BAB I

PENDAHULUAN

A. Latar Belakang

Perkembangan teknologi informasi yang pesat telah membawa dampak signifikan pada berbagai aspek kehidupan manusia, termasuk sektor pariwisata. Teknologi informasi saat ini digunakan sebagai alat untuk meningkatkan efisiensi dalam publikasi dan promosi, yang berperan penting dalam menarik wisatawan (Atmaja, 2023). Salah satu pemanfaatan teknologi informasi dalam promosi adalah melalui *website*. *Website* sebagai media promosi berbasis digital memiliki keunggulan karena dapat diakses tanpa batasan ruang dan waktu, sehingga mampu menjangkau audiens yang lebih luas serta memberikan informasi secara *real-time*. Selain itu, *website* juga memungkinkan penyedia layanan wisata untuk memberikan pengalaman yang lebih interaktif kepada calon wisatawan, seperti melalui galeri foto, video, serta integrasi dengan peta digital.

Seiring dengan meningkatnya digitalisasi, berbagai layanan berbasis web semakin berkembang untuk mempermudah akses informasi dan layanan bagi pengguna. Namun, perkembangan teknologi ini juga membawa tantangan baru dalam hal keamanan siber, karena semakin banyak ancaman yang dapat membahayakan data serta operasional sistem (Rahman Najwa, 2024). Jika *website* tidak memiliki sistem keamanan yang memadai, maka informasi penting yang disediakan oleh *website* tersebut

dapat dimanipulasi atau bahkan dihapus oleh pihak tidak bertanggung jawab, yang dapat berakibat pada berkurangnya kepercayaan wisatawan terhadap layanan yang disediakan.

Keamanan siber menjadi aspek yang sangat penting dalam pengelolaan *website*, terutama bagi platform yang menangani data sensitif pengguna. *Website* sering kali menjadi target utama serangan siber, baik oleh individu maupun kelompok yang berniat mengeksploitasi celah keamanan. Berbagai jenis serangan seperti *SQL Injection, Cross-Site Scripting (XSS),* dan *Distributed Denial of Service (DDoS)* dapat membahayakan integritas data serta mengganggu operasional sistem (Prasetyo et al., 2024). Jika tidak ditangani dengan baik, serangan ini dapat menyebabkan kebocoran data, pencurian informasi pribadi, hingga gangguan layanan yang berdampak luas. Dalam konteks pariwisata, serangan terhadap *website* resmi destinasi wisata atau instansi pemerintahan dapat mengakibatkan penyebaran informasi palsu, manipulasi harga tiket, serta penipuan yang berdampak negatif pada pengalaman wisatawan.

Ancaman keamanan siber semakin meningkat dari tahun ke tahun. Berdasarkan data dari Badan Siber dan Sandi Negara (BSSN), tercatat telah terjadi 370,02 juta serangan siber terhadap Indonesia pada tahun 2022. Dibandingkan dengan tahun sebelumnya (terjadi 266,74 juta serangan siber), jumlah ini meningkat sebesar 38,72%. Sektor administrasi pemerintahan menjadi target utama serangan siber di Indonesia dengan serangan berjumlah 284,09 juta. Fakta ini menunjukkan betapa pentingnya

penerapan keamanan data pada *website*, termasuk yang digunakan dalam sektor pariwisata. *Website* instansi pariwisata yang tidak memiliki sistem keamanan yang memadai berpotensi menjadi sasaran serangan siber, yang pada akhirnya tidak hanya merugikan pemerintah daerah, tetapi juga dapat menurunkan kepercayaan wisatawan dalam mencari informasi dan layanan wisata secara online.

Salah satu insiden yang pernah terjadi adalah gangguan pada website Dinas Pariwisata, Kebudayaan, Pemuda, dan Olahraga (Disparbudpora) Kabupaten Pacitan pada bulan April 2025, di mana situs tersebut mengalami kerusakan hingga harus dibangun ulang dari awal menggunakan instalasi WordPress yang baru. Insiden ini menimbulkan kekhawatiran akan adanya kelemahan dalam sistem keamanan yang diterapkan. Mengingat peran strategis website ini sebagai media resmi promosi potensi wisata daerah, maka kestabilan dan keamanannya menjadi sangat krusial.

Sebagai respons terhadap kondisi tersebut, pihak Disparbudpora menyampaikan kebutuhan untuk dilakukan pengujian keamanan pada dua situs resmi yang mereka kelola, yaitu disparbudpora.pacitankab.go.id dan wisata.pacitankab.web.id. Menanggapi permintaan tersebut, peneliti melakukan pengujian keamanan dengan pendekatan penetration testing mengacu pada standar NIST SP 800-115. Pengujian dilaksanakan dengan akses terbatas hingga panel admin, tanpa otorisasi ke sisi server maupun basis data. Tujuan dari pengujian ini adalah untuk mengidentifikasi potensi kerentanan, mengukur tingkat risiko, serta memberikan rekomendasi

mitigasi yang tepat guna meningkatkan ketahanan sistem terhadap potensi serangan siber di masa mendatang.

Salah satu pendekatan yang digunakan untuk menguji ketahanan sistem terhadap ancaman siber adalah *penetration testing*. Pendekatan ini bertujuan untuk mengidentifikasi celah keamanan yang dapat dieksploitasi oleh pihak yang tidak bertanggung jawab (Prasetya, I. A., & Safriadi, 2024). Dengan melakukan pengujian penetrasi *(penetration testing)*, pengelola sistem dapat memahami tingkat risiko yang ada dan mengambil langkah-langkah mitigasi yang tepat sebelum terjadi eksploitasi yang lebih luas. Selain itu, dalam konteks pariwisata, *penetration testing* juga dapat membantu meningkatkan kepercayaan pengunjung terhadap *website* karena memberikan jaminan keamanan dalam mengakses informasi.

