BAB I
PENDAHULUAN

1.1 Latar Belakang

Perkembangan teknologi informasi telah mendorong berbagai organisasi memanfaatkan sistem informasi berbasis website untuk mendukung aktivitas operasional, penyimpanan data, serta penyampaian layanan kepada pengguna secara lebih efisien. Website menjadi salah satu platform utama dalam pengelolaan informasi karena dapat diakses secara luas melalui jaringan internet. Namun, peningkatan penggunaan sistem berbasis web juga diikuti dengan meningkatnya ancaman keamanan siber yang dapat menganggu kerahasiaan, integritas, serta ketersediaan data dalam suatu sistem informasi [1]. Kondisi tersebut menunjukkan bahwa keamanan sistem informasi menjadi aspek penting dalam menjaga stabilitas dan keandalan layanan digital.

Ancaman keamanan pada aplikasi web sering muncul dalam bentuk kerentanan sistem yang dapat dimanfaatkan oleh pihak yang tidak bertanggung jawab untuk memperoleh akses tidak sah terhadap data atau sistem. Berbagai penelitian menunjukkan bahwa aplikasi web sering kali memiliki celah keamanan yang berpotensi menimbulkan risiko seperti pencurian data, manipulasi informasi, hingga kerusakan sistem [2]. Serangan terhadap aplikasi web juga dapat memberikan dampak kerugian bagi organisasi baik dari sisi finansial, reputasi, maupun kepercayaan pengguna terhadap layanan yang disediakan [3].

Salah satu pendekatan yang banyak digunakan dalam proses pengujian keamanan aplikasi web adalah Open Web Application Security Project (OWASP) Top 10, yaitu standar yang mengidentifikasi sepuluh jenis kerentanan keamanan web yang paling umum terjadi. Pendekatan ini digunakan untuk membantu proses identifikasi serta evaluasi celah keamanan pada sistem sehingga dapat diketahui potensi risiko yang terdapat pada suatu website [4]. Selain itu, beberapa jenis serangan seperti SQL Injection juga menjadi ancaman serius karena mampu mengeksploitasi input pengguna untuk memperoleh akses ilegal terhadap database sistem jika tidak terdapat mekanisme validasi yang baik [5].

Selain melakukan identifikasi kerentanan sistem, organisasi juga perlu memastikan bahwa pengelolaan keamanan informasi telah sesuai dengan standar internasional serta mematuhi regulasi hukum yang berlaku. Salah satu standar yang banyak digunakan adalah ISO/IEC 27001:2022 yang menyediakan kerangka kerja Sistem Manajemen Keamanan Informasi (SMKI) untuk membantu organisasi dalam mengidentifikasi, mengelola, sera memitigasi risiko keamanan informasi secara sistematis [6]. Kepatuhan terhadap standar dan regulasi menjadi penting karena organisasi yang mengelola sistem elektronik wajib menjaga kerahasiaan, integritas, dan ketersediaan data sesuai ketentuan peraturan perundang-undangan, seperti Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi, Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik, Peraturan Pemerintah Nomor 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik, serta Peraturan Menteri Komunikasi dan Informatika Nomor 4 Tahun 2016 tentang Sistem Manajemen Pengamanan Informasi dan Peraturan Menteri Komunikasi dan Informatika Nomor 20 Tahun 2016 tentang Pelindungan Data Pribadi dalam Sistem Elektronik [7][8]. Namun, dalam implementasinya masih terdapat organisasi yang belum sepenuhnya siap menerapkan standar dan memenuhi regulasi tersebut sehingga diperlukan metode evaluasi untuk mengetahui kesenjangan antara kondisi keamanan yang ada dengan standar yang diharapkan. Oleh karena itu, penelitian ini dilakukan untuk menganalisis kerentanan keamanan aplikasi website menggunakan pendekatan OWASP Top 10:2021 serta mengevaluasi kesiapan penerapan ISO/IEC 27001:2022 melalui metode Gap Analysis.

