Abstrak

Salah satu metode yang dipakai untuk melakukan penyerangan terhadap aplikasi *website* adalah SQL *injection*. SQL *injection* adalah teknik yang meng-eksploitasi celah keamanan yang muncul di sekitar lapisan basis data dan aplikasinya. Celah keamanan tersebut ditunjukkan pada saat *user* memasukkan nilai *string* dan karakter kontrol lain yang ada dalam instruksi SQL atau *user* memasukkan *string* dengan tipe data tidak sama yang seharusnya tidak diproses [3].

Dengan besarnya ancaman dari SQL *injection* maka mendorong para peneliti untuk melakukan evaluasi baik dari segi bahasa pemrograman maupun *database* seperti yang dilakukan oleh Chris Anley yang mencoba menerapkan SQL *injection* pada *website* berbasis bahasa pemrograman Active Server Pages dengan database SQL Server 2000 (SQL 1) [2]. Dari pengujian tersebut di dapatkan hasil bahwa masih banyak teknik SQL *injection* yang belum tertangani oleh sebuah *website* dengan konfigurasi tersebut. Oleh karena itu, perlu dilakukan penanganan dengan lebih memanfaatkan kemampuan, fungsi dan konfigurasi yang dimiliki oleh bahasa pemrograman dan *database* dalam sebuah aplikasi *website*.

Berdasarkan hasil pengujian dan melihat kemampuan .Net yang merupakan simbol berubahnya model pengembangan *website* yang menggunakan *framework* [11], serta melihat versi terbaru dari SQL Server adalah SQL Server 2008 (SQL 2) yang memiliki beberapa keunggulan dalam hal penanganan SQL *injection* dibandingkan dengan SQL 1 [12], maka dapat disimpulkan bahwa penggunaan .Net Framework dan SQL 2 lebih baik dibandingkan dengan penggunaan .Net Framework dan SQL 1 dari segi *vulnerability* terutama pada kasus SQL *injection*. Sehingga didapatkan hasil perbandingan antara kedua konfigurasi tersebut serta dapat diketahui bagaimana pengaruh bahasa pemrograman maupun *database* terhadap penanganan serangan SQL *injection* pada sebuah *website*.

Kata kunci : *SQL Injection, SQL Server 2000, SQL Server 2008, .Net Framework*