BAB I
PENDAHULUAN

1.1. Latar Belakang

Sistem informasi dan dunia digital di era modern ini telah menjadi bagian yang tidak terpisahkan, teknologi semakin berkembang untuk menjadi kebutuhan utama dalam sebuah pembaruan. Namun, dibalik keutamaannya, terdapat kerentanan pada desain sistem informasi yang dapat membawa resiko pada keamanan data dan kemajuan pada teknologi. Keamanan situs website sangat penting dalam memudahkan pengguna dalam mencari kebutuhan informasi dan data, serta melindungi data pribadi dari pengguna. Sistem informasi dan dunia digital menjadi satu kesatuan di era modern ini, yang menjadikan banyak orang dapat bergantung pada teknologi yang telah disuguhkan.Kita hidup di zaman dimana keamanan website adalah hal yang sangat penting dalam memudahkan pengguna dalam mencari berita, pengumuman, data yang diinginkan serta melindungi data pribadi dari pengguna. Namun, ada kondisi tertentu pada saat kapasitas desain sistem informasi masih belum bisa dikatakan sempurna, sehingga mengakibatkan kebocoran data melalui berbagai titik dapat menimbulkan resiko terhadap kelangsungan kemajuan atau perkembangan teknologi. Kerentanan pada situs website dapat menimbulkan konsekuensi yang serius, seperti rusaknya reputasi dan kredibilitas perusahaan atau organisasi. Keamanan informasi pengguna yang tersimpan dalam database website dapat terancam oleh serangan akan menjadi masalah yang signifikan. Maka dari itu, penting untuk menerapkan langkah-langkah pengamanan yang tepat utuk mencegah kebocoran data dan potensi kerugian yang besar.

Perlindungan data adalah tugas yang harus diprioritaskan dalam pekerjaan yang dapat mendeteksi kerentanan sistem keamanan dan aplikasi website. Tujuan dari perlindungan tersebut adalah untuk mencari metode sebagai pengidentifikasi gap pada infrastruktur jaringan, sehingga dapat mengantisipasi serangan hacker pada aplikasi website. Keberadaaan web analytics dan methodologies assessment yang digunakan untuk mengumpulkan data sangat penting dalam mengidentifikasi dan mengurangi ancaman siber. Analisis uji kerentanan ini dapat dinilai dari tingkat

kematangan dengan kesamaan sistem software. Terdapat beberapa form implementasi yang meliputi kerahasiaan data, integritas data, dan kontingensi ketersediaan aplikasi dalam kesalahan formulir. Melakukan pengujian analisis kerentanan, tidak hanya analisis dasar, tetapi juga melibatkan proses otentikasi, saat mengidentifikasi dengan memberikan akses tertentu untuk melacak. Karena itu, proses tersebut harus diimplementasikan dengan baik agar sistem yang ada berfungsi dengan baik. Administrator harus tergantung pada tiga faktor, yaitu metode ie, paket, dan dependensi sehingga kemungkinan untuk diretas melalui server menjadi lebih sedikit.

Sistem informasi dan dunia digital mengalami perkembangan yang pesat di era modern ini, teknologi menjadi tidak terpisahkan dari kehidupan sehari-hari banyak orang. Namun, kemajuan teknologi juga membawa resiko yang signifikan, terutama dalam hal keamanan situs website. Kerentanan keberadaan di situs web dapat berdampak serius tentang perusahaan atau organisasi, mengancam reputasi dan kepercayaan pengguna. Kebocoran data akibat serangan cyber dapat mengakibatkan kerugian finansial dan kerugian kehilangan kepercayaan yang sulit untuk dipulihkan. Statistik dan contoh nyata dari pelanggaran data dapat memberikan pemahaman lebih dalam tentang pentingnya keamanan website. Berbagai perusahaan dan organisasi bahkan bisa menjadi korban serangan dunia maya, dengan data pengguna yang dicuri atau disalahgunakan. Misalnya beberapa kasus terkenal yang melibatkan pencurian data pribadi seperti informasi kartu kredit atau informasi yang mengakibatkan hilangnya identitas keuangan dan pencemaran nama baik untuk perusahaan yang terkena dampak.

