ABSTRAK

DB XML adalah suatu sistem penyimpanan *database* yang memanfaatkan teknologi XML. DB XML ini dianggap sebagai solusi lain untuk mengganti *database* relasional. Kelebihannya dibanding *database* relasional adalah mengurangi ukuran dan kompleksitas aplikasi, meningkatkan efisiensi dan fleksibilitas penyimpanan, performansi aplikasi yang dihasilkan lebih baik, serta fleksibel, karena *platform independent* dan *language independent*. Namun kekurangan dari DB XML adalah tidak adanya pendefinisian hak akses *user*. Dengan kata lain, siapapun dapat mengakses DB XML tersebut tanpa ada perbedaan *privilege*. Di sinilah terjadi celah keamanan terhadap penggunaan DB XML. *Malicious user* dari suatu *web service yang* berbasis SOAP (*Simple Object Access Protocol*) dapat memanfaatkan celah keamanan ini untuk melakukan teknik-teknik serangan tertentu, salah satunya adalah XPath *Injection*. XPath *Injection* memungkinkan seorang penyerang dapat berkomunikasi secara langsung kepada *database* XML lewat *user input* yang disediakan oleh aplikasi sehingga *attacker* dapat mengakases informasi-informasi sensitif dari DB XML.

Pada tugas akhir ini dibangun suatu *service* tambahan yang berfungsi sebagai modul untuk meminimalisir terjadinya serangan XPath *Injection*, dengan menggunakan empat buah metode yang berbeda, yaitu *data type validation, input validation, integrity check, dan parameterized query.* Pengujian akan dilakukan dengan menganalisis jumlah vektor *query* injeksi yang berhasil ditangani, vektor *query* injeksi yang berhasil lolos (tidak tertangani), dan pengaruh *average execution time* dari masing-masing modul terhadap sistem.

Berdasarkan hasil penelitian, didapat bahwa metode *input validation, integrity check,* dan *parameterized query* adalah metode yang cukup baik dalam meminimalkan terjadinya serangan XPath *Injection* dilihat dari segi jumlah vektor *query* yang berhasil ditangani.

Kata kunci: DB XML, XPath *Injection, Web Service, SOAP*