BAB I
PENDAHULUAN

1.1 Latar Belakang

Pengembangan sebuah situs web menjadi semakin masif seiring dengan perkembangan teknologi internet, dimana pada era yang serba digital ini kebutuhan akan internet menjadi sebuah hal yang lumrah. Teknologi internet sendiri berkembang semakin cepat dan cepat untuk dapat memenuhi kebutuhan manusia yang semakin banyak menggunakan internet, begitu juga dengan teknologi web yang berkembang pesat dan sudah mencapai teknologi Web 4.0 dan semakin masif pengembangan dan penggunaannya. Menurut data dari Hootsuite, di Indonesia sendiri sebanyak 202,6 juta orang yang saat ini telah menggunakan internet yang sebagian besar mengakses sebuah situs web, baik dari jenis situs web portal berita, hiburan, hingga blog dan situs web belanja daring atau *e-Commerce* (Hootsuite, 2021). Menurut (Yuhefizar, dkk. 2009) pada bukunya menjelaskan mengenai jenis web berdasarkan tujuannya, pertama ada *Personal Web*, yaitu sebuah situs web yang dibuat dengan tujuan untuk menjadikan situs web tersebut menjadi wadah untuk menunjukkan informasi pribadi, selanjutnya ada *Corporate Web* yaitu sebuah situs web perusahaan, selanjutnya *Portal Web* yaitu situs web yang menjadi tempat untuk penyedia layanan, informasi, portal berita, dan banyak layanan lainnya, selanjutnya *Forum Web* yaitu situs web untuk melakukan diskusi, selain itu ada juga jenis web *e-Commerce*, *e-Payment*, *e-Banking*, *e-Procurement* dan *e-Government*.

Penggunaan situs web juga sudah merambah pada jenis situs web pemerintahan, pemerintahan sendiri juga sudah menggunakan sebuah situs web baik jenis web yang digunakan untuk menampilkan informasi sampai kepada aplikasi web, salah satu pemerintah daerah yang sudah menerapkan teknologi web adalah Bagian Pengadaan Barang dan Jasa Sekretariat Daerah Kabupaten Buleleng. Bagian Pengadaan Barang dan Jasa Sekretariat Daerah Kabupaten Buleleng atau BPBJ Sekretariat Daerah Kabupaten Buleleng mengembangkan sebuah aplikasi web bernama Sistem Informasi Aplikasi Pengadaan atau yang disingkat Z. Pada aplikasi Z dimana saat dilakukan wawancara langsung kepada narasumber,

dijelaskan bahwa aplikasi ini merupakan aplikasi yang digunakan untuk dapat membuat pengadaan paket tender dari pihak/perusahaan yang tertarik untuk masuk ke dalam proyek tender yang akan diadakan BPBJ Sekretariat Daerah Kabupaten Buleleng. Pada aplikasi Z tersebut, keperluan paket tender berupa dokumen-dokumen pelengkap administrasi nantinya dapat diajukan pada aplikasi Z. Aplikasi Z sendiri dikembangkan oleh pihak BPBJ Sekretariat Daerah Kabupaten Buleleng dengan menggunakan *framework* CI 3 dan menggunakan mysql sebagai basis datanya, serta dapat digunakan pada browser seperti Chrome dan Mozilla Firefox.

Pengembangan situs web di zaman sekarang sudah menjadi hal yang perlu ada dan semakin merambah ke segala bidang, hal ini sebenarnya memiliki dampak yang positif karena banyaknya variasi konten dan kegunaan dari situs web berbeda yang bisa diakses dari berbagai situs web, namun hal ini tidak dibarengi dengan keamanan pada data dan informasi yang ada pada situs web. Keamanan sebuah data dan informasi yang ada di internet memang selalu menjadi perdebatan karena masih seringnya terjadi pelanggaran privasi dan pencurian data yang ada di internet akibat dari kurangnya kualitas keamanan situs web tersebut. Melansir dari CNBC Indonesia, salah satu *e-Commerce* Indonesia yaitu Tokopedia pernah mengalami peretasan oleh *hacker* yang dimana data dan informasi yang dicuri berupa 91 juta data akun pengguna dan 7 juta akun *merchant* yang dimana data tersebut secara tidak bertanggung jawab dijual pada sebuah *dark* web bernama Empire Market (CNBC Indonesia, 2020), hal ini yang menjadi contoh bagaimana sebuah keamanan dari situs web menjadi sangat vital untuk mencegah hal seperti ini terjadi. Kasus lainnya, dilansir melalui Tempo.co dijelaskan telah terjadi kebocoran data oleh BPJS Kesehatan terkait dengan data dari 279 juta penduduk di Indonesia yang dimana data tersebut dijual pada *Raid Forums* dengan harga 0,15 bitcoin (Tempo, 2021). Keamanan sebuah situs web sangat penting dan harus sering diperhatikan apakah terdapat celah keamanan atau kerentanan pada setiap situs web yang dibangun, terlepas dari jenis situs web yang dibangun dan informasi serta data yang dimuat pada situs web tersebut. Pada jurnal (I. Riadi, A. Y. Y. W. 2019), yang berjudul "Analisis Keamanan *Website Open Journal System* Menggunakan Metode *Vulnerability Assessment*" menjelaskan bahwa dengan tingkat keamanan situs web yang rendah menjadikan para *hacker* dapat dengan mudah mengakses data penting,

