Abstracts

SQL Injection represents the most popular technique hacking at web application principally overcome the comands SQL pass the web application to be executed by database back-end. Weakness will emerge in the event of logic mistakes at the time of making program and user's input is not filtered or not to be good filtered till finally be executed. Identifying the weakness of *SQL Injection* will entangle the process of auditing of the entire web application. Prevention of *SQL Injection* can be done by reckoning the program logic and observe the input variable of application web

This final project give one of solution in the form of preventative application module of *SQL Injection* named *srex*. *Srex* integrated at web application base on the PHP 5.0 CodeIgniter and ASP .NET 2.0 by pursuant to the exist rules in *regex*. There are two examination forms, that is examination of attack of *SQL Injection* to both *web* application without inserted by module of *srex* and examination of attack of *SQL Injection* to both *web* application insertedly by *srex* module. Result of analysis in the form of efektivity inculcating of *srex* module at *web* applications owned the framework and also comparison the mount security PHP 5.0 Codeigniter and ASP. NET 2.0 in maintaining themself to attacks of *SQL Injection*

Keywords: *Web Security, SQL Injection,* ASP .NET 2.0, PHP 5.0 Code Igniter, *framework, regex*