ABSTRACT

The development of web technologies and its simplicity encourage developers to develop various web-based applications. Then, along with the growth of internet users, online store application emerges to facilitate the users. However, there are new security concerns because the amounts of sensitive informations are exchanged. Often in design phase, designers are not fully aware of security aspects and make vulnerabilities in their system. Some people who are usually called cracker using this condition to exploit system and steal information for their benefit, makes the existing informations are lost or stolen.

This Final Project is about designing the security system on a web application with case studies is digital music store as an example of web appilcation on retail sector. Security system in this application is intended to prevent application level attacks on a web application such as SQL Injection, Cross Site Scripting, Username Enumeration, Session Hijacking and CSRF. The designs are being implemented using a server-side programming languages such as PHP scripting and other web programming languages like HTML running on Apache web server and MySQL RDBMS.

The system tested the level of security. Tests carried out with two approaches, manual testing and automated testing. Manual testing is the tests performed directly by human beings with common attack methods. While the automated testing done using Acunetix, an application to audit web application security until the results reach low-level threat. From the testing results, the security design that used in this final project can prevents web application threats.

Keywords : ***Web Application, Web Security, Analysis and System Designing***