ABSTRAK

SIMULASI ANCAMAN KEAMANAN PADA APLIKASI BERBASIS WEB

Oleh

GIRINDRO PRINGGO DIGDO
10108262

Aplikasi web merupakan aplikasi yang diakses menggunakan penjelajah web melalui suatu jaringan seperti Internet atau Intranet. Aplikasi web menjadi populer karena kemudahan tersedianya aplikasi *client* untuk mengaksesnya. Kemampuan untuk memperbarui dan memelihara aplikasi web tanpa harus mendistribusikan dan menginstalasi perangkat lunak pada ribuan komputer klien merupakan alasan kunci popularitasnya.

Namun dampak dari kemudahan tersebut, aplikasi web juga berpeluang dari ancaman orang luar yang tidak bertanggung jawab. Ancaman yang paling sering terjadi pada aplikasi web adalah ancaman pada *database*. Ancaman tersebut adalah *SQL Injection.*

SQL Injection merupakan metode ancaman yang mengizinkan *client* untuk mengeksekusi *database* melalui URL dan mendapatkan akses untuk memperoleh informasi penting. Selain dari ancaman *SQL Injection*, aplikasi web juga rentan terhadap ancaman *Cross Site Scripting.*

Cross Site Scripting merupakan metode ancaman yang memaksa situs web untuk menampilkan kode berbahaya yang dijalankan pada browser web pengguna.

Untuk menanggulangi ancaman tersebut, maka dibutuhkan suatu mekanisme pertahanan terhadap ancaman yang dilakukan. *Validating Input* adalah metode pengujian masukan yang diterima oleh aplikasi terhadap standar yang telah didefinisikan.

Berdasarkan pengujian yang telah dilakukan disimpulkan bahwa metode *Validating Input* yang dibangun dapat menjadi mekanisme pertahanan terhadap serangan *SQL Injection* dan *Cross Site Scripting.*

Kata Kunci: *SQL Injection, Cross Site Scripting, Validating Input*.