplikasi *web*, khususnya pada lingkungan pendidikan berbasis keterampilan (Putra *et al.*, 2023). Pelaksanaan kegiatan dilakukan secara bertahap dan sistematis agar peserta dapat memahami konsep keamanan aplikasi *web* sekaligus mampu mengimplementasikannya secara langsung. Tahapan pelaksanaan meliputi :

1. Analisis Kebutuhan Mitra

Tahap awal dilakukan melalui koordinasi dengan pihak sekolah untuk mengidentifikasi tingkat pemahaman awal peserta terkait keamanan aplikasi *web*. Analisis ini menjadi dasar dalam penyusunan materi pelatihan agar sesuai dengan kebutuhan dan tingkat kompetensi peserta (Watini *et al.*, 2024).

2. Penyusunan Materi dan Modul Pelatihan

Materi pelatihan disusun mengacu pada praktik terbaik keamanan aplikasi *web*, termasuk OWASP Top 10. Modul dirancang secara sistematis dan aplikatif agar dapat digunakan sebagai bahan ajar berkelanjutan di lingkungan sekolah (OWASP Foundation, 2023).

3. Pelaksanaan Pelatihan Teori

Tahap ini mencakup penyampaian konsep dasar keamanan aplikasi *web*, jenis ancaman siber, serta prinsip enkripsi dan *hashing*. Penyampaian dilakukan secara interaktif untuk memperkuat pemahaman konseptual peserta sebelum praktik (Almubarak *et al.*, 2023).

4. Praktik Penerapan Enkripsi

Peserta melakukan praktik langsung penerapan enkripsi pada *source code* dan *database* menggunakan PHP *CodeIgniter* 3 dan MySQL. Praktik difokuskan pada pengamanan data sensitif dan autentikasi pengguna melalui implementasi AES, RSA, dan *hashing* SHA-256. Pendekatan ini terbukti efektif dalam meningkatkan kemampuan teknis peserta (Rahman *et al.*, 2024; Putra *et al.*, 2023).

5. Evaluasi dan Pendampingan

Evaluasi dilakukan menggunakan metode *pre-test* dan *post-test* untuk mengukur peningkatan pemahaman peserta secara kuantitatif. Selain itu, dilakukan penilaian terhadap hasil praktik untuk mengukur kemampuan implementasi enkripsi.

Pendampingan teknis diberikan selama dan setelah pelatihan untuk membantu peserta mengatasi kendala yang dihadapi, seperti kesalahan konfigurasi enkripsi dan pengelolaan kunci. Pendekatan ini bertujuan memastikan peserta mampu menerapkan konsep keamanan aplikasi *web* secara mandiri dan berkelanjutan.

Teknik Analisis Data

Data diperoleh dari hasil *pre-test* dan *post-test*, observasi selama praktik, serta evaluasi hasil implementasi peserta. Data dianalisis secara deskriptif kuantitatif dengan membandingkan tingkat pemahaman dan keterampilan peserta sebelum dan sesudah pelatihan dalam bentuk persentase. Metode pelaksanaan ini diharapkan mampu meningkatkan kompetensi mitra dalam memahami dan menerapkan keamanan aplikasi *web* secara praktis, serta mendukung penerapan standar pengembangan perangkat lunak yang aman dan relevan dengan kebutuhan industri.

HASIL DAN PEMBAHASAN

Deskripsi Hasil Kegiatan

Kegiatan pengabdian kepada masyarakat berupa pelatihan penerapan enkripsi pada *source code* dan *database* telah dilaksanakan sesuai dengan tahapan yang direncanakan, meliputi koordinasi dengan mitra, penyusunan modul, penyampaian materi teori keamanan aplikasi *web*, praktik penerapan enkripsi, serta evaluasi kegiatan. Peserta terdiri atas guru dan siswa jurusan Rekayasa Perangkat Lunak SMK Ibu Pawaiyatan Tamansiswa Yogyakarta. Pelaksanaan pelatihan dirancang berbasis praktik untuk memastikan peserta memperoleh pemahaman konseptual sekaligus keterampilan teknis secara langsung. Hasil kegiatan menunjukkan peningkatan signifikan pada pemahaman dan keterampilan peserta dalam menerapkan keamanan aplikasi *web*, khususnya pada perlindungan data melalui enkripsi dan *hashing*. Sebelum pelatihan, sebagian besar peserta belum mampu menerapkan enkripsi pada *source code* dan *database* secara praktis serta masih memiliki pemahaman terbatas mengenai konsep keamanan aplikasi *web*. Setelah mengikuti pelatihan, peserta mampu mengimplementasikan enkripsi dasar menggunakan PHP *CodeIgniter* 3 dan MySQL, terutama dalam pengamanan data autentikasi dan data sensitif. Ringkasan peningkatan pemahaman dan keterampilan peserta sebelum dan sesudah pelatihan disajikan pada Tabel 2. Data menunjukkan adanya peningkatan pada seluruh indikator penilaian, dengan rata-rata peningkatan sebesar 40–50%, serta penurunan signifikan pada persepsi tingkat kesulitan penerapan keamanan aplikasi *web*.

