BAB I PENDAHULUAN

1.1 *Latar Belakang*

Di era kemajuan teknologi seperti saat ini, kita tidak terlepas dari penggunaan internet. Internet telah merubah berbagai aktivitas manusia menuju gaya hidup digital, memungkinkan pertukaran informasi, komunikasi global, dan akses ke sumber daya digital secara instan (Rohaya, 2008). Fenomena ini tidak hanya menciptakan revolusi dalam cara manusia berkomunikasi, tetapi juga memberikan manfaat mulai dari dunia bisnis, industri, pendidikan dan pergaulan sosial (Mochamad Aziz, 2021).

Perkembangan teknologi informasi yang kian pesat telah membawa banyak manfaat bagi peradaban manusia. Namun, di sisi lain, menimbulkan masalah baru, salah satunya adalah keamanan siber (Muftiadi et al., 2022). Kejahatan siber menjadi sebuah masalah serius yang dapat mengancam di bidang ekonomi, politik, hingga pertahanan negara (Muhamad Rizki Hapizon et al., n.d.). Di tahun 2022, kerugian akibat kejahatan siber di seluruh dunia mencapai US$ 8,44 triliun atau sekitar Rp 130 triliun. Nominal tersebut menunjukkan peningkatan sebesar 40,9 persen dibanding tahun sebelumnya yang sebesar US$ 6 triliun (Bisnis Tekno, 2022). Peningkatan ini menunjukkan perlunya perlindungan dan keamanan siber global, yang berdampak besar terhadap perekonomian dunia.

Di indonesia, menurut Badan Siber dan Sandi Negara (BSSN), jumlah anomali lalu lintas internet mencatat angka yang sangat tinggi. Sepanjang tahun 2021, Sebanyak 1,6 miliar anomali, kemudian mengalami penurunan pada tahun 2022 menjadi 976,4 juta (Antara News, 2023). Di semester 1 tahun 2023, telah terjadi empat kali kebocoran data RI yang terkemuka. Pertama, BPJS Ketenagakerjaan Indonesia dengan 19,5 juta pelanggan pada 12 Maret 2023. Kedua, Bank Syariah Indonesia (BSI) alami kebocoran data karena serangan ransomware Lockbit dan berhasil mencuri data pribadi pengguna BSI dengan ukuran data sebesar 1,5 terabyte (TB). Ketiga, dugaan kebocoran 35 juta data dari pengguna My IndiHome pada Juni 2023 oleh Bjorka. Keempat, pada Juli 2023, Bjorka diduga membocorkan sebanya 34,9 juta data paspor WNI

(Dataindonesia.id, 2023). Kurangnya kesadaran keamanan siber pada pengguna digital juga menjadi faktor yang memperburuk situasi ini. Selain itu kebijakan dan regulasi yang tidak memadai dalam menangani kejahatan siber, kurangnya kemampuan teknis dalam melawan serangan siber, dan rendahnya tingkat sinergi antara sektor publik dan swasta dalam menghadapi kejahatan siber (Muftiadi et al., 2022).

Sebuah lembaga yang memiliki tanggung jawab dalam menjalankan tugasnya mengandalkan situs web resmi sebagai sarana untuk menyampaikan informasi dan berita terkait kegiatan institusional. Situs web ini berfungsi sebagai sumber informasi terpercaya yang harus dilindungi dari berbagai ancaman keamanan siber. Selain itu, situs lain yang dikelola oleh lembaga ini juga menyimpan data pribadi pengguna, seperti alamat email, nomor telepon, alamat, dan Kartu Tanda Penduduk (KTP). Karena data tersebut sangat sensitif dan tidak boleh bocor. Ditambah lagi Lembaga XYZ ini sering mengadakan acara besar. Oleh karena itu, dilakukanlah penelitian uji penetrasi sebagai langkah proaktif untuk mengidentifikasi dan mengatasi potensi celah keamanan sebelum dimanfaatkan oleh pihak yang tidak bertanggung jawab. Metode penelitian menggunakan panduan OWASP Top 10 2021 yang merupakan pendekatan yang relevan dan efektif dalam mengidentifikasi, mengevaluasi, dan memberikan rekomendasi perbaikan terhadap kerentanan keamanan web. Alasan pemilihan panduan OWASP Top 10 2021 karena memberikan wawasan mendalam mengenai kerentanan keamanan yang paling umum, tetapi juga merefleksikan tren terkini dalam dunia keamanan situs web. Dengan mengikuti panduan terkini dari OWASP, penelitian ini dapat memberikan kontribusi untuk meningkatkan tingkat keamanan situs web Lembaga XYZ. Dengan penerapan standar keamanan situs web yang berkualitas, pengguna akan merasa lebih aman saat menggunakan situs tersebut. Upaya peretasan kemungkinan akan sulit dilakukan dan memiliki tingkat keberhasilan yang rendah. Perbaikan keamanan yang diimplementasikan diharapkan dapat menjaga integritas informasi web, sehingga lembaga XYZ dapat mempertahankan reputasinya sebagai penyedia informasi yang kredibel karena situs web tidak rentan terhadap manipulasi data dan pencurian data pribadi pengguna oleh pihak yang tidak berwenang.

1.2 *Perumusan Masalah*

Dari uraian latar belakang diatas, terdapat rumusan masalah dari penelitian ini:

1. Bagaimana proses pengujian penetrasi yang dilakukan pada situs web XYZ?
2. Jenis kerentanan apa yang ditemukan pada situs web XYZ?
3. Tindakan apa yang perlu diambil untuk memperbaiki kerentanan pada situs web XYZ?

1.3 *Tujuan Penelitian*

Adapun tujuan dan manfaat yang menjelaskan apa yang ingin dicapai dari penelitian ini:

1. Mengetahui proses dan tahapan pengujian penetrasi yang dilakukan pada situs web lembaga XYZ.
2. Mengetahui jenis kerentenan yang ditemukan situs web lembaga XYZ.
3. Memberikan rekomendasi perbaikan dari hasil temuan kerentanan setelah dilakukannya uji penetrasi.

1.4 *Batasan Penelitian*

Batasan masalah bertujuan untuk membatasi ruang lingkup masalah yang akan diteliti atau dibahas agar penelitian lebih fokus, efektif, dan efisien. Berikut batasan masalah dari penelitian ini:

1. Subjek penelitian adalah situs A dan situs B.
2. Pengujian penetrasi menggunakan metode berjenis *black box*.
3. Pengujian penetrasi menggunakan *framework* OWASP top 10 2021.

1.5 *Metodologi Penelitian*

Alur penelitian yang mengusung serangkaian tahapan keamanan sistem informasi situs web lembaga XYZ. Dimulai dengan studi literatur, penelitian mencari pemahaman mendalam terhadap konsep-konsep keamanan informasi yang relevan. Tahap *planning* menjadi landasan utama untuk menetapkan situs web mana yang akan dijadikan target. Informasi gathering dilakukan dengan mengumpulkan data terkait infrastruktur dan potensi celah keamanan, seperti

arsitektur yang digunakan. Tahapan selanjutnya *vulnerability scanning* untuk mengidentifikasi potensi kerentanan secara otomatis. Pada tahap attacking, sistem diuji dengan melakukan serangan ke situs web dengan berdasarkan kerangka kerja OWASP Top 10 2021. Setelah menemukan kerentanan, selanjutnya adalah tahap validasi guna memastikan keakuratan temuan. Analisa hasil dilakukan untuk mengevaluasi temuan dan rekomendasi perbaikan. Pada tahap reporting menyajikan tabel yang berisi ringkasan terkait jenis kerentanan serta rekomendasi perbaikan.