BAB I
PENDAHULUAN

1.1 Latar Belakang

Berdasarkan hasil observasi penulis selama terlibat dalam proses pengembangan sistem di PT Neurogs Inovasi Teknologi, ditemukan bahwa pada versi awal produk internal perusahaan (versi 1), sistem belum menerapkan mekanisme autentikasi JSON Web Token (JWT) dan token berlapis menggunakan refresh token serta belum mengimplementasikan Role-Based Access Control (RBAC) secara terstruktur. Penggunaan single access token tanpa mekanisme rotasi atau pembaruan token berpotensi meningkatkan risiko apabila token terekspos dan masih berada dalam masa berlaku. Selain itu, belum adanya pembatasan akses berbasis peran menyebabkan kontrol otorisasi belum terdefinisi secara granular antar pengguna sistem. Kondisi ini menjadi bahan evaluasi dalam pengembangan versi selanjutnya agar aspek autentikasi dan otorisasi dapat diperkuat secara sistematis.

Temuan tersebut menunjukkan bahwa meskipun sistem telah berjalan secara fungsional, aspek keamanan belum sepenuhnya dirancang sebagai bagian terintegrasi dalam siklus pengembangan perangkat lunak. Dalam rekayasa perangkat lunak modern, sistem berbasis web tidak hanya dituntut mampu memenuhi kebutuhan fungsional, tetapi juga harus memperhatikan skalabilitas, maintainability, dan keamanan sejak tahap perencanaan (Pressman & Maxim, 2020). Keamanan yang diterapkan secara parsial pada tahap implementasi sering kali menimbulkan celah yang baru teridentifikasi setelah sistem digunakan.

Secara umum, perkembangan teknologi informasi mendorong organisasi untuk mengadopsi sistem berbasis web dalam mendukung aktivitas operasionalnya. Sistem informasi manajemen digunakan untuk mengelola data karyawan, proyek, serta administrasi perusahaan secara terintegrasi agar proses kerja menjadi lebih efektif dan terdokumentasi dengan baik (Laudon & Laudon, 2020). Integrasi sistem menjadi penting terutama ketika data yang dikelola bersifat internal dan memiliki tingkat sensitivitas tertentu.

PT Neurogs Inovasi Teknologi merupakan perusahaan yang bergerak di bidang cyber security. Sebagai perusahaan yang berfokus pada keamanan informasi, pengelolaan data internal seperti data karyawan, evaluasi kinerja, dan manajemen proyek seharusnya

mengikuti prinsip kerahasiaan, integritas, dan ketersediaan data. Namun dalam praktik operasional sehari-hari, pengelolaan administrasi dan proyek masih memanfaatkan Microsoft Team. Data absensi, reimbursement, serta evaluasi Key Performance Indicator (KPI) belum terintegrasi dalam satu sistem terpusat, sehingga proses rekapitulasi dan validasi masih dilakukan secara manual.

Kondisi tersebut menimbulkan beberapa permasalahan operasional seperti risiko inkonsistensi data, keterlambatan proses administrasi, serta potensi kesalahan dalam perhitungan KPI. Permasalahan ini pada dasarnya merupakan isu manajemen sistem. Namun apabila sistem internal dikembangkan tanpa mekanisme kontrol akses dan pengamanan autentikasi yang memadai, maka risiko tersebut dapat berkembang menjadi isu keamanan informasi, khususnya apabila melibatkan data sensitif dan kredensial pengguna.

Dalam konteks keamanan perangkat lunak, sistem internal yang mengelola data karyawan dan proyek harus memiliki mekanisme autentikasi dan otorisasi yang jelas. Penerapan Role-Based Access Control (RBAC) diperlukan untuk memastikan bahwa setiap pengguna hanya dapat mengakses data sesuai dengan perannya. Selain itu, penguatan mekanisme JWT melalui implementasi refresh token memungkinkan pengelolaan sesi yang lebih aman dengan membatasi masa berlaku access token serta mengurangi risiko penyalahgunaan token apabila terjadi eksposur. Kombinasi autentikasi berbasis token berlapis dan kontrol akses berbasis peran menjadi fondasi penting dalam menjaga integritas dan kerahasiaan data sistem.

Namun demikian, penerapan mekanisme keamanan seperti JWT berlapis dan RBAC tidak cukup apabila hanya dilakukan sebagai penambahan fitur teknis. Penguatan keamanan perlu diintegrasikan dalam keseluruhan siklus pengembangan perangkat lunak agar risiko dapat diidentifikasi sejak awal. Pendekatan Secure Software Development Life Cycle (SSDLC) menekankan integrasi aspek keamanan pada setiap fase pengembangan, mulai dari perencanaan, analisis kebutuhan, perancangan, implementasi, hingga pengujian. Salah satu metode pendukung dalam tahap pengujian adalah Static Application Security Testing (SAST), yaitu teknik analisis source code untuk mengidentifikasi potensi kerentanan sejak tahap pengembangan (McGraw, 2018; Shahriar & Zulkernine, 2020).

Berdasarkan hasil observasi serta kebutuhan peningkatan keamanan sistem tersebut, diperlukan pengembangan sistem manajemen proyek dan administrasi karyawan berbasis web yang tidak hanya terintegrasi secara fungsional, tetapi juga dirancang menggunakan pendekatan Secure Software Development Life Cycle (SSDLC). Penelitian ini berfokus pada penerapan Role-Based Access Control (RBAC), penguatan autentikasi menggunakan mekanisme JWT dengan refresh token, serta evaluasi tingkat keamanan sistem melalui Static Application Security Testing (SAST) untuk menganalisis potensi kerentanan pada source code yang dikembangkan.

