BAB I
PENDAHULUAN

1.1 Latar Belakang

Dengan perkembangan teknologi informasi yang didorong oleh inovasi dalam jaringan komputer, yaitu internet, data dapat dikirim dari satu tempat ke tempat lain dalam waktu yang sangat singkat. Selain itu, pemerintah Indonesia menggunakan kemajuan teknologi untuk meningkatkan pelayanan publik dan meningkatkan transparansi birokrasi [1]. Pemanfaatan situs web di lembaga pemerintah merupakan salah satu implementasi penting dari kemajuan ini, sangat penting untuk memiliki website di instansi pemerintah, khususnya di pemerintah Kota Tarakan. Website ini berfungsi sebagai cara resmi untuk memberikan informasi kepada warga, berinteraksi dengan warga, mengukur seberapa aktif kegiatan pemerintah, menyampaikan aspirasi warga, dan memudahkan warga untuk mengenal pemimpin mereka [2].

Namun, dengan ketergantungan yang meningkat pada situs web layanan publik, muncul masalah baru terkait keamanan siber. Studi sebelumnya yang dilakukan oleh (Raihan, S. D., Prabowo, S., & Oktaria, D. (2024)) telah menyelidiki dan menangani potensi ancaman keamanan untuk aplikasi berbasis web. OWASP berfungsi dengan baik dalam pengujian keamanan web, tetapi tidak cukup untuk membangun prosedur keamanan yang cukup [3]. Sehingga dibutuhkan metode PTES, yang menawarkan kerangka kerja pengujian penetrasi yang sistematis, karena mencakup pre-engagement, exploitation hingga pelaporan dan saran [4]. Selain itu, standar NIST 800-115, yang berfokus pada pedoman untuk menilai dan menguji keamanan informasi website, untuk menghasilkan laporan tentang celah keamanan yang memungkinkan peretas menyerang [5].

Karena kemajuan teknologi, banyak orang yang tidak bertanggung jawab yang disebut sebagai hacker atau peretas mencuri data. Hacker mencari lubang di server web dengan berbagai alasan untuk mendapatkan informasi tentang organisasi, perusahaan, atau lembaga pemerintah sehingga mereka dapat merugikan orang lain [6]. Oleh karena itu, penting untuk mengevaluasi sebuah situs web dengan cermat untuk mencegah serangan yang dapat merugikan perusahaan yang dilakukan oleh

peretas atau hacker system [7]. Dalam situasi ini Penetration testing sangat penting untuk simulasi serangan yang dilakukan oleh seseorang untuk mengidentifikasi kelemahan pada sistem jaringan organisasi atau perusahaan tertentu. Tujuan dari pengujian penetrasi adalah untuk mengidentifikasi dan memahami serangan-serangan yang mungkin terjadi terhadap kelemahan yang ada dalam sistem, serta untuk memahami efek dari eksploitasi yang dapat dilakukan oleh penyerang terhadap perusahaan [8].

Sebuah dokumen yang dikeluarkan oleh National Institute of Standards and Technology (NIST), dokumen NIST SP 800-115, mencakup metode yang digunakan untuk melakukan Penetration Testing dan Evaluasi Keamanan. Dokumen ini juga mencakup alat pendukung yang diperlukan untuk melakukan Evaluasi Keamanan [9]. Selain NIST, ada juga Penetration Test Execution Standard (PTES) yang merupakan prosedur di mana seseorang berusaha untuk mereplikasi serangan yang mungkin terjadi pada jaringan sebuah perusahaan atau organisasi tertentu. Ini dilakukan dengan mempraktekkan serangan melalui celah dan kerentanan keamanan serta melakukan analisis keamanan sistem untuk mengidentifikasi kelemahan [10]. Menurut Silaban dan Wijaya, Metode NIST SP 800-115 adalah panduan lengkap untuk pengujian keamanan informasi yang membantu perusahaan menemukan dan menilai bug pada sistem informasi mereka, termasuk situs web instansi pemerintah [9]. Menurut Fikri et al., Metode Penetration Testing Execution Standard (PTES) menawarkan sebuah kerangka kerja yang sistematis, terdiri dari tujuh tahapan yang meliputi mulai dari pre-engagement hingga reporting. Metode ini telah terbukti efektif dalam mengidentifikasi dan mengevaluasi kerentanan yang mungkin ada pada sistem informasi di situs web pemerintah [10].

