ABSTRAK

SQL Injection tetap menjadi salah satu ancaman paling kritis pada aplikasi web modern. Salah satu variannya, *Time-Based Blind SQL Injection (TBB-SQLi),* menjadi lebih berbahaya karena tidak menghasilkan keluaran langsung dan hanya mengandalkan jeda *delay* sebagai indikator keberhasilan injeksi. Tantangan utama dari teknik ini adalah proses eksploitasi yang lambat dan membutuhkan jumlah permintaan yang banyak. Penelitian ini mengembangkan sistem otomatisasi eksploitasi *TBB-SQLi* berbasis *Python* dengan mengimplementasikan tiga algoritma pencarian *Linear Search, Binary Search*, dan *Ternary Search* untuk mengetahui efesiensi eksploitasi ada proses ekstraksi data sensitif dari *database*. Evaluasi performa dilakukan menggunakan dua parameter utama, yaitu waktu eksekusi *runtime* dan jumlah *request,* pada enam skenario *sleep delay* (1–6 detik). Hasil pengujian menunjukkan pola performa yang berbeda disetiap skenario *delay* menunjukan bahwa *Binary Search* merupakan algoritma paling efisien, dengan *runtime* 2.054–11.007 detik dan 1.945–2.113 *request*. *Ternary Search* menempati posisi tengah dengan *runtime* 3.720–10.361 detik dan 2.652–4.552 *request*, sementara *Linear Search* menjadi yang paling lambat di delay rendah, yakni 3.780–6.932 detik dengan total *request* paling tinggi mencapai 6.167. Sistem yang dihasilkan mampu mengekstraksi *database*, tabel, serta kredensial administrator secara otomatis. Secara keseluruhan, *Binary Search* terbukti paling optimal dalam menyeimbangkan efisiensi waktu dan jumlah *request* pada proses eksploitasi.

Kata Kunci : *Time-Based Blind SQL Injection*, Otomatisasi Eksploitasi, *Binary Search, Linear Search, Ternary Search*, Keamanan Web.