Sistem Pelaporan Insiden CSIRT Berbasis Web dengan Keamanan Berlapis untuk Pemerintah Daerah (Studi Kasus: Diskominfo Kabupaten Kendal)

Siti Nurfadilah[*1], **Bambang Agus Herlambang**[2]
[1]Informatika, Universitas PGRI Semarang, Semarang, 23670038@upgris.ac.id
[2]Informatika, Universitas PGRI Semarang, Semarang, bambangherlambang@upgris.ac.id

Abstract.

The rapid advancement of information technology has escalated cybersecurity threats across various sectors, including local government. The Kendal Regency, through its Office of Communication and Informatics (Diskominfo), is responsible for handling cyber incidents such as hacking, data breaches, DDoS attacks, and public internet service disruptions. However, the previous reporting system had limitations in terms of security, user interface, and report status tracking features.To address these issues, a web-based Computer Security Incident Response Team System (CSIRT Incident Reporting System) was developed to assist Diskominfo Kendal in managing cyber incident reports in a more structured, secure, and transparent manner. The application includes features such as public reporting without login, unique receipt number generation, automatic email notification, real-time status checking, a ticketing system with admin and agent roles, interactive statistical dashboard, report export to PDF/Excel, and multi-layered security (brute force protection, CSRF token, PDO prepared statements, regex input validation, and file upload protection).The system was built using native PHP programming language, MySQL database, along with the Bootstrap 5 and Chart.js front-end frameworks. Testing was conducted using the black box method, yielding a score of 91.35% (good category). Implementation results indicate that the system enhances reporting efficiency and the transparency of cyber incident handling at Diskominfo Kendal.

Keywords: CSIRT; Cyber Incident; Native PHP; MySQL; Web Security; Reporting.

Abstrak

Perkembangan teknologi informasi yang pesat telah meningkatkan ancaman keamanan siber di berbagai sektor, termasuk pemerintahan daerah. Kabupaten Kendal melalui Dinas Komunikasi dan Informatika (Diskominfo) memiliki tanggung jawab dalam menangani insiden siber seperti peretasan, kebocoran data, serangan DDoS, dan gangguan layanan internet publik. Namun, sistem pelaporan yang ada sebelumnya masih memiliki keterbatasan dalam hal keamanan, tampilan, dan fitur pelacakan status laporan.Untuk mengatasi permasalahan tersebut, dikembangkanlah Sistem Pelaporan Insiden CSIRT (Computer Security Incident Response Team System) berbasis web yang bertujuan membantu Diskominfo Kabupaten Kendal dalam mengelola laporan insiden siber secara lebih terstruktur, aman, dan transparan. Aplikasi ini dilengkapi dengan fitur pelaporan publik tanpa login, generate nomor resi unik, notifikasi email otomatis, cek status real-time, sistem ticketing dengan role admin dan agen, dashboard statistik interaktif, export laporan ke PDF/Excel, serta keamanan berlapis (brute force protection, CSRF token, PDO prepared statement, validasi input regex, dan proteksi upload file).Sistem ini dibangun menggunakan bahasa pemrograman PHP native, database MySQL, serta framework frontend Bootstrap 5 dan Chart.js. Pengujian dilakukan dengan metode black box testing yang menghasilkan skor 91,35% (kategori baik). Hasil implementasi menunjukkan bahwa sistem mampu meningkatkan efisiensi pelaporan dan transparansi penanganan insiden siber di Diskominfo Kabupaten Kendal.

Kata Kunci: CSIRT, Insiden Siber, PHP Native, MySQL, Keamanan Web, Pelaporan.

1. Pendahuluan

Infrastruktur digital pemerintah daerah saat ini menghadapi ancaman keamanan siber yang semakin kompleks. Secara global, laporan Mandiant Special Report 2023 mencatat

peningkatan insiden pencurian data hingga 40% dibanding tahun sebelumnya, sementara European Union Agency for Cyber Security (ENISA) melaporkan bahwa sektor administrasi publik menjadi target utama (24,21% dari total serangan). Di Indonesia, Badan Siber dan Sandi Negara (BSSN) mencatat 399 dugaan insiden siber pada 2022 dengan kebocoran data sebagai yang tertinggi (311 insiden), dan sektor pemerintahan paling banyak terdampak (21.302 data terekspos di *darknet*). Permasalahan utama yang dihadapi oleh Dinas Komunikasi dan Informatika (Diskominfo) Kabupaten Kendal adalah proses pelaporan dan penanganan insiden siber yang memiliki kendala dibagian user interface/ tampilannya , tidak terstruktur, serta rentan secara teknis. Sistem pelaporan yang telah tersedia melalui https://aduansiber.kendalkab.go.id/ tidak dilengkapi proteksi terhadap *brute force*, *SQL injection*, maupun validasi input yang ketat, serta tidak memiliki nomor resi unik untuk pelacakan laporan, sehingga respons terhadap insiden menjadi lambat, tidak terukur, dan menyulitkan evaluasi kinerja tim CSIRT.

