BAB 1 PENDAHULUAN

1.1 Latar Belakang

Adopsi teknologi digital pada banyak sektor yang didorong oleh keadaan pandemi COVID-19 semakin meningkat, menurut IMF pandemi telah mempercepat digitalisasi terutama diekonomi atau industri yang tertinggal, pada negara maju digitalisasi telah meningkat rata – rata enam persen [1].

Salah satu teknologi digital yang sering dipakai adalah *website*, saat ini banyak organisasi memberikan informasi kepada klien, karyawan, atau masyarakat secara *online* melalui *web* [2], keuntungan menggunakan *website* sebagai aplikasi sistem informasi adalah kemudahan untuk akses dimanapun dan kapanpun. Tetapi melakukan proses digitalisasi juga memiliki tantangan yang tidak bisa diabaikan, penelitian oleh Almeida [3] berjudul "*Tantangan dan Peluang Digitalisasi dalam Masa Setelah Pandemi*" mengatakan bahwa *cybersecurity* serta privasi menjadi dua elemen kunci untuk mendukung integrasi teknologi. Meningkatnya aktivitas digital juga memicu peningkatan serangan siber, pada tahun 2022 kasus kebocoran data di Indonesia mengalami peningkatan. Menurut perusahaan keamanan siber *Surfshark*, pada kuartal tiga tahun 2022 Indonesia menduduki peringkat ketiga disusul oleh perancis pada peringkat dua dan rusia di urutan pertama [4]. Dari tahun 2021 sampai 2023 Indonesia sering mengalami masalah dalam serangan siber terutama kasus kebocoran data. Pada tahun 2021 sebanyak 279 juta data penduduk Indonesia peserta Badan Penyelenggara Jaminan Sosial Kesehatan atau BPJS bocor dan dijual pada sebuah forum jual beli data [5].

Kemudian kasus seorang *hacker* bernama bjorka yang sempat menghebohkan Indonesia, kasus bjorka meliputi dugaan peretasan: 3,2 Miliar data *PeduliLindungi*; 44,2 juta data *MyPertamina*; 1,3 Miliar data registrasi SIM *Card* Kominfo, dan sebagainya. Data – data yang bocor tersebut merupakan data privasi pengguna dan atau masyarakat yang seharusnya dilindungi dan tidak disebar luaskan. Keamanan dalam pengembangan sebuah aplikasi *website* juga tidak dapat diabaikan, salah satu contoh serangan yang sering diterima oleh *website* adalah *web defacement.* Serangan *web defacement* sendiri adalah serangan terhadap situs *web* yang bertujuan untuk merusak atau mengubah konten pada halaman situs *web* tersebut,

dalam “Lanskap Keamanan Siber” Badan Sandi Siber Nasional (BSSN) *web defacement* selalu masuk ke dalam tiga teratas insiden dalam layanan BSSN, pada tahun 2021 terdapat 5.940 kasus *web defacement* dan selama tahun 2022 terjadi 2.348 kasus serangan *web defacement* [6], menurut BSSN selama tahun 2022 sektor yang paling banyak terkena serangan *web defacement* adalah sektor administrasi pemerintahan dengan jumlah kasus 885 kasus.

Sebuah studi oleh Frost dan Sullivan yang diprakasai oleh Microsoft pada tahun 2018 [7] mengungkapkan bahwa potensi kerugian ekonomi rata – rata pada perusahan besar dapat mencapai 30 milliar *dollar* AS atau setara dengan 450 trilliun rupiah. Untuk itu, penting dilakukan analisis keamanan agar mengetahui apakah aplikasi yang sudah dibangun memiliki keamanan sudah memenuhi standar. Salah satu standar internasional untuk manajemen keamanan informasi adalah ISO 27001, PT XYZ atau disingkat menjadi PT XYZ telah memiliki sertifikat ISO 27001 namun dalam rangka mempersiapkan diri untuk audit *surveillance* maka pada penelitian kali ini akan dilakukan analisis keamanan berupa uji penetrasi terhadap tiga aplikasi berbasis *website* pada PT XYZ. Uji penetrasi merupakan simulasi serangan secara langsung yang diluncurkan terhadap aplikasi, menggunakan metode ini dapat ditemukan kerentanan keamanan pada aplikasi *website* serta mengetahui bagaimana sistem keamanan bekerja dalam menghadapi serangan langsung. Uji penetrasi akan dilakukan mengikuti *Open Worldwide Security Application Project - Web Security Testing Guide* (OWASP – WSTG). Pengujian menggunakan OWASP WSTG yang merupakan sebuah standar industri yang diakui oleh banyak organisasi dan profesional keamanan siber di seluruh dunia, WSTG memberikan panduan langkah-demi-langkah yang mudah dipahami dan diikuti, mencakup berbagai aspek keamanan *web*, menyediakan skenario pengujian spesifik, dan didukung oleh komunitas aktif yang terus memperbarui dan meningkatkan kualitas panduan. Pengujian keamanan pada penelitian ini akan difokuskan pada kategori *Authentication Testing* serta *Input Validation Testing*. Selain dari keterbatasan waktu, kategori tersebut dipilih karena fitur autentikasi merupakan fitur penting dalam menjaga keamanan sistem dan termasuk fundamental dalam *web security* [2]. Kemudian alasan pemilihan *input validation testing* dikarenakan validasi dan sanitasi *input* yang benar merupakan tantangan

dalam pembuatan sebuah *website* [8]. Hasil dari pengujian ini akan berguna untuk analisis kerentanan keamanan aplikasi pada PT XYZ sehingga mampu memberikan rekomendasi guna meningkatkan keamanan aplikasi pada perusahaan.

1.2 Rumusan Masalah

Dari permasalahan pada latar belakang dapat diambil rumusan masalah sebagai berikut:

1. Bagaimana tingkat keamanan aplikasi *website* pada PT XYZ berdasarkan *OWASP Framework*?
2. Apa saja langkah yang dapat dilakukan untuk meningkatkan keamanan aplikasi *website* pada PT XYZ?
3. Bagaimana urutan prioritas implementasi keamanan yang harus dilakukan oleh PT XYZ?

1.3 Tujuan dan Manfaat

Adapun tujuan dan manfaat dari penelitian ini adalah:

1. Mengetahui tingkat keamanan aplikasi *website* PT XYZ.
2. Meningkatkan keamanan aplikasi *website* PT XYZ.
3. Mengetahui prioritas implementasi keamanan aplikasi *website* PT XYZ.

1.4 Batasan Masalah

Agar penelitian ini dapat berjalan sesuai fokus maka dirumuskan beberapa batasan sebagai berikut:

1. Aplikasi yang diuji hanya aplikasi berbasis *website*.
2. Aplikasi yang diuji hanya tiga aplikasi yaitu *website* A, *Website* B, *Website* C.
3. Pengujian mengikuti petunjuk OWASP *Web* Security *Testing* Guide dan berfokus pada kategori *Authentication Testing* dan *Input Validation Testing*.
4. Pengujian menggunakan teknik *black box testing.*