Selain itu, serangan siber pada website pemerintah juga mengakibatkan permasalahan yang serius. Serangan siber pada website pemerintah dapat mengakibatkan terganggunya pelayanan publik, menghalangi akses informasi penting, hingga dapat merusak keamanan yang berskala nasional, karena itu penting untuk memahami kerentanan dan menerapkan langkah-langkah keamanan yang tepat, untuk melindungi situs website dan data pengguna. Dinas XY merupakan instansi pemerintah yang berada di Jawa Timur, yang bertujuan untuk mewujudkan pelayanan publik yang bermutu dan efektif. Kedua lembaga ini berperan penting

dalam memenuhi semua kebutuhan publik dalam upaya mengembangkan administrasi dan dokumen-dokumen yang dibutuhkan oleh masyarakat. Kondisi ini mampu memberikan keterkaitan dengan pola hidup masyarakat dan beberapa perusahaan. Misalnya, masyarakat akan difasilitasi dalam mempersiapkan segala kebutuhan, terutama untuk online, karena hal ini juga merupakan bentuk usaha untuk mengaplikasikan layanan tersebut untuk masyarakat yang dilakukan oleh XY Office.

Berdasarkan analisis yang dilakukan terdapat beberapa masalah seperti kurangnya pemahaman tentang penyebab faktor keamanan serangan pada sistem informasi website layanan XY. Kesenjangan penelitian terletak pada identifikasi dan analisis akar alasan serangan keamanan tertentu, misalnya kelemahan desain sistem atau praktik keamanan dengan sebaik-baiknya. Selanjutnya kurangnya penelitian yang berfokus pada analisis kerentanan yang mungkin terjadi di layanan situs website XY. Kesenjangan penelitian dapat terletak pada penelitian mendalam tentang jenis kemungkinan serangan terjadi, seperti serangan peretasan, serangan pishing, atau serangan malware lalu bagaimana kerentanannya dapat diidentifikasi dan dikoreksi. Selama ini, belum ada evaluasi secara menyeluruh terhadap langkah-langkah keamanan yang telah diterapkan pada layanan situs website XY. Kesenjangan penelitian dapat terletak pada penelitian yang menguji dan menganalisis langkah-langkah efektivitas keamanan yang ada, serta menggali potensi celah keamanan yang belum teratasi, kurangnya pemahaman tentang praktik keamanan yang diterapkan ke layanan situs website XY. Kesenjangan penelitian ini juga dapat terletak pada penelitian yang menganalisis kebijakan keamanan yang ada, pemantauan keamanan, serta pembaruan prosedur sistem yang diterapkan dengan peningkatan tujuan kesadaran akan mempraktikkan keamanan yang benar dan mencegah kemungkinan serangan yang bisa terjadi, serta solusi kekurangan dalam penelitian terfokus pada mitigasi efektif terhadap kerentanan yang ditemukan di layanan situs web XY. Riset kesenjangan dapat terletak pada pengembangan dan penerapan solusi khusus untuk mengatasi kerentanan yang dimiliki dan diidentifikasi, seperti penggunaan teknologi enkripsi yang lebih kuat atau mekanisme aplikasi dengan otentikasi yang lebih aman.

Berdasarkan permasalahan di atas Kajian ini berfokus pada penilaian kerentanan pada website Dinas XY sebuah lembaga pemerintahan di Jawa Timur. Kajian Ini bertujuan untuk mengidentifikasi dan mengevaluasi kerentanan spesifik, termasuk serangan seperti XSS (Cross-site Scripting). Dalam konteks inilah, penelitian ini bertujuan untuk melakukan analisis yang komprehensif terhadap layanan situs website XY, sebuah instansi pemerintah di Jawa Timur. Studi ini akan fokus pada penilaian kerentanan dan percobaan serangan untuk mengidentifikasi dan mengevaluasi kerentanan spesifik, termasuk serangan seperti XSS (Cross-site Scripting). Penelitian ini akan menggunakan berbagai alat keamanan seperti OWASP ZAP, Burp Suite, Skipfish, Wapiti, Rapidscan, dan Nikto Untuk mendukung analisis kerentanan dan trial attack. Fokus penelitian ini akan ditujukan untuk identifikasi dan evaluasi kerentanan tertentu, termasuk serangan seperti XSS (Cross-site Scripting) dan penggunaan alat keamanan seperti OWASP ZAP, Burp Suite, Skipfish, Wapiti, Rapidscan, dan Nikto. Melalui penelitian ini diharapkan dapat ditemukan kemungkinan solusi dan rekomendasi peningkatan keamanan layanan situs website XY sehingga memberikan kontribusi yang signifikan dalam menyediakan dan meningkatkan kualitas dan efektifitas pelayanan kepada publik.

