BAB I PENDAHULUAN

1.1 Latar Belakang

Transformasi digital telah mendorong PT Kereta Cepat Indonesia China (KCIC) untuk mengembangkan sistem manajemen inventori berbasis web guna meningkatkan efisiensi operasional. Pengembangan sistem informasi manajemen (SIM) merupakan langkah krusial dalam era digital untuk mendukung pengambilan keputusan yang lebih cepat dan akurat [1], serta memberikan manfaat signifikan bagi organisasi bisnis [2][3]. Sebagai operator infrastruktur kritis nasional, keandalan dan keamanan sistem digital PT KCIC merupakan prioritas utama. Proses pengembangan aplikasi internal ini, sebagaimana dibuktikan oleh rekrutmen untuk pengembang aplikasi web, mengindikasikan adanya fokus strategis pada pembangunan kapabilitas teknologi internal.

Fokus awal dari pengembangan ini adalah pada perancangan antarmuka (UI/UX) yang intuitif dan responsif untuk memastikan adopsi pengguna yang tinggi. Ini adalah prinsip fundamental dalam desain produk digital modern yang menekankan bahwa pengalaman pengguna yang baik mencakup riset pengguna, pengujian, dan penerimaan [4] secara langsung memengaruhi efektivitas sebuah sistem [5]. Namun, di samping fungsionalitas dan kemudahan penggunaan, aspek fundamental yang tidak dapat diabaikan adalah keamanan dan kinerja teknis dari aplikasi itu sendiri.

Dari sisi keamanan, aplikasi yang terhubung ke internet rentan terhadap berbagai serangan siber. Ancaman yang paling umum dan merusak termasuk serangan pada lapisan aplikasi seperti *SQL Injection* (SQLi) dan *Cross-Site Scripting* (XSS), yang menempati peringkat atas dalam daftar risiko keamanan OWASP Top 10 [6]. Selain itu, tanpa enkripsi yang kuat, data sensitif yang transit di jaringan sangat berisiko untuk disadap [7][8].

Mengingat status PT KCIC, kegagalan dalam salah satu aspek baik kinerja maupun keamanan dapat berdampak signifikan. Oleh karena itu, penelitian ini melakukan analisis komprehensif yang tidak hanya menguji kualitas UI/UX, tetapi juga merancang, mengimplementasikan, dan memvalidasi dua kontrol keamanan esensial: *Web Application Firewall* (WAF) dan enkripsi HTTPS

dengan konfigurasi yang diperkuat (hardened), sejalan dengan studi terapan lainnya mengenai penguatan infrastruktur server web [9].

1.2 Rumusan Masalah dan Solusi

Berdasarkan latar belakang yang telah diuraikan, penelitian ini dirumuskan untuk menjawab serangkaian permasalahan fundamental yang terbagi dalam dua domain utama: penerimaan pengguna dan keamanan sistem.

Pada domain penerimaan pengguna, pertanyaan utama yang diajukan adalah bagaimana cara memvalidasi bahwa desain antarmuka pengguna (UI/UX) yang dikembangkan dapat diterima serta digunakan secara efektif dan efisien oleh pengguna akhir di lingkungan PT KCIC. Untuk menjawab tantangan ini, solusi yang diterapkan adalah metode *User Acceptance Testing* (UAT)[10][11], yaitu sebuah proses pengujian yang melibatkan pengguna akhir secara langsung untuk memastikan perangkat lunak yang dikembangkan telah memenuhi harapan dan kebutuhan mereka. Pengujian ini akan dieksekusi menggunakan platform Maze guna mengukur metrik kuantitatif dan kualitatif dari interaksi pengguna.

Dari sisi keamanan, penelitian ini menangani dua tingkat risiko. Pertama, untuk mengatasi masalah keamanan aplikasi dari ancaman serangan umum seperti SQL Injection (SQLi) dan Cross-Site Scripting (XSS), solusi yang diimplementasikan adalah sebuah *Web Application Firewall* (WAF). WAF ini dibangun menggunakan ModSecurity yang dikonfigurasi dengan OWASP Core Rule Set (CRS)[6]. Pendekatan ini sejalan dengan praktik standar industri di mana WAF berfungsi untuk mendeteksi lalu lintas berbahaya berdasarkan aturan yang telah ditetapkan sebelumnya. OWASP menyediakan kerangka kerja dan daftar kerentanan yang paling umum, yang menjadi acuan dalam konfigurasi aturan keamanan tersebut.

Kedua, untuk mengatasi masalah keamanan data dari risiko penyadapan selama transmisi, solusi yang diterapkan adalah pengaktifan enkripsi melalui protokol HTTPS. Implementasi ini diperkuat dengan praktik *hardening*, yaitu serangkaian konfigurasi untuk memperkuat keamanan protokol Transport Layer Security (TLS). Proses ini mencakup penonaktifan protokol versi lama yang rentan dan pemilihan *cipher suite* yang kuat untuk memastikan kerahasiaan dan integritas data.[7]

1.3 Tujuan

Berdasarkan rumusan masalah yang telah dijabarkan, penelitian ini memiliki beberapa tujuan spesifik sebagai berikut:

1. Melakukan validasi terhadap desain antarmuka pengguna (UI/UX) melalui *User Acceptance Testing* (UAT) untuk mengukur tingkat penerimaan, efektivitas, dan efisiensi sistem dari perspektif pengguna akhir.
2. Merancang dan mengimplementasikan arsitektur keamanan berlapis yang mencakup *Web Application Firewall* (WAF) untuk mitigasi ancaman pada level aplikasi, serta enkripsi HTTPS yang diperkuat untuk melindungi data pada level transport.
3. Mengevaluasi dan memverifikasi efektivitas dari setiap kontrol keamanan yang diimplementasikan melalui serangkaian skenario pengujian terukur, termasuk simulasi serangan dan analisis konfigurasi teknis.

1.4 Penjadwalan Kerja

Berikut adalah jadwal kerja magang yang dapat saya sajikan

Tabel 1. 1 Penjadwalan Kerja

No	Deskripsi Kerja	Feb				Mar				Apr				Mei				Jun				Jul			
		1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4
1	Analisis Kebutuhan																								
2	Perancanaan																								
3	Perancangan Sistem																								
4	Pengembangan awal																								
5	Pengujian																								
6	Dokumentasi																								
7	Laporan, Jurnal & PPT																								