Jurnal Informatika Terpadu

https://journal.nurulfikri.ac.id/index.php/JIT
ISSN ONLINE : 2460-8998

PENGEMBANGAN SISTEM INFORMASI CSIRT BERBASIS WEB MENGGUNAKAN *FRAMEWORK LARAVEL* DENGAN METODE *PROTOTYPING* PADA DISKOMINFO PURWAKARTA

Muhammad Rifky Akbar[1], Aidah Nur Fadhilah[2], Aji Primajaya[3]

[1,3] Informatika, Universitas Singaperbangsa Karawang
[2]Manajemen, Universitas Islam Dr. KHEZ Muttaqien
[1,3]Karawang, Jawa Barat, Indonesia 41361
[2]Purwakarta, Jawa Barat, Indonesia 41111
2210631170088@student.unsika.ac.id, aidahnurf012@gmail.com, aji.primajaya@staff.unsika.ac.id

Abstract

The increasing threat of cybersecurity attacks on regional government infrastructure requires a structured incident handling mechanism. However, cybersecurity incident handling at the Diskominfo of Purwakarta Regency is still conducted manually, resulting in slow responses and unstructured documentation. Previous studies discuss policies for CSIRT formation and Laravel-based system security, but none have developed a web-based CSIRT information system for the operational needs of incident response teams at the regional government level. This study aims to develop a web-based CSIRT (Computer Security Incident Response Team) information system using the prototyping method at the Diskominfo of Purwakarta Regency. The development process includes the stages of requirements analysis, design, prototyping, customer evaluation, review and refinement, development, testing, and release. Data collection is conducted through observation, interviews, and literature study. Testing uses Black Box Testing across 12 scenarios covering authentication, incident ticket management, incident reporting, security vulnerability notification letters, and report recapitulation, achieving a 100% success rate. It is concluded that this system can improve the effectiveness of cybersecurity incident handling through structured documentation and integrated report management. It is recommended that the system be integrated with the BSSN reporting system and developed as a mobile application.

Keywords: *Black Box Testing, CSIRT, Cyber Security, Information System, Prototyping*

Abstrak

Meningkatnya ancaman keamanan siber terhadap infrastruktur pemerintah daerah menuntut mekanisme penanganan insiden yang terstruktur. Namun, penanganan insiden siber di Diskominfo Kabupaten Purwakarta masih dilakukan secara manual, menyebabkan respons lambat dan dokumentasi tidak terstruktur. Penelitian terdahulu membahas kebijakan pembentukan CSIRT dan keamanan sistem berbasis Laravel, namun belum ada yang mengembangkan sistem informasi CSIRT berbasis web untuk operasional tim tanggap insiden di tingkat pemerintah daerah. Penelitian ini bertujuan mengembangkan sistem informasi CSIRT (*Computer Security Incident Response Team*) berbasis web menggunakan metode *prototyping* pada Diskominfo Kabupaten Purwakarta. Pengembangan melalui tahapan re*quirements analysis, design, prototyping, customer evaluation, review and refine, develop, test*, dan *release*. Pengumpulan data melalui observasi, wawancara, dan studi pustaka. Pengujian menggunakan *Black Box Testing* terhadap 12 skenario mencakup autentikasi, manajemen tiket insiden, pelaporan insiden, surat pemberitahuan celah keamanan, dan rekap laporan menunjukkan keberhasilan 100%. Disimpulkan bahwa sistem ini mampu meningkatkan efektivitas penanganan insiden keamanan siber melalui dokumentasi terstruktur dan pengelolaan laporan terintegrasi. Direkomendasikan agar sistem diintegrasikan dengan sistem pelaporan BSSN serta dikembangkan dalam bentuk aplikasi *mobile*.

Kata kunci: *Black Box Testing*, CSIRT, Keamanan Siber, Sistem Informasi, *Prototyping*

1. PENDAHULUAN

Transformasi digital yang berlangsung pesat dalam tata kelola pemerintahan di Indonesia telah membawa dampak signifikan terhadap peningkatan ancaman keamanan siber [1]. Sepanjang tahun 2024, jumlah serangan siber yang tercatat di Indonesia mencapai ratusan juta insiden dan

Diterima 30 Januari 2026, Direvisi 23 Februari 2026, Diterima untuk publikasi 15 April 2026

menunjukkan peningkatan dibandingkan tahun sebelumnya[2]. Serangan *malware* mengalami kenaikan yang cukup tajam, seiring dengan semakin kompleksnya pola dan metode serangan yang digunakan oleh pelaku kejahatan siber. Kondisi ini menempatkan Indonesia sebagai salah satu negara yang paling sering menjadi sasaran serangan siber secara global.

Pemerintah daerah sebagai bagian integral dari penyelenggaraan *e-government* tidak luput dari ancaman serangan siber tersebut [3]. Berbagai layanan dan aplikasi pemerintahan yang diuji menunjukkan masih ditemukannya ribuan kerentanan keamanan, termasuk kerentanan dengan tingkat risiko tinggi dan kritis. Jenis serangan yang menjadi ancaman utama *meliputi ransomware, phishing, Distributed Denial of Service* (DDoS), *web defacement*, serta *Advanced Persistent Threat* (APT) [4] yang secara khusus menargetkan infrastruktur penting nasional dan lembaga pemerintahan.