1.2 Rumusan Masalah

1. Sejauh mana kesiapan Perusahaan PT Bumi Suksesindo dalam memenuhi persyaratan ISO/IEC 27001:2022 berdasarkan hasil GAP Analysis menggunakan tools Indeks KAMI 5.0?

2. Bagaimana tingkat kerentanan keamanan pada aplikasi website Perusahaan PT Bumi Suksesindo berdasarkan pengujian Penetration Testing dengan pendekatan OWASP Top 10:2021?
3. Apakah terdapat keterkaitan antara kerentanan aplikasi website dengan gap kontrol keamanan informasi berdasarkan hasil evaluasi Indeks KAMI 5.0 pada PT Bumi Suksesindo?

1.3 Batasan Masalah

Agar Penelitian ini lebih terarah dan tidak melebar dari tujuan yang telah ditetapkan, maka batasan masalah dalam penelitian ini adalah sebagai berikut:

1. Objek penelitian dibatasi pada aplikasi website milik Perusahaan yang dapat diakses sesuai dengan ruang lingkup (Scope) yang telah disepakati, tanpa melakukan pengujian pada sistem internal lain yang berada di luar cakupan tersebut.
2. Pengujian kerentanan pada Penelitian ini menggunakan pendekatan OWASP Top 10:2021 sebagai kerangka utama dalam identifikasi dan klasifikasi kerentanan aplikasi web. Selain itu, penelitian juga mencakup pengujian tambahan terhadap aspek availability layanan untuk mendukung evaluasi keamanan sistem secara lebih menyeluruh.
3. Analisis tingkat risiko kerentanan menggunakan metode Common Vulnerability Scoring System (CVSS) versi 3.0, tanpa melakukan perhitungan risiko berbasis dampak finansial atau anlisis risiko kuantitaif lainnya.
4. Evaluasi kesiapan implementasi ISO.IEC 27001:2022 dilakukan melalui metode GAP Analysis menggunakan indeks KAMI 5.0, tanpa mencakup proses sertifikasi resmi maupun audit eksternal oleh lembaga sertifikasi.
5. Penelitian ini tidak mencakup perancangan ulang arsitektur sistem atau implementasi langsung dari seluruh rekomendasi perbaikan, melainkan berfokus pada penyusunan rekomendasi sebagai bahan pertimbangan bagi Perusahaan PT Bumi Suksesindo.

1.4 Tujuan Penelitian

Tujuan yang ingin dicapai dalam penelitian adalah sebagai berikut:

1. Menganalisis tingkat kesiapan keamanan informasi PT Bumi Suksesindo dalam memenuhi persyaratan ISO/IEC 27001:2022 berdasarkan hasil Gap Analysis menggunakan Indeks KAMI 5.0.
2. Mengidentifikasi dan menganalisis tingkat kerentanan keamanan pada aplikasi website PT Bumi Suksesindo melalui pengujian Penetration Testing menggunakan pendekatan OWASP Top 10:2021.
3. Menganalisis keterkaitan antara kerentanan aplikasi website yang ditemukan melalui Penetration Testing dengan kesenjangan (gap) kontrol keamanan informasi berdasarkan hasil evaluasi Indeks KAMI 5.0, serta menyusun rekomendasi perbaikan sebagai upaya peningkatan keamanan informasi dan persiapan implementasi Sistem Manajemen Keamanan Informasi (SMKI) di PT Bumi Suksesindo.

1.5 Manfaat Penelitian

Penelitian ini diharapkan dapat memberikan manfaat baik secara teoritis maupun praktis sebagai berikut:

1. Manfaat Teoritis

   Hasil penelitian ini diharapkan dapat menjadi refrensi akademik dalam pengembangan kajian keamanan informasi, khususnya yang berkaitan dengan penerapan OWASP Top 10:2021 dalam identfikasi kerentanan aplikasi website serta penggunaan GAP Analysis sebagai langkah persiapan implementasi ISO/IEC 27001:2022. Selain itu, penelitian ini dapat menjadi bahan pembanding bagi penelitian selanjutnya yang mengkaji itegrasi kerangka analisis.

