Abstract

SQL Injection is an attack that exploits weaknesses in applications that can be used to access data in the database. Fuzzing is one of the most effective methods for detecting SQL Injection vulnerabilities in an application. In general, the testing process using the fuzzing method by entering the malformat input and then analyzing the feedback given by the application. The process of generating test data generally uses a random-based technique, which combines several random characters by following predetermined rules. However, the random-based technique has drawbacks when used for the SQL query creation process, because SQL queries have a writing standard that refers to RFC 6922. Genetic algorithm is a technique that can be used to find the best solution according to predetermined criteria or can also be referred to as a fitness function. In general, genetic algorithms use binary numbers for data processing, but if the encoding and decoding techniques use binary numbers, the SQL query results obtained are not in accordance with the SQL query semantics. So, improvised genetic algorithms are carried out by adjusting the SQL query writing standards. Based on test-data generation analysis (DVWA) and test-data generation analysis (OWASP Juice Shop), the improvised genetic algorithm technique finds higher accuracy and more variety of SQL Injection attack type.

Keywords: SQL Injection, Fuzzing, Cartesian Product, Genetic Algorithm, Web Application Security