Sebagai respons terhadap meningkatnya ancaman keamanan siber, pemerintah membentuk *Government Computer Security Incident Response Team* (Gov-CSIRT) [5] Indonesia sebagai tim tanggap insiden siber sektor pemerintah yang mewadahi seluruh instansi pemerintah pusat dan daerah. Pembentukan CSIRT di tingkat daerah juga diamanatkan melalui berbagai regulasi nasional yang mengatur perlindungan infrastruktur informasi vital dan penanganan insiden siber [6]. Hingga tahun 2024, jumlah tim tanggap insiden siber yang terbentuk di tingkat nasional dan daerah telah melampaui target yang ditetapkan dalam rencana pembangunan nasional.

Dinas Komunikasi dan Informatika (Diskominfo) Kabupaten Purwakarta sebagai salah satu Organisasi Perangkat Daerah (OPD) yang mengemban fungsi pengelolaan teknologi informasi dan komunikasi menghadapi tantangan dalam menangani pelaporan dan pengelolaan insiden keamanan siber di lingkungan pemerintah daerah. Proses penanganan insiden yang masih dilakukan secara manual menyebabkan dokumentasi yang kurang terstruktur, respons insiden yang relatif lambat [7], serta kesulitan dalam melakukan pelacakan dan analisis pola serangan secara komprehensif. Berdasarkan observasi lapangan, Diskominfo Kabupaten Purwakarta belum memiliki sistem informasi terintegrasi yang dapat mendukung operasional tim CSIRT dalam menerima, memproses, dan menindaklanjuti laporan insiden keamanan siber dari berbagai OPD.

Beberapa penelitian membahas implementasi kebijakan pembentukan CSIRT di Kementerian Perdagangan dengan pendekatan kualitatif [8]. Sementara itu, penelitian tentang peningkatan keamanan sistem informasi berbasis Laravel dengan Rate Limiting dan *Role-Based Access Control* (RBAC) juga telah dilakukan untuk memperkuat keamanan sistem dari serangan siber [9]. Namun demikian, belum terdapat penelitian yang secara khusus mengembangkan sistem informasi CSIRT berbasis web menggunakan *framework* Laravel dengan metode *prototyping* untuk mendukung operasional tim tanggap insiden siber di tingkat pemerintah daerah. Pemilihan metode *prototyping* didasarkan pada keunggulannya dalam melibatkan pengguna secara aktif sejak tahap awal pengembangan, sehingga umpan balik dapat diperoleh lebih cepat dan risiko ketidaksesuaian sistem dengan kebutuhan pengguna dapat diminimalkan. Selain itu, metode ini memungkinkan perubahan kebutuhan diakomodasi secara fleksibel melalui proses iterasi tanpa perlu mengulang seluruh tahapan dari awal, sehingga lebih efisien dibandingkan dengan model sekuensial seperti Waterfall.

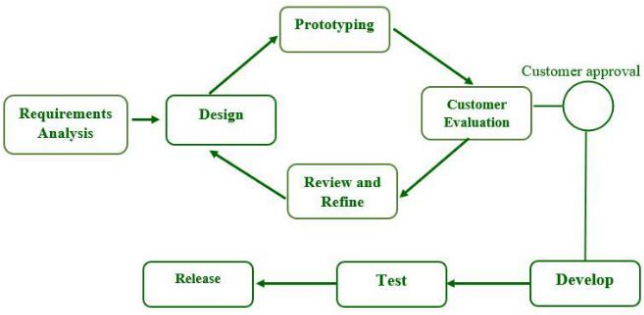
Sistem yang dikembangkan mencakup beberapa fitur utama, yaitu: (1) sistem tiket pelaporan insiden keamanan siber dengan klasifikasi tingkat keparahan; (2) manajemen surat pemberitahuan celah keamanan dengan fitur pembuatan dokumen PDF secara otomatis; (3) *dashboard* rekapitulasi dan statistik insiden keamanan siber; serta (4) sistem notifikasi melalui email kepada administrator. Diharapkan sistem ini dapat meningkatkan efektivitas dan efisiensi penanganan insiden keamanan siber di lingkungan Pemerintah Kabupaten Purwakarta.

Batasan masalah dalam penelitian ini meliputi: (1) sistem dikembangkan untuk lingkungan internal Diskominfo Kabupaten Purwakarta; (2) pengujian sistem dilakukan menggunakan metode *Black Box Testing.*

2. METODE PENELITIAN

2.1 Tahapan Penelitian

Penelitian ini menggunakan metode *Software Development Life Cycle* (SDLC) model *Prototyping*. Model ini dipilih karena memungkinkan pengembangan sistem secara iteratif dengan melibatkan partisipasi aktif pengguna dalam mengevaluasi setiap prototipe yang dibangun [10]. Tahapan model *Prototyping* ditunjukkan pada Gambar 1.



