BAB V
Penutup

5.1 Kesimpulan

Dari penelitian dan rangkaian pengujian yang telah dilakukan, terdapat beberapa hasil kesimpulan yang didapat:

1. Nilai parameter yang dienkripsi dengan *AES-256* dapat melindungi nilai parameter dari serangan *sql injection*. Hal ini dibuktikan dengan pengujian *sql injection* secara manual dimanah tidak ditemukan petunjuk berupa *error* yang dibutuhkan untuk melakukan pengujian sesuai skenario. Serta pengujian *sql injection* dengan alat *SQL Map* yang melaporkan bahwa parameter yang dijadikan target tidak dapat dilakukan *sql* injeksi.
2. Situs yang dibangun dengan metode *prepare statement* dapat melindungi nilai parameter dari serangan *sql injection*. Hal ini dibuktikan dari pengujian *sql injection* yang sama pada pengujian pada nilai parameter dengan enkripsi yang menghasilkan hasil luaran yang sama yakni dimanah tidak ditemukan petunjuk berupa *error* yang dibutuhkan untuk melakukan pengujian sesuai skenario dan alat *SQL Map* yang melaporkan bahwa parameter yang dijadikan target tidak dapat dilakukan *sql* injeksi.
3. Mengenai dampak serangan *sql injection* didapatkan kesimpulan bahwa dampak serangan *sql injection* sangatlah serius dimanah saat pengujian pada situs tanpa enkripsi dan tanpa penggunaan metode *prepare statement* bisa didapatkannya data sensitif berupa profil pengguna yaitu username dan pass*word*. Data sensitif ini dapat diperoleh dari pengujian secara manual dan pengujian menggunakan alat *sqlmap*. Selain itu selama proses pengujian, data sensitif lain seperti informasi kumpulan *database*, tabel, kolom dan record(data) pada DBMS bisa ditampilkan secara jelas dan menyeluruh serta data dapat disalin ke komputer penyerang. Ini menjelaskan kasus penyerangan ini berbahaya dan bisa berujung ke kasus penjualan data serta illegal akses terhadap basis data pada situs web seperti yang dijelaskan pada latar belakang.

5.2 Saran

Diharapkan pada penelitian selanjutnya dalam penggunaan *AES-256* bisa ditambahkan penambahan fitur enkripsi kunci untuk *AES* 256 dan fitur mengahasilkan kata acak untuk kunci yang digunakan untuk *AES 256*. Serta diharapkan pada penilitian selanjutnya untuk dilakukan uji coba alternatif metode pengamanan *SQL* pada sisi aplikasi atau situs web

terhadap *SQL injection* yang tertera pada OWASP seperti halnya *input validation* agar nilai parameter terhindar dari *paylod sql injection* sebelum di isikan ke parameter *URL*.