BAB V
PENUTUP

Temuan dari keseluruhan proses studi disajikan dalam bab ini, mulai dari perancangan, implementasi, hingga pengujian sistem. Selain itu, penutup ini terdapat saran untuk pengembangan lebih lanjut yang dapat dilakukan di masa mendatang berdasarkan temuan dan batasan dari penelitian yang telah dilaksanakan.

5.1 Kesimpulan

1. Implementasi metode Rijndael (AES) telah berhasil diterapkan sebagai lapisan pertahanan pasif yang efektif. Metode ini terbukti mampu melindungi kerahasiaan data kredensial pengguna saat disimpan di dalam basis data (data at rest) dengan mengubahnya menjadi format ciphertext yang tidak dapat dibaca.
2. Hasil pengujian keamanan secara empiris memvalidasi bahwa sistem yang dibangun tahan terhadap serangan In-band SQL Injection. Keberhasilan dalam menggagalkan serangan ini secara langsung membuktikan efektivitas dari praktik pengkodean aman menggunakan parameterized query sebagai pertahanan aktif. Hal ini, saat dikombinasikan dengan enkripsi Rijndael sebagai pertahanan data pasif, menegaskan bahwa pendekatan keamanan berlapis (defense in depth) adalah strategi esensial untuk melindungi integritas sistem dan mencegah akses tidak sah secara menyeluruh .

5.2 Saran

Meskipun penelitian ini telah berhasil mencapai tujuannya, Untuk meningkatkan keamanan dan fungsionalitas sistem secara keseluruhan, sejumlah fitur dapat dikembangkan lebih lanjut. Berikut beberapa ide untuk studi tambahan:

a. Manajemen Kunci yang Lebih Dinamis:

Kunci enkripsi pada penelitian ini masih bersifat statis (di-hardcode dalam aplikasi). Untuk meningkatkan keamanan, penelitian selanjutnya

dapat mengembangkan sistem manajemen kunci (Key Management System) yang lebih dinamis, misalnya dengan menghasilkan kunci yang unik untuk setiap pengguna atau melakukan rotasi kunci secara berkala.

b. Implementasi Salting dan Hashing:

Walaupun enkripsi Rijndael sudah kuat, pra ktik keamanan modern untuk password umumnya merekomendasikan penggunaan algoritma hashing yang lambat (seperti Argon2 atau bcrypt) yang dikombinasikan dengan salt unik untuk setiap pengguna. Penelitian selanjutnya bisa membandingkan pendekatan enkripsi Rijndael menggunakan hashing untuk memeriksa manfaat dan kekurangan masing-masing terkait dengan keamanan sistem login.

c. Pengujian Keamanan yang Lebih Luas:

Pengujian pada penelitian ini difokuskan pada serangan SQL Injection. Pengembangan selanjutnya dapat memperluas cakupan pengujian keamanan untuk mencakup kerentanan umum lainnya pada aplikasi web, seperti Cross-Site Scripting (XSS), Cross-Site Request Forgery (CSRF), dan Broken Access Control untuk membangun sistem yang lebih tangguh secara menyeluruh.

d. Pengembangan Fitur Aplikasi:

Aplikasi yang dibangun masih berupa prototipe. Untuk menjadi aplikasi yang siap pakai, dapat ditambahkan fitur-fitur lain seperti proses pemesanan yang fungsional, manajemen menu oleh admin, riwayat transaksi yang detail, dan sistem pembayaran.