ABSTRAK

Peningkatan jumlah kerentanan keamanan informasi yang tercatat dalam Common Vulnerabilities and Exposures (CVE) dari tahun ke tahun menandakan perlunya pemahaman yang mendalam terhadap karakteristik dan pola yang muncul. Penelitian ini bertujuan untuk menganalisis data CVE tahun 2020–2024 guna mengetahui karakteristik data, jenis kerentanan yang paling umum, serta mengevaluasi implikasi tren terhadap strategi mitigasi keamanan informasi. Proses analisis dimulai dari pembersihan dan transformasi data, dilanjutkan dengan analisis statistik, pemodelan deret waktu menggunakan ARIMA, dan klasifikasi jenis kerentanan berdasarkan kode CWE. Hasil menunjukkan bahwa tren CVE cenderung meningkat dengan fluktuasi musiman, dan jenis kerentanan yang paling umum adalah CWE-79 (Cross-site Scripting). Model ARIMA terbaik yang diperoleh adalah ARIMA(2,0,2), dengan hasil evaluasi MAE sebesar 256, RMSE sebesar 256, dan MAPE sebesar 13,1%. Penelitian ini memberikan kontribusi berupa dasar yang kuat untuk merumuskan langkah mitigasi risiko yang lebih kontekstual dan responsif terhadap perkembangan tren kerentanan.

Kata kunci: ARIMA, CVE, CWE, kerentanan, mitigasi risiko, tren keamanan