Abstrak

SQL Injection merupakan teknik *hacking* paling populer pada aplikasi *web* dengan prinsip melewatkan perintah-perintah *SQL* lewat aplikasi *web* untuk dieksekusi oleh *database back-end*. Kelemahan akan muncul apabila terjadi kesalahan logika pada saat pembuatan program dan inputan *user* tidak disaring atau difilter dengan sempurna hingga akhirnya dieksekusi. Mengidentifikasi kelemahan *SQL Injection* akan melibatkan proses auditing aplikasi web secara keseluruhan. Pencegahan *SQL Injection* dapat dilakukan dengan memperhitungkan logika pemprograman dan mengawasi variabel input pada aplikasi *web*.

Tugas akhir ini memberikan salah satu solusi berupa modul aplikasi pencegahan *SQL Injection* dengan nama *srex*. *Srex* diintegrasikan pada aplikasi *web* berbasis PHP 5.0 Code Igniter dan ASP .NET 2.0 dengan berdasarkan *rules* yang ada pada *regex.* Terdapat dua bentuk pengujian yaitu pengujian serangan *SQL Injection* terhadap kedua aplikasi *web* tanpa disisipkan modul *srex* dan pengujian serangan *SQL Injection* terhadap kedua aplikasi *web* dengan disisipkan modul *srex.* Hasil analisis berupa keefektifitasan ditanamkannya modul *srex* pada aplikasi *web* yang telah memiliki *framework* serta perbandingan tingkat keamanan PHP 5.0 CodeIgniter dan ASP .NET 2.0 dalam mempertahankan diri terhadap serangan *SQL Injection.*

.

Kata kunci: Keamanan Aplikasi *Web*, *SQL Injection*, ASP .NET 2.0, PHP 5.0 Code Igniter, *framework*, r*egex*