BAB V
PENUTUP

5.1 Simpulan

Berdasarkan hasil pengujian keamanan terhadap aplikasi Web *G-Entry* dapat disimpulkan bahwa:

a. Aplikasi web *G-entry* memiliki kerentanan terhadap serangan SQL Injection (SQLi) pada fitur login dan registrasi. Hal ini terbukti dari keberhasilan manipulasi input yang memungkinkan bypass autentikasi dan menampilkan error basis data. Eksploitasi lanjutan menggunakan SQLMap juga memungkinkan pengambilalihan data sensitif dari database.

b. Fitur input buku tamu memiliki kerentanan terhadap serangan *Cross-Site Scripting (XSS)*. Celah ini memungkinkan penyerang menyisipkan skrip berbahaya yang akan dieksekusi di sisi pengguna, dibuktikan dengan munculnya pop-up JavaScript saat data ditampilkan ulang.

c. Pengujian ini berhasil menjawab tujuan penelitian, yaitu mengidentifikasi potensi kerentanan, membuktikan potensi eksploitasi, serta mendokumentasikan temuan untuk digunakan sebagai dasar evaluasi dan peningkatan keamanan aplikasi web di masa mendatang.

5.2 Saran

Adapun saran yang dapat dilakukan sebagai tidak lanjut dalam penelitian ini adalah :

a. Terapkan validasi input dan output secara menyeluruh pada seluruh form yang menerima data pengguna untuk mencegah eksekusi kode berbahaya.

b. Gunakan *prepared statements* dan parameter binding pada query basis data untuk mencegah serangan SQL Injection.

c. Implementasikan encoding output menggunakan fungsi seperti *htmlspecialchars()* untuk memfilter karakter berbahaya guna mencegah serangan XSS.

d. Lakukan pengujian keamanan lanjutan dengan cakupan lebih luas, termasuk fitur-fitur tambahan, agar potensi risiko keamanan dapat diantisipasi lebih menyeluruh dan sistem lebih siap menghadapi ancaman dunia nyata.