BAB I

PENDAHULUAN

1.1 Latar Belakang

Sistem informasi berbasis web telah menjadi bagian penting dalam penyelenggaraan layanan publik karena mampu mempermudah masyarakat dalam memperoleh informasi dan mengakses berbagai layanan secara cepat, mudah, dan efisien. Namun, pemanfaatan teknologi tersebut juga memerlukan perlindungan terhadap aspek keamanan web untuk mencegah kebocoran data maupun gangguan layanan. Laporan Badan Siber dan Sandi Negara (BSSN) menunjukkan bahwa sepanjang tahun 2024 terdeteksi sebanyak 330.527.636 anomali trafik siber di Indonesia yang menargetkan berbagai sektor, termasuk layanan digital pemerintah [1]. Reonaldi *et al.* menyatakan bahwa gangguan keamanan pada aplikasi web dapat memengaruhi kualitas layanan informasi yang diberikan kepada masyarakat serta menurunkan kepercayaan pengguna terhadap instansi penyelenggara layanan [2]. Selain itu, Darojat *et al.* menjelaskan bahwa data yang dikelola oleh suatu instansi merupakan aset yang harus dilindungi melalui penerapan mekanisme keamanan yang memadai. Apabila sistem memiliki celah keamanan, pihak yang tidak berwenang berpotensi memperoleh akses terhadap data pribadi maupun informasi penting yang tersimpan di dalam sistem [3]. Oleh sebab itu, evaluasi keamanan perlu dilakukan secara berkala agar potensi kerentanan dapat diketahui sejak dini sebelum dimanfaatkan oleh pihak yang tidak bertanggung jawab.

Penelitian sebelumnya menunjukkan bahwa aplikasi web masih memiliki beragam kerentanan yang dapat mengganggu keamanan sistem. Prihanto *et al.* menemukan bahwa kelemahan pada validasi masukan, pengelolaan sesi, serta kesalahan konfigurasi pada aplikasi web sehingga meningkatkan risiko serangan *Cross-Site Scripting* (XSS) dan *SQL Injection* [4]. Penelitian lainnya pada lingkungan pendidikan juga menunjukkan masih ditemukannya kerentanan dengan tingkat *medium* hingga *high* yang disebabkan oleh kurangnya pembaruan sistem serta tidak dilaksanakannya pengujian keamanan secara berkala [5].Selain itu

Hasabi (2025) yang menerapkan kerangka *Penetration Testing Execution Standard* (PTES) pada web pemerintah daerah menemukan kelemahan berupa konfigurasi server yang kurang aman dan penggunaan perangkat lunak yang telah usang sehingga meningkatkan peluang terjadinya eksploitasi [6]. Menggunakan NIST SP 800-115 dan OWASP Testing Guide juga menemukan kelemahan berupa autentikasi yang lemah, plugin rentan, serta belum diterapkannya beberapa konfigurasi keamanan dasar pada aplikasi web [7].

Meskipun berbagai penelitian tersebut berhasil mengidentifikasi kerentanan pada aplikasi web, sebagian besar penelitian masih menggunakan satu *vulnerability scanner* atau hanya berfokus pada satu pendekatan pengujian. Akibatnya, jenis kerentanan yang berhasil diidentifikasi sangat bergantung pada kemampuan tools yang digunakan sehingga cakupan hasil pengujian menjadi relatif terbatas. Selain itu, sebagian penelitian hanya menyajikan tingkat keparahan (*severity)* berdasarkan hasil bawaan tools atau menggunakan *Common Vulnerability Scoring System* (CVSS) sebagai dasar penilaian risiko. Pendekatan tersebut lebih berorientasi pada karakteristik teknis kerentanan dan belum secara komprehensif mempertimbangkan kemungkinan terjadinya eksploitasi serta dampaknya terhadap organisasi. Berdasarkan kondisi tersebut, masih terdapat ruang penelitian untuk mengombinasikan beberapa *vulnerability scanner* yang memiliki mekanisme deteksi berbeda serta menggunakan metode penilaian risiko yang mampu mengevaluasi peluang eksploitasi dan dampak kerentanan secara lebih menyeluruh.