1.2 Rumusan Masalah

Berdasarkan latar belakang yang sudah diuraikan, terdapat beberapa susunan permasalahan sebagai berikut:

1. Bagaimana kondisi dan keterbatasan sistem yang saat ini digunakan dalam pengelolaan proyek, KPI, absensi, dan reimbursement di PT. Neurogs Inovasi Teknologi?
2. Bagaimana merancang dan mengimplementasikan sistem manajemen karyawan berbasis web menggunakan pendekatan Secure Software Development Life Cycle (SSDLC) berbasis Waterfall dengan penerapan Role-Based Access Control (RBAC) dan autentikasi JSON Web Token (JWT)?
3. Bagaimana hasil evaluasi sistem berdasarkan aspek fungsionalitas serta pengujian keamanan menggunakan Static Application Security Testing (SAST) setelah penerapan SSDLC?

1.3 Tujuan

Tujuan dari implementasi sistem sebagai berikut ini:

1. Menganalisis kondisi dan keterbatasan sistem yang berjalan dalam pengelolaan proyek, KPI, absensi, dan reimbursement.
2. Merancang dan mengimplementasikan sistem manajemen karyawan berbasis web menggunakan pendekatan SSDLC berbasis Waterfall dengan penerapan mekanisme keamanan RBAC dan autentikasi JWT.

3. Mengevaluasi hasil implementasi sistem berdasarkan pengujian fungsional dan pengujian keamanan menggunakan SAST untuk mengidentifikasi serta meminimalkan potensi kerentanan aplikasi.

1.4 Manfaat

Penelitian ini harapkan memberikan manfaat seperti:

1. Manfaat Perusahaan
   - Memberikan solusi sistem manajemen karyawan dengan pengaturan hak akses yang terintegrasi bagi PT Neurogs Inovasi Teknologi sehingga proses administrasi karyawan, evaluasi kinerja karyawan dan manajemen proyek karyawan dapat dilakukan secara efisien dan terstruktur.
   - Membantu perusahaan mengurangi ketergantungan pada aplikasi pihak ketiga berbasis subscription dengan memberikan sistem internal yang dapat dikembangkan sesuai kebutuhan perusahaan.
   - Memberikan potensi kendali yang lebih baik atas data perusahaan melalui implementasi sistem manajemen karyawan dengan pengaturan hak akses serta implementasi on-premises yang dikelola oleh perusahaan sendiri.
   - Memberikan gambaran awal terhadap kualitas keamanan aplikasi melalui penerapan evaluasi keamanan statis sebagai bagian dari proses pengujian sistem.
2. Manfaat Akademis
   - Menjadi bahan pembelajaran bagi pengembangan sistem informasi manajemen karyawan berbasis web.
   - Memberikan kontribusi dalam penerapan sistem integrasi dan otomatisasi proses bisnis pada operasional perusahaan berskala kecil dan menengah.
   - Memberikan referensi penerapan Static Application Security Testing (SAST) sebagai metode evaluasi keamanan pada pengembangan sistem informasi manajemen karyawan berbasis web.

1.5 Ruang Lingkup Masalah

Berdasarkan permasalahan yang sudah jelaskan diatas, ada batasan pada ruang lingkup masalah seperti:

1. Sistem yang dikembangkan hanya diterapkan pada internal perusahaan PT Neurogs Inovasi Teknologi
2. Modul yang dibahas pada penelitian ini adalah manajemen proyek, key performance indicator (KPI) karyawan, reimbursement, absensi karyawan.
3. Pengaturan hak akses pengguna berdasarkan peran dan tanggung jawab masing masing dalam perusahaan.
4. Arsitektur sistem dengan RESTful API sebagai backend yang menghubungkan frontend dengan database postgresql.
5. Pengujian sistem dilakukan pada server internal perusahaan.
6. Penelitian ini tidak mencakup integrasi dengan aplikasi eksternal perusahaan.
7. Evaluasi keamanan aplikasi dibatasi pada pengujian statis kode sumber menggunakan pendekatan Static Application Security Testing (SAST), tanpa mencakup pengujian dinamis atau penetration testing.
8. Konfigurasi infrastruktur yang meliputi penggunaan Cloudflare, firewall Fortigate, segmentasi DMZ, serta deployment pada Virtual Machine Ubuntu Server dibahas terbatas pada arsitektur dan implementasi yang dilakukan untuk mendukung operasional sistem, tanpa membahas secara mendalam terkait konfigurasi keamanan jaringan, hardening server, maupun audit keamanan infrastruktur.

1.6 Sistematika Penelitian

BAB I PENDAHULUAN

Pada bagian ini, akan dijelaskan latar belakang masalah, perumusan masalah, tujuan penelitian, manfaat penelitian, ruang lingkup masalah, dan sistematika penelitian.

BAB II TINJAUAN PUSTAKA

Pada bagian ini, akan dibahas teori-teori yang didukung oleh literatur yang relevan dengan penelitian ini.

BAB III METODE PENELITIAN

Pada bagian ini, akan diuraikan langkah-langkah implementasi dan perancangan sistem, use case diagram, sequence diagram, workflow, metode pengujian dan evaluasi penggunaan.

BAB IV HASIL DAN PEMBAHASAN

Pada bagian ini, akan dijelaskan hasil dari implementasi yang dilakukan serta pembahasan mengenai hasil implementasi tersebut.

BAB V PENUTUP

Pada bagian ini, akan disampaikan kesimpulan dari implementasi yang telah dilakukan, beserta saran-saran untuk perbaikan dan pengembangan fitur dan modul aplikasi selanjutnya.