Tabel II. Perbandingan Pemahaman dan Kemampuan Peserta Sebelum dan Sesudah Pelatihan Keamanan Aplikasi Web.

Aspek yang Dinilai	Sebelum (%)	Sesudah (%)
Memahami konsep dasar keamanan aplikasi web	45	85
Mengetahui fungsi enkripsi pada aplikasi web	40	90
Mampu menerapkan enkripsi pada source code	30	80
Mampu menerapkan enkripsi pada database	25	75
Memahami penggunaan hashing untuk autentikasi	35	85
Persepsi kesulitan penerapan keamanan web (tinggi)	70	25

Keterangan: Persentase diperoleh dari hasil pre-test, post-test, observasi praktik, dan diskusi selama pelatihan.

Peningkatan capaian tersebut menunjukkan bahwa metode pelatihan yang mengombinasikan teori dan praktik langsung efektif dalam meningkatkan kompetensi keamanan aplikasi web. Hal ini sejalan dengan temuan (Putra *et al.*, 2023) serta (Watini *et al.*, 2024) yang menyatakan bahwa pendekatan pembelajaran berbasis praktik mampu meningkatkan pemahaman konseptual sekaligus keterampilan teknis secara lebih optimal dibandingkan pendekatan teoritis semata. Dengan keterlibatan aktif peserta dalam praktik, proses internalisasi konsep keamanan menjadi lebih mendalam dan aplikatif. Dokumentasi kegiatan pelatihan yang ditampilkan pada Gambar 1 tidak hanya menunjukkan keterlibatan aktif peserta, tetapi juga menggambarkan proses pembelajaran berbasis praktik yang intensif. Selama sesi praktik, peserta dihadapkan pada berbagai kendala teknis, khususnya dalam implementasi algoritma enkripsi AES dan RSA. Kendala yang paling sering ditemui meliputi kesalahan dalam pengelolaan kunci enkripsi, kesulitan dalam mengintegrasikan *library* kriptografi pada *framework* CodeIgniter 3, serta kurangnya pemahaman dalam membedakan antara proses enkripsi dan *hashing*, terutama dalam konteks autentikasi pengguna. Untuk mengatasi kendala tersebut, tim pengabdian memberikan pendampingan teknis secara langsung melalui metode debugging bersama, penyederhanaan contoh kasus, serta penyediaan template kode yang dapat digunakan sebagai acuan. Selain itu, dilakukan penjelasan ulang secara kontekstual mengenai perbedaan fungsi enkripsi dan *hashing* dalam sistem keamanan aplikasi web. Pendekatan ini terbukti mampu mengurangi hambatan teknis peserta serta meningkatkan kepercayaan diri dalam mengimplementasikan keamanan aplikasi web secara mandiri.

**Gambar 1.** Proses Diskusi dan Praktik Pelatihan Penerapan Enkripsi oleh Tim Pengabdian dan Peserta.

Secara komparatif, hasil kegiatan ini memperkuat temuan bahwa pelatihan keamanan *web* berbasis praktik memiliki efektivitas yang lebih tinggi dibandingkan pendekatan konseptual semata. Keunggulan kegiatan ini terletak pada integrasi langsung antara teori dan implementasi enkripsi pada *source code* dan *database* menggunakan *framework* yang umum digunakan dalam pembelajaran. Hal ini menjadikan proses pembelajaran lebih kontekstual, aplikatif, dan berkelanjutan. Temuan ini juga konsisten dengan penelitian sebelumnya yang menunjukkan bahwa algoritma AES-256, RSA, dan SHA-256 mampu memberikan tingkat keamanan yang tinggi tanpa mengganggu performa sistem secara signifikan (Halimi, 2024; Siregar, 2025; Aditya *et al.*, 2025). Selain itu, penerapan keamanan sejak tahap pengembangan awal sejalan dengan prinsip *Secure Software Development Lifecycle* (S-SDLC) yang menjadi kebutuhan utama dalam industri pengembangan perangkat lunak modern (Islam *et al.*, 2025; Anderies *et al.*, 2025). Temuan ini menunjukkan bahwa pendekatan pelatihan berbasis praktik tidak hanya meningkatkan kompetensi teknis, tetapi juga mempercepat kesiapan peserta dalam menghadapi kebutuhan industri berbasis keamanan aplikasi.

