BAB I
PENDAHULUAN

1.1 Latar Belakang

Perkembangan teknologi informasi yang pesat telah mendorong digitalisasi di berbagai sektor, termasuk sektor pemerintahan. Digitalisasi ini diwujudkan melalui kehadiran *website* resmi pemerintah daerah sebagai sarana informasi publik dan pelayanan kepada masyarakat. *Website* pemerintah menjadi representasi dari transparansi, efisiensi, dan keterbukaan informasi publik. Namun demikian, semakin tingginya ketergantungan pada sistem digital juga meningkatkan potensi risiko keamanan siber yang dapat mengancam integritas, ketersediaan, dan kerahasiaan data. Menurut Darojat et al,. 2022 [1], *website* pemerintah yang digunakan sebagai media pelayanan publik rentan terhadap berbagai jenis kerentanan keamanan, seperti *SQL Injection* dan XSS, apabila tidak dilakukan pengujian keamanan secara berkala. Penelitian mereka menunjukkan bahwa masih banyak *website* e-government yang memiliki celah keamanan signifikan yang dapat dimanfaatkan oleh pihak yang tidak bertanggung jawab.

Website Pemerintah Kabupaten Bima merupakan salah satu platform digital yang digunakan untuk menyampaikan berbagai informasi dan layanan kepada masyarakat, seperti berita pemerintahan, data sektoral, layanan pengaduan publik, hingga informasi anggaran daerah. Namun demikian, sebagai bagian dari sistem informasi publik, *website* ini juga menjadi target potensial bagi berbagai ancaman siber. Nursyabani [2] menemukan bahwa *website* milik pemerintah Kota depok memiliki lima jenis kerentanan dengan tingkat risiko tinggi, di antaranya adalah *Hash Disclosure* dan kemungkinan serangan DDoS melalui DNS *Spoofed Request*, yang menandakan urgensi dilakukan evaluasi keamanan secara menyeluruh.

Dalam konteks keamanan siber, salah satu pendekatan yang dapat dilakukan adalah metode *Vulnerability Assessment*, yaitu proses sistematis dalam mengidentifikasi, menganalisis, dan mengevaluasi potensi kerentanan dalam suatu sistem informasi Efendi et al., 2024 [3]. Penilaian ini memungkinkan organisasi

untuk mengetahui sejauh mana tingkat keamanannya dan menetapkan prioritas mitigasi berdasarkan tingkat risiko yang ditemukan. Studi oleh Firman Syech [4] pada *website* pemerintah daerah di Kalimantan Selatan juga menegaskan pentingnya *Vulnerability Assessment*, karena meskipun beberapa *website* menunjukkan tingkat risiko rendah, tetap ditemukan kerentanan yang dapat dimanfaatkan jika tidak segera diperbaiki. Selain itu, Alfi et al., 2023 [5] menekankan bahwa dalam transformasi digital pelayanan publik di Indonesia, perlindungan terhadap data dan sistem digital menjadi krusial untuk menjaga kepercayaan publik dan keberlangsungan layanan.

Berdasarkan latar belakang tersebut, penelitian ini bertujuan untuk menganalisis keamanan *website* Pemerintah Kabupaten Bima dengan pendekatan *Vulnerability Assessment*, guna memperoleh gambaran mengenai kondisi keamanannya serta memberikan rekomendasi mitigasi terhadap potensi serangan siber.

1.2 Rumusan Masalah

Berdasar latar belakang masalah seperti di 1.1, dapat dirumuskan sebuah permasalahan, "Bagaimana cara mengidentifikasi dan mengklasifikasikan kerentanan keamanan pada *Website* Pemerintah Kabupaten Bima menggunakan metode *Vulnerability Assessment* berbasis *tools* Who.is, Nslookup, dan OWASP ZAP?"

1.3 Batasan Masalah

Agar pembahasan dalam penelitian ini lebih terarah, maka penelitian dibatasi pada hal-hal berikut:.

1. Objek yang dianalisis hanya terbatas pada *website* resmi Pemerintah Kabupaten Bima.
2. Penelitian dilakukan menggunakan metode *vulnerability assessment* dengan pendekatan *non-intrusive* (tidak merusak sistem atau mengeksploitasi celah secara aktif).

3. Tools yang digunakan dalam penelitian adalah *tools* open-source seperti Who.is V5.6.1, Nslookup dan OWASP ZAP V2.16.1 untuk keperluan scanning dan analisis kerentanan
4. Fokus penelitian hanya pada aspek keamanan aplikasi web (web application security), tidak termasuk keamanan infrastruktur jaringan secara menyeluruh.

1.4 Tujuan Penelitian

Adapun Tujuan yang ingin dicapai dalam penelitian ini adalah Untuk mengidentifikasi dan memberikan informasi mengenai celah-celah keamanan yang ditemukan pada *Website* Pemerintah Kabupaten Bima, sehingga dapat menjadi dasar dalam upaya peningkatan keamanan sistem *website* tersebut.

1.5 Manfaat Penelitian

Adapun manfaat penelitian ini adalah sebagai berikut.

1. Manfaat Teoritis
   - Memberikan kontribusi terhadap pengembangan ilmu pengetahuan di bidang keamanan jaringan dan aplikasi web.
   - Menjadi referensi ilmiah bagi penelitian selanjutnya dalam bidang cybersecurity, khususnya yang menggunakan metode vulnerability assessment.
2. Manfaat Praktisi
   - Memberikan informasi awal kepda pihak pengelola *website* Pemerintah Kabupaten Bima terkait potensi kerentanan keamanan yang perlu segera ditangani.
   - Memberikan panduan teknis dalam melakukan evaluasi keamanan sistem informasi berbasis web secara mandiri.
   - Menumbuhkan kesadaran akan pentingnya perlindungan sistem informasi publik dari ancaman siber.

1.6 Sistematika Penulisan

Sistematika penulisan skripsi ini disusun sebagai berikut:

BAB I PENDAHULUAN

Bab ini memuat latar belakang masalah, rumusan masalah, batasan masalah, tujuan penelitian, manfaat penelitian dan sistematika penulisan. Bab ini menjelaskan alasan dilakukannya penelitian serta ruang lingkup kajian yang akan dibahas.

BAB II TINJAUAN PUSTAKA

Berisi teori-teori yang mendukung penelitian seperti konsep dasar keamanan informasi, *website*, OWASP, Standar keamanan OWASP Top 10, *Information Gathering*, *vulnerability assessment*, dan Tools yang digunakan. Selain itu, disertai tinjauan terhadap penelitian-penelitian sebelumnya.

BAB III METODE PENELITIAN

Berisi pendekatan penelitian yang digunakan, objek dan lokasi penelitian, metode pengumpulan data, serta *tools* dan langkah-langkah dalam melakukan vulnerability assessment.

BAB IV HASIL DAN PEMBAHASAN

Berisi hasil analisis kerentanan *website* yang diperoleh dari proses scanning, klasifikasi jenis kerentanan, dan rekomendasi teknis terhadap hasil temuan.

BAB V PENUTUP

Berisi kesimpulan dari hasil penelitian serta saran-saran untuk perbaikan dan penelitian lanjutan.