Gambar 1. SDLC Model Prototipe

a) *Requirements Analysis* (Analisis Kebutuhan)

Tahap pertama dalam model *prototyping* adalah analisis kebutuhan [11]. Pada tahap ini dilakukan identifikasi kebutuhan sistem melalui observasi langsung terhadap proses penanganan insiden keamanan siber yang berjalan di

Diskominfo Kabupaten Purwakarta, wawancara dengan Kepala Bidang Persandian dan Keamanan Informasi serta staf Tim CSIRT, dan studi pustaka mengenai sistem informasi CSIRT serta regulasi keamanan siber. Hasil dari tahap ini adalah dokumen spesifikasi kebutuhan yang memuat kebutuhan fungsional dan non-fungsional sistem.

b) *Design* (Perancangan)

Pada tahap ini dilakukan perancangan sistem berdasarkan kebutuhan yang telah diidentifikasi. Perancangan meliputi *Use Case Diagram* untuk menggambarkan interaksi aktor dengan sistem, *Activity Diagram* untuk menggambarkan alur proses [12] pelaporan insiden, *Entity Relationship Diagram* (ERD) untuk merancang struktur basis data, serta perancangan antarmuka pengguna (*User Interface*) [13].

c) *Prototyping* (Pembuatan Prototipe)

Tahap ini dilakukan pembangunan prototipe awal sistem menggunakan *framework* Laravel 8, bahasa pemrograman PHP 8.0, Bootstrap 5 untuk *front-end*, dan MySQL 8.0 sebagai basis data [14]. Prototipe dibangun dengan mengimplementasikan fitur-fitur inti sistem seperti modul pelaporan insiden keamanan siber, manajemen tiket, dan surat pemberitahuan celah keamanan.

d) *Customer Evaluation* (Evaluasi Pengguna)

Prototipe yang telah dibangun diserahkan kepada pengguna yaitu tim CSIRT Diskominfo Kabupaten Purwakarta untuk dievaluasi. Evaluasi dilakukan untuk memastikan kesesuaian sistem dengan kebutuhan operasional [15], kemudahan penggunaan antarmuka, serta kelengkapan fitur yang dibutuhkan.

e) *Customer Approval* (Persetujuan Pengguna)

Pada tahap ini pengguna memberikan keputusan apakah prototipe sudah sesuai dengan kebutuhan atau belum [16]. Jika pengguna menyetujui prototipe, maka proses dilanjutkan ke tahap *Develop*. Jika tidak disetujui, maka proses kembali ke tahap *Review and Refine* untuk dilakukan perbaikan [17].

f) *Review and Refine* (Tinjauan dan Perbaikan)

Tahap ini dilakukan jika terdapat masukan atau revisi dari pengguna terhadap prototipe [18]. Perbaikan dilakukan sesuai dengan umpan balik yang diberikan, kemudian proses kembali ke tahap *Design* untuk memperbaiki perancangan dan membangun prototipe baru. Proses iterasi ini berlangsung hingga pengguna menyetujui prototipe yang dikembangkan.

g) *Develop* (Pengembangan)

Setelah prototipe disetujui oleh pengguna, tahap selanjutnya adalah pengembangan sistem secara lengkap [19]. Pada tahap ini dilakukan implementasi seluruh fitur sistem secara utuh, optimasi kode program dan basis data, penerapan fitur keamanan seperti *CSRF protection*, validasi *input*, dan enkripsi *password*, serta integrasi seluruh modul sistem.

h) *Test* (Pengujian)

Pengujian sistem dilakukan menggunakan metode *Black Box Testing* untuk memvalidasi fungsionalitas sistem [20]. Pengujian difokuskan pada validasi *input* pada formulir, proses *CRUD* (*Create, Read, Update, Delete*) pada setiap modul, fungsionalitas *generate* PDF, sistem autentikasi dan otorisasi pengguna, serta notifikasi *email* kepada administrator.

i) *Release* (Rilis)

Tahap akhir adalah rilis atau *deployment* sistem ke lingkungan produksi. Sistem yang telah lolos pengujian di-*deploy* ke web *hosting* agar dapat diakses oleh pengguna. Dokumentasi sistem juga disusun pada tahap ini sebagai panduan penggunaan bagi tim CSIRT Diskominfo Kabupaten Purwakarta.

3. HASIL DAN PEMBAHASAN

3.1 Hasil Analisis Kebutuhan

Bagian ini menjelaskan tentang data-data hasil penelitian dan pembahasan yang memiliki hubungan logis dan memiliki fokus pada kesimpulan. Bagian ini juga dapat diperkuat dengan sajian tabel/gambar/skema yang harus Berdasarkan tahap *Requirements Analysis*, diperoleh kebutuhan sistem sebagai berikut.

a) Kebutuhan Fungsional

Berdasarkan hasil wawancara dengan Kepala Bidang Persandian dan Keamanan Informasi serta observasi langsung terhadap alur kerja penanganan insiden siber, diidentifikasi tujuh kebutuhan fungsional utama yang harus dipenuhi oleh sistem. Kebutuhan fungsional ini mencakup seluruh proses bisnis inti operasional tim CSIRT, mulai dari pengelolaan pengguna dengan tiga level hak akses (*Super Admin*, *Admin*, dan *User*) [21], penerimaan dan pengelolaan laporan insiden siber dengan klasifikasi tingkat keparahan (*severity level*), manajemen tiket pengaduan dengan alur status yang terstruktur (*New*, *Assigned*, *In Progress*, *Resolved*, dan *Closed*), hingga pembuatan surat pemberitahuan celah keamanan secara otomatis dalam format PDF. Selain itu, sistem juga harus mampu menyajikan *dashboard* rekapitulasi dan statistik insiden, mengirimkan notifikasi melalui *email* kepada administrator, serta mengelola konten *website* seperti berita, panduan, dan layanan. Rincian kebutuhan fungsional sistem disajikan pada Tabel 1.

