BAB V

PENUTUP

5.1 Kesimpulan

Setelah melakukan analisis keamanan *Zimbra Mail Server*, dan melakukan proses percobaan serangan keamanan terhadap *Mail Server* tersebut, maka penulis mengambil kesimpulan sebagai berikut:

1. Serangan keamanan dengan menggunakan metode *SQL Injectiion* hanya bisa menyerang sistem informasi yang berbasis web, yang menyimpan seluruh datanya menggunakan sistem basis data.
2. Penulis mendapatkan bahwa *Mail Server Zimbra* tidak dapat di serang menggunakan *SQL Injection* di karenakan *Mail Server Zimbra* tidak menyimpan *file* serta user login pada *database*, melainkan disimpan pada *FileSystem*, sehingga *Mail Server Zimbra* aman.
3. Metode SQL Injection memiliki keterbatasan dalam melakukan injeksi terhadap website yaitu hanya menyerang website yang memiliki sistem basis data.

5.2 Saran

Saran dari penulis untuk pengembangan penelitian dimasa yang akan datang sebagai berikut:

1. Penyerangan atau injeksi terhadap website tidak hanya dapat dilakukan dengan satu metode saja, akan tetapi ada beberapa metode lain yang dapat di analisis yaitu seperti, metode *Social Engineering*, *Hardware Error*, *Software Error*, dan Kesalahan User.
2. Komputer yang ada di masa kini memiliki kemampuan yang terus meningkat, sehingga ancaman keamanan terhadap suatu *website* tidak dapat dianggap sebagai hal yang tidak mungkin, akan tetapi setiap waktu dan setiap saat dapat terjadi dengan adanya suatu serangan keamanan dari grup komputer seperti *botnet*.
3. Aplikasi yang digunakan oleh *website* tidak dapat dikelola dengan mudah, dikarenakan setiap user memiliki pola dan tindak tanduk penggunaan yang berbeda – beda., sehingga ada kemungkinan serangan keamanan berasal dari pihak internal sendiri. Sehingga diharapkan ada rancangan keamanan untuk menghadapi serangan dari pihak internal.