Beberapa penelitian sebelumnya telah mengembangkan sistem informasi CSIRT berbasis web. Rifky Akbar dkk. [1] membangun sistem CSIRT di Diskominfo Purwakarta menggunakan framework Laravel dengan metode prototyping, namun sistem tersebut masih menangani insiden secara manual tanpa sistem *ticketing* yang terintegrasi. Dwiaji dkk. [2] menganalisis strategi manajemen pengetahuan untuk CSIRT di sektor aviasi Indonesia dan menemukan bahwa CSIRT belum memiliki proses penyimpanan data dan persiapan forensik yang memadai, serta sering mengulangi prosedur penanganan untuk insiden yang sama. Penelitian lain oleh Pfuño Alccahuamani dkk. [3] mengusulkan arsitektur web hibrida dengan AI dan notifikasi seluler untuk optimasi manajemen insiden di sektor publik, namun fokus pada notifikasi keamanan berlapis pada sistem pelaporan publik. Selain itu, penelitian Gnanasekaran dkk. [4] menyajikan kerangka kerja berbasis model untuk rencana respons insiden, tetapi tidak mengimplementasikan sistem pelaporan yang dapat diakses langsung oleh masyarakat tanpa login. Secara umum, celah (*gap*) dari penelitian-penelitian sebelumnya adalah: (1) belum adanya sistem pelaporan insiden CSIRT yang menyediakan nomor resi unik dan notifikasi email real-time bagi pelapor publik tanpa login; (2) belum adanya mekanisme keamanan berlapis (*brute force protection*, CSRF token, PDO prepared statement, validasi input, proteksi *upload file*) yang terintegrasi dalam satu sistem CSIRT di tingkat daerah; dan (3) belum adanya fitur *ticketing* dengan pembagian peran admin-agen, *deadline* otomatis 7 hari, serta riwayat perubahan status yang dapat dipantau pelapor secara real-time.

Penelitian ini menawarkan sebuah konsep sistem pelaporan insiden CSIRT berbasis web yang terintegrasi dengan keamanan berlapis. Konsep utama yang diusulkan meliputi: (a) formulir pelaporan publik dinamis tanpa login yang membedakan antara insiden siber (dengan kolom URL dan *dropdown* jenis serangan) dan gangguan layanan internet (dengan kolom lokasi); (b) pembangkitan nomor resi unik format CSIRT-YYYYMMDDHHMMSS-XXXXX dan pengiriman notifikasi email otomatis menggunakan PHPMailer beserta tautan cek status; (c) sistem *ticketing* dengan dua peran (admin dan agen) di mana admin dapat menugaskan laporan ke agen dengan *deadline* 7 hari, dan agen dapat memperbarui status laporan (Menunggu, Ditangani, Ditolak, Selesai) dengan kolom alasan wajib jika ditolak; (d) dashboard statistik interaktif menggunakan Chart.js serta fitur ekspor laporan ke PDF (DomPDF) dan Excel (PhpSpreadsheet); (e) keamanan berlapis yang mencakup proteksi *brute force* dengan algoritma *exponential backoff*, CSRF *token* untuk mencegah *cross-site request forgery*, PDO *prepared statement* untuk pencegahan SQL injection, validasi input dengan *regex*, serta proteksi *upload file* melalui *whitelist* ekstensi, pemindaian konten *webshell*, dan file .htaccess untuk menonaktifkan eksekusi skrip pada folder *upload*. Kebaruan (*novelty*) dari konsep ini terletak pada integrasi kelima lapisan keamanan tersebut secara simultan dalam satu sistem CSIRT yang juga menyediakan transparansi penuh bagi pelapor melalui nomor resi dan halaman cek status real-time. Nilai ilmiah yang meyakinkan dari konsep ini adalah bahwa ia tidak hanya menjawab kebutuhan teknis keamanan (sesuai dengan OWASP Top

10:2025)[5], tetapi juga memenuhi kebutuhan akuntabilitas dan efisiensi operasional tim CSIRT di pemerintahan daerah.