selain data penting yang diretas, dapat juga menanamkan virus ataupun serangan yang mengakibatkan sebuah situs web menjadi sangat lambat, maka dari itu pentingnya untuk selalu memperbaharui sistem keamanan pada situs web yang akan dibangun ataupun yang telah dibangun. Pada jurnal lainnya (A. Elanda, R. L. Buana, 2020) yang berjudul "Analisis Keamanan Sistem Informasi Berbasis *Website* Dengan Metode *Open Web Application Security Project* (OWASP) Versi 4: *Systematic Review*" menjelaskan dengan mengetahui celah keamanan, belum tentu meningkatkan keamanan pada aplikasi web tersebut secara langsung, tapi dengan melakukan pengujian dan mengetahui celah tersebut maka akan memberikan penjelasan lebih jelas mengenai celah keamanan apa saja yang terdapat pada aplikasi yang dibangun sehingga dapat memprioritaskan bagian mana saja yang memiliki risiko lebih tinggi sehingga dapat ditangani terlebih dahulu.

Pengembangan aplikasi berbasis *website* memang tak luput dari serangan-serangan pihak yang kurang bertanggung jawab, sebut saja lembaga pemerintahan yang memiliki sebuah aplikasi sistem informasi berbasis *website* yang sering diberitakan bahwa data telah dicuri dan diperjual belikan oleh pihak-pihak tidak bertanggung jawab tersebut, hal ini yang mendorong untuk dapat dilakukannya analisis keamanan pada aplikasi Z milik BPBJ Sekretariat Daerah Kabupaten Buleleng. Analisis keamanan ini diperlukan karena hal ini menyangkut pada bagaimana data yang di *input* untuk keperluan tender sudah aman atau belum pada aplikasi Z tersebut, dijelaskan juga saat wawancara, pada aplikasi Z saat dikembangkan belum dilakukan uji keamanan, dimana pada aplikasi Z, dengan menggunakan hasil *scan automation* awal menggunakan OWASP ZAP, ditemukan peringatan kerentanan-kerentanan yang memang terdapat pada aplikasi Z dimana rinciannya dapat dilihat pada Lampiran 3, karena hal tersebut dan hasil diskusi dengan narasumber maka perlu dilakukan pengujian keamanan dengan menggunakan *framework* OWASP, ini karena OWASP ZAP berjalan dengan menggunakan *framework* OWASP dan perlu dilakukan analisis keamanan untuk dapat memastikan bahwa itu merupakan *false alarm* atau tidak, serta melihat bagaimana pentingnya dan rahasia data tersebut, maka perlu dilakukan analisis keamanan yang relevan dengan kebutuhan aplikasi Z dengan *framework* OWASP (*Open Web Application Security Project*) dengan metode *Input Validation Testing*.

OWASP sendiri dilansir langsung dari laman resmi web mereka (owasp.org), bahwa OWASP (*Open Web Application Security Project*) adalah sebuah organisasi nirlaba yang bekerja untuk meningkatkan keamanan perangkat lunak khususnya aplikasi web. Pada buku OWASP *Web Security Testing Guide* versi 4.2 dijelaskan untuk melakukan pengujian keamanan aplikasi web dapat dilakukan dengan 12 metode untuk dapat menguji kerentanan yang dimana metode tersebut dapat dibagi ke beberapa detail apa saja yang akan dicari kerentanannya, pada penelitian ini, dari 12 metode yang ada hanya akan berfokus pada metode *Input Validation Testing*. Metode *Input Validation Testing* ini merupakan salah satu dari 12 metode *active testing* yang terdiri dari *Information Gathering, Configuration and Deployment Management Testing, Identity Management Testing, Authentication Testing, Authorization Testing, Session Management Testing, Input Validation Testing, Error Handling, Cryptography, Business Logic Testing, Client-side Testing,* dan *API Testing* yang digunakan untuk dapat menemukan celah keamanan pada sebuah aplikasi web. Metode *Input Validation Testing* juga digunakan pada penelitian yang dilakukan oleh (Tamam Achmad Hanafi, dkk., 2019), dimana menggunakan metode *Input Validation Testing* untuk membuat sebuah aplikasi untuk dapat mencari celah keamanan. Berdasarkan buku OWASP *Web Security Testing Guide* versi 4.2, metode *input validation testing* digunakan sebagai metode mencari celah keamanan dengan jenis aplikasi web yang memiliki *input* seperti teks, *file*, gambar, dan suara yang mana ini juga selaras dengan publikasi OWASP mengenai OWASP *Top Ten* tahun 2017 yang mana memberikan peringkat bahwa keamanan paling rentan nomor satu adalah *injection*.

Berdasarkan deskripsi di atas, peneliti bermaksud untuk dapat menyelesaikan permasalahan tersebut dengan melakukan analisis keamanan dengan *framework* OWASP menggunakan metode *Input Validation Testing* yang dimana relevan dengan aplikasi Z yang proses bisnisnya banyak melakukan *submit* data-data penting yang harus aman dan terjaga kerahasiaannya. Pada saat melakukan pengujian menggunakan metode *Input Validation Testing* akan berfokus pada celah keamanan *SQL Injection*, *Reflected Cross Site Scripting (XSS)*, *Stored Cross Site Scripting (XSS)*, *Command Injection*, *Http Smuggling*. Pada jurnal (Ghozali, B. dkk., 2018) untuk mengukur tingkat risiko keamanan menggunakan

tabel risiko yang dapat dibagi menjadi tiga kategori, nilai 0 sampai <3 itu *low* (rendah), 3 sampai <6 *medium* (menengah), 6 sampai 9 *high* (tinggi) yang mana setelah ditemukan kerentanan tersebut, maka akan diukur tingkat risiko keamanan pada aplikasi Z, ini juga sangat memberikan keuntungan pada pihak yang peneliti uji karena dapat memberikan informasi mengenai apakah aplikasi web tersebut terdapat celah kerentanan atau tidak, serta memberikan rekomendasi perbaikan terkait kerentanan tersebut.

1.2 Rumusan Masalah

Berdasarkan latar belakang yang telah dibahas di atas, dapat dirumuskan permasalahan sebagai berikut :

1.2.1 Bagaimana hasil dari kerentanan pada aplikasi Z dengan metode *Input Validation Testing*?

1.2.2 Bagaimana tingkat risiko keamanan pada aplikasi Z?

1.2.3 Bagaimana rekomendasi perbaikan pada keamanan aplikasi Z?

1.3 Batasan Masalah

Terkait dengan batasan masalah, pada penelitian ini penulis membatasi batasan masalah sebagai berikut:

1.3.1 Analisis keamanan sistem informasi pada aplikasi Z dengan metode *Input Validation Testing* ini dibatasi hanya dengan memilih beberapa teknik yang dilakukan sesuai dengan kebutuhan aplikasi Z.

1.3.2 Analisis keamanan hanya menggunakan *tools-tools* rekomendasi OWASP dan penelitian sebelumnya.

1.3.3 Penentuan tingkat risiko keamanan dinilai hanya dari segi teknis saja.

1.3.4 Penggunaan *script payload* pada *Injection* dan *Cross Site Scripting (XSS)* digunakan sesuai dengan standar OWASP.

1.3.5 Hasil analisis keamanan nantinya berupa dokumen hasil analisis kerentanan dengan metode *Input Validation Testing* dan hasil tingkat risiko pada aplikasi Z.

1.4 Tujuan Penelitian

Berdasarkan dari rumusan masalah yang dibahas sebelumnya, dapat ditarik tujuan sebagai berikut :

1.4.1 Dapat mendeskripsikan hasil dari kerentanan pada aplikasi Z dengan metode *Input Validation Testing*.

1.4.2 Dapat mendeskripsikan tingkat risiko keamanan pada aplikasi Z.

1.4.3 Dapat mendeskripsikan rekomendasi perbaikan pada keamanan aplikasi Z.

1.5 Manfaat Penelitian

Adapun manfaat yang dapat diperoleh dengan penelitian Analisis Keamanan Sistem Informasi Dengan Metode *Input Validation Testing* Pada Aplikasi Z Di Bagian Pengadaan Barang Dan Jasa Sekretariat Daerah Kabupaten Buleleng adalah sebagai berikut:

1.5.1 Bagi BPBJ Sekretariat Daerah Kabupaten Buleleng Dan Pembaca

a) Dapat memberikan hasil celah keamanan dengan menggunakan metode *Input Validation Testing* sebagai acuan untuk dapat menganalisis aplikasi Z,
b) Dapat mengetahui tingkat risiko keamanan pada aplikasi Z dan bagaimana hasil yang dapat diberikan sehingga menjadi bahan pertimbangan pada perbaikan aplikasi Z oleh BPBJ Sekretariat Daerah Kabupaten Buleleng.
c) Dapat menjadi referensi untuk penggunaan metode *Input Validation Testing* pada analisis keamanan.

1.5.2 Bagi Peneliti

Manfaat lain yang di dapat adalah untuk peneliti, yaitu dapat mengimplementasikan ilmu yang sudah diperoleh selama melaksanakan perkuliahan di Universitas Pendidikan Ganesha serta semakin mendalami pengetahuan dalam bidang keamanan aplikasi web khususnya dengan metode *Input Validation Testing*.