BAB V

KESIMPULAN DAN SARAN

5.1 Kesimpulan

Berdasarkan penelitian yang dilakukan mengenai simulasi ancaman keamanan pada aplikasi berbasis web, maka dapat diperoleh kesimpulan sebagai berikut:

1. Ancaman keamanan pada aplikasi web dapat diketahui melalui simulasi.
2. Metode *Input_Encoding* belum dapat mencegah ancaman *Cross Site Scripting* karena metode tersebut memerlukan pendefinisian pada tiap karakter.
3. Metode *Base64_Encode* belum dapat mencegah ancaman *SQL Injection* karena metode tersebut masih dapat dimanipulasi dengan mengkonversikan *string* kebentuk *Base64_Encode*.
4. Metode *Validating Input* merupakan metode yang dapat menangani ancaman *Cross Site Scripting* dan *SQL Injection*.

5.2 Saran

Untuk lebih meningkatkan analisis pada simulasi ancaman keamanan pada aplikasi web, maka ada beberapa saran yang dapat dijadikan pertimbangan, yaitu:

1. *Error Handling* pada *SQL Injection* dapat dibuat sebuah *log* dengan isi *log* berupa data *IP Address client*, waktu eksekusi, *URL* yang dieksekusi, serta informasi yang berhubungan dengan ancamanan yang terjadi.

2. Pembuatan sebuah aplikasi yang berfungsi untuk mem-*patch* sistem secara *user friendly* sehingga pengguna dengan mudah mengamankan aplikasi web yang sedang dikelola.
3. Pembuatan *time limit* yang mencatat setiap *IP Address* yang diidentifikasi melakukan ancaman, sehingga pada rentang waktu tertentu *IP Address* tersebut tidak bisa mengakses aplikasi web/di blokir.
4. Penggunaan metode *HTTPOnly Cookie* dan *Secure Flag* pada ancaman *Cross Site Scripting.*