BAB 1 PENDAHULUAN

1.1. Latar Belakang

Keamanan perangkat lunak menjadi faktor krusial dalam pengembangan perangkat lunak di era digital yang penuh dengan ancaman siber yang semakin canggih. Setiap celah keamanan dalam aplikasi dapat dimanfaatkan oleh pihak yang tidak bertanggung jawab untuk mengeksploitasi data sensitif, merusak sistem, atau mengganggu operasional bisnis. Menurut laporan dari Cybersecurity ventures, kerugian akibat kejahatan siber diperkirakan mencapai $10,5 triliun pertahun dan mengalami peningkatan sebesar 15% setiap tahunnya [1]. Oleh karena itu, para pengembang dituntut untuk menerapkan strategi dan praktik terbaik guna melindungi integritas, kerahasiaan, dan ketersediaan data pengguna.

Dalam upaya untuk meningkatkan keamanan perangkat lunak, salah satu pendekatan yang dapat diterapkan adalah pengujian keamanan pada kode sumber menggunakan alat *Static Application Security Testing* (SAST), seperti menggunakan Bearer CLI. Metode ini digunakan pada tahap awal pengembangan perangkat lunak guna mendeteksi kerentanan sebelum aplikasi dieksekusi. Metode ini dapat diotomatisasi, konsisten dan dapat diulang tanpa memerlukan lingkungan pengujian terpisah atau sistem yang diisolasi untuk seluruh aplikasi, serta memungkinkan perbaikan masalah lebih awal [2]. Penelitian lain juga menunjukkan bahwa alat analisa Bearer CLI memiliki tingkat akurasi sebesar 83,32% [3]. Selain itu, dengan mengintegrasikan model Large Language Model (LLM) dalam proses pengujian, pengembang dapat memanfaatkan kecerdasan buatan untuk menganalisis pola dan memberikan rekomendasi perbaikan yang lebih akurat.

Dengan semakin meningkatnya jumlah serangan siber dan kerentanan yang terdeteksi, menunjukkan perlunya pengembang untuk mengadopsi metode alat pengujian efektif dan efisien. Dengan Mengintegrasikan alat Bearer CLI dan model LLM, kedua teknik ini tidak hanya memungkinkan deteksi masalah

lebih dini, tetapi juga membantu meningkatkan ketahanan aplikasi terhadap potensi serangan yang semakin berkembang. Untuk itu, riset lebih lanjut dan penerapan sistem pengujian berbasis SAST dan model LLM dapat membuka jalan untuk meningkatkan kualitas dan keamanan perangkat lunak di masa depan. Dengan demikian, penting untuk terus mengembangkan dan menyempurnakan sistem ini guna menciptakan aplikasi yang lebih aman dan dapat diandalkan, dengan mengedepankan keamanan sebagai bagian penting dari proses pengembangan perangkat lunak.

1.2. Rumusan Masalah

1. Bagaimana merancang aplikasi pendeteksi kerentanan pada kode dengan mengintegrasikan alat SAST pada aplikasi ?
2. Bagaimana cara menerapkan metode deteksi menggunakan LLM untuk aplikasi pendeteksi kerentanan pada kode?
3. Bagaimana tingkat akurasi metode deteksi Bearer CLI dan LLM dalam mendeteksi kerentanan yang digunakan oleh aplikasi pendeteksi kerentanan pada kode

1.3. Tujuan

1. Merancang dan mengembangkan aplikasi pendeteksi kerentanan pada kode dengan mengintegrasikan alat SAST, guna mempermudah proses identifikasi dan penilaian kerentanan dalam perangkat lunak secara otomatis.
2. Menerapkan metode deteksi kerentanan menggunakan Large Language Model (LLM) pada aplikasi pendeteksi kerentanan.
3. mengevaluasi dan membandingkan tingkat akurasi metode deteksi Bearer CLI dan Large Language Models (LLM) dalam mengidentifikasi kerentanan pada kode sumber.

1.4. Batasan Masalah

1. Pengembangan aplikasi dirancang aplikasi berbasis web, dan hanya mendukung beberapa bahasa pemprograman seperti python,javascript dan php.
2. aplikasi tidak dirancang untuk memperbaiki kode sumber secara otomatis sehingga perbaikan pada kode yang rentan harus diperbaiki secara manual oleh pengembang.