Penelitian ini menggunakan pendekatan *Vulnerability Assessment*, yaitu proses sistematis untuk mengidentifikasi, menganalisis, dan mengevaluasi kerentanan pada sistem informasi berbasis web sebelum kerentanan tersebut dimanfaatkan oleh pihak yang tidak berwenang [8]. Dalam penelitian ini digunakan tiga *vulnerability scanner*, yaitu Nuclei, Nikto, dan Wapiti. Nuclei merupakan *template-based vulnerability scanner* yang mampu mendeteksi berbagai jenis kerentanan, *security misconfiguration*, serta *Common Vulnerabilities and Exposures* (CVE) berdasarkan ribuan template yang terus diperbarui oleh komunitas keamanan [9]. Nikto merupakan *tool*s yang berfokus pada pengujian

konfigurasi *web server*, *security header*, file yang terekspos, serta kelemahan umum pada layanan HTTP [10]. Sementara itu, Wapiti merupakan *black-box web vulnerability scanner* yang melakukan pengujian terhadap parameter masukan aplikasi web untuk mendeteksi kerentanan seperti *Cross-Site Scripting* (XSS), *SQL Injection*, dan *Local File Inclusion* (LFI) [11]. Perbedaan karakteristik tersebut menyebabkan ketiga tools saling melengkapi sehingga mampu memberikan cakupan identifikasi kerentanan yang lebih luas dibandingkan apabila hanya menggunakan satu *tools.* Setelah proses identifikasi kerentanan dilakukan, diperlukan metode untuk menentukan tingkat risiko sehingga dapat diketahui prioritas penanganan setiap temuan. Penelitian ini menggunakan OWASP Risk Rating karena metode tersebut tidak hanya mempertimbangkan karakteristik teknis kerentanan seperti pada CVSS, tetapi juga memperhitungkan kemungkinan terjadinya eksploitasi (*Likelihood*) melalui *Threat Agent Factors* dan *Vulnerability Factors*, serta besarnya dampak (*Impact*) melalui *Technical Impact* dan *Business Impact*. Dengan mempertimbangkan kedua aspek tersebut, hasil penilaian risiko mampu memberikan gambaran yang lebih komprehensif mengenai tingkat risiko keamanan sistem sehingga lebih sesuai diterapkan pada web layanan publik yang mengelola data masyarakat.

Objek penelitian ini adalah web resmi Dinas Kependudukan dan Pencatatan Sipil Kota Lhokseumawe. Web tersebut dipilih karena digunakan sebagai media penyelenggaraan layanan administrasi kependudukan dan penyediaan informasi kepada masyarakat. Layanan yang diselenggarakan berkaitan dengan pengelolaan data kependudukan yang bersifat penting, sehingga keamanan web perlu menjadi perhatian. Apabila terdapat kerentanan pada sistem, risiko yang dapat timbul antara lain kebocoran informasi, perubahan data oleh pihak yang tidak berwenang, maupun terganggunya ketersediaan layanan yang dapat memengaruhi kualitas pelayanan kepada masyarakat. Oleh karena itu, diperlukan evaluasi keamanan untuk mengetahui kondisi keamanan web serta menyusun rekomendasi perbaikan yang sesuai.

Berdasarkan uraian tersebut, penelitian ini mengangkat judul **Analisis Tingkat Kerentanan Sistem Informasi Berbasis Web Menggunakan Nuclei, Nikto, dan Wapiti (Studi Kasus: Dinas Kependudukan dan Pencatatan Sipil Kota Lhokseumawe).** Penelitian dilakukan menggunakan pendekatan *Vulnerability Assessment* dengan memanfaatkan Nuclei, Nikto, dan Wapiti untuk mengidentifikasi kerentanan pada web, kemudian seluruh temuan dianalisis menggunakan metode OWASP Risk Rating guna menentukan tingkat risiko keamanan dan rekomendasi perbaikan disusun dengan mengacu pada OWASP Cheat Sheet Series. Hasil penelitian diharapkan dapat memberikan gambaran kondisi keamanan web, menjadi dasar dalam menentukan prioritas perbaikan keamanan bagi instansi.