KESIMPULAN

Kegiatan pengabdian kepada masyarakat ini memberikan kontribusi nyata dalam penguatan kompetensi keamanan aplikasi *web* di lingkungan SMK Ibu Pawiyatan Tamansiswa Yogyakarta. Selain meningkatkan pemahaman dan keterampilan teknis peserta, kegiatan ini menghasilkan luaran berupa modul pelatihan dan dokumentasi implementasi enkripsi yang dapat dimanfaatkan sebagai bahan ajar berkelanjutan dalam proses pembelajaran. Keberadaan modul tersebut memungkinkan integrasi materi keamanan aplikasi *web* ke dalam kurikulum secara lebih sistematis dan aplikatif, sehingga mendukung pembentukan kompetensi peserta yang selaras dengan kebutuhan industri. Dengan demikian, dampak kegiatan tidak hanya bersifat jangka pendek, tetapi juga berkontribusi terhadap peningkatan kualitas pembelajaran berbasis praktik di lingkungan sekolah mitra. Sebagai pengembangan lanjutan, disarankan adanya perluasan materi ke aspek pengujian keamanan aplikasi *web* (*security testing*) dan keamanan API, serta pendampingan berkelanjutan guna memastikan penerapan keamanan dapat dilakukan secara konsisten dalam pengembangan aplikasi *web* di lingkungan pendidikan. Secara keseluruhan, kegiatan ini menunjukkan peningkatan rata-rata kompetensi peserta sebesar $\pm 45\%$, yang mengindikasikan efektivitas pendekatan pelatihan berbasis praktik dalam pembelajaran keamanan aplikasi *web*.

UCAPAN TERIMA KASIH

Penulis mengucapkan terima kasih kepada LPPM Universitas Respati Yogyakarta atas dukungan pendanaan melalui skema Hibah Internal Pengabdian kepada Masyarakat. Ucapan terima kasih juga disampaikan kepada Fakultas Sains dan Teknologi Universitas Respati Yogyakarta atas dukungan akademik dan fasilitas kegiatan. Apresiasi diberikan kepada SMK Ibu Pawiyatan Tamansiswa Yogyakarta atas kerja sama dan partisipasi aktif selama pelaksanaan pengabdian. Terima kasih disampaikan kepada seluruh tim pengabdian dan narasumber yang telah berkontribusi dalam kegiatan ini. Dukungan seluruh sivitas akademika Universitas Respati Yogyakarta sangat berperan dalam keberhasilan kegiatan pengabdian kepada masyarakat ini.

REFERENSI

- Aditya, F., & Romli, M. A. (2025). Implementasi metode kriptografi AES-256bit untuk pengamanan dokumen digital. *Terapan Informatika Nusantara (TIN)*, 6(6), 707–714. <https://doi.org/10.47065/tin.v6i6.8637>
- Almubarak, A., Alenezi, M., & Khan, S. (2023). Web application security vulnerabilities: A systematic literature review. *Journal of Information Security and Applications*, 73, 103446. <https://doi.org/10.1016/j.jisa.2023.103446>

- Anderies, A., et al. (2025). Systematic literature review on secure software development practices (S-SDLC). *EMACS Journal*, 7(1), 45–58. <https://doi.org/10.1109/ACCESS.2022.3140181>
- Carvalho, M., Sá, F., & Bernardino, J. (2025). Evaluation of the impact of AES encryption on query read performance across relational databases. *Cryptography*, 9(4), 77. <https://doi.org/10.3390/cryptography9040077>
- Halimi, A. (2024). Optimasi keamanan data penerimaan mahasiswa pada sistem MySQL menggunakan algoritma AES-256. *JUSTIFY: Jurnal Sistem dan Teknologi Informasi*, 4(2), 102–113. <https://doi.org/10.35316/justify.v3i1.5107>
- Islam, M. S., & Li, X. (2025). Guardians of the web: The evolution and future of website information security. *arXiv preprint*. <https://arxiv.org/abs/2505.04308>
- Naimnrule, F. A. (2025). Implementation of AES encryption for data security on web-based information systems. *Jurnal Keamanan dan Data Nasional*, 13(1), 15–24. <https://doi.org/10.58982/krisnadana.v4i3.836>
- Nugraha, R. D. (2025). Strengthening web-based login security using dual-layer encryption combining Vigenère and AES. *Jurnal Online Teknologi Informasi*, 14(2), 89–98. <https://doi.org/10.37802/joti.v7i1.954>
- OWASP Foundation. (2023). OWASP Top 10: The ten most critical web application security risks. <https://owasp.org/Top10/>
- Putra, R. A., & Nugroho, Y. (2023). Peningkatan kompetensi keamanan aplikasi web melalui pelatihan berbasis praktik. *Jurnal Teknologi Informasi dan Ilmu Komputer*, 10(3), 457–466. <https://doi.org/10.25126/jtiik.2023.457>
- Rahman, F., et al. (2024). Implementation of AES encryption in web-based information systems. *Procedia Computer Science*, 234, 112–119. <https://doi.org/10.1016/j.procs.2024.01.015>
- Siregar, M. Z. M. (2025). Implementation of security on library system login using a combination of AES and RSA cryptography. *Jurnal Teknologi dan Komunikasi*, 8(1), 30–42. <https://journal.technolabs.co.id/index.php/jotechcom/article/view/74>
- Watini, S., Davies, G., & Andersen, N. (2024). Cybersecurity in learning systems: Data protection and privacy in digital learning platforms. *International Journal on Information Technology & Education Excellence*, 3(1), 665–679. <https://doi.org/10.33050/itee.v3i1.665>