

Abstract

In the era of rapid technological developments, security testing is the most important move if the system is planned to published online. Systems that are not tested for security are particularly vulnerable to hacker attacks. Data from OWASP said, SQL Injection attacks are the most widely used attacks by attackers. Although SQL injection attack schemes are often used, automation in this scheme is still rarely made so PenTester takes a long time to carry out attacks and does not know about the best test algorithms. To solve the problem, this final project develops SQL injection automation with the Blind SQL method. Designed of this automation has a brute force concept that penetrates the website by providing input questions that produce true or false and provide output in the form of letters that are designed into an answer. This application is divided into three algorithms scenarios, linear search scenario, binary search scenarios and interpolation search scenario. The research conducted was to measure the time performance of each algorithms. Based on the research that has been done the results of performance based on the time of the three algorithms found that the binary search algorithm is the fastest with a time of 1,7852 seconds, the second position is interpolation search with 1,789 seconds and the last is linear search with 1,902 seconds.

Keywords: penetration testing, blind sql injection, brute force, OWASP.