Tabel 1. Kebutuhan Fungsional

No	Kebutuhan Fungsional	Keterangan
1	Sistem dapat mengelola data pengguna	Terdapat tiga level pengguna, yaitu *Super Admin*, *Admin*, dan *User*

No	Kebutuhan Fungsional	Keterangan
2	Sistem dapat menerima laporan insiden siber	Menyediakan formulir pelaporan dengan klasifikasi jenis insiden dan tingkat keparahan (*severity level*)
3	Sistem dapat mengelola tiket pengaduan	Manajemen tiket dengan status *New*, *Assigned*, *In Progress*, *Resolved*, dan *Closed*
4	Sistem dapat membuat surat pemberitahuan celah keamanan	Sistem mampu melakukan *auto-generate* dokumen PDF menggunakan *template* resmi
5	Sistem dapat menampilkan rekap dan statistik	Menampilkan *dashboard* rekapitulasi laporan insiden dan tiket
6	Sistem dapat mengirim notifikasi email	Mengirimkan notifikasi otomatis melalui *email* kepada administrator
7	Sistem dapat mengelola konten *website*	Manajemen konten berupa berita, panduan, layanan, dan *file*

b) Kebutuhan Non-Fungsional

Selain kebutuhan fungsional, diidentifikasi pula kebutuhan non-fungsional yang menjadi standar kualitas sistem yang dikembangkan. Kebutuhan non-fungsional berperan penting dalam menjamin aspek keamanan, kenyamanan penggunaan, kinerja, dan kompatibilitas sistem agar dapat dioperasikan secara optimal oleh tim CSIRT. Dari sisi keamanan, sistem menerapkan proteksi *Cross-Site Request Forgery* (CSRF) [22], validasi *input* pada setiap formulir, serta enkripsi *password* untuk melindungi data pengguna. Dari sisi *usability*, antarmuka dirancang agar mudah digunakan dan responsif sehingga dapat diakses melalui berbagai ukuran layar. Sistem juga ditargetkan memiliki *response time* kurang dari tiga detik untuk memastikan performa yang memadai, serta kompatibel dengan berbagai *browser* modern. Rincian kebutuhan non-fungsional sistem disajikan pada Tabel 2.

Tabel 2. Kebutuhan Non-Fungsional

No	Kebutuhan Non-Fungsional	Keterangan
1	Keamanan	Proteksi CSRF, validasi *input*, enkripsi *password*
2	*Usability*	Antarmuka yang mudah digunakan dan responsif
3	Performa	*Response time* kurang dari 3 detik
4	Kompatibilitas	Dapat diakses melalui berbagai browser

3.2 Hasil Perancangan Sistem

1) *Use Case Diagram*

Gambar 2. *Use Case Diagram* Sistem Informasi CSIRT

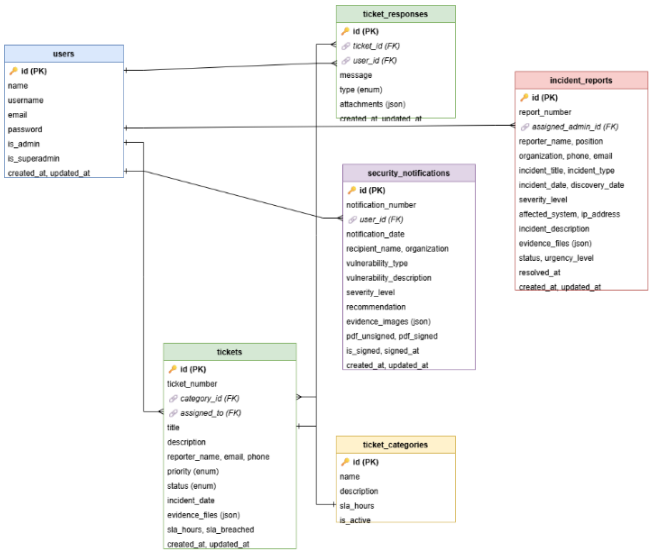
Gambar 2 menunjukkan *Use Case Diagram* sistem informasi CSIRT yang menggambarkan interaksi aktor dengan sistem. Aktor dalam sistem terdiri dari:

a) **Super Admin**: Memiliki hak akses penuh terhadap seluruh fitur sistem termasuk manajemen pengguna dan konfigurasi sistem

b) **Admin**: Dapat mengelola tiket, laporan insiden, dan konten website

c) ***User*/Pelapor**: Dapat membuat tiket pengaduan dan melihat status tiket

2) *Entity Relationship Diagram* (ERD)



Gambar 3. *Entity Relationship Diagram* (ERD)

