BAB V

PENUTUP

5.1 Simpulan

Hasil pengujian keamanan terhadap aplikasi web forum diskusi menunjukkan adanya kerentanan signifikan, khususnya pada fitur yang memproses input pengguna. Kerentanan *SQL Injection* ditemukan pada fitur login, memungkinkan bypass autentikasi dan akses ke data sensitif. Sementara itu, celah *Cross-Site Scripting (XSS)* terdeteksi pada kolom komentar dan Registrasi, yang memungkinkan eksekusi skrip berbahaya di sisi pengguna.

Pengujian ini berhasil memenuhi tujuan penelitian dengan membuktikan adanya potensi eksploitasi melalui pendekatan *greybox testing* dan standar *OWASP ASVS*.

5.2 Saran

Sebagai tindak lanjut dari hasil penelitian, berikut beberapa saran yang dapat diberikan:

1. Lakukan validasi dan sanitasi input secara menyeluruh di seluruh titik input pengguna termasuk formulir login, registrasi, dan komentar diskusi.
2. Gunakan mekanisme *prepared statements* dan *parameter binding* dalam semua query basis data untuk mencegah eksploitasi *SQL Injection*.
3. Terapkan filter karakter khusus dan *encoding output* pada data yang ditampilkan kembali kepada pengguna, guna mencegah eksekusi skrip berbahaya *Cross-Site Scripting (XSS)*.