ABSTRACT

SQL injection is a method to insert sql command as input through website application to get access database. Securing website application can be done by installing a firewall, antivirus, or similar software on the server. But more important is to make the codes is free from bugs. Because the best firewall will not be useful, if the codes are created by developers are not free from *error* of logic programming.

PHP dan *Codeigniter* are examples scripting that often use developer to build website application. Its influenced some factor, there are small size and fast, easy to configure, have a library validation, fully documentation, easy to configure, support PHP 4 and PHP 5, and provide many functions like encryption, session, cookies, xss filtering. In this final project, is analysed about Handling *SQL Injection* for database *MySQL* with *framework Codeigniter* dan without *framework* (*PHP*) that use 4 scenario in testing *SQL* Injection. There are testing of character that have sense in query sql, testing of modify input login when username is known, testing of modify input login when username and password are not known, and testing of injection url.

Based on the result of testing and analyzing, *SQL Injection* attack *on PHP* and *Codeigniter* can be prevented well with function of ***mysql_real_escape_string*** **(**for *PHP***)** and ***library active record*****,** ***uri segment***(for *Codeigniter*) which from the result of testing can be obtained that is 0% error *query* and 0% injected(4 scenario of testing) from 104 vector attack.

Kata Kunci : ***Code Igniter , MySQL, PHP, SQL Injection.***