Penelitian ini bertujuan untuk melakukan analisis komprehensif terhadap layanan situs website XY dengan fokus pada penilaian kerentanan dan percobaan serangan. Penelitian ini bertujuan untuk mengidentifikasi dan mengevaluasi kerentanan tertentu, seperti serangan XSS (Cross-site Scripting), juga untuk mengevaluasi kinerja alat keamanan seperti OWASP ZAP, Burp Suite, Skipfish, Wapiti, Rapidscan, dan Nikto dalam konteks situs website. Dengan melakukan penelitian ini diharapkan bisa menemukan kemungkinan solusi dan rekomendasi meningkatkan keamanan layanan situs web XY. Kontribusi secara signifikan dalam meningkatkan kualitas dan efektivitas layanan publik yang disediakan untuk melindungi data pribadi pengguna dengan lebih baik dan membangun kepercayaan pengguna terhadap institusi tersebut. Studi ini akan menghasilkan perbaikan signifikan dalam eksperimen desain dan mendapatkan bukti empiris yang kuat. Dalam kajian ini, akan diidentifikasi beberapa indikator keamanan khusus berdasarkan jenis serangan yang berbeda, terutama serangan phishing di situs

website. Perbaikan akan menghasilkan struktur yang lebih efektif dan khusus, yang memberikan pengaruh kuat dalam meningkatkan keamanan. Selain itu, analisis link website akan dilakukan dengan mengekstrak sejumlah fitur yang relevan, dan akan dilakukan evaluasi menggunakan pendeteksi kerentanan XSS (Cross-site Scripting).

Oleh karena itu, penulis akan melakukan kajian dengan analisis evaluasi kerentanan dan trial attack yang meliputi penggunaan jumlah dalam layanan situs website XY menggunakan sejumlah alat (OWASP ZAP, Burp Suite, Skipfish, Wapiti, Rapidscan, dan Nikto). Harapannya penelitian ini akan memberikan analisis yang komprehensif terhadap layanan website XY juga memberikan kontribusi yang signifikan dalam meningkatkan kualitas dan efektifitas layanan publik. Hal ini akan dicapai dengan memperhatikan keamanan struktur dari website lembaga tersebut. Pelajari implikasi praktis yang signifikan dalam peningkatan kualitas dan efektivitas layanan yang diberikan oleh Kantor XY. Dengan melakukan analisis layanan situs website XY menggunakan metode evaluasi kerentanan dan serangan percobaan dan penelitian. Hal ini akan menghasilkan pemahaman yang mendalam tentang kerentanan dan kelemahan yang ada pada website. Temuan penelitian ini akan memberikan manfaat nyata dalam beberapa aspek. Pertama, dengan mengidentifikasi dan memperbaiki kerentanan, jika keamanan ditemukan, kantor XY akan dapat meningkatkan keamanan situs website dan melindungi data pribadi pengguna dengan lebih baik. Hal ini akan membangun kepercayaan pengguna untuk meningkatkan kualitas lembaga, reputasi serta kredibilitas. Kedua, dengan mengevaluasi kerentanan deteksi alat kinerja seperti OWASP ZAP, Burp Suite, Skipfish, Wapiti, Rapidscan, dan Nikto dalam konteks website XY, penelitian ini akan memberikan panduan berharga dalam memilih dan menggunakan alat yang efektif dalam mengurangi keamanan ancaman.

Selain itu, analisis yang dilakukan dalam penelitian ini akan membantu mengidentifikasi kebutuhan perbaikan dan pengembangan lebih lanjut di website XY. Dengan mengetahui kerentanan yang ada dalam institusi. Hal ini dapat mengambil tindakan preventif dan proaktif untuk meningkatkan keamanan dan kualitas pelayanan yang mereka berikan kepada masyarakat. Dengan demikian,