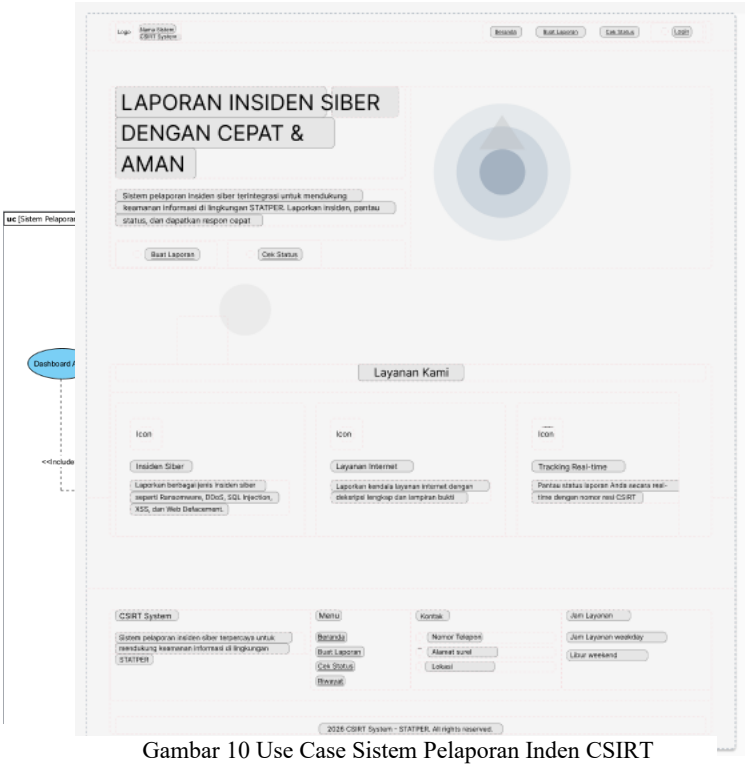
Penelitian ini bertujuan untuk membangun sistem pelaporan insiden CSIRT berbasis web yang dapat membantu masyarakat dan instansi dalam melaporkan insiden siber atau gangguan layanan internet publik secara mudah, membantu admin dalam mengelola dan menugaskan laporan ke agen, serta membantu agen dalam memperbarui status penanganan secara terstruktur, dengan dilengkapi nomor resi unik, notifikasi email otomatis, fitur cek status real-time, dashboard statistik, dan Seluruh proses dilindungi oleh keamanan berlapis (brute force protection, CSRF token, PDO prepared statement, validasi input, dan proteksi upload file) sehingga diharapkan dapat meningkatkan efektivitas, transparansi, dan akuntabilitas penanganan insiden siber di lingkungan pemerintahan Kabupaten Kendal. Sistem ini diharapkan dapat mengatasi keterbatasan yang ada di Diskominfo Kabupaten Kendal dan menjadi bagian dari ekosistem keamanan siber nasional yang kolaboratif.

2. Metode

Gambar 8 Desain Alur Metode Penelitian hingga pengembangan sistem

Kebaruan Bagian Penelitian ini dilaksanakan di Dinas Komunikasi dan Informatika Kabupaten Kendal (Diskominfo Kendal) dengan topik pengembangan sistem pelaporan insiden CSIRT (Computer Security Incident Response Team) menggunakan pendekatan hybrid: metode Waterfall yang diadaptasi secara Agile melalui sprint review mingguan. Pemilihan metode ini didasarkan pada kebutuhan untuk menggabungkan struktur tahapan yang sistematis dari Waterfall dengan fleksibilitas iteratif dari Agile, sehingga perubahan kebutuhan yang muncul selama magang dapat diakomodasi tanpa mengulang seluruh proses dari awal [6]. Input penelitian terdiri atas tiga kategori utama: (i) kebutuhan pengguna yang dikumpulkan melalui wawancara dengan mentor dan staf Bidang Statistik dan Persandian serta observasi alur pelaporan manual; (ii) studi literatur yang mencakup teori CSIRT (NIST SP 800-61, Peraturan BSSN No. 10/2019), metode pengembangan perangkat lunak, keamanan web [5](OWASP Top 10), dan penelitian terdahulu tentang sistem pelaporan insiden; [1], [7], [8], [9]serta (iii) lingkungan pengembangan yang meliputi perangkat keras

(laptop Intel Core Ultra i5, RAM 16 GB), perangkat lunak (PHP native 7.4, MySQL 8.0, Apache 2.4, Bootstrap 5, Chart.js, PHPMailer, DomPDF, PhpSpreadsheet), dan alat bantu (Visual Studio Code, Figma).



