BAB V

KESIMPULAN DAN SARAN

5.1 Kesimpulan

Berdasarkan hasil penelitian, dapat disimpulkan bebapa hal sebagai berikut:

1. Methode kombinasi *mekle-hellman knapsack* dan AES bekerja dengan melakukan proses enkripsi *merkle-hlellman knapsack* dengan mengggunakan *private key* sebagai objeck untuk melakukan dekripsinya setlah melakukan perhitungan matematk yang ditentukan . dari pengolahan *private key* menghasilkan *public key* untuk proses enkripsi dari knapsack tersebut. Proses enkripsi *merkle-hellman knapsack* dikomponasikan dengan AES 256 dimana proses enkripsi terhadap AES-256 dengan format blok CBC terlebih dahulu dengan menentukan panjang iv (*initialization vector*) dan *key* serta pembacaan *plaintext* melalui input data dari proses *Create* atau *Update* dengan hasil berupa *ciphertext* dari AES-256.
2. Hasil serangan sql injection menunjukan bahwa system berjalan dengan baik dibuktikan dengan terjadinya error Ketika melakukan sqlmap. Errornya sqlmap membuat data yang terenkripsi tidak dapat diambil dan tidak dapat terbaca.
3. Hasil akhir dari penelitian menunjukan jika kombinasi *merkle-hellman knapsack* dan AES 256 dapat mengamankan data pada *database*. Karenakan data yang muncul akan selalu berupa chipertext aes 256.

5.2 Saran

Penelitian ini bisa dibilang masih kurang sempurna karena memiliki banyak kekurangan, diantaranya adalah sistem yang masih sangat sederhana. Dan juga masih ada proses pengujian web yang belum diujikan :

1. Pengujian menggunakan sistem *database* yang berbeda seperti Oracle, PostgreSQL ataupun Microsoft SQL Server.

2. Pengujian bisa dengan mendapatkan halaman web tersebut atau melakukan inspect pada webnya.
3. Perbaikan sistem secara keseluruhan dimana banyak aspek yang dapat ditingkatkan seperti penerapan *framework* (*Laravel*, *Code Igniter* dan lain-lain).
4. Semoga kedepannya penelitian ini bermanfaat untuk pembaca serta dapat menjadi sarana untuk penelitian lain agar menjadi penelitian yang lebih baik.