

ABSTRAK

Sistem informasi pendaftaran ulang mahasiswa baru (PUMABA) Universitas Malikussaleh banyak menyimpan data mahasiswa Universitas sehingga membutuhkan perlindungan keamanan yang optimal. Celah keamanan *SQL Injection* merupakan salah satu kerentanan yang umum terdapat pada aplikasi *website* yang menggunakan basis data. Pada penelitian ini, dilakukan pengujian celah keamanan *SQL Injection* menggunakan metode *fuzzing* pada seluruh *request form input* yang ada pada *website* PUMABA Universitas Malikussaleh. Sebanyak 50 data *request form input* diambil untuk dianalisis. Hasil pengujian menunjukkan bahwa dari 50 data yang diuji, terdapat 22 *request form input* yang rentan terhadap celah keamanan *SQL Injection*. Penelitian ini juga mengimplementasikan langkah-langkah perbaikan untuk mengatasi celah keamanan *SQL Injection* menggunakan teknik *Parameterized Queries* dan *Query Binding*.

Kata Kunci: Fuzzing, Penetration Testing, SQL Injection

ABSTRACT

Malikussaleh University's new student registration information system (PUMABA) stores a lot of University student data so it requires optimal security protection. SQL Injection security vulnerability is one of the common vulnerabilities found in website applications that use databases. In this study, a SQL Injection security vulnerability was tested using the fuzzing method on all input request forms on the PUMABA website. A total of 50 request input forms were taken for analysis. The test results show that of the 50 data tested, there are 22 input form requests that are vulnerable to SQL Injection security holes. This research also implements remedial measures to overcome SQL Injection security vulnerabilities using Parameterized Queries and Query Binding techniques.

Keywords: Fuzzing, Penetration Testing, SQL Injection