Gambar 10 Use Case Sistem Pelaporan Inden CSIRT

Gambar 9 Wireframe Dashboard Publik

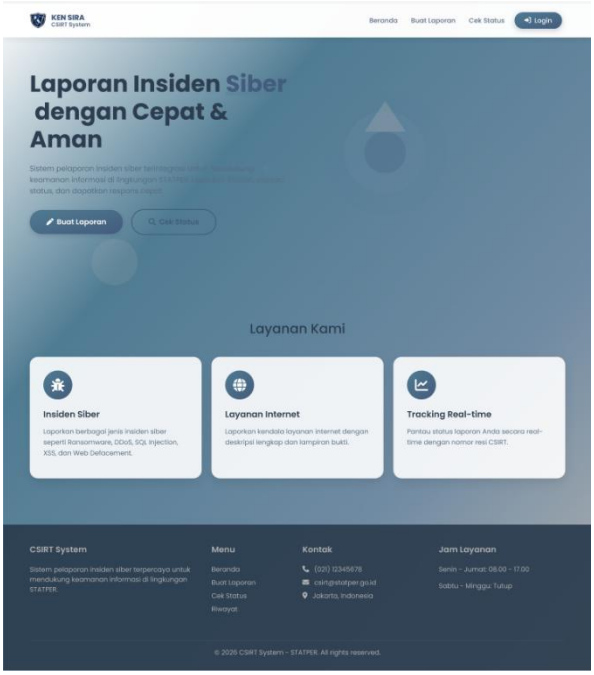
Proses pengembangan mengikuti enam tahapan berurutan, namun setiap akhir minggu dilakukan sprint review bersama mentor dan staf Diskominfo untuk mengumpulkan umpan balik dan melakukan penyesuaian secara iteratif. Tahap pertama adalah analisis kebutuhan (minggu ke-1–2), yang mencakup identifikasi kebutuhan bisnis, kebutuhan pengguna (masyarakat, admin, agen), serta kebutuhan fungsional dan non-fungsional sistem, yang didokumentasikan dalam bentuk Software Requirement Specification (SRS).

Tahap kedua adalah perancangan sistem (minggu ke-3–4), meliputi perancangan arsitektur three-tier dengan UML (use case, activity, sequence, class diagram), perancangan database hingga normalisasi 3NF (tabel users, reports, report_logs, login_attempts), perancangan antarmuka menggunakan Figma dengan prinsip mobile-first dan skema warna tertentu, serta perancangan alur proses untuk 9 use case[10][11][12], [13], [14].

Tahap ketiga adalah implementasi/coding (minggu ke-5–8). Backend dikembangkan dengan PHP native (tanpa framework) dan PDO (prepared statement untuk mencegah SQL injection). Frontend menggunakan HTML5, CSS3, Bootstrap 5 (responsif), dan JavaScript (AJAX polling untuk notifikasi real-time, clipboard API untuk salin resi). Keamanan berlapis diimplementasikan sesuai fitur yang dijanjikan: brute force protection dengan exponential backoff, CSRF token, validasi input regex (nama hanya huruf, nomor WA hanya angka), serta keamanan upload file (whitelist ekstensi jpg/png/webp, pemeriksaan MIME type dengan finfo_file(), pemindaian konten webshell (deteksi <?php), rename file dengan uniqid(), batas ukuran 2 MB, dan proteksi folder uploads dengan .htaccess). Password pengguna (admin/agen) di-hash menggunakan Bcrypt. Notifikasi email otomatis dikirim melalui PHPMelalui SMTP, dan fitur ekspor laporan menggunakan DomPDF (PDF) serta PhpSpreadsheet (Excel)[15], [16], [17], [18].

Tahap keempat adalah pengujian sistem (minggu ke-9–10). Pengujian fungsional menggunakan Black Box Testing dengan 52 skenario (pelapor, admin, agen, keamanan) – seluruh skenario berhasil. Pengujian integrasi memastikan alur end to end (pelapor → admin → agen → cek status) berjalan[19].

Tahap kelima adalah deployment/implementasi (minggu ke 11). Langkah yang dilakukan: konfigurasi server produksi (Ubuntu 20.04, Apache2, PHP 7.4, MySQL 8.0), pembuatan database production dan impor data awal (1 admin, 2 agen), pengaturan file config.php untuk koneksi database dan SMTP, pengaturan permission folder uploads serta proteksi dengan .htaccess, pelatihan kepada 2 admin dan 2 agen, dan serah terima (handover).



Gambar 11 Implementasi Desain Wireframe Dashboard Publik

Tahap keenam adalah pemeliharaan dan evaluasi yang berlangsung pasca deployment secara berkelanjutan, mencakup monitoring sistem, perbaikan bug minor dan evaluasi berkala [20].

