BAB I
PENDAHULUAN

1.1 Latar Belakang Masalah

Perkembangan pesat teknologi informasi dan komunikasi telah mengubah cara penyampaian informasi dan layanan publik, menjadikan *website* sebagai salah satu saluran utama bagi interaksi antara pemerintah dan masyarakat. Namun, dengan meningkatnya penggunaan teknologi ini, ancaman terhadap keamanan *website* juga menjadi semakin signifikan. Keamanan siber yang baik melibatkan berbagai aspek, termasuk manajemen risiko, penerapan kontrol keamanan, dan kepatuhan terhadap standar internasional. Pada tahun 2022, terdapat lebih dari 100 juta insiden serangan siber yang mencakup berbagai bentuk serangan yang dapat membahayakan kerahasiaan dan integritas data publik [1]. *Website* ini juga menyediakan layanan sistem informasi manajemen kepegawaian seperti pengajuan cuti, kenaikan pangkat, dan pensiun. Selain sebagai alat manajemen internal, web XYZ berfungsi sebagai media informasi publik untuk meningkatkan transparansi dan efisiensi pelayanan kepegawaian di lingkungan Pemerintah Kabupaten XYZ.

Beberapa *website* Kabupaten XYZ telah menghadapi tantangan serius dalam hal keamanan, yang terlihat dari beberapa insiden yang terjadi. Salah satu contohnya adalah adanya penyisipan iklan yang tidak diinginkan ke dalam situs resmi, yang menunjukkan kelemahan dalam pengelolaan konten dan perlindungan akses oleh pengelola. Kejadian ini mengindikasikan kemungkinan adanya celah dalam kontrol akses yang bisa dimanfaatkan oleh pihak yang tidak bertanggung jawab. Selain masalah iklan, keberadaan sistem yang tidak diperbarui atau kadaluwarsa juga menjadi faktor kritis dalam kerentanan ini. Banyak *website* pemerintah yang tidak mendapatkan pembaruan perangkat lunak secara berkala, sehingga celah-celah keamanan yang ada tidak teratasi. Situasi ini membuat situs menjadi target empuk bagi serangan siber.

Kurangnya edukasi mengenai keamanan siber di kalangan pengelola dan pengguna juga berkontribusi pada masalah ini. Banyak pengguna yang belum

memahami pentingnya melindungi data pribadi dan mengidentifikasi potensi risiko yang ada. Kondisi ini menciptakan lingkungan yang meningkatkan peluang terjadinya serangan, serta mengurangi kepercayaan masyarakat terhadap website resmi. Situasi ini sangat memerlukan perhatian dan langkah-langkah preventif yang efektif untuk memastikan bahwa insiden-insiden serupa tidak terulang di masa mendatang. Oleh karena itu, penting untuk segera menerapkan tindakan konkret dalam meningkatkan keamanan siber, seperti melakukan audit keamanan secara rutin, memberikan pelatihan kepada pengelola dan pengguna, serta menerapkan protokol keamanan yang lebih ketat.

Dalam menghadapi tantangan ini, diperlukan langkah-langkah strategis dan berbasis standar internasional untuk meningkatkan keamanan *website*. Metodologi *Open Web Application Security Project* (OWASP) diaplikasikan untuk menganalisis kerentanan keamanan pada *website* Sistem Informasi XYZ. OWASP dipilih dalam penelitian ini karena fleksibilitasnya dalam mengamankan aplikasi web, dengan panduan yang dirancang secara khusus untuk mengatasi ancaman spesifik yang dihadapi aplikasi web modern [2]. Di sisi lain, PTES (Penetration Testing Execution Standard) menonjol dengan panduan teknis untuk pengujian penetrasi, tetapi cenderung lebih sesuai untuk pengujian tingkat organisasi yang membutuhkan analisis lanjutan daripada mitigasi ancaman spesifik aplikasi *web* [3].

Open Source Security Testing Methodology Manual (OSSTMM) menawarkan pendekatan terintegrasi untuk pengujian keamanan, termasuk aspek fisik dan manusia, tetapi kompleksitasnya sering menjadi kendala untuk aplikasi *web* yang membutuhkan langkah mitigasi sederhana [4]. Dengan pendekatan yang fokus pada aplikasi *web*, pembaruan reguler terhadap ancaman terkini, serta ketersediaan panduan yang praktis, OWASP menjadi pilihan yang lebih efisien dibandingkan dengan kerangka kerja lainnya.

Metode ini mencakup langkah-langkah yaitu planing, analsisis kebutuhan, analisis kerentanan yang mencakup *information gathering* dan *exploitasi*, penyusunan rekomendasi dan penguatan. OWASP terbukti efektif dalam

mengidentifikasi celah keamanan pada situs *web* Dinas Tenaga Kerja dan menghasilkan rekomendasi untuk mitigasi risiko. Selain itu penelitian pada *website* Pemerintahan Kabupaten XYZ menyoroti pentingnya integrasi OWASP dengan metode PTES untuk memberikan keamanan yang lebih komprehensif [5].