1.2 Rumusan Masalah

Berdasarkan latar belakang yang telah dijelaskan, maka rumusan masalah dalam penelitian ini adalah sebagai berikut:

1. Apa saja jenis kerentanan yang ditemukan menggunakan Nuclei, Nikto, dan Wapiti pada sistem informasi berbasis web Dinas Kependudukan dan Pencatatan Sipil Kota Lhokseumawe berdasarkan hasil pengujian ?
2. Bagaimana tingkat risiko kerentanan sistem informasi berbasis web Dinas Kependudukan dan Pencatatan Sipil Kota Lhokseumawe berdasarkan perhitungan *Likelihood, Impact*, dan *Overall Risk Severity* menggunakan OWASP Risk Rating?
3. Apa rekomendasi perbaikan yang dapat diberikan untuk meningkatkan keamanan sistem berdasarkan hasil analisis kerentanan ?

1.3 Batasan Masalah

Berdasarkan uraian latar belakang yang telah disampaikan, maka batasan masalah dalam penelitian ini adalah sebagai berikut:

1. Penelitian dilakukan pada web resmi Dinas Kependudukan dan Pencatatan Sipil Kota Lhokseumawe sebagai objek pengujian keamanan sistem berbasis web.

2. Pengujian kerentanan dilakukan setelah memperoleh izin dari pihak Dinas Kependudukan dan Pencatatan Sipil Kota Lhokseumawe sebagai pemilik web, serta dilaksanakan sesuai dengan etika penelitian dan ketentuan yang berlaku tanpa melakukan tindakan yang dapat mengganggu operasional sistem.
3. Penelitian menggunakan pendekatan *vulnerability assessment* untuk mengidentifikasi kerentanan keamanan pada web yang menjadi objek penelitian.
4. Pengujian keamanan dilakukan menggunakan tools Nuclei, Nikto, dan Wapiti dengan fokus pengujian pada kerentanan *security misconfiguration, missing security header, information disclosure, exposed* file, serta kelemahan konfigurasi keamanan web.
5. Input penelitian hanya berupa alamat web target yang diuji menggunakan *tools vulnerability scanner.*
6. Penelitian hanya mencakup proses identifikasi dan analisis kerentanan tanpa melakukan *penetration testing* dan eksploitasi yang dapat mengubah, merusak, maupun mengganggu layanan web yang diuji.
7. Hasil penelitian berupa identifikasi jenis kerentanan, analisis tingkat risiko kerentanan, dokumentasi hasil pengujian, dan rekomendasi keamanan sistem berdasarkan temuan yang diperoleh, tanpa melakukan implementasi perbaikan pada web yang diuji.

1.4 Tujuan Penelitian

Tujuan dari penelitian ini adalah:

1. Mengidentifikasi kerentanan keamanan yang terdapat pada sistem informasi berbasis web Dinas Kependudukan dan Pencatatan Sipil Kota Lhokseumawe.
2. Menganalisis tingkat risiko kerentanan sistem informasi berbasis web menggunakan OWASP Risk Rating berdasarkan hasil *Vulnerability Scanning* yang diperoleh dari Nuclei, Nikto, dan Wapiti.

3. Memberikan rekomendasi perbaikan keamanan untuk meningkatkan kesiapan sistem terhadap ancaman siber.

1.5 Manfaat Penelitian

Manfaat Teoretis :

1. Menambah referensi ilmiah terkait penerapan metode *vulnerability assessment* dalam mengukur tingkat kerentanan sistem informasi berbasis web pada instansi pemerintah.
2. Memberikan kontribusi dalam pengembangan keilmuan di bidang keamanan sistem informasi, khususnya pada pemanfaatan *tools* seperti Nuclei, Nikto, dan Wapiti sebagai instrumen analisis keamanan.
3. Menjadi acuan bagi peneliti selanjutnya yang ingin melakukan pengujian keamanan web dengan pendekatan kombinasi beberapa *tools Vulnerability Scanning* untuk memperoleh hasil yang lebih komprehensif.

Manfaat Praktis

1. Bagi Instansi

   Memberikan informasi mengenai kondisi keamanan sistem informasi yang digunakan, serta menyajikan rekomendasi perbaikan yang dapat diterapkan untuk meningkatkan perlindungan data dan keandalan layanan.
2. Bagi Peneliti

   Menambah pengalaman praktis dalam melakukan *vulnerability assessment* menggunakan beberapa *tools Vulnerability Scanning*, serta menjadi dasar pemahaman dalam proses analisis kerentanan sistem informasi berbasis web.
3. Bagi Akademisi

   Menjadi referensi tambahan dalam kegiatan penelitian dan pembelajaran di bidang keamanan sistem informasi, khususnya terkait metode pengujian kerentanan pada web.