Standar keamanan dari National Institute of Standards and Technology (NIST) serta pendekatan pengujian penetrasi yang diterapkan (PTES) diterapkan dalam studi ini untuk mengidentifikasi kelemahan keamanan pada Portal Pemerintah Kota Tarakan. NIST digunakan sebagai acuan dalam evaluasi dan rekomendasi perbaikannya, dan PTES digunakan untuk pengujian penetrasi untuk menemukan celah keamanan. Hasil penelitian ini diharapkan dapat meningkatkan keamanan portal dan menawarkan pertahanan siber yang lebih baik.

1.2 Rumusan Masalah

Berdasarkan tantangan keamanan yang dijelaskan di atas, rumusan masalah berikut ini dirancang untuk mengidentifikasi solusi yang tepat:

a. Bagaimana cara mengetahui jenis kerentanan keamanan apa saja yang dapat dieksploitasi pada situs web Portal Pemerintah Kota Tarakan?
b. Bagaimana cara penerapan metode PTES dalam melaksanakan pengujian penetrasi dan bagaimana metode NIST SP 800-115 dimanfaatkan untuk menilai serta memberikan saran terkait hasil pengujian keamanan situs web Portal Pemerintah Kota Tarakan?

1.3 Tujuan Penelitian

Sesuai dengan isu yang diuraikan dalam rumusan masalah sebelumnya, penelitian ini bertujuan untuk mencapai hal-hal berikut:

a. Untuk mengetahui berbagai jenis kerentanan keamanan yang ada pada situs web Portal Pemerintah Kota Tarakan yang mungkin bisa dimanfaatkan oleh pihak yang tidak bertanggung jawab.
b. Menerapkan metode *Penetration Testing Execution Standard (PTES*) dalam melaksanakan proses keamanan pada situs web, serta menggunakan *NIST SP 800-115* sebagai pedoman dalam mengevaluasi hasil pengujian dan memberikan saran perbaikan terkait kerentanan yang terdeteksi.

1.4 Batasan Masalah

Batasan yang ditetapkan dalam penelitian ini adalah sebagai berikut:

a. Fokus dari penelitian ini adalah menilai keamanan situs web Portal Pemerintah Kota Tarakan, tanpa mempertimbangkan infrastruktur jaringan atau sistem lain yang digunakan oleh pemerintah Kota Tarakan. Pembatasan ini bisa memengaruhi hasil penelitian karena pengujian hanya dilakukan pada aspek website, sehingga potensi kerentanan di jaringan atau sistem backend tidak dievaluasi secara menyeluruh.

b. Penelitian ini berfokus pada penerapan metode *PTES* dan *NIST*, yang keduanya telah terbukti efektif dalam mengidentifikasi dan mengurangi kerentanan.
c. Hasil pengujian hanya digunakan untuk analisis akademis dan saran perbaikan; tidak ada perubahan sistem atau mitigasi.
d. Pengujian yang dilakukan tidak mencakup eksploitasi yang dapat berisiko menganggu layanan, seperti serangan *Dos* atau *DDOS,* maupun yang dapat menyebabkan kerusakan sistem secara langsung. Disamping itu, seluruh pengujian dilaksanakan dalam lingkungan yang telah mendapatkan izin, sehingga ruang lingkup evaluasi evaluasi terbatas hanya aspek-aspek yang telah disetujui oleh pihak-pihak terkait.