Penerapan OWASP melibatkan proses identifikasi kelemahan seperti injeksi, autentikasi yang tidak aman, dan konfigurasi keamanan yang salah. Dengan demikian, penelitian ini tidak hanya berfokus pada pengidentifikasian masalah, tetapi juga pada penyediaan solusi teknis dan operasional yang dapat meningkatkan integritas, kerahasiaan, dan ketersediaan sistem informasi. Penelitian ini diharapkan dapat memberikan kontribusi signifikan dalam bidang keamanan siber, terutama dalam pengelolaan *website* pemerintahan Kabupaten. Dengan pendekatan berbasis standar internasional seperti OWASP, penelitian ini juga dapat meningkatkan kesadaran pengelola *website* tentang pentingnya keamanan aplikasi *web*. Selain itu, hasil penelitian ini dapat menjadi referensi bagi Kabupaten-Kabupaten lain dalam mengembangkan praktik terbaik keamanan siber yang lebih efektif dan berkelanjutan.

Studi ini mengangkat judul "Analisis Kerentanan dan Penguatan Keamanan Website pada Sistem Informasi XYZ Menggunakan Metodologi Open Web Application Security Project (OWASP)". Hasil dari analisis ini kemudian digunakan untuk memberikan rekomendasi yang spesifik, termasuk penerapan patch keamanan, penggunaan *firewall* aplikasi *web*, dan pembaruan sistem yang lebih mutakhir. Implementasi langkah-langkah tersebut bertujuan untuk meningkatkan keamanan *website* secara signifikan, menjaga data sensitif dari ancaman pencurian, serta memperbaiki kepercayaan masyarakat terhadap layanan digital Kabupaten.

1.2 Rumusan Masalah

Berdasarkan latar belakang yang telah disajikan, rumusan masalah penelitian ini dapat dirumuskan sebagai berikut :

1. Apa saja kerentanan keamanan yang terdapat pada *website* Pemerintah

Kabupaten XYZ?

2. Bagaimana langkah-langkah mitigasi yang dapat dilakukan untuk meningkatkan keamanan *website* tersebut?

1.3 Tujuan dan Manfaat

Adapun tujuan penelitian dan penyusunan tugas akhir ini adalah:

1. Mengidentifikasi kerentanan keamanan pada *website* Sistem Informasi XYZ menggunakan OWASP ZAP dan *tools penetration testing*.
2. Merancang strategi penguatan keamanan berdasarkan temuan kerentanan.

Adapun manfaat penelitian dan penyusunan tugas akhir ini adalah:

a. Manfaat Teoritis

   1. Menambah literatur dan referensi ilmiah dalam bidang keamanan siber, khususnya terkait penerapan metodologi OWASP dalam identifikasi dan mitigasi kerentanan aplikasi *web*.
   2. Memberikan kontribusi terhadap pengembangan ilmu pengetahuan di bidang teknologi informasi dan keamanan aplikasi *web*, khususnya dalam konteks pemerintahan daerah.

b. Manfaat Teoritis

   1. Memberikan informasi konkret mengenai tingkat kerentanan pada website Sistem Informasi XYZ, yang dapat digunakan sebagai dasar pengambilan keputusan dalam perbaikan sistem keamanan.
   2. Menyediakan rekomendasi teknis yang dapat langsung diterapkan oleh pengelola *website* pemerintah untuk meningkatkan keamanan, seperti penerapan *patch* keamanan, penggunaan *firewall* aplikasi *web*, dan pembaruan sistem.

3. Meningkatkan kesadaran dan pemahaman pengelola *website* pemerintah terhadap pentingnya keamanan aplikasi *web* dan perlunya implementasi kontrol keamanan yang berkelanjutan.
4. Menjadi acuan atau referensi bagi pemerintah daerah lain dalam menerapkan praktik terbaik keamanan siber guna menjaga integritas, kerahasiaan, dan ketersediaan layanan publik digital.

1.4 Batasan Masalah

Agar penelitian ini lebih terfokus dan tidak menyimpang dari tujuan utama, maka batasan masalah dalam penelitian ini ditentukan sebagai berikut:

1. Penelitian ini hanya dilakukan pada *website* resmi Sistem XYZ, tidak mencakup sistem informasi atau aplikasi lain di luar *website* tersebut.
2. Analisis kerentanan keamanan dilakukan menggunakan metodologi OWASP, yang mencakup jenis kerentanan paling umum pada aplikasi *web*.
3. Proses pengujian kerentanan menggunakan alat bantu seperti OWASP ZAP dan *tools penetration testing* lainnya yang relevan dan sesuai standar.
4. Penelitian ini hanya mencakup identifikasi kerentanan dan pemberian rekomendasi perbaikan yang dapat menguatkan *website* tersebut.

1.5 Metode Penelitian

Berikut merupakan subjek dan objek dalam penelitian ini.

1. Subjek Penelitian

Subjek penelitian mencakup pengelola *website*, yang bertanggung jawab atas pemeliharaan dan keamanan situs, serta pengguna *website*, yaitu warga kabupaten yang mengakses layanan dan informasi. Melalui wawancara dan pengumpulan data.

2. Objek Penelitian

Objek penelitian dalam studi ini adalah *website* Sistem Informasi XYZ Kabupaten XYZ, yang berfungsi sebagai *platform* informasi dan layanan publik bagi masyarakat kabupaten, dengan fokus pada analisis keamanan melalui metodologi *Open Web Application Security Project* (OWASP) untuk mengidentifikasi dan menilai kerentanan sistem.