ABSTRAK

Dalam era digital saat ini, keamanan aplikasi web menjadi aspek krusial seiring dengan meningkatnya ancaman serangan siber, seperti SQL Injection dan Cross-Site Scripting, yang dapat menyebabkan kebocoran data sensitif. Untuk memitigasi risiko tersebut secara proaktif, penelitian ini merancang dan menguji sebuah model deteksi otomatis terhadap serangan *code injection* dengan menerapkan algoritma Support Vector Machine, yang dikenal memiliki kemampuan unggul dalam mengklasifikasikan data berdimensi tinggi. Dengan pendekatan klasifikasi multi-kelas, model dirancang untuk mengidentifikasi tiga jenis input: SQL Injection, XSS, dan input normal. Dataset yang digunakan merupakan data hasil simulasi serangan otomatis pada aplikasi OWASP Juice Shop. Seluruh data HTTP log kemudian diproses melalui tahapan preprocessing dan rekayasa fitur, termasuk tokenisasi serta representasi vektor menggunakan Word2Vec. Hasil pengujian menunjukkan bahwa model SVM yang telah dioptimasi memberikan performa terbaik dibandingkan model pembanding lainnya, yakni Random Forest, Logistic Regression, dan K-Nearest Neighbors, dengan tingkat akurasi mencapai 97,49%. Lebih lanjut, ketika diterapkan dalam sistem deteksi secara *real-time*, model SVM menunjukkan performa yang andal dengan tingkat deteksi keseluruhan sebesar 88,39%, mencakup deteksi SQLi sebesar 82,81% dan XSS sebesar 98,93%. Temuan ini menunjukkan bahwa SVM merupakan pendekatan yang efektif dan layak untuk diimplementasikan dalam sistem keamanan aplikasi web secara praktis..

Kata Kunci:. *SQL Injection, Cross-Site Scripting (XSS), Support Vector Machine (SVM), Klasifikasi Multi-Kelas*