Abstrak

SQL Injection adalah serangan yang yang memanfaatkan kelemahan pada aplikasi yang dapat digunakan untuk mengakses data pada database . Fuzzing merupakan salah satu metode paling efektif untuk mendeteksi kerentanan SQL Injection pada suatu aplikasi. Pada umumnya proses pengujian dengan menggunakan metode fuzzing, dilakukan dengan cara memasukkan malformat input kemudian menganalisis feedback yang diberikan oleh aplikasi. Pada proses generasi test data umumnya menggunakan teknik random-based, yang dimana menggabungkan beberapa karakter acak dengan mengikuti rule yang telah ditentukan. Namun teknik random-based tersebut memiliki kekurangan jika digunakan untuk proses generasi query SQL, dikarenakan query SQL memiliki standar penulisan yang mengacu pada RFC 6922. Algoritma genetika merupakan salah satu teknik yang dapat digunakan untuk melakukan pencarian solusi terbaik sesuai dengan kriteria yang telah ditentukan atau dapat juga disebut sebagai fungsi fitness. Pada umumnya algoritma genetika menggunakan bilangan biner untuk pemrosesan data, namun jika teknik encoding dan decoding menggunakan bilangan biner, maka hasil query SQL yang didapatkan tidak sesuai dengan semantik query SQL. Sehingga dilakukan improvisasi algoritma genetika dengan menyesuaikan standar penulisan query SQL. Berdasarkan pengujian Analisis generasi test-data (DVWA) dan Analisis generasi test-data (OWASP Juice Shop), teknik improvisasi algoritma mendapati akurasi lebih tinggi dan temuan lebih banyak dibandingkan dengan teknik Generational Genetic Algorithm (GGA) dan Cartesian Product (CP). Pada penelitian ini teknik tersebut dapat melakukan deteksi serangan SQL Injection dengan tipe Error-based, Union-based dan Time-based.

Kata kunci : SQL Injection, Fuzzing, Cartesian Product, Algoritma Genetika, Web Application Security