BAB I

PENDAHULUAN

1.1 Latar Belakang

Pesatnya perkembangan dunia internet saat ini mengakibatkan ada usaha maksimal dari suatu organisasi dan individu untuk membuat sebuah keamanan dalam sistem dan jaringan karena sangat memungkinkan datangnya sebuah serangan. *Hacker* merupakan seseorang yang memiliki kemampuan dalam pemrograman serta jaringan komputer. Indonesia tercatat sebagai Negara peringkat 5 yang paling banyak terinfeksi *ransomware* di Asia Tenggara dengan jumlah rata-rata 14 kasus terjadi setiap hari, menurut riset yang dilakukan perusahaan peranti lunak antivirus *Symantec.*

Keamanan sistem informasi adalah salah satu isu utama dalam perkembangan teknologi informasi dan komunikasi. Selain itu, bisnis penting untuk melindungi aset informasi organisasi dengan mengikuti pendekatan yang konprehensif dan terstruktur untuk memberikan perlindungan dari resiko organisasi yang mungkin di hadapi. Upaya memecahkan masalah keamanan dibutuhkan penerapan metode yang dapat menjamin keamanan data, transaksi, dan komunikasi (W, 2021).

Aplikasi web digunakan oleh hampir semua organisasi di semua sektor untuk berbagai tujuan, termasuk *e-commerce, e-banking, e-learning,* dan jejaring sosial. Organisasi yang gagal melindungi aplikasi web mereka berisiko menjadi sasaran penyerang. Ini dapat mengakibatkan pengungkapan informasi, kehilangan pendapatan, hubungan klien yang rusak, dan banyak lagi (Althunayyan, 2022).

Penggunaan internet di pemerintahan untuk mendorong realisasi *e-government* diharapkan dapat memberikan manfaat peningkatan kekuatan masyarakat dengan meningkatkan akses informasi, meningkatkan pelayanan pemerintah kepada

masyarakat, memperkuat interaksi antara pemerintah dan swasta di industri terkait, serta meningkatkan kemudahan dan keterbukaan pengelolaan pemerintahan (Elsa Prisanda & Rury Febrina, 2021)

E-government merupakan sebuah mekanisme baru dari interaksi antara pemerintah dengan masyarakat memanfaatkan teknologi komunikasi sehingga dapat meningkatkan kualitas layanan publik. Sistem Pemerintahan Berbasis Elektronik (SPBE) atau selanjutnya disebut *e-government* adalah penyelenggaraan pemerintahan yang memanfaatkan teknologi informasi dan komunikasi untuk memberikan layanan kepada pengguna. Manajemen SPBE meliputi manajemen risiko, manajemen keamanan informasi, manajemen data, manajemen aset teknologi informasi dan komunikasi, manajemen sumber daya manusia, manajemen pengetahuan, manajemen perubahan, dan manajemen Layanan SPBE. (Darojat, 2022).

Salah satu strategi efektif *e-government* adalah menyederhanakan pelayanan kepada masyarakat, menghilangkan jenjang pada birokrasi pemerintah dan memfasilitasi apa yang sebelumnya dilakukan oleh masyarakat, kalangan bisnis, dan pemerintah yang sebelumnya dianggap sulit menjadi mudah (Taufik et al., 2022)

Pembangunan pelayanan publik menjadi suatu titik strategis untuk menciptakan *good governance* yang efektif dan efisien. Hal ini dikarenakan pelayanan publik melibatkan kepentingan semua unsur pemerintahan yakni pemerintah sebagai representasi dari negara, masyarakat sipil, serta para pelaku usaha yang memiliki pengaruh terhadap mekanisme pasar. Indonesia menyelenggaraan urusan pemerintahan berbasis digital atau yang dikenal sebagai sistem *e-government* sudah mulai diterapkan. Masalah terbesar dari setiap pemanfaatan teknologi adalah persoalan keamanan "*privacy*" sehingga sistem elektronik yang digunakan terutama sistem yang terkait dengan banyak orang harus mempunyai kelayakan dalam menjamin perlindungan data pribadi tidak terkecuali pada pelaksanaan *e-government*. Keamanan pada sektor publik terutama dalam penerapan sistem *e-government* merupakan hal yang perlu diperhatikan pemerintah karena merupakan hal sensitif sebab rentan disalahgunakan oleh pihak yang tidak berhak dan akan berpengaruh pada kepercayaan publik pada pelaksanaannya (Iswandari, 2021).

Keamanan *e-government* menjadi isu yang sangat penting mengingat sensitivitas informasi yang dikelola oleh instansi pemerintah. Serangan *cyber* seperti peretasan *(hacking)* dan pelanggaran data dapat mengakibatkan kerugian besar baik

dalam hal kerahasiaan, integritas, maupun ketersediaan data. Oleh karena itu, perlu adanya upaya yang serius untuk memastikan bahwa sistem *e-government* memiliki tingkat keamanan yang optimal.