penelitian ini akan memberikan kontribusi yang signifikan dalam meningkatkan kualitas dan efektifitas pelayanan publik yang disediakan oleh kantor XY melalui pemahaman yang lebih baik tentang kerentanan situs web mereka, perlindungan data lebih baik, dan menggunakan alat yang efektif dalam menghadapi ancaman keamanan. Kajian ini akan menggunakan metode evaluasi kerentanan dan uji coba yang melibatkan serangan menggunakan sejumlah alat dan teknik tertentu. Lebih detail, untuk melanjutkan tentang metodologi yang akan digunakan, seperti kerentanan evaluasi, kerentanan evaluasi metode akan digunakan untuk mengidentifikasi dan mengevaluasi keamanan kerentanan pada situs website XY. Sejumlah alat yang akan digunakan dalam evaluasi ini termasuk OWASP ZAP, Burp Suite, Skipfish, Wapiti, Rapidscan, dan Nikto. Alat Ini akan digunakan untuk memindai dan menganalisis situs web dengan tujuan mengidentifikasi kerentanan yang ada, seperti serangan XSS (Cross-site Scripting), injeksi SQL, dan kerentanan lainnya. Test Attack, setelah identifikasi kerentanan selesai, penelitian Ini akan melibatkan uji serangan Untuk menguji kerentanan yang ditemukan. Teknik yang akan digunakan termasuk uji serangan XSS, injeksi SQL, dan serangan lain yang relevan dengan situs website XY. Melalui uji serangan ini, penelitian akan menguji sejauh mana kerentanan yang dapat dimanfaatkan dan dievaluasi tingkat ketahanan sistem untuk menyerang. Selain itu penelitian ini akan melibatkan fitur analisis pada link website. Dalam analisis ini, beberapa fitur pada tautan situs web akan diekstraksi dan dievaluasi untuk mengidentifikasi potensi indikator serangan phishing atau upaya menyerang orang lain. Metodologi ini akan memberikan pendekatan yang komprehensif dalam mengidentifikasi, mengevaluasi, dan menguji keamanan kerentanan di situs web XY. Dengan menggunakan alat yang sudah terbukti, teknik yang efektif dan relevan, penelitian ini akan memberikan pemahaman yang mendalam tentang keadaan keamanan situs web dan memberikan wawasan berharga untuk pengembangan dan peningkatan keamanan di masa mendatang.

Penelitian ini akan membawa kontribusi baru dalam bidang sistem keamanan informasi dan website dengan konteks fokus kepada dinas XY. Ini akan memberikan pandangan baru tentang kerentanan dan solusi spesifik keamanan

untuk jenis organisasi. Kajian ini sendiri bertujuan utama untuk memberikan kontribusi baru dalam bidang keamanan sistem informasi dan website, dengan fokus pada konteks Dinas XY. Dalam konteks ini, penelitian ini diharapkan dapat memberikan pandangan baru tentang kemungkinan kerentanan yang ada pada sistem informasi dan website yang digunakan oleh jenis organisasi. Dengan menganalisis dan mengidentifikasi kerentanan khusus untuk layanan XY. Penelitian ini diharapkan akan membantu memahami keamanan terkait ancaman dan memberikan solusi yang sesuai. Di dunia yang semakin hari semakin terhubung secara digital, keamanan informasi menjadi aspek yang sangat penting bagi organisasi. Dalam konteks ini, penelitian ini akan menyelidiki berbagai kemungkinan kerentanan ada dalam sistem informasi dan website untuk layanan XY, seperti konfigurasi kerentanan, serangan brute force, dan keamanan mekanisme kelemahan. Dengan mengidentifikasi kerentanan ini, penelitian ini akan memberikan pemahaman yang lebih baik tentang keamanan risiko dihadapi oleh organisasi dan memberikan dasar untuk mengembangkan solusi yang efektif.

Melalui penelitian ini diharapkan adanya upaya untuk meningkatkan keamanan sistem informasi dan website organisasi. Dengan memperhatikan temuan dan rekomendasi dari penelitian ini, dinas XY dapat mengambil langkah-langkah proaktif dalam memperbaiki kelemahan keamanan yang ada dan menerapkan praktik terbaik untuk melindungi sistem yang mereka miliki dari ancaman yang ada. Berikut beberapa contoh ulasan literatur yang tersedia menjadi referensi di studi dalam jenis studi seperti, memahami kesadaran kerentanan keamanan, insentif perusahaan, dan ICT pengembangan di Pan-Asia, penelitian ini meninjau kerentanan dan ancaman yang sering ditemukan di aplikasi website. Hasilnya dapat memberikan pandangan tentang kerentanan yang mungkin juga relevan dengan layanan situs website dinas XY. Berikutnya analisis skala besar android — hibridisasi web [11], Riset ini melihat praktik terbaik dalam mengamankan situs web pemerintah. Tinjauan literatur ini dapat memberikan pedoman dan rekomendasi yang tersedia diadaptasi untuk meningkatkan keamanan website layanan XY yang merupakan bagian dari instansi pemerintah. Terlebih lagi penelitian tentang metode survei eksploitasi dan deteksi kerentanan XSS [12],

