
Abstract

SQL Injection is an attack that attempts to gain unauthorized access to a database by injecting code and exploiting SQL queries. SQL injection is an attack that is easy to carry out but difficult to detect and classify because of the variety of types. The SQLI vulnerability resulted from improper user input validation, which allowed attackers to manipulate programmer requests by adding new SQL operators. In this study, a classifier model has been designed to detect SQL injection attacks.

Attacks are classified as union, tautology, and blind. The method used in the classification is machine learning using the Naive Bayes algorithm model. From the test results obtained an accuracy value of 79.82%. Then it can be concluded that the machine learning method using the Naive Bayes model has succeeded in classifying SQL Injection

Keywords: Naïve bayees classifier, SQL injection

