ABSTRAK

Keamanan perangkat lunak merupakan aspek vital dalam pengembangan aplikasi modern, terutama di tengah meningkatnya ancaman siber yang menyebabkan kerugian global mencapai $10,5 triliun per tahun dengan pertumbuhan 15% tahunan. Untuk mengatasi tantangan ini, penelitian ini mengembangkan aplikasi web yang dirancang untuk mendeteksi kerentanan pada kode sumber dengan memanfaatkan integrasi antara Static Application Security Testing (SAST) melalui Bearer CLI dan kemampuan analisis Large Language Model (LLM) seperti GPT-4. Aplikasi ini memungkinkan pengguna untuk mengunggah kode, melakukan analisis kerentanan, dan memperoleh rekomendasi perbaikan yang relevan dengan kerentanan yang ditemukan. Metodologi penelitian mencakup tahapan analisis kebutuhan, perancangan sistem, implementasi, serta pengujian menggunakan Black Box Testing dan evaluasi akurasi dengan dataset OWASP Benchmark dan Skf labs. Hasil penelitian menunjukkan bahwa aplikasi berhasil dikembangkan dengan tingkat keberhasilan pengujian fungsional mencapai 100%. Dalam hal akurasi, Bearer CLI menunjukkan variasi antara 45,04% hingga 90,69%, sementara model LLM GPT-4 mencapai akurasi 85%, precision 88,88%, dan recall 94,11%. Namun, specificity yang rendah (33,33%) menunjukkan adanya kebutuhan untuk mengurangi false positive. Penelitian ini membuktikan bahwa integrasi SAST dan LLM efektif dalam mendeteksi kerentanan dan memberikan rekomendasi perbaikan. Meskipun hasil yang dicapai cukup baik, penelitian ini menyoroti perlunya peningkatan lebih lanjut untuk mengurangi false positive pada LLM dan meningkatkan akurasi SAST guna memperkuat kualitas dan keamanan perangkat lunak secara keseluruhan.

Kata Kunci : keamanan perangkat lunak, SAST, Bearer CLI, Large Language Model, pengujian keamanan, deteksi kerentanan.