Tinjauan literature ini mengidentifikasi dan mendeskripsikan berbagai ancaman umum tentang keamanan siber yang dihadapi di lingkungan organisasi. Informasi ini dapat membantu dalam memahami berbagai serangan yang mungkin juga berlaku untuk layanan situs web dinas XY. Berikutnya sebuah survei pada alat penilaian kerentanan dan database untuk aplikasi web berbasis cloud [13], Penelitian ini dilakukan untuk meninjau literatur yang komprehensif tentang analisis kerentanan dalam sistem informasi ini bisa memberi pandangan tentang metode dan pendekatan yang digunakan dalam mengidentifikasi dan mengatasi kemungkinan kerentanan yang tersedia di layanan situs website dinas XY.

Riset kontribusi yang dapat dilakukan berdasarkan latar belakang di atas adalah tentang Enhancement Security. Kajian sistem informasi pada situs website layanan XY ini terfokus kepada melakukan analisis kerentanan (penilaian kerentanan) dan upaya yang melibatkan serangan berbagai jenis serangan, seperti serangan brute force, menggunakan sejumlah alat (OWASP ZAP, Burp Suite, Skipfish, Wapiti, Rapidscan, dan Nikto). Tujuan utamanya adalah untuk mengidentifikasi dan mengatasi kerentanan keamanan yang ada di situs web Layanan XY. Dalam studi ini, bisa mengembangkan strategi dan langkah-langkah keamanan yang lebih kuat Untuk melindungi data dan informasi sensitif yang tersimpan di dalamnya sistem database website. Kontribusi selanjutnya adalah metodologi aplikasi analisis kerentanan pada pemerintah. Kajian website ini akan fokus pada analisis metode penyebaran kerentanan yang efektif dan efisien situs web pemerintah, terutama di situs web Layanan XY. metode yang dapat melibatkan penggunaan alat analisis kerentanan, seperti analisis web, untuk mengumpulkan data dan mengidentifikasi keamanan kerentanan. Tujuan utamanya adalah untuk memberikan rekomendasi yang tepat dalam mengatasi kerentanan yang ditemukan, sehingga dapat meningkatkan keamanan dan integritas sistem situs website pemerintah. Kajian ini dapat memberikan panduan dan pedoman praktis bagi organisasi pemerintah dalam menghadapi ancaman keamanan siber dan melindungi data pengguna. Kontribusi kedua di atas dapat memberikan kontribusi yang signifikan kontribusi untuk pemahaman dan peningkatan sistem keamanan informasi, khususnya pada pemerintah layanan situs website seperti dalam dinas

XY. Dengan meningkatkan keamanan dan perlindungan data, reputasi dan kepercayaan publik agar lembaga pemerintahan dapat dipertahankan dan ditingkatkan.

1.2. Rumusan Masalah

1. Bagaimana pendekatan pengujian *brute force* diterapkan terhadap penelitian yang dilakukan?
2. Apakah dengan metode *brute force* yang digunakan dalam penelitian dapat mendeteksi kerentanan suatu pada layanan situs website dinas XY?

1.3. Tujuan Penelitian

Penerapan metode *brute force* dengan mendeteksi kerentanan suatu website Dinas XY di Jawa Timur dengan memberikan rekomendasi yang tepat dalam mengatasi kerentanan yang ditemukan, sehingga dapat meningkatkan keamanan dan integritas sistem situs website pemerintah. Kajian ini dapat memberikan panduan dan pedoman praktis bagi organisasi pemerintah dalam menghadapi ancaman keamanan siber dan melindungi data pengguna. Kontribusi kedua di atas dapat memberikan kontribusi yang signifikan kontribusi untuk pemahaman dan peningkatan sistem keamanan informasi, khususnya pada pemerintah layanan situs website seperti dalam dinas XY. Dengan meningkatkan keamanan dan perlindungan data, reputasi dan kepercayaan publik agar lembaga pemerintahan dapat dipertahankan dan ditingkatkan.

1.4. Batasan Masalah

Melalui penelitian ini diharapkan adanya upaya untuk meningkatkan keamanan sistem informasi dan website organisasi. Dengan memperhatikan temuan dan rekomendasi dari penelitian ini, dinas XY dapat mengambil keputusan terbaik dalam memperbaiki kelemahan pada keamanan serta menerapkan praktik yang sesuai untuk melindungi sistem yang mereka miliki dari berbagai ancaman. Jadi, batasan masalah dalam penelitian ini berfokus pada layanan situs website saja