Abstrak

Serangan SQL injection merupakan ancaman serius bagi aplikasi web dan sistem basis data. Studi ini mengevaluasi efektivitas integrasi antara Security Information and Event Management (SIEM) dengan multi-agent Wazuh dan berbagai Web Application Firewalls (WAF) dalam mendeteksi serangan SQL injection secara kolaboratif. Sistem dirancang menggunakan dua server web yang masing-masing dilindungi oleh WAF berbeda—ModSecurity dan NAXSI—serta sebuah server SIEM terpusat yang menggunakan Wazuh. Pengujian dilakukan dengan berbagai teknik SQL injection, termasuk Time-Based Blind, Error-Based, dan Union-Based. Hasil penelitian menunjukkan bahwa ModSecurity lebih efektif dalam mendeteksi dan mengatasi serangan SQL injection berbasis Time-Based dan Error-Based, sementara kedua WAF memiliki performa yang serupa dalam menangani serangan Union-Based. Platform Wazuh berhasil mengumpulkan dan melaporkan data serangan dengan efisien, memberikan tim keamanan pandangan yang jelas dan terpusat mengenai ancaman yang terdeteksi. Integrasi ini membuktikan bahwa penerapan deteksi ancaman secara kolaboratif menggunakan SIEM dan berbagai WAF dapat meningkatkan keamanan aplikasi web terhadap serangan SQL injection.

Kata Kunci-SQL injection, SIEM, WAF, multi-agent, cybersecurity, deteksi kolaboratif