Pengujian penetrasi *(penetration testing)* dapat dilakukan dengan berbagai metode, salah satunya adalah metode **NIST SP 800-115** yang dikembangkan oleh ***National Institute of Standards and Technology* (NIST).** Metode ini menyediakan kerangka kerja sistematis dalam melakukan pengujian keamanan sistem informasi melalui tahapan-tahapan seperti *planning*, *discovery*, *attack*, dan *reporting*. Pengujian ini mencakup identifikasi kelemahan pada komponen sistem, seperti aplikasi web, mekanisme autentikasi, serta konfigurasi yang tidak aman. Dengan pendekatan yang terstruktur, potensi celah keamanan dapat ditemukan dan dianalisis lebih awal, sehingga dapat diambil tindakan mitigasi sebelum dimanfaatkan oleh pihak yang tidak bertanggung jawab. Metode ini relevan

diterapkan pada *website* instansi publik, termasuk *website* penyedia layanan informasi wisata, guna memastikan integritas, ketersediaan, dan kerahasiaan data yang ditampilkan kepada masyarakat.

Selain itu, penelitian ini juga akan mengeksplorasi berbagai teknik dan strategi dalam pengujian penetrasi *(penetration testing)* serta memberikan rekomendasi perbaikan berdasarkan hasil temuan. Dengan menerapkan strategi keamanan yang lebih baik, diharapkan sistem keamanan *website* dapat diperkuat dan lebih tangguh dalam menghadapi berbagai ancaman siber. Dalam jangka panjang, peningkatan keamanan *website* instansi pariwisata dapat berkontribusi pada peningkatan pengalaman wisatawan serta menjaga reputasi destinasi wisata di era digital.

Dengan meningkatnya kesadaran akan pentingnya keamanan dalam dunia digital, hasil dari penelitian ini diharapkan dapat memberikan manfaat luas bagi pengembang sistem, pengguna, serta pemilik *website* dalam menjaga keamanan informasi mereka. Selain itu, penelitian ini juga diharapkan dapat menjadi referensi bagi instansi pemerintahan maupun pengelola destinasi wisata lainnya dalam menerapkan praktik terbaik dalam keamanan siber.

B. Batasan Penelitian

Adapun batasan masalah dalam penelitian ini yaitu:

1. Objek penelitian dilakukan pada instansi Dinas Pariwisata, Kebudayaan, Pemuda, dan Olahraga (Disparbudpora) Kabupaten

Pacitan dan berfokus pada *website*nya, yaitu *disparbudpora.pacitankab.go.id dan wisata.pacitankab.web.id/.*

2. Metode yang akan digunakan pada penelitian ini adalah metode kualitatif dengan pendekatan studi kasus.
3. Penelitian menggunakan dokumen *NIST SP 800-115* tentang *penetration testing* dari *NIST (National Institute of Standards and Technology)* sebagai pedoman dalam tahapan *penetration testing*, yang meliputi *planning*, *discovery*, *attack*, dan *reporting*.
4. Penelitian ini dibatasi pada pengujian keamanan terhadap sistem informasi *website* tanpa menyentuh aspek infrastruktur server.
5. Proses *Discovery* memanfaatkan beberapa perangkat lunak populer seperti *whatweb, google dorking, Nmap, Burp Suite, nikto, gobuster, WPScan,* dan *Uniscan* untuk mengumpulkan informasi awal. Sementara pada tahap *attack,* eksploitasi menggunakan tools *Clickjacking, Subfinder, Dig, Github, Burp Suite, Sqlmap, cURL* dan *WPScan.*

C. Rumusan Masalah

Dari latar belakang diatas, dapat dirumuskan suatu masalah, yaitu:

1. Berapakah tingkat kerentanan keamanan yang dimiliki oleh *website* Disparbudpora?
2. Apa saja rekomendasi keamanan yang diperlukan untuk meningkatkan keamanan *website* yang dimiliki oleh Disparbudpora?

3. Bagaimana implementasi rekomendasi keamanan sistem informasi pada *website* Disparbudpora?

D. Tujuan Penelitian

Dari rumusan masalah dapat diambil tujuan apa yang ingin dicapai dalam penelitan ini:

1. Mengetahui seberapa jauh tingkat kerentanan keamanan yang dimiliki oleh *website* Disparbudpora.
2. Mengidentifikasi rekomendasi keamanan berdasarkan celah yang ditemukan dalam *website* Disparbudpora.
3. Mengetahui implementasi rekomendasi keamanan sistem informasi untuk meningkatkan perlindungan pada *website* Disparbudpora.

E. Manfaat Penelitian

Adapun manfaat dari penelitian ini adalah:

1. Bagi Peneliti
    a. Memberikan pengalaman langsung dalam melakukan penetration testing berbasis metode *NIST SP 800-115.*
    b. Menjadi bekal akademik dan profesional untuk pengembangan diri di bidang keamanan siber.
2. Bagi Kampus
    a. Menjadi referensi ilmiah bagi mahasiswa lain dalam menyusun penelitian serupa.
    b. Mendorong peningkatan kualitas penelitian di bidang teknologi informasi dan keamanan siber.

3. Bagi Instansi Terkait Dinas Pariwisata, Kebudayaan, Pemuda, dan Olahraga (Disparbudpora)
    a. Menyediakan informasi teknis mengenai kondisi keamanan *website* instansi.
    b. Memberikan rekomendasi strategis untuk perbaikan dan peningkatan sistem keamanan digital.