BAB I
PENDAHULUAN

1.1 Latar belakang

Perkembangan teknologi informasi yang sangat pesat telah mendorong digitalisasi di berbagai sektor, termasuk dalam industri pariwisata dan perjalanan. Salah satu wujud nyata dari digitalisasi ini adalah kehadiran *Online Travel Agent* (*OTA*), yaitu platform digital yang memungkinkan pengguna untuk memesan tiket pesawat, hotel, serta layanan perjalanan lainnya secara daring. Kemudahan dan kecepatan yang ditawarkan menjadikan *OTA* sebagai pilihan utama masyarakat dalam merencanakan perjalanan. Namun, di balik kenyamanan tersebut, terdapat tantangan besar dalam hal keamanan sistem dan perlindungan data pengguna.[1]

Karena sifatnya yang berbasis web dan menyimpan banyak data sensitif, sistem *OTA* sangat rentan terhadap serangan siber. Ancaman seperti *SQL Injection*, *Cross-Site Scripting* (*XSS*), dan *Clickjacking* merupakan contoh serangan yang dapat mengeksploitasi celah keamanan dalam aplikasi web. Jika celah ini tidak segera ditemukan dan ditangani, maka potensi penyalahgunaan informasi dan kerugian pengguna dapat terjadi.[2]

Untuk mengatasi permasalahan tersebut, diperlukan suatu pendekatan sistematis dalam mengidentifikasi dan menilai kerentanan pada sistem, salah satunya melalui *Vulnerability Risk Assessment*. Metode ini berfungsi untuk menganalisis tingkat risiko dari setiap celah keamanan yang ditemukan. Dalam penelitian ini, digunakan pendekatan berbasis *OWASP* (*Open Web Application Security Project*), yaitu standar terbuka yang banyak digunakan dalam pengujian keamanan aplikasi web. *OWASP* menyediakan daftar *Top* 10 yang berisi jenis-jenis kerentanan paling umum dan berbahaya yang harus diwaspadai oleh pengembang sistem.[3]

Metode yang digunakan pada penelitian ini adalah *Vulnerability Risk Assessment* dengan bantuan *tools* dari *OWASP*, yang secara khusus dirancang untuk

menguji dan mengevaluasi keamanan situs web.[4] Penggunaan *tools* ini memungkinkan penulis untuk mengidentifikasi masalah keamanan secara akurat pada platform *Online Travel Agent*. Berdasarkan urgensi dan konteks tersebut, penulis mengangkat topik ini ke dalam skripsi dengan judul **"Pengujian *Vulnerability Risk Assessment* Pada Sistem *Online Travel Agent (OTA)* Menggunakan Metode *OWASP*".**

1.2 Rumusan Masalah

Berdasarkan latar belakang tersebut, permasalahan yang dapat dirumuskan yaitu sebagai berikut :

1. Bagaimana cara menemukan celah keamanan yang terdapat pada platform *OTA*?
2. Bagaimana menilai tingkat risiko dari kerentanan keamanan pada tiap platform *OTA*?
3. Bagaimana solusi perbaikan sistem yang dapat diterapkan untuk meningkatkan keamanan pada masing-masing aplikasi *OTA*?

1.3 Batasan Masalah

Penelitian ini memiliki beberapa batasan yang telah ditetapkan sesuai dengan ruang lingkup dan tujuan studi. Aspek-aspek yang dibatasi dalam penelitian ini meliputi :

1. Penelitian ini difokuskan pada empat situs web yang beroperasi dalam platform *Online Travel Agent* (*OTA*).
2. Penelitian ini memanfaatkan *OWASP ZAP*, sebuah alat *open-source* untuk mengidentifikasi kerentanan pada aplikasi web, dan mengacu pada kerangka kerja *Vulnerability Risk Assessment* untuk menilai tingkat risiko dari kerentanan yang ditemukan.
3. Aspek rekayasa sosial tidak menjadi bagian dari ruang lingkup penelitian ini.

4. Hasil pengujian menghasilkan rekomendasi yang dapat digunakan untuk meningkatkan sistem dan menilai tingkat keamanan pada setiap platform *OTA*.
5. Penelitian ini menghasilkan dokumen tertulis yang merangkum seluruh proses dan temuan yang diperoleh.

1.4 Tujuan Penelitian

1. Untuk melakukan evaluasi keamanan pada platform *Online Travel Agent* (*OTA*) dengan menerapkan pendekatan dari *Open Web Application Security Project* (*OWASP*).
2. Untuk melakukan penilaian risiko kerentanan untuk menentukan tingkat keamanan pada setiap platform *Online Travel Agent* (*OTA*).
3. Untuk menyarankan langkah-langkah perbaikan yang dapat diimplementasikan dalam sistem guna memperkuat aspek keamanannya.

1.5 Manfaat Penelitian

Berikut adalah manfaat yang diharapkan dari penelitian ini :

1. Dapat dijadikan acuan untuk pengembangan pengetahuan dan penelitian berikutnya yang menerapkan metode dan kasus serupa.
2. Memberikan informasi tambahan serta usulan perbaikan yang dapat diterapkan guna meningkatkan tingkat keamanan sistem.
3. Pemahaman dan kesadaran terhadap aspek keamanan dalam sistem informasi.