Salah satu alat yang digunakan untuk mengidentifikasi kerentanan dalam aplikasi web adalah *Acunetix Web Vulnerability*. Alat ini adalah sebuah *scanner* keamanan yang dapat secara otomatis mendeteksi kerentanan umum dalam aplikasi web, termasuk serangan *SQL injection*, *Cross-Site Scripting (XSS)*, dan lainnya. Dalam studi kasus ini, fokus penelitian difokuskan pada penerapan *Acunetix Web Vulnerability* untuk menganalisis dan perbaikan keamanan situs web yang digunakan oleh Pemerintah Kota Padang khususnya Dinas Penaman Modal dan Pelayanan Satu Pintu (DPMPTSP) Kota Padang.

DPMPTSP Kota Padang telah menerapkan sistem *e-government* untuk memberikan pelayanan publik yang lebih efisien dan transparan kepada warganya. Namun, semakin kompleksnya ancaman keamanan *cyber* yang ada saat ini membuat perlindungan terhadap sistem *e-government* menjadi sangat penting. Salah satu formasi pemerintahan Kota Padang yang menggunakan *e-government* sebagai sistem pelayanan publik berbasis elektronik yaitu DPMPTSP Kota Padang yang bertugas menyelenggarakan pelayanan administrasi di bidang perizinan. Layanan pada website DPMPTSP salah satunya adalah kemudahan dalam mengurus perizinan berbasis online.

Penelitian terdahulu yang dilakukan oleh (Dan, 2022) tentang analisis keamanan website menggunakan metode *Vulnerability Assessment* dan perhitungan *security matriks*. Data yang digunakan adalah website New Kuta Golf menghasilkan pengujian keamanan website menggunakan *acunetix web vulnerability* menghasilkan hasil yang detail. Dapat menentukan keamanan website menggunakan *security matriks*. Hasil *vulnerabily* pada new kuta golf adalah bernilai *high*.

Selanjutnya penelitian yang dilakukan oleh (Akmal et al., 2022) tentang analisis keamanan website dengan metode *Vulnerability Assessment*. Data yang digunakan yaitu website Universitas Singaperbangsa Karawang. Hasil penelitian yaitu ditemukan 2 kerentanan dengan tingkat risiko *high*, 3 kerentanan dengan tingkat risiko *medium*, 5 kerentanan dengan tingkat risiko *low*, dan 2 kerentanan dengan tingkat risiko *informational.*

Penelitian yang dilakukan oleh (Sandy & Solihin, 2021) tentang audit keamanan dan manajemen resiko *e-learning* menggunakan framework NIST, serta

aplikasi *acunetix vulnerability* sebagai alat pengujian keamanan sistem, menghasilkan nilai rata–rata 76,09% atau pada level 3 (*Implemented Procedures and Controls*). Sementara itu level yang hendak dicapai adalah level 4 (*Tested and Review Procedures and Controls*). Untuk dapat mencapai level tersebut, berdasarkan *framework NIST* SP 800-26 sebaiknya dilakukan beberapa aktivitas rekomendasi

Penelitian yang dilakukan oleh (Darojat et al., 2022) tentang *vulnerability ssessment* Website *E-Government* , metode yang digunakan yaitu NIST SP 800-115 dan *OWASP Web Vulnerability Scanner*. Data yang digunakan yaitu pemindaian kerentanan pada dua jenis web *e-government* yang berbeda, yaitu web *e-government* milik pemerintah daerah dan milik pemerintah desa, penilaian sampel menggunakan website semarangkab.go.id milik pemerintah daerah Kabupaten Semarang Provinsi Jawa Tengah dan gunungtumpeng.id yaitu website *e-government* resmi milik Pemerintah Desa Gunung Tumpeng, Kecamatan Suruh, Kabupaten Semarang, Provinsi Jawa Tengah Indonesia. Hasil penelitian menunjukkan adanya kesamaan penilaian dari segi kategori tingkat ancaman dan jumlah kerentanan menggunakan kedua alat pemindaian kerentanan web, dan hasil yang berbeda ditemukan pada durasi, kecepatan pemindaian, dan jenis temuan kerentanan. Kedua parameter OWASP dapat memberikan kompleksitas petunjuk dan penjelasan untuk membantu pengembang atau pemerintah daerah mengambil keputusan tentang keamanan informasi yang dikelola jaringan *e-government*.

Penelitian yang dilakukan oleh (Putra & Soewito, 2022) tentang pengukuran kinerja sistem keamanan pada website kepegawaian di pemerintahan, menggunakan metode *scanning vulnerability assessment.* Data yang digunakan yaitu website sistem informasi kepegawaian di lingkungan Pemerintahan. Hasil analisis penelitian ini menjelaskan bahwa website pemerintah mempunyai 8 celah keamanan. Berdasarkan hasil perhitungan menunjukan perbaikan guna meningkatkan keamanan website.