Gambar 3 menunjukkan struktur basis data sistem yang terdiri dari beberapa tabel utama. Tabel utama dalam sistem meliputi:

a) ***users***: Menyimpan data pengguna

b) ***tickets***: Menyimpan data tiket pengaduan

c) ***ticket_categories***: Menyimpan kategori tiket

d) ***ticket_responses***: Menyimpan respons tiket

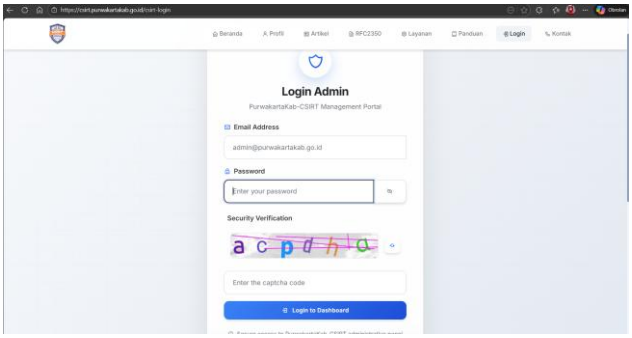
e) ***incident_reports***: Menyimpan laporan insiden siber

f) ***security_notifications***: Menyimpan surat pemberitahuan celah keamanan

g) ***dinas_reports***: Menyimpan laporan per dinas/OPD

3.3 Hasil Implementasi Sistem

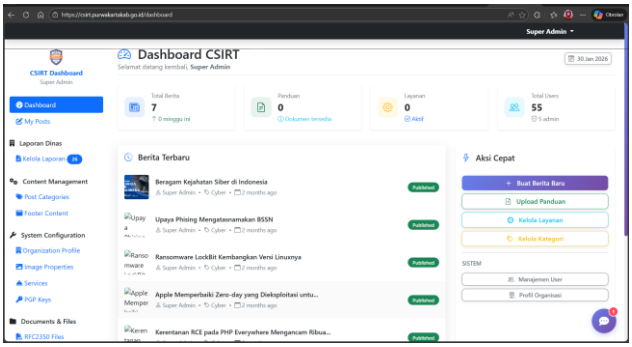
1) Halaman *Login*



Gambar 4. Halaman *Login*

Gambar 4 menunjukkan halaman *login* sistem yang dilengkapi dengan validasi *input* dan proteksi keamanan.

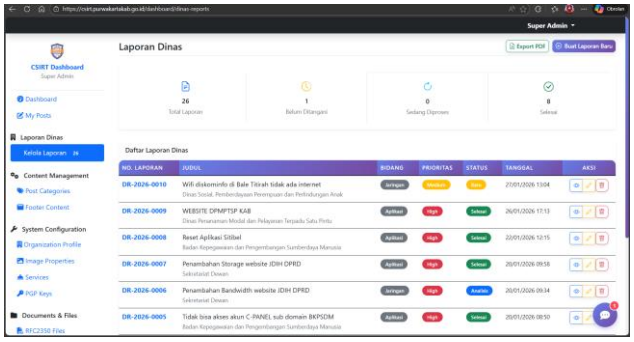
2) *Dashboard*



Gambar 5. Halaman *Dashboard*

Gambar 5 menunjukkan halaman *dashboard* administrator yang menampilkan laporan insiden, tiket, dan informasi penting lainnya. Perancangan *dashboard* mengacu pada prinsip desain berbasis pengguna agar data insiden dapat divisualisasikan secara efektif dan mendukung proses pengambilan keputusan [23].

3) Halaman Manajemen Laporan



Gambar 6. Halaman Manajemen Laporan

Gambar 6 menunjukkan halaman manajemen laporan dinas yang menampilkan tabel laporan *user*. Fitur manajemen tiket meliputi:

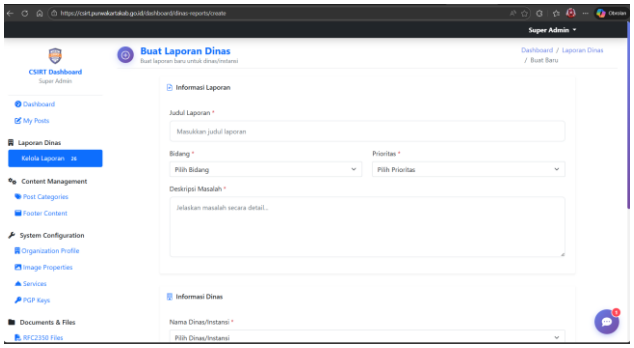
a) Detail tiket dengan informasi lengkap pelapor dan insiden

b) Sistem respons tiket dengan komentar

c) Perubahan status tiket.

d) Penugasan tiket kepada administrator

4) Halaman Laporan Insiden Siber



Gambar 7. Halaman Laporan Insiden Siber

Gambar 7 menunjukkan halaman formulir pelaporan insiden siber. Formulir pelaporan insiden mencakup:

a) Data pelapor (nama, jabatan, organisasi, kontak)

b) Detail insiden (tanggal, jenis, deskripsi)

