1. Pendahuluan

Latar Belakang

SQL Injection merupakan salah satu ancaman yang serius dalam keamanan aplikasi berbasis web. Penyerangan menggunakan SQL Injection dengan memanfaatkan celah pada aplikasi dapat digunakan untuk mengakses database. Hal ini dapat menyebabkan kebocoran data-data sensitif seperti data informasi pribadi, data finansial dan lain sebagainya.[3] Fuzzing merupakan salah satu metode paling efektif untuk mendeteksi kerentanan pada suatu aplikasi[5]. Pada umumnya proses pengujian dengan menggunakan metode fuzzing, dilakukan dengan cara memasukkan malformat input kemudian menganalisis feedback yang diberikan oleh aplikasi. Input yang digunakan diambil dari kumpulan test data yang telah di generasi sesuai dengan rule yang telah ditetapkan untuk pengujian aplikasi[4]. Pada proses generasi test data umumnya menggunakan teknik random-based, yang dimana menggabungkan beberapa karakter acak dengan mengikuti rule yang telah ditentukan[1]. Namun teknik random-based tersebut memiliki kekurangan jika digunakan untuk proses generasi query SQL, dikarenakan query SQL memiliki standar penulisan yang mengacu pada RFC 69221 . Algoritma genetika merupakan salah satu teknik yang dapat digunakan untuk menemukan solusi optimal dari permasalahan yang mempunyai banyak solusi. Teknik tersebut akan melakukan pencarian solusi terbaik sesuai dengan kriteria yang telah ditentukan atau dapat juga disebut sebagai fungsi fitness[10]. Pada umumnya algoritma genetika menggunakan bilangan biner sebagai proses encoding dan decoding data, dan melakukan pengacakan bilangan biner pada saat proses crossover. Namun jika teknik encoding dan decoding menggunakan bilangan biner tersebut digunakan pada proses pembuatan query SQL, maka hasil yang didapatkan akan sama dengan teknik fuzzing menggunakan random-based. Keterbatasan teknik tersebut untuk melakukan proses generasi query SQL, merupakan salah satu tantangan pada penelitian ini. Sehingga dibutuhkan suatu metode untuk melakukan generasi query SQL sesuai dengan standar RFC 6992. Pada penelitian ini dilakukan improvisasi algoritma genetika dengan mengubah proses encoding, crossover, dan mutasi data dengan mengikut standar penulisan SQL. Dengan ini, diharapkan pengujian kerentanan terhadap serangan SQL Injection dapat lebih melingkupi cakupan yang lebih luas dan beragam. Topik dan Batasannya Berdasarkan latar belakang masalah yang telah dipaparkan, maka rumusan masalah yang diangkat oleh penulis pada penelitian ini yaitu Bagaimana mendeteksi dini celah SQL Injection pada suatu aplikasi, Pengukuran waktu generasi test data dan Pengukuran akurasi dari penerapan improvisasi algoritma genetika. Pada proses pendeteksian celah SQL Injection, dilakukan dengan cara membangun sistem fuzzer dengan menggunakan improvisasi algoritma genetika pada proses generasi test data. Metode tersebut akan melakukan pemecahan query menjadi beberapa unit mengikuti semantik query SQL. Pengukuran akurasi payload menggunakan confusion matrix dengan parameter total celah yang ditemukan. Pengujian dilakukan menggunakan dua aplikasi vulnerable web yaitu DVWA dan OWASP Juice Shop. Payload akan dinyatakan valid apabila dapat melakukan serangan menggunakan teknik SQL Injection berikut, antara lain: Error-based, Union-based dan Time-based. Tujuan Tugas akhir ini bertujuan untuk membangun sistem yang dapat mendeteksi SQL Injection dengan menggunakan improvisasi algoritma genetika, dengan memodifikasi proses crossover dan mutation. Adapun parameter keberhasilan payload diukur dari total akurasi, total temuan vulnerability SQL Injection dan waktu generasi test data. Keberhasilan payload dapat dibuktikan dengan melakukan pengujian manual salah satu payload pada aplikasi web testing DVWA dan OWASP Juice Shop. Organisasi Tulisan Buku tugas akhir ini disusun menjadi lima bagian yaitu Bab 1-Pendahuluan yang berisikan latar belakang, topik dan batasannya, dan tujuan dari penelitian ini. Bab 2-Studi terkait berisi penelitian yang sudah dilakukan sebelumnya yang merupakan

acuan untuk penelitian ini serta dasar teori penelitian. Bab 3-Gambaran dan Alur dari sistem yang diimplementasikan pada penelitian ini. Bab 4-Implementasi dan Evaluasi, menjelaskan tentang hasil pengimplementasian sistem dan analisis hasil penelitian. Bab 5-Penutup yang berisi kesimpulan penelitian dan saran untuk penelitian selanjutnya.