A HYBRID APPROACH TO DETECT AND PREVENT SQL AND NOSQL INJECTION ATTACKS ON SERVER-SIDE APPLICATION

K. P. D Meraj Vindira

A dissertation submitted in partial fulfilment for the requirement for Bachelor of Engineering (Honours) degree in Software Engineering

School of Computing

Informatics Institute of Technology, Sri Lanka

in collaboration with

University of Westminster, UK

2023

Abstract

Cyber-attacks are one of the most serious concerns facing individuals at all levels, particularly in enterprises, as they can maliciously destroy systems and steal data. The big data available on the internet motivates hackers to launch new kinds of attacks. SQL injection (SQLi) is the most common attack vector accounting for over 50% of all web application attacks, nowadays not only the SQLi also NoSQL injection attacks are getting trending among the hackers due to the lack of security optimization regarding NoSQL databases.

This suggested solution detects SQL injection from web application input forms and suggests a SQL injection validation model based on a hybrid approach that combines CNN and RNN (Convolutional Neural Network and Recurrent Neural Network) with BERT (Bidirectional Encoder Representations from Transformers). High-dimensional elements of SQL injection behavior can be exploited to fix the web application vulnerability. A actual web application input form with typical input form validation using regex, input sanitization, and the firewall approach is used to test the recommended strategy. The results of the recommended model analysis demonstrate that compared to earlier methods, the NLP-based model has a higher percentage of accuracy, recall, precision, and F1 score, making it more accurate in validating assaults.

This study demonstrates that vulnerabilities in a web application can be prevented. Advanced technologies have been used, which will assist the developer in avoiding SQL injections in a correct and secure manner. Due to this hybrid model, there is less chance of SQL injection hacking. As a result, SQL injection cannot be used by hackers to gain access to systems or data.