BAB 1. PENDAHULUAN

1.1 Latar Belakang

Perkembangan Teknologi Informasi (TI), banyak menyebabkan perubahan dan cara pandang manusia dalam kehidupan sehari - hari. Perkembangan TI hingga sekarang ini terus mengalami perubahan, sehingga zaman sekarang sudah memasuki zamannya teknologi yang lebih cepat dari yang pernah dibayangkan sebelumnya.

Dengan adanya kemudahan yang didapatkan di zaman sekarang ini, jarang ditemukannya satu sisi kehidupan yang tidak menggunakan TI sebagai sarana untuk membantu dalam menyelesaikan pekerjaannya baik bersifat sederhana sampai dengan yang kompleks. Saat ini timbul suatu kebutuhan *security* atau keamanan untuk sebuah sistem komputer. Kebutuhan keamanan komputer dalam setiap sistem komputer mempunyai keamanan yang berbeda - beda sesuai dengan aplikasi-aplikasi yang dikandungnya, contohnya dalam sebuah sistem akademik tentunya keamanan sistemnya berbeda dengan sistem yang ada diperbankan.

Banyak kasus pada dunia komputer, khususnya jaringan internet dalam menghadapi serangan *virus, worm, trojan, Dos, Web Deface*, pembajakan software, sampai dengan masalah pencurian kartu kredit. Seperti yang telah dikutip Tribunnews pada Jum'at 21 September 2018 mengatakan bahwa data yang didapatkannya dari International Data Corporation (IDC), mayoritas perusahaan yang ada di ASEAN termasuk masih fokus pada keamanan operasional dasar, belum masuk pada level pengelolaan yang baik dan teroptimalkan. Sekitar 69,4% perusahaan ASEAN terutama Indonesia masih tahap adhoc, dan 0,2% perusahaan sudah mencapai tahap optimized, padahal serangan terhadap keamanan Sistem Informasi (SI) semakin berkembang dan meluas secara cepat. Ancaman yang terjadi sepanjang 2018 berasal dari empat hal, mulai dari *Malware*, *Supply Chain Attack*, hingga *Ransomware*. "Hampir 40% dari perusahaan global menilai Teknik deteksi lanjutan (*Advanced Detection Technique*) sebagai cara paling efektif untuk mendeteksi ancaman keamanan cyber", ujar Munindra, *Senior Research Manager*

for Consulting and Head of Operations at International Data Corporation (IDC) Indonesia, di acara "*Enabling Security in Digital Transformation Journey*" yang diadakan oleh Telkomtelstra berkolaborasi dengan IDC, di Jakarta, Rabu 19 September 2018 (Haryadi, 2018).

Salah satu contoh kejahatan *cyber* yang paling popular yang telah terjadi pada tahun 2020, dikutip dari CNBC Indonesia 04 May 2020 adalah salah satu perusahaan e-*Commerce* yaitu Tokopedia yang merupakan salah satu perusahaan e-*Commerce* terbesar di Indonesia. Tokopedia sendiri diretas oleh kelompok *hacker* dengan inisial nama "*Whysodank*" yang membuat 91 juta data dari hasil peretasan itu di jual dengan harga US$5.000 atau setara Rp 75 Juta, di *Empire Market*, salah satu pasar gelap di *Dark Web*.

Pada salah satu perguruan tinggi XYZ pada unit bagian umum memiliki sistem informasi, dimana sistem tersebut berfungsi untuk memudahkan para pegawai dalam mengelola barang dan inventaris milik negara sehingga pencatatan seluruh transaksi akan terekam secara digital pada sistem. Mengingat kompleksnya operasional yang dijalankan setiap hari maka ada resiko ancaman celah keamanan yang dapat terjadi di masa mendatang sehingga perlu adanya sebuah pencegahan untuk mengantisipasi hal tersebut.

Dari penjelasan latar belakang yang telah dipaparkan maka akan dilakukan penelitian tentang pengujian keamanan sistem informasi berbasis *web* yang nantinya akan disebut dengan Sistem Informasi Umum dan BMN (SIUB) dan tidak banyak yang melakukan akses terhadap aplikasi ini, karena masih dalam pengujian keamanan. Sehingga SIUB akan dijadikan alat atau media dalam menemukan celah keamanan pada aplikasi berbasis website dengan menggunakan metode DAST (*Dynamic Application Security Testing).*

1.2 Rumusan Masalah

Berdasarkan latar belakang masalah yang sudah dijelaskan maka didapatkan beberapa rumusan masalah, antara lain :

1) Bagaimana melakukan pengujian keamanan aplikasi berbasis *web* [redacted].polije.ac.id menggunakan metode DAST (*Dynamic Application Security Testing)*
2) Bagaimana cara memperbaiki celah keamaan yang ditemukan pada *website* [redacted].polije.ac.id.

1.3 Tujuan

Tujuan dari penelitian adalah sebagai berikut :

1) Melakukan pengujian dan analisis untuk mengetahui kondisi serta melakukan pengukuran tingkat kerentanan sistem informasi pada *website* Sistem Infomarsi Umum dan BMN ([redacted].polije.ac.id).
2) Menjabarkan celah serta mengukur tingkat kerentanan yang perlu untuk segera diperbaiki sehingga dapat membantu untuk memperbaiki kegagalan dalam mempertahankan keamanan sistem informasi di sub bagian Umum dan BMN.

1.4 Manfaat

Manfaat yang diharapkan pada penelitian adalah sebagai berikut :

1) Diharapkan dengan adanya penelitian ini, ketika akan membuat *website* kita akan mengetahui salah satu celah keamanan yang memungkinkan sistem dapat dimanfaatkan oleh pihak-pihak yang tidak bertanggung jawab.
2) Diharapakan penelitian dalam skripsi ini dapat digunakan sebagai acuan untuk bahan evaluasi keamanan Sistem Informasi Umum dan BMN.

1.5 Batasan Penelitian

Pada penelitian ini hanya membatasi pada ruang lingkup dalam melakukan pengujian dengan alamat domain polije.ac.id, sebagai berikut :

1) Penelitian ini menggunakan konsep *ethical hacking*.
2) Aplikasi berbasis *web* yang akan dilakukan pengujian yaitu Sistem Informasi Umum dan BMN [redacted].polije.ac.id.
3) Penelitian ini melakukan pengujian keamanan menggunakan metode DAST *(Dynamic Application Security Test)*
4) Penerapan dari hasil penelitian ini akan direkomendasikan dan diserahkan sepenuhnya pada pihak pengembang.