Abstrak

SQL Injection adalah suatu serangan yang dilakukan dengan cara menyisipkan suatu perintah *query SQL* ke dalam bagian *input* agar dapat mengakses *database* yang terdapat pada aplikasi *web*. *SQL Injection* sering terjadi karena tidak adanya *filtering* yang dilakukan pada saat data *input* masuk ke dalam *database*. Oleh karena itu, diperlukan sebuah pencegahan agar *input* yang masuk dapat diseleksi terlebih dahulu sebelum masuk ke dalam *database*. Pencegahan tersebut dapat diperoleh dari fungsi yang terdapat pada bahasa pemrograman serta *framework* dari bahasa pemrograman tersebut.

Pada penelitian ini, dilakukan analisis dan perbandingan akurasi pencegahan serangan *SQL injection* pada *framework* CodeIgniter dan *framework* Laravel. Pada *framework* CodeIgniter digunakan fungsi *escaping query* untuk mencegah serangan *SQL injection*. Sedangkan, pada *framework* Laravel digunakan fungsi *eloquent ORM* untuk mencegah serangan *SQL injection*.

Berdasarkan hasil pengujian dan analisa diperoleh bahwa serangan *SQL injection* pada *framework* CodeIgniter dan *framework* Laravel dapat dicegah dengan sama baik menggunakan fungsi *escaping query* pada *framework* CodeIgniter dan fungsi *eloquent ORM* pada *framework* Laravel. Dari hasil pengujian diperoleh akurasi 100% dari 293 serangan *SQL injection*.

Kata kunci : *SQL*, *SQL Injection*, CodeIgniter, Laravel, Akurasi