BAB I
PENDAHULUAN

1.1 Latar Belakang

Keamanan aplikasi web merupakan aspek penting dalam pengembangan perangkat lunak, terutama di era digital yang sangat bergantung pada sistem online. Aplikasi sederhana seperti To-Do List pun tetap beresiko menjadi sasaran serangan jika tidak dibekali dengan mekanisme keamanan yang memadai. Oleh karena itu, pengujian keamanan atau penetration testing dibutuhkan untuk mendeteksi celah kerentanan sejak dini.

Penelitian ini memfokuskan pengujian terhadap dua jenis serangan umum yaitu SQL Injection dan Cross Site Scripting (XSS). SQLi ini memungkinkan penyerang memanipulasi query database untuk memperoleh akses tidak sah, sedangkan XSS memungkinkan penyisipan skrip berbahaya yang dieksekusi di sisi pengguna. Umumnya, kedua serangan ini terjadi akibat kurangnya validasi input dan sanitasi data pada aplikasi.

Objek pengujian adalah aplikasi To-Do List dengan fitur login, registrasi, tambah tugas, dan edit tugas seluruhnya berinteraksi langsung dengan database. Pengujian dilakukan secara manual dengan menggunakan Burp Suite untuk menganalisis trafik HTTP, memodifikasi parameter, serta menyisipkan payload eksploitasi. Hasil pengujian didokumentasikan dalam bentuk Vulnerability of Concern (VOC), lengkap dengan dampak dan rekomendasi mitigasi.

Pengujian ini mengacu pada OWASP Top 10 tahun 2021,khususnya kategori A03: Injection dan A07: Cross Site Scripting (XSS). Penelitian ini dilaksanakan dalam rangka program magang di PT. Sekuriti Siber Indonesia dan dibimbing langsung oleh tim profesional untuk memahami proses pengujian secara teknis maupun praktis sebagai bentuk kontribusi dalam meningkatkan keamanan aplikasi.

1.2 Deskripsi Pekerjaan

Selama menjalani program magang, saya berfokus pada bagian tugas yang berkaitan dengan keamanan siber, mencakup pemantauan , pelaporan,serta pengujian kerentanan pada aplikasi web. Lingkup pekerjaan yang saya lakukan adalah sebagai berikut:

a. Pembelajaran dan Praktik Penetration Testing

   Mendalami teori dan teknik penetration testing untuk mengidentifikasi kerentanan keamanan pada aplikasi web. Aktivitas ini meliputi eksplorasi alat-alat pengujian seperti OWASP ZAP dan Burp Suite, serta pemahaman kerangka kerja pengujian seperti OWASP untuk memastikan pengujian dilakukan secara terstruktur.

b. Pelaksanaan Penetration Testing pada Aplikasi Web

   Mengaplikasikan metode penetration testing pada aplikasi web untuk mengidentifikasi kerentanan, seperti SQL Injection, Cross Site Scripting (XSS). Proses ini mencakup tahap perencanaan eksplorasi kerentanan, hingga tahap dokumentasi hasil yang diperoleh dari pengujian dan rekomendasi perbaikan yang mendetail untuk pengembangan aplikasi.

Dalam lingkup magang ini mencerminkan keseriusan dan kompleksitas yang menuntut ketelitian, kemampuan analisis, serta pemahaman yang mendalam terkait dengan keamanan siber. Setiap tugas dilakukan dengan cara berkolaborasi sebagai tim untuk memastikan sistem yang dikelola tetap aman dan sesuai dengan standar kamanan.

1.3 Tujuan

Tujuan dari penelitian ini adalah untuk melakukan pengujian keamanan terhadap aplikasi web To-Do List, dengan fokus pada identifikasi dan analisis kerentanan Cross Site Scripting (XSS) dan SQL Injection menggunakan metode penetration testing yang mengacu pada standar OWASP Top 10 tahun 2021. Selain itu penelitian ini bertujuan untuk memberikan rekomendasi perbaikan terhadap temuan yang ditemukan, serta mendukung pengembang aplikasi web yang lebih aman dan sesuai dengan standar keamanan informasi.

1.4 Manfaat

Manfaat dari penelitian ini adalah memberikan pemahaman yang lebih mendalam mengenai pentingnya pengujian keamanan pada aplikasi web, khususnya dalam mengidentifikasi dan menangani kerentanan terhadap serangan XSS dan SQL Injection. Melalui studi ini, diharapkan pengembang aplikasi dan praktisi keamanan siber dapat menerapkan langkah-langkah mitigasi yang efektif untuk meningkatkan keamanan sistem sejak tahap awal pengembangan. Selain itu, penelitian ini juga bermanfaat sebagai referensi edukatif dalam dunia akademik maupun industri, khususnya bagi PT. Sekuriti Siber Indonesia dalam mendukung proses pembelajaran berbasis kasus nyata di bidang keamanan aplikasi web.