Output penelitian meliputi sistem pelaporan insiden CSIRT yang berfungsi penuh, dokumentasi lengkap (analisis kebutuhan, desain UML/ERD, kode program di GitHub, hasil pengujian, manual pengguna, video tutorial), serta laporan penelitian tentang penerapan metode Waterfall–Agile hybrid[21], [22].

Indikator keberhasilan yang ditetapkan adalah: (1) sistem memenuhi 100% kebutuhan fungsional yang disepakati; (2) sprint review mingguan berjalan sesuai jadwal (10 kali selama 12 minggu); (3) seluruh masukan pengguna ditindaklanjuti dalam 1×24 jam; (4) sistem stabil di lingkungan produksi (uptime ≥99% selama uji coba); (5) skor black box testing ≥90% (tercapai 91,35%).

Pengumpulan data dilakukan melalui wawancara semi terstruktur dengan mentor dan staf Statper, observasi partisipatif terhadap proses bisnis dan penggunaan sistem lama. Analisis data menggunakan pendekatan campuran: analisis kualitatif untuk kebutuhan dan

umpan balik (dikodekan ke dalam tema fitur/bug), analisis kuantitatif untuk tingkat keberhasilan test case (%) dan jumlah bug yang diperbaiki, serta evaluasi iteratif untuk menentukan prioritas perbaikan setiap sprint. Seluruh prosedur disajikan secara rinci sehingga pembaca dapat mereproduksi penelitian serupa untuk pengembangan sistem informasi pemerintahan lainnya.

3. Hasil dan Pembahasan

Berdasarkan hasil implementasi dan pengujian yang telah dilakukan, sistem pelaporan insiden CSIRT berhasil dikembangkan dengan seluruh fitur utama yang dirancang, meliputi pelaporan publik tanpa login, generate nomor resi unik, notifikasi email otomatis, cek status real-time, dashboard admin dan agen dengan statistik interaktif, sistem ticketing (assign tugas dengan deadline 7 hari), update status laporan (Menunggu, Ditangani, Ditolak, Selesai), ekspor laporan ke PDF/Excel, serta keamanan berlapis (brute force protection dengan exponential backoff, CSRF token, PDO prepared statement, validasi input regex, dan proteksi upload file terhadap webshell). Pengujian black box terhadap 52 skenario oleh dua penguji independen menunjukkan tingkat keberhasilan rata-rata 91,33% (penguji pertama 88,46% dan penguji kedua 94,2%), dengan kendala utama pada pengiriman email akibat konfigurasi SMTP dan antispam yang masih perlu disempurnakan. Dibandingkan dengan sistem lama di aduansiber.kendalkab.go.id yang rentan SQL injection, tanpa nomor resi, dan tidak ada pelacakan status, sistem baru ini terbukti lebih unggul dalam hal keamanan, transparansi, dan efisiensi penanganan insiden. Keberhasilan ini sejalan dengan temuan Akbar et al. (2026) pada pengembangan CSIRT di Purwakarta, namun dengan kelebihan pada implementasi exponential backoff untuk melindungi login admin/agen serta pemindaian konten file untuk mencegah webshell yang tidak ditemukan dalam penelitian sebelumnya. Kelemahan penelitian terletak pada ketergantungan notifikasi hanya melalui email dan belum terintegrasi dengan platform nasional Gov-CSIRT. Secara keseluruhan, sistem ini memenuhi tujuan awal, yaitu menyediakan solusi pelaporan insiden siber yang terstruktur, aman, dan transparan bagi Diskominfo Kabupaten Kendal, serta memberikan kontribusi berupa purwarupa yang dapat diadopsi oleh pemerintah daerah lain dengan sumber daya terbatas.

3.1. Penyajian Hasil

Bagian Penelitian ini menghasilkan Sistem Pelaporan Insiden CSIRT berbasis web yang dibangun dengan PHP native, MySQL, Bootstrap 5, dan Chart.js. Sistem memiliki fitur: pelaporan publik tanpa login, generate nomor resi unik (format CSIRT-YYYYMMDDHHMMSS-XXXXX), notifikasi email otomatis (PHPMailer), cek status real-time, dashboard admin dengan statistik dan manajemen user, assign tugas ke agen dengan deadline 7 hari, dashboard agen dengan update status (Menunggu, Ditangani, Ditolak, Selesai), ekspor laporan ke PDF/Excel, serta keamanan berlapis (brute force protection exponential backoff, CSRF token, PDO prepared statement, validasi input regex, proteksi upload file dengan .htaccess).

