BAB I

PENDAHULUAN

1.1 Latar Belakang

Keamanan pada aplikasi web menjadi aspek krusial di era digital saat ini, di mana aktivitas berbasis internet semakin mendominasi berbagai bidang kehidupan. Aplikasi web yang tampak sederhana seperti G-Entry pun tidak luput dari risiko keamanan, terutama jika tidak dilengkapi dengan praktik perlindungan yang memadai. Salah satu cara yang dapat dilakukan untuk menjaga keamanan sistem adalah melalui pengujian keamanan (penetration testing), yang bertujuan untuk mengidentifikasi dan memetakan potensi celah (vulnerabilities) yang bisa dieksploitasi oleh pihak tidak bertanggung jawab. Dua jenis serangan yang masih sering ditemukan hingga kini adalah SQL Injection (SQLi) dan Cross-Site Scripting (XSS). SQLi memanfaatkan kelemahan dalam pengolahan query database untuk mendapatkan akses atau melakukan manipulasi data secara ilegal, sedangkan XSS memungkinkan penyerang menyisipkan skrip berbahaya yang dijalankan di sisi pengguna untuk mencuri data atau mengganggu tampilan situs. Penelitian ini difokuskan pada pengujian keamanan terhadap aplikasi G-Entry, yaitu sistem buku tamu digital, yang memiliki fitur login, registrasi akun, serta form pengisian pesan – komponen yang berpotensi rawan jika tidak dilindungi dengan validasi input yang baik. Proses pengujian dilakukan secara manual menggunakan Burp Suite, sebuah tools yang digunakan untuk menganalisis trafik data, memodifikasi parameter, dan menyisipkan payload eksploitasi ke dalam permintaan HTTP. Pengujian ini mengacu pada standar OWASP Top 10, terutama pada kategori serangan injection dan XSS. Kegiatan ini merupakan bagian dari program magang di PT. Sekuriti Siber Indonesia, perusahaan yang bergerak di bidang keamanan siber dan menyediakan layanan pentest, operasional SOC, serta pelatihan keamanan informasi. Dengan bimbingan langsung dari para profesional, pengujian dilakukan secara sistematis dan menyeluruh, tidak hanya pada

aspek teknis, tetapi juga pada pemahaman pentingnya keamanan sejak tahap awal pengembangan. Harapannya, hasil pengujian ini dapat menjadi acuan untuk meningkatkan keamanan aplikasi serupa di masa mendatang.

1.2 Deskripsi Pekerjaan

Dalam pelaksanaan tugas akhir ini, penulis berperan dalam menyusun dan mengimplementasikan proses pengujian terhadap aspek keamanan aplikasi web G-Entry. Kegiatan difokuskan pada upaya mengidentifikasi serta mengevaluasi kelemahan sistem yang berkaitan dengan serangan SQL Injection (SQLi) dan Cross-Site Scripting (XSS). Selain itu, seluruh hasil pengujian didokumentasikan guna menjadi dasar penyusunan langkah mitigasi yang relevan. Penjabaran lengkap mengenai aktivitas tersebut disampaikan pada bagian berikut..

1.3 Tujuan

Penelitian ini bertujuan untuk menguji keamanan aplikasi web G-Entry dengan menitikberatkan pada identifikasi serta analisis celah keamanan berupa SQL Injection (SQLi) dan Cross-Site Scripting (XSS), menggunakan metode penetration testing yang berpedoman pada standar OWASP Top 10. Selain itu, penelitian ini juga dimaksudkan untuk membuktikan potensi eksploitasi pada fitur input pengguna seperti form login, registrasi, dan pengisian pesan pada sistem buku tamu. Setiap temuan kerentanan akan didokumentasikan dalam bentuk Vulnerability of Concern (VoC) yang dilengkapi dengan bukti teknis serta analisis dampaknya. Penelitian ini juga menyusun saran perbaikan teknis untuk membantu meningkatkan keamanan sistem di kemudian hari, sekaligus menjadi bagian dari pembelajaran langsung selama kegiatan magang di PT. Sekuriti Siber Indonesia dalam rangka memperdalam pemahaman praktis terhadap proses pengujian keamanan aplikasi web.

1.4 Manfaat

Penelitian ini bermanfaat dalam meningkatkan pemahaman tentang pentingnya melakukan pengujian keamanan pada aplikasi web, khususnya untuk mengidentifikasi dan mengatasi kerentanan terhadap serangan XSS dan SQL Injection. Secara praktis, temuan dari penelitian ini dapat dijadikan panduan oleh para pengembang dan profesional keamanan dalam menerapkan langkah-langkah mitigasi sejak awal proses pengembangan aplikasi. Selain itu, penelitian ini juga memiliki nilai edukatif, karena dapat dimanfaatkan sebagai bahan pembelajaran baik di lingkungan akademik maupun industri. Khususnya bagi PT. Sekuriti Siber Indonesia, hasil penelitian ini mendukung penguatan program magang berbasis studi kasus nyata dalam konteks pengujian keamanan aplikasi web.