2. Manfaat Praktis

   a) Bagi Perusahaan PT Bumi Suksesindo, hasil penelitian ini dapat dimanfaatkan sebagai bahan evaluasi terhadap kondisi keamanan

aplikasi website serta sebagai dasar dalam menentukan prioritas perbaikan berdasarkan tingkat risiko kerentanan yang ditemukan.

b) Hasil GAP Analysis dapat digunakan sebagai acuan dalam mempersiapkan pembentukan dan penerapan Sistem Manajemen Keamanan Informasi (SMKI) sesuai dengan persyaratan ISO/IEC 27001:2022.

c) Rekomendasi yang dihasilkan dapat membantu organisasi dalam meningkatkan pengendalian keamanan informasi secara lebih terstruktur dan terukur guna mendukung keberlangsungan operasional perusahaan.

1.6 Sistematika Penulisan

Sistematika penulisan dalam penelitian ini disusun untuk memberikan gambaran mengenai struktur dan isi dari setiap bab yang terdapat dalam laporan skripsi. Adapun sistematika penulisan penelitian ini adalah sebagai berikut:

BAB I PENDAHULUAN

Bab ini berisi latar belakang masalah yang menjelaskan alasan dilakukannya penelitian, rumusan masalah yang menjadi fokus penelitian, batasan masalah untuk membatasi ruang lingkup penelitian, tujuan penelitian yang ingin dicapai, manfaat penelitian baik secara teoritis maupun praktis, serta sistematika penulisan skripsi secara keseluruhan.

BAB II TINJAUAN PUSTAKA

Bab ini berisi studi literatur dan landasan teori yang digunakan sebagai dasar dalam penelitian. Pembahasan meliputi teori-teori yang berkaitan dengan keamanan informasi, keamanan aplikasi web, OWASP Top 10:2021, OWASP Web Security Testing Guide (WSTG), Common Vulnerability Scoring System (CVSS), ISO/IEC 27001:2022, Gap Analysis, Indeks KAMI 5.0, serta penelitian terdahulu yang relevan.

BAB III METODE PENELITIAN

Bab ini menjelaskan metode penelitian yang digunakan, meliputi objek penelitian, alur penelitian, alat dan bahan penelitian, metode pengumpulan data, serta metode analisis data. Selain itu, bab ini juga menjelaskan tahapan evaluasi keamanan informasi menggunakan Indeks KAMI 5.0, pelaksanaan penetration testing menggunakan pendekatan OWASP Top 10:2021, penggunaan OWASP WSTG sebagai panduan validasi temuan kerentanan, analisis tingkat risiko menggunakan CVSS, dan pemetaan kerentanan dengan kontrol keamanan informasi berdasarkan hasil evaluasi Indeks KAMI 5.0.

BAB IV HASIL DAN PEMBAHASAN

Bab ini berisi hasil penelitian dan pembahasan yang meliputi identifikasi objek penelitian, pengumpulan data organisasi, hasil evaluasi tingkat kesiapan keamanan informasi menggunakan Indeks KAMI 5.0, hasil penetration testing aplikasi web menggunakan pendekatan OWASP Top 10:2021, validasi temuan kerentanan menggunakan OWASP WSTG, analisis tingkat risiko kerentanan berdasarkan CVSS, pemetaan temuan kerentanan terhadap kontrol keamanan informasi berdasarkan hasil evaluasi Indeks KAMI 5.0, serta penyusunan rekomendasi peningkatan keamanan informasi.

BAB V PENUTUP

Bab ini berisi kesimpulan yang diperoleh berdasarkan hasil penelitian untuk menjawab rumusan masalah yang telah ditetapkan. Selain itu, bab ini juga memuat saran dan rekomendasi sebagai bahan pertimbangan bagi perusahaan dalam meningkatkan keamanan aplikasi web dan keamanan informasi sesuai standar ISO/IEC 27001:2022.