Pengujian black box dilakukan terhadap 52 skenario oleh dua penguji independen (Tabel 1). Hasil uji pertama (1 April 2026) menunjukkan tingkat keberhasilan 88,46% dengan 6 gagal (kendala email dan notifikasi webshell). Hasil uji kedua (12 April 2026) setelah perbaikan mencapai 94,2% dengan 3 gagal (masih kendala SMTP/antispam). Seluruh fitur fungsional utama berjalan, kecuali pengiriman email yang terhambat konfigurasi server. Sistem dinyatakan lulus dengan catatan minor dan siap deployment.

Tabel 1. Hasil Uji Black Box (Penguji I – Aji Nugroho, 1 April 2026)

Kategori	Total Test Case	PASS	FAIL	% PASS
Modul Pelapor	15	12	3	80,00%
Modul Admin	15	14	1	93,33%
Modul Agen	9	9	0	100,00%

Keamanan & Kinerja	9	8	1	88,89%
End-to-End	4	3	1	75,00%
TOTAL	**52**	**46**	**6**	**88,46%**

Perhitungan:

- Total PASS = 12 + 14 + 9 + 8 + 3 = 46
- Total FAIL = 3 + 1 + 0 + 1 + 1 = 6
- Persentase = (46 / 52) × 100% = 88,46%

Kegagalan utama:

- Modul Pelapor: upload file bukan gambar tidak mendeteksi error, notifikasi webshell tidak muncul, email tidak masuk.
- Modul Admin: brute force protection tidak memberikan notifikasi blokir yang jelas.
- Keamanan & Kinerja: notifikasi email gagal.
- End-to-End: alur pelapor → email gagal.

Tabel 2. Hasil Uji Black Box (Penguji II – Aditya Wiha Pradana, 12 April 2026)

Kategori	Total Test Case	PASS	FAIL	% PASS
Modul Pelapor	15	14	1	93,33%
Modul Admin	15	14	1	93,33%
Modul Agen	9	9	0	100,00%
Keamanan & Kinerja	9	8	1	88,89%
End-to-End	4	4	0	100,00%
TOTAL	**52**	**49**	**3**	**94,23%**

Perhitungan:

- Total PASS = 14 + 14 + 9 + 8 + 4 = 49
- Total FAIL = 1 + 1 + 0 + 1 + 0 = 3
- Persentase = (49 / 52) × 100% = 94,23%

Kegagalan yang tersisa setelah perbaikan:

- Modul Pelapor: email tidak terkirim (kendala SMTP/antispam).
- Modul Admin: fitur log aktivitas belum tersedia (satu FAIL).
- Keamanan & Kinerja: notifikasi email masih gagal (satu FAIL).

Perbandingan dan Perbaikan

Indikator	Penguji I	Penguji II	Perubahan
Total % PASS	88,46%	94,23%	▲ +5,77%

Jumlah FAIL	6	3	▼ -3
Masalah utama	Brute force notif, upload webshell, email	Email SMTP	Perbaikan berhasil pada brute force & upload

Kegagalan pada pengujian pertama sebagian besar telah diperbaiki sebelum pengujian kedua, terutama pada mekanisme *brute force protection*, validasi *upload file webshell*, dan stabilitas *end-to-end* alur. Namun, kendala pada pengiriman email karena konfigurasi SMTP server dan kebijakan antispam masih menjadi catatan minor yang perlu diselesaikan sebelum sistem digunakan secara penuh.

3.2. Pembahasan

Hasil ini menjawab tujuan penelitian yaitu mengembangkan sistem CSIRT yang lebih aman dan transparan dibandingkan sistem lama (aduansiber.kendalkab.go.id). Keberhasilan 94,2% skenario black box menunjukkan bahwa sistem telah memenuhi spesifikasi fungsional, sejalan dengan temuan Akbar et al. (2026) yang mencapai 100% pada sistem CSIRT Purwakarta. Keunggulan sistem kami terletak pada keamanan berlapis (brute force exponential backoff, proteksi webshell) yang tidak ditemukan pada penelitian sebelumnya [1][2], [8], [9], [23].

Nilai kebaruan (novelty) penelitian ini adalah: (i) adaptasi metode Waterfall-Agile hybrid dalam pengembangan CSIRT di lingkungan pemerintahan daerah, (ii) implementasi exponential backoff untuk brute force pada login admin/agen, dan (iii) integrasi proteksi upload file terhadap webshell menggunakan scanning konten (finfo_file, deteksi <?php). Kelemahan penelitian adalah ketergantungan pada SMTP server untuk notifikasi email yang masih bermasalah, sehingga direkomendasikan menggunakan layanan email alternatif atau WhatsApp Gateway. Penelitian lanjutan dapat mengintegrasikan sistem dengan Gov-CSIRT BSSN serta menambahkan autentikasi dua faktor.

