ABSTRACT

In today's digital era, web application security has become a crucial aspect amid the rising threat of cyber attacks, such as SQL Injection and Cross-Site Scripting, which can lead to sensitive data leakage. To proactively mitigate these risks, this study designs and tests an automatic detection model for code injection attacks by implementing the Support Vector Machine algorithm, which is known for its superior capability in classifying high-dimensional data. With a multi-class classification approach, the model is designed to identify three types of input: SQL Injection, XSS, and normal input. The dataset used is data from an automated attack simulation on the OWASP Juice Shop application. All HTTP log data is then processed through preprocessing and feature engineering stages, including tokenization and vector representation using Word2Vec. The test results show that the optimized SVM model provides the best performance compared to other comparison models, namely Random Forest, Logistic Regression, and K-Nearest Neighbors, with an accuracy level of 97.49%. Furthermore, when implemented in a real-time detection system, the SVM model shows reliable performance with an overall detection rate of 88.39%, comprising 82.81% for SQLi detection and 98.93% for XSS detection. These findings indicate that SVM is an effective and feasible approach to be implemented in a practical web application security system.

Keywords: *SQL Injection, Cross-Site Scripting (XSS), Support Vector Machine (SVM), Multi-Class Classification*