ABSTRAK

Framework Codeigniter merupakan aplikasi open source, tetapi *Framework* ini rentan terhadap SQL *Injection*. Padahal penggunaan aplikasi sangat banyak digunakan untuk *webserver* pelayanan umum, seperti di pemerintahan. Salah satunya adalah pemerintahaan Sumatera Barat. Untuk itu diperlukan suatu metode yang tepat dalam memantau kelemahaan aplikasi ini, sehingga dapat dijaga kelancarannya dalam akses oleh pemakai. Tujuan dari penelitian adalah mengidentifikasi celah SQL *Injection* pada *Framework Codeigniter* menggunakan model forensik. Melalui identifikasi ini dapat dilakukan tindakan pencegahan awal. *Webserver* yang diidentifikasi adalah subdomain Sikamek pemerintahan Sumatera Barat. Data pengujian yang diolah adalah celah kritis. Tahapan identifikasi terdiri atas *Collection*, *Examination*, *Analysis*, *Reporting*, dan *Execution*. Hasil pengujian terhadap model ini berupa informasi celah SQL *Injection*. Informasi ini dibuktikan dengan vulnerable dari urlnya. Terdapat 10 jenis *Blind* SQL dan 2 *Error-based* SQL pada masing-masing url. Beberapa dari celah dapat mengakses *database* , hal ini menjadikan pedoman untuk memperbaiki keamanan sistem. Informasi dari pengolahan ini adalah mendapatkan kelemahan SQL *Injection* subdomain web server pemerintahan Sumatera Barat. Maka penelitian ini menjadi rekomendasi dalam meningkatkan pencegahaan terjadinya celah di masa yang akan datang.

Kata Kunci : *Codegniter*, Kelemahan Subdomain, Model Forensik, SQL *Injection*