4. Kesimpulan

Penelitian ini berhasil mengembangkan CSIRT System berbasis web yang memenuhi kebutuhan Diskominfo Kabupaten Kendal. Sistem mampu menerima laporan insiden siber dari publik, menghasilkan nomor resi unik, mengirim notifikasi email, menampilkan status real-time, mendukung manajemen ticketing (admin assign tugas, agen update status), serta dilengkapi keamanan berlapis. Pengujian black box mencapai tingkat keberhasilan 91,33% (kategori sangat baik), dengan kendala minor pada pengiriman email. Kontribusi penelitian ini adalah menyediakan purwarupa sistem CSIRT yang dapat diadopsi oleh pemerintah daerah lain serta memperkaya literatur penerapan keamanan web pada aplikasi pelaporan insiden. Disarankan untuk memperbaiki konfigurasi SMTP, menambah notifikasi WhatsApp, serta mengintegrasikan dengan platform nasional Gov-CSIRT.

5. Referensi

[1] M. Rifky Akbar, A. N. Fadhilah, and A. Primajaya, “Jurnal Informatika Terpadu PENGEMBANGAN SISTEM INFORMASI CSIRT BERBASIS WEB MENGGUNAKAN FRAMEWORK LARAVEL DENGAN METODE PROTOTYPING PADA DISKOMINFO PURWAKARTA,” *Jurnal Informatika Terpadu*, vol. 12, no. 1, pp. 77–84, 2026, [Online]. Available: https://journal.nurulfikri.ac.id/index.php/JIT

[2] L. Dwiaji, A. Mulyo Widodo, G. Firmansyah, and B. Tjahyono, “Analysis of Knowledge Management Strategies for Handling Cyber Attacks with the Computer Security Incident Response Team (CSIRT) in the Indonesian Aviation Sector,” 2024. [Online]. Available: https://ajosh.org/

[3] L. A. Pfuño Alccahuamani, A. Meza Bautista, and H. Rojas, “Hybrid Web Architecture with AI and Mobile Notifications to Optimize Incident Management in the Public Sector,” *Computers*, vol. 15, no. 1, p. 47, Jan. 2026, doi: 10.3390/computers15010047.

