BAB V

KESIMPULAN DAN SARAN

5.1. Kesimpulan

Setelah dilakukan uji coba dan evaluasi pada Aplikasi Belajar Web Hacking ini, maka dapat diambil kesimpulan sebagai berikut:

1. Aplikasi dapat menyajikan berbagai misi (soal) sebanyak 22 misi dengan total poin (skor) 1000 yang meliputi materi tentang Protokol HTTP, SQL Injection pada MySQL 5, *Javascript*, kelemahan password, enkripsi, *dictionary attack* dan kemampuan membuat *script*. Misi-misi terbagi dalam tiga kategori yaitu *Basic Mission* dengan 7 misi (150 poin), *Javascript Mission* dengan 8 misi (150 poin), dan *Realistic Mission* dengan 7 misi (700 poin). Prosentase penyelesaian misi dari tiap-tiap kategori dan rata-rata perolehan poin dari 10 *web developer* yang diuji adalah *Basic Mission* 34,28% (35,7 poin), *Javascript Mission* 58,75% (74,4 poin) dan Realistic Mission 22,85% (61,6 poin). Dengan demikian aplikasi dapat digunakan untuk mengevaluasi kemampuan *web developer* melalui serangkaian misi dan pemberian poin dimana setelah dilakukan pengujian prosentase tingkat penyelesaian *web developer* cukup rendah untuk kategori *Basic Mission* dan *Realistic Mission* yaitu dibawah 50%.
2. Berdasarkan hasil uji coba, didapatkan bahwa aplikasi dapat terintegrasi dengan jejaring sosial Facebook dimana aktifitas yang dilakukan pada aplikasi dapat terlihat pada akun Facebook pengguna. Hal tersebut terindikasi ketika proses otentikasi dimana pengguna hanya memerlukan akun Facebook untuk dapat terotentikasi, kemudian ketika pengguna berhasil

menyelesaikan misi dan saat pengguna berhasil menyalip perolehan skor dari pengguna lain, aktifitas-aktifitas tersebut terlihat pada akun Facebook pengguna.

5.2. Saran

Saran yang dapat diberikan untuk pengembangan aplikasi lebih lanjut adalah sebagai berikut:

1. Pemberian status tingkatan atas pencapaian yang dilakukan pengguna pada aplikasi. Sebagai contoh status tingkatan yang dapat diberikan adalah "Hacker", "Newbie", dan "Script Kiddie". Salah satu cara untuk membuat status tingkatan dapat dilihat berdasarkan skor yang diperoleh atau berdasarkan materi penyusun soal-soal yang diselesaikan.
2. Materi pembelajaran keamanan aplikasi berbasis web yang dapat ditambahkan pada aplikasi adalah tentang *Cross-site Scripting* (XSS) dan *Cross-site Request Forgery* (CSRF). Dimana aplikasi harus dapat mensimulasikan hubungan antara tiga objek yaitu penyerang, korban, dan server.
3. Disediakan sebuah *mission creator* untuk membuat soal-soal baru tanpa harus melakukan upload file ke server secara manual.