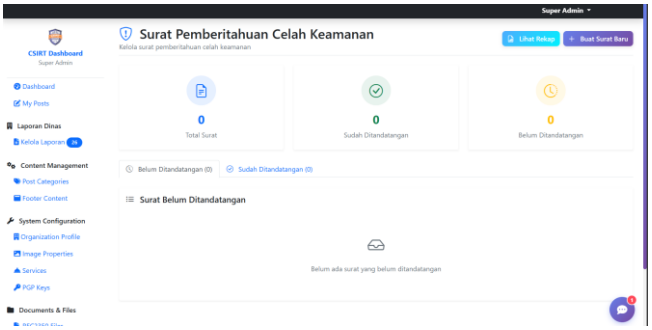
c) Klasifikasi *severity level* (*Low*, *Medium*, *High*, *Critical)*

d) Sistem yang terdampak

e) Bukti pendukung (*upload file*)

f) Bantuan yang dibutuhkan

5) Halaman Surat Pemberitahuan Celah Keamanan



Gambar 8. Halaman Surat Pemberitahuan Celah Keamanan

Gambar 8 menunjukkan halaman manajemen surat pemberitahuan celah keamanan dengan fitur *auto-generate* PDF. Fitur surat pemberitahuan meliputi:

a) Formulir pembuatan surat dengan detail kerentanan

b) Klasifikasi *severity* (*Critical*, *High*, *Medium*, *Low*)

c) *Upload* bukti gambar (*evidence*)

d) *Generate* PDF otomatis dengan template resmi

e) Rekap surat yang belum dan sudah ditandatangan

3.4 Hasil Pengujian Sistem

Pengujian sistem dilakukan menggunakan metode *Black Box Testing* untuk memvalidasi fungsionalitas sistem [24]. Hasil pengujian ditunjukkan pada Tabel 3.

Tabel 3. Hasil Pengujian *Black Box Testing*

No	Skenario Pengujian	Hasil yang Diharapkan	Hasil Aktual	Status
1	*Login* dengan *username* dan *password* valid	Masuk ke *dashboard* sesuai level pengguna	Sesuai	✓ Valid
2	*Login* dengan *password* salah	Menampilkan pesan *error*	Sesuai	✓ Valid
3	Membuat tiket baru dengan data lengkap	Tiket tersimpan dan nomor tiket ter-*generate*	Sesuai	✓ Valid
4	Membuat tiket dengan data tidak lengkap	Menampilkan validasi *error*	Sesuai	✓ Valid
5	Mengubah status tiket	Status tiket berubah dan tersimpan	Sesuai	✓ Valid
6	Menambah respons tiket	Respons tersimpan dan ditampilkan	Sesuai	✓ Valid
7	Membuat laporan insiden baru	Laporan tersimpan dengan nomor otomatis	Sesuai	✓ Valid
8	*Upload* bukti insiden	*File* berhasil di-*upload*	Sesuai	✓ Valid
9	Membuat surat celah keamanan	Surat tersimpan dan PDF ter-*generate*	Sesuai	✓ Valid
10	*Download* PDF surat	PDF berhasil di-*download*	Sesuai	✓ Valid
11	*Export* rekap laporan ke PDF	PDF rekap berhasil di-*generate*	Sesuai	✓ Valid
12	Mengelola data pengguna	CRUD pengguna berfungsi dengan baik	Sesuai	✓ Valid

Berdasarkan hasil pengujian, seluruh skenario pengujian menunjukkan hasil yang sesuai dengan yang diharapkan. Hal ini menunjukkan bahwa sistem telah berfungsi dengan baik sesuai dengan kebutuhan yang telah didefinisikan.

3.5 Pembahasan

Sistem informasi CSIRT yang dikembangkan menggunakan *framework* Laravel berhasil memenuhi kebutuhan operasional tim CSIRT Diskominfo Kabupaten Purwakarta. Penggunaan model *prototyping* dalam pengembangan sistem memungkinkan keterlibatan aktif pengguna dalam setiap iterasi, sehingga sistem yang dihasilkan sesuai dengan kebutuhan pengguna [25]. Kelebihan sistem yang dikembangkan meliputi:

a) Terintegrasi dalam satu platform untuk seluruh aktivitas CSIRT

b) Nomor tiket dan laporan ter-*generate* secara otomatis

c) *Auto-generate* PDF untuk surat pemberitahuan celah keamanan

d) Klasifikasi *severity level* untuk prioritas penanganan

e) Notifikasi *email* otomatis kepada administrator

Keterbatasan sistem yang perlu dikembangkan lebih lanjut meliputi:

a) Belum terintegrasi dengan sistem eksternal seperti BSSN

b) Belum tersedia aplikasi *mobile*

4. KESIMPULAN

Penelitian ini telah berhasil mengembangkan Sistem Informasi CSIRT berbasis web menggunakan *framework* Laravel dengan metode *prototyping* pada Diskominfo Kabupaten Purwakarta. Penggunaan metode *prototyping* memungkinkan pengembangan sistem secara iteratif dengan melibatkan partisipasi aktif pengguna, sehingga sistem yang dihasilkan sesuai dengan kebutuhan operasional tim CSIRT dalam menangani insiden keamanan siber di lingkungan pemerintah daerah.

