BAB V
PENUTUP

5.1 Simpulan

Berdasarkan hasil dari pengujian keamanan terhadap aplikasi web To-Do List, dapat disimpulkan bahwa:

a. Aplikasi terbukti memiliki kerentanan terhadap SQL Injection pada fitur login dan registrasi. Kerentanan ini memungkinkan penyerang melakukan bypass autentikasi hanya dengan memanipulasi input form menggunakan payload SQl Injection, sehingga bisa mengakses dashboard admin tanpa kredensial yang sah.
b. Selain SQL Injection ditemukan juga kerentanan Cross Site Scripting (XSS) pada fitur tambah tugas dan edit tugas. Celah ini memungkinkan penyerang menyisipkan skrip berbahaya yang akan dijalankan secara otomatis di sisi klient saat halam dimuat, terbukti melalui munculnya pop-up setelah payload XSS berhasil dieksekusi.
c. Hasil pengujian ini telah menjawab permasalahan yang diangkat dalam penelitian, yaitu mengidentifikasi dan membuktikan adanya kerentanan XSS dan SQL Injection pada aplikasi web To-Do List. Temuan ini kemudian di dokumentasikan dalam bentuk VOC dan digunakan sebagai dasar untuk menyusun rekomendasi perbaikan untuk memperkuat aspek keamanan aplikasi dalam proses pengembangannya.

5.2 Saran

Berdasarkan hasil temuan dan analisis terhadap kerentanan aplikasi web To-Do List,berikut adalah saran yang ditujukan kepada pengembang aplikasi dan pihak pengelola sistem, yang tidak dapat dilakukan oleh penguji keamanan namun penting untuk diterapkan guna meningkatkan keamanan aplikasi secara menyeluruh:

a. Implementasi Mekanisme Validasi dan Sanitasi di SIsi Server
b. Penggunaan Prepared Statements di Seluruh Query Basis Data
c. Penerapan Output Encoding Secara Menyeluruh

d. Peningkatan Keamanan Hak Akses Basis Data
e. Audit atau Peninjauan Keamanan Secara Berkala

Dengan menerapkan saran-saran tersebut, aplikasi web To-Do List akan memiliki ketahanan yang lebih baik terhadap serangan umum seperti SQL Injection dan XSS, serta mendukung praktik pengembangan perangkat lunak yang lebih