Abstract

SQL Injection is an attack carried out by inserting a SQL query command into the input section in order to access the database contained in the web application. SQL Injection often occurs because there is no filtering done when input data enters the database. Therefore, we need a precaution so that incoming input can be selected before entering the database. Prevention can be obtained from the functions contained in the programming language and the framework of the programming language.

In this study, an analysis and comparison of the accuracy of preventing SQL injection attacks on the CodeIgniter and Laravel frameworks was carried out. In the CodeIgniter framework the escaping query function is used to prevent SQL injection attacks. Meanwhile, the Laravel framework uses the ORM eloquent function to prevent SQL injection attacks.

Based on the results of testing and analysis, it was found that SQL injection attacks on the CodeIgniter framework and the Laravel framework can be prevented equally by using the escaping query function on the CodeIgniter framework and the ORM eloquent function on the Laravel framework. From the test results obtained 100% accuracy of 293 SQL injection attacks.

Keywords: SQL, SQL Injection, CodeIgniter, Laravel, Accuracy