Sistem yang dikembangkan memiliki fitur-fitur utama meliputi manajemen tiket pengaduan insiden siber dengan klasifikasi prioritas dan *Service Level Agreement* (SLA),

pelaporan insiden keamanan siber dengan klasifikasi *severity level*, pembuatan surat pemberitahuan celah keamanan dengan fitur *auto-generate* PDF, serta *dashboard* rekap dan statistik untuk monitoring insiden. Hasil pengujian menggunakan metode *Black Box Testing* menunjukkan bahwa seluruh fungsionalitas sistem berjalan sesuai dengan yang diharapkan.

Secara teoretis, penelitian ini berkontribusi dengan menghasilkan model pengembangan sistem informasi CSIRT berbasis web yang dapat dijadikan referensi bagi penelitian selanjutnya, khususnya dalam domain keamanan siber di lingkungan pemerintah daerah serta penerapan metode *prototyping* yang menekankan keterlibatan aktif pengguna akhir. Secara praktis, sistem yang dikembangkan mampu memberikan solusi nyata bagi Diskominfo Kabupaten Purwakarta dalam pengelolaan insiden keamanan siber secara lebih terstruktur dan terdokumentasi, sehingga dapat menggantikan proses manual yang selama ini digunakan, mempercepat respons, serta meningkatkan akuntabilitas penanganan insiden. Dari sisi kebijakan, hasil penelitian ini dapat dijadikan acuan bagi pemerintah daerah lainnya dalam mengembangkan sistem serupa sebagai bentuk implementasi pembentukan CSIRT di tingkat daerah, sekaligus mendukung terciptanya ekosistem keamanan siber nasional yang terintegrasi sesuai dengan regulasi perlindungan infrastruktur informasi vital.

Untuk pengembangan ke depan, sistem disarankan dapat terintegrasi dengan sistem pelaporan BSSN guna mendukung koordinasi penanganan insiden secara nasional, dilengkapi fitur notifikasi *real-time*, serta dikembangkan dalam bentuk aplikasi *mobile* agar memudahkan proses pelaporan insiden.

Ucapan Terima Kasih

Penulis mengucapkan terima kasih kepada Dinas Komunikasi dan Informatika Kabupaten Purwakarta yang telah memberikan kesempatan untuk melaksanakan penelitian magang dan dukungan dalam pengembangan Sistem Informasi CSIRT ini. Terima kasih juga disampaikan kepada dosen pembimbing yang telah memberikan arahan dan bimbingan selama penelitian berlangsung.

DAFTAR PUSTAKA

[1] M. Alfi, N. P. Yundari, and A. Tsaqif, "Analisis Risiko Keamanan Siber dalam Transformasi Digital Pelayanan Publik di Indonesia," *Jurnal Kajian Stratejik Ketahanan Nasional*, vol. 6, no. 2, p. 5, 2023.

[2] A. S. A. Ilaina and I. F. Nugraha, "Kesenjangan Kapabilitas Keamanan Siber Indonesia dalam Mitigasi Serangan Siber pada Layanan Publik Digital tahun 2020-2025," *Triwikrama: Jurnal Ilmu Sosial*, vol. 8, no. 6, pp. 141–150, 2025.

[3] S. Susniwati, A. Ardiyansah, and D. Sukorina, "Good governance di era digital: Studi kasus implementasi e-government di Indonesia," *PANDITA: Interdisciplinary Journal of Public Affairs*, vol. 8, no. 1, pp. 220–234, 2025.

[4] S. S. Harahap, M. Halkis, and R. Sutanto, "Advanced Persistent Threat (APT) sebagai Ancaman Perang Siber Asimetris Terhadap Pemerintah Indonesia," *Innovative: Journal Of Social Science Research*, vol. 5, no. 3, pp. 4465–4485, 2025.

[5] M. Alfikri and I. Ahmad, "Evaluasi Implementasi Kebijakan Pembentukan Tim Tanggap Insiden Siber pada Sektor Pemerintah," *Matra Pembaruan: Jurnal Inovasi Kebijakan*, vol. 6, no. 1, pp. 1–14, 2022.

[6] D. K. Iqram, I. Agusyanda, and D. H. Sitorus, "Revisi Undang-Undang TNI Dan Hak Digital Warga Negara: Antara Keamanan Nasional Dan Tantangan Demokrasi Digital," *Journal Kompilasi Hukum*, vol. 10, no. 2, pp. 412–429, 2025.

[7] I. N. Rachmawati, S. R. Natasia, and I. P. D. A. S. Prabowo, "Perancangan Dokumen Standard Operating Procedure (SOP) Pada Proses Incident Management Di PT. XYZ," *Jurnal Sistem Informasi dan Ilmu Komputer*, vol. 4, no. 1, pp. 15–22, 2020.

[8] A. Najiyya and S. S. Wulandari, "Eksplorasi Implementasi Kebijakan Pembentukan Computer Security Incident Response Team (Csirt) di Kementerian Perdagangan: Sebuah Studi Kualitatif," *JRAM (Jurnal Riset Akuntansi Multiparadigma)*, vol. 10, no. 1, pp. 50–55, 2023.

[9] T. Mary and N. Febriyani, "Peningkatan Keamanan Sistem Informasi Berbasis Laravel 12 dengan Rate Limiting dan Role-Based Access Control (RBAC)," *Jurnal Teknologi Dan Sistem Informasi Bisnis*, vol. 7, no. 3, pp. 473–481, 2025.

