ABSTRACT

SQL injection attack is one of the most popular attack and frequently used to conduct attacks in web applications. This attack is performed by the attacker by injecting the SQL query into the form or parameters contained in the web application. SQL injection attacks can be used to retrieve data, modify data, and delete data illegally. To anticipate SQL injection attacks need to identify the pattern of attacks and prevent such attacks from being executed by the database. In this study, the authors designed a SQL injection attack prevention system using a combination of methods of SQL injection free secure algorithms and the classification of naïve bayes. The accuracy testing model uses SQL injection free secure constants and uses the number of naïve bayes datasets.. There are two test scenarios, first using the constant value 5 and the number of datasets 125, the second using the constant value 3 and the number of datasets 250. The second test results get a better accuracy value than the first test. In efficiency testing, testing uses load time how fast the page is accessed. In combination the method produces a low efficiency value because there are checks and arithmetic operations that affect the speed of access. In addition to the system for detecting and preventing, the research that the author designs there is a monitoring system to find out what attacks have been prevented.

Keyword – SQL injection, web application , SQL injection free secure, naïve bayes