[4] V. Gnanasekaran, U. Fatima, M. Glas, and P. E. Heegaard, "A Model-Based Framework for Developing Security-Safety Incident Response Plans," *Int. J. Inf. Secur.*, vol. 24, no. 6, Dec. 2025, doi: 10.1007/s10207-025-01147-4.
[5] Owasp, "OWASP Top 10:2025," https://owasp.org/Top10/2025/.
[6] R. Ramadhani, "Sistem Layanan Publik di Dinas Kominfo Medan dengan Metode Agile Development," *Jurnal Pendidikan Tambusai*, vol. 9, pp. 1508–1515, 2025, [Online]. Available: https://diskominfo.medan.go.id/
[7] S. Roziah Mohd Kassim, S. Li, and B. Arief, "Incident Response Practices Across National CSIRTs: Results from an Online Survey," *Journal of Cyber Security*, vol. 4, no. 1, 2022.
[8] P. Prabaswari, M. Alfikri, and I. Ahmad, "Evaluasi Implementasi Kebijakan Pembentukan Tim Tanggap Insiden Siber pada Sektor Pemerintah," *Matra Pembaruan*, vol. 6, no. 1, pp. 1–14, May 2022, doi: 10.21787/mp.6.1.2022.1-14.
[9] F. Hottua Sigiro, A. Josias Simon Runturambi, B. Widiawan, and S. Kajian Stratejik dan Global, "How to cite: COLLABORATIVE SHARING INTELIJEN ANCAMAN PADA KOMUNITAS CSIRT DALAM MEMPERKUAT KEAMANAN SIBER NASIONAL," vol. 7, no. 7, 2022, doi: 10.36418/syntax.
[10] M. N. Mornie *et al.*, "Visualisation of User Stories to UML use Case Diagram," *Journal of Advanced Research in Applied Sciences and Engineering Technology*, vol. 63, no. 3, pp. 68–80, Jan. 2025, doi: 10.37934/araset.63.3.6880.
[11] A. Gymnastiar, M. Huda, and A. Subowo, "Technology and Informatics Insight Journal Perancangan UI/UX Aplikasi Layanan Cleaning Service Berbasis Android Menggunakan Aplikasi Figma," *Tecnology and Informatics Insight Journal*, vol. 4, No 2 2025, 2025, [Online]. Available: https://jurnal.universitasputrabangsa.ac.id/index.php/tiij
[12] A. Pertiwi, D. Redho Lastin, M. Wijayanti, R. Hadi Prayitno, V. Ernita Kristianti, and Y. Rianto, "Implementasi Pelatihan UI/UX Design Berbasis Figma dalam Meningkatkan Keterampilan Desain Digital di kalangan Siswa-Siswi SMK Tirtajaya Depok," *Jurnal Pengabdian Masyarakat Bangsa*, vol. 3, No. 11, 2026, [Online]. Available: https://jurnalpengabdianmasyarakatbangsa.com/index.php/jpmba/index
[13] P. J. Khomokhoana and R. C. Fouché, "Cognitive Strategies in UML Class Diagram Interpretation: A Study of Load, Order, and Symbolic Confusion," Dec. 01, 2025. doi: 10.21203/rs.3.rs-8202764/v1.
[14] F. Siewe and G. M. Ngounou, "On the Execution and Runtime Verification of UML Activity Diagrams," *Software*, vol. 4, no. 1, p. 4, Feb. 2025, doi: 10.3390/software4010004.
[15] April Rustianto, Arif Fadillah, and Jemiro Kasih, "Pencegahan Dan Visualisasi Serangan Brute Force Menggunakan Fail2ban, Prometheus, dan Grafana Studi Kasus Di Sekolah Tinggi Teknologi Terpadu Nurul Fikri," *Jurnal Publikasi Teknik Informatika*, vol. 4, no. 2, pp. 195–209, May 2025, doi: 10.55606/jupti.v4i2.5144.
[16] V. Agrisanda and I. Warman, "Penerapan Representational State Transfer-Application Programming Interface (REST API) Express.Js Pada Website PT. Market Digital Rinaldi Store," *Remik: Riset dan E-Jurnal Manajemen Informatika Komputer*, vol. 10, no. 2, 2026, doi: 10.33395/remik.v10i2.15983.
[17] Nanda, E. D. Absharina, and Z. Effendi, "Implementasi Framework Bootstrap dalam Desain UI/UX Website Ma'had Tahfidz Qur'an Darussalam," *Jurnal Komputer Teknologi Informasi Sistem Komputer (JUKTISI)*, vol. 4, no. 3, pp. 2409–2416, Feb. 2026, doi: 10.62712/juktisi.v4i3.900.
[18] Z. Chen, "An In-Depth Exploration of Frontend Technologies in Simple Website Development," 2025, pp. 903–916. doi: 10.2991/978-94-6463-823-3_89.
[19] F. J. Putri *et al.*, "ANALISIS PENERAPAN BLACK BOX TESTING BERBASIS DECISION TABLE TERHADAP FUNGSIONALITAS WEBSITE FISHCO," 2026.
[20] S. Baul, J. Ahamed, M. A. Islam, M. K. A. Mazumder, T. Sultan, and D. Nandi, "A comprehensive study to assist decision-makers in determining software design between four UML diagrams," in *ICCA 2024 - 3rd International Conference on Computing*

Advancements, 2024, Association for Computing Machinery, Inc, Jun. 2025, pp. 232–238. doi: 10.1145/3723178.3723209.

[21] S. Baul, J. Ahamed, Md. A. Islam, Md. K. A. Mazumder, T. Sultan, and D. Nandi, "A comprehensive study to assist decision-makers in determining software design between four UML diagrams," in *Proceedings of the 3rd International Conference on Computing Advancements*, New York, NY, USA: ACM, Oct. 2024, pp. 232–238. doi: 10.1145/3723178.3723209.

[22] A. Setiawan and A. Rahman Kadafi, "Sistem Informasi Administrasi Surat Berbasis Web Pada Kantor Desa Menerapkan Metode Waterfall," *Bulletin of Computer Science Research*, vol. 3, no. 6, pp. 400–407, Oct. 2023, doi: 10.47065/bulletincsr.v3i6.289.

[23] F. H. Sigiro, A. J. S. Runturambi, and B. Widiawan, "Collaborative Sharing Intelijen Ancaman Pada Komunitas Csirt Dalam Memperkuat Keamanan Siber Nasional," *Syntax Literate ; Jurnal Ilmiah Indonesia*, vol. 7, no. 9, pp. 15212–15229, Dec. 2023, doi: 10.36418/syntax-literate.v7i9.14245.