[10] N. Farid and T. Sutabri, "Rancangan Aplikasi Penjualan Berbasis Web Dengan Metode Prototype," *Jurnal Sains dan Teknologi*, vol. 3, no. 2, pp. 9–14, 2024.

[11] V. A. Kurniyanti and D. Murdiani, "Perbandingan Model Waterfall Dengan Prototype Pada Pengembangan System Informasi Berbasis Website," *Jurnal Syntax Fusion*, vol. 2, no. 08, pp. 669–675, 2022.

[12] M. R. Wayahdi and F. Ruziq, "Pemodelan sistem penerimaan anggota baru dengan unified modeling language (UML)(Studi kasus: Programmer

Association of Battuta)," *Jurnal Minfo Polgan*, vol. 12, no. 1, pp. 1514–1521, 2023.

[13] J. Friadi, D. P. Yani, M. Zaid, and A. Sikumbang, "Perancangan Pemodelan Unified Modeling Language Sistem Antrian Online Kunjungan Pasien Rawat Jalan pada Puskesmas," *Jurnal Ilmu Siber dan Teknologi Digital*, vol. 1, no. 2, pp. 125–133, 2023.

[14] M. R. Wicaksono, "Rancang Bangun Sistem Informasi Donor Darah Berbasis Web Menggunakan Framework Laravel (Studi Kasus: UDD PMI Provinsi Lampung)," Skripsi, Fakultas Matematika dan Ilmu Pengetahuan Alam, Universitas Lampung, Bandar Lampung, 2024.

[15] S. Rahmawati, A. P. Juledi, and V. Sihombing, "Implementasi sistem informasi manajemen dalam perguruan tinggi: Studi kasus tentang efisiensi operasional dan pelayanan mahasiswa," *Jurnal Ilmu Komputer Dan Sistem Informasi (Jikomsi)*, vol. 7, no. 1, pp. 75–77, 2024.

[16] W. P. Tambunan, R. Fauzi, and E. N. Alam, "Perancangan Front End Peer-To-Peer Lending Syariah Berbasis Website Menggunakan Metode Prototyping Untuk Memenuhi Kebutuhan Pengguna," *JIPI (Jurnal Ilmiah Penelitian dan Pembelajaran Informatika)*, vol. 9, no. 2, pp. 669–682, 2024.

[17] A. Satrio, D. Yusup, and C. Carudin, "Perancangan Sistem Layanan Restoran Dengan Metode Design Thinking Dan Prototyping Berbasis Web," *JATI (Jurnal Mahasiswa Teknik Informatika)*, vol. 7, no. 6, pp. 3128–3134, 2023.

[18] N. Khairunnisa, R. R. Danny, and R. Tantowi, "Perancangan aplikasi review kuliner berbasis Android dengan metode prototype pada Kedai Griya Kuliner," *Indonesian Journal of Networking and Security (IJNS)*, vol. 13, no. 2, 2024.

[19] A. Z. D. N. Adiya, D. L. Anggraeni, and I. Albana, "Analisa Perbandingan Penggunaan Metodologi Pengembangan Perangkat Lunak (Waterfall, Prototype, Iterative, Spiral, Rapid Application Development (RAD))," *Merkurius: Jurnal Riset Sistem Informasi dan Teknik Informatika*, vol. 2, no. 4, pp. 122–134, 2024.

[20] I. Sommerville, *Software Engineering. 10th Edition*. Pearson Education, 2016.

[21] N. Rahma and N. Mayesti, "Pengendalian Hak Akses pada Electronic Document and Records Management System di Kementerian Kelautan dan Perikanan Republik Indonesia," *Jurnal Kajian Ilmu Perpustakaan, Informasi dan Kearsipan. Departemen Ilmu Perpustakaan dan Informasi, Fakultas Ilmu Budaya, Universitas Indonesia. ISSN*, pp. 2302–4666, 2019.

[22] N. P. Berniawan, H. Saptono, and E. Zaida, "Pengembangan Antarmuka Web Analitik Log Deteksi Intrusi Jaringan Berbasis Suricata Menggunakan Dash," *Jurnal Informatika Terpadu*, vol. 11, no. 2, pp. 151–157, 2025.

[23] M. I. Wahyudi and E. P. Silmina, "Desain Web Dashboard Berbasis Pengguna: Menggunakan Design Thinking untuk Meningkatkan Pengelolaan Data," *Jurnal Informatika Terpadu*, vol. 11, no. 2, pp. 85–91, 2025.

[24] U. Saputra, N. Astrianda, B. R. Nasution, A. A. Anggara, R. S. Qaisa, and A. E. Jakfar, "Analisa Pengujian Sistem Informasi Website E-Commerce Bali-Store Menggunakan Metode Black Box Testing," *Jurnal Teknologi Informasi*, vol. 2, no. 2, pp. 95–102, 2023.

[25] H. Situmorang and M. I. Zul, "Implementasi Metodologi Prototype dalam Pengembangan Sistem Manajemen Kehadiran Pegawai Perusahaan Berbasis Web," *Jurnal Teknologi Informasi dan Multimedia*, vol. 6, no. 3, pp. 260–270, 2024.