Abstract

At present, Web applications have been used for most of our life activities increasingly, and they affected by Structured Query Language Injection Attacks (SQLIAs). This attack is a method that attackers employ to impose the database in most of the web applications, by manipulate SQL queries, which sent to the Relational Database Management System (RDBMS). Hence, change the behavior of the applications. In This paper, developing Web Application SQLI Protector (WASP) tool in real-time web application to detect SQL injection attacks in stored procedures. Then, evaluated and analyze the developed tool respect to efficiency and effectiveness in practices. The propose technique uses real-time based on positive tainting, accurate and efficiency taint propagation, and syntax aware evaluation of the query strings at the application level to detect illegal queries before they reach at the database by using Microsoft ASP.NET. The developed tool effective due to it capable of detect and stop all SQLI attacks in real-time environment and did not generate any false negative, a few-false positive values in the results and impose minimal deploy requirements.
References


Index Terms

Computer Science  Information Sciences

Keywords

Web applications, SQL Injection, Detection, WASP, Techniques