ABSTRAK

SQL Injection merupakan salah satu jenis serangan siber pada *Web Application*. Serangan ini ditempatkan pada kategori paling berbahaya (A1) oleh *Open Web Application Security Project* (OWASP). Serangan siber tersebut dapat dilakukan secara otomatis dengan *tool SQLMap*. Serangan siber yang dilakukan dengan *tool* ini dicatat pada sebuah *Log Web Server*. *Regular Expression* (Regex) merupakan salah satu metode yang digunakan untuk menyelesaikan permasalahan pemrosesan atau manipulasi teks. Dalam penelitian ini, *Regular Expression* digunakan dalam pencocokan *data request HTTP* dengan pola serangan pada *Log Web Server*. Penelitian ini menggunakan metode *Regular Expression* pada *Log Web Server Apache* berdasarkan pola *payload default* yang dihasilkan oleh *tool SQLMap* untuk mendeteksi serangan siber *SQL Injection*. Metode *Regular Expression* digunakan untuk mendeteksi pola pada *payload default* yang dihasilkan *tool SQLMap*. Hasil penelitian menunjukkan data uji *Log Web Server* dapat diperiksa dengan metode *Regular Expression*. Pola *payload default tool SQLMap* dapat ditemukan dengan tingkat akurasi ≥90%. Aplikasi yang dibangun dapat mendeteksi *file* dengan ekstensi **.log* dan ukuran *file access log* yang dimasukkan ≤1 *Gigabyte*.

Kata kunci : *SQL Injection*, *SQLMap*, *Log Web Server*, *Regular Expression*