Berdasarkan latar belakang yang telah diuraikan, peneliti mengangkat kajian penelitian dengan judul tesis **"Audit Web E-Government dengan Acunetix Web Vulnerability Guna Menganalisis dan Perbaikan Celah Keamanan Website (Studi Kasus Di Dinas Penanaman Modal dan Pelayanan Terpadu Satu Pintu Kota Padang)".**

1.2 Rumusan Masalah

Berdasarkan latar belakang yang telah disampaikan, dapat diidentifikasi beberapa permasalahan yang dapat diangkat dalam penelitian ini. Beberapa masalah yang menjadi fokus penelitian meliputi :

1. Bagaimana melakukan audit web *e-government* dengan *acunetix web vulnerability* guna menganalisis dan perbaikan celah keamanan website DPMPTSP Kota Padang ?
2. Bagaimana langkah – langkah dalam menganalisis keamanan *e – government* menggunakan *acunetix web vulnerability* ?
3. Bagaimana perbaikan dari hasil analisis keamanan terhadap website DPMPTSP Kota padang menggunakan *acunetix web vulnerability* ?

1.3 Batasan Masalah

Berdasarkan rumusan masalah yang telah disampaikan, dapat diidentifikasi beberapa batasan masalah yang dapat diangkat dalam penelitian ini. Beberapa batasan masalah yang menjadi fokus penelitian meliputi :

1. Penelitian dilakukan pada website *e-government* DPMPTSP Kota Padang
2. Penggunaan *Acunetix Web Vulnerability Scanner* sebagai alat menganalisis keamanan *e-government* DPMPTSP Kota Padang.
3. Analisis akan dilakukan pada website SINOPEN (Sistem Informasi Non Perizinan) dengan url : https://nonperizinan.web.dpmptsp.padang.go.id/sinopen
4. Analisis perbaikan dan pengujian dilakukan pada level kerentanan *high* hingga *medium.*

1.4 Tujuan Penelitian

Berdasarkan rumusan masalah yang telah disampaikan, berikut ini adalah tujuan dari penelitian yaang dilaksanakan. Beberapa tujuan yang menjadi fokus penelitian meliputi :

1. Melakukan audit web *e-government* dengan *acunetix web vulnerability* guna menganalisis dan perbaikan celah keamanan website DPMPTSP Kota Padang.
2. Melakukan langkah – langkah analisis keamanan *e–government* menggunakan *acunetix web vulnerability*.
3. Melakukan perbaikan dari hasil analisis keamanan terhadap website DPMPTSP Kota Padang menggunakan *acunetix web vulnerability*.

1.5 Manfaat Penelitian

Berdasarkan dari penjabaran sebelumnya tentang audit web *e-government* dengan *acunetix web vulnerability* guna menganalisis dan perbaikan celah keamanan website DPMPTSP Kota Padang. Adapun uraian manfaat penelitian berikut ini :

1. DPMPTSP dapat mengetahui celah keamanan yang terdapat pada website
2. Dapat memberikan panduan dan rekomendasi bagi DPMPTSP Kota Padang untuk meningkatkan keamanan sistem *e-government*.
3. Dapat memberikan kontribusi dalam pemahaman umum tentang pentingnya keamanan website *e-government* dan bagaimana tools *Acunetix Web Vulnerability* dapat digunakan untuk mengidentifikasi dan mengatasi kerentanan keamanan dalam aplikasi web.

1.6 Sistematika Penulisan

Sub bab ini membahas sistematika penulisan, sebuah landasan yang memberi struktur pada setiap kata. Berikut ini adalah sistematika yang digunakan dalam penyusunan tesis sebagai berikut :

BAB I PENDAHULUAN

Bab ini beriisikan tentang latar belakang, rumusan masalah, batasan masalah, tujuan penelitian, manfaat penelitian, dan sistematika penulisan

BAB II TINJAUAN PUSTAKA

Bab ini berisikan tentang audit keamanan website, *e-governmet*, keamanan *e-government,* dan *acunetix web vulnerability scanner*

BAB III METODOLOGI PENELITIAN

Bab ini menjelaskan jenis pnelitian yang dilakukan, pendekatan yang digunakan, sumber data, lokasi penelitian, metode dan alat pengumpulan data serta teknik pengolahan data dan analisa

BAB IV ANALISA DAN PERANCANGAN

Bab ini berisi tentang tahapan analisis dan perancangan yang berisikan tentang data yang diperoleh, menganalisis data, dan perancangan

BAB V IMPLEMENTASI DAN HASIL

Bab ini berisi tentang implememtasi dan perancangan yang dilakukan serta detail pengujian dan perbaikan hasil dari pengujian yang dilakukan

BAB VI KESIMPULAN DAN SARAN

Bab ini berisikan kesimpulan dari penyusunan tesis serta saran – saran untuk pengembangan selanjutnya