BAB I
PENDAHULUAN

1.1. Latar Belakang

Di era yang berpusat pada teknologi saat ini, perbincagan mengenai keamanan dan integritas digital merupakan hal yang lazim. Dengan semakin banyaknya pengguna yang bergabung dengan internet setiap harinya, permintaan akan sistem keamanan komputer yang kuat pun semakin meningkat. Hal ini karena beberapa pihak yang tidak bertanggung jawab dapat melakukan tindak kejahatan *cyber*. Aplikasi berbasis web dipilih karena ringan dan bekerja di berbagai *platform.* Seiring dengan terus berkembangnya layanan web dan aplikasi di berbagai bidang, terjadi peningkatan signifikan dalam permintaan pengguna terhadap layanan ini.

Aplikasi *e-learning* sangat penting saat ini karena memberikan banyak manfaat dalam proses pembelajaran *online*. Hal ini membuat materi lebih terstruktur daripada pembelajaran tatap muka, membantu melengkapi dan mempermudah pelajaran, meningkatkan efisiensi dan efektivitas penyampaian informasi, serta mengatasi kendala waktu dan ruang [1].

Karena meningkatnya penggunaan dan keuntungan yang dirasakan oleh pengguna *e-learning*, tidak menutup kemungkinan bahwa aplikasi *e-learning* memiliki masalah keamanan informasi. Akibatnya, perlu dilakukan analisis terhadap masalah keamanan informasi yang terkait dengan aplikasi *e-learning* tersebut. Keamanan informasi menurut Rohim dan setiyani, adalah upaya untuk mencegah atau mendeteksi kecurangan dalam sistem berbasis informasi di mana informasinya sendiri tidak memiliki arti [2]. John mengatakan bahwa keamanan komputer yaitu tentang mencegah seseorang menggunakan komputer atau mengakses jaringan yang tidak bertanggung jawab. Adapun Gollman mengatakan bahwa keamanan komputer adalah tentang pencegahan dan deteksi gangguan sistem komputer yang tidak dikenali. Ahli keamanan komputer Garfinkel dan Spafford menyatakan bahwa komputer Perangkat lunaknya dikatakan aman jika dapat diandalkan dan bekerja dengan baik [2].

Pengujian sistem sangat penting untuk menemukan celah keamanan. Menurut hermanto dan haeruddin, *Open Web Application Security Project (OWASP)* adalah

sebuah kerangka kerja *open source* yang memberikan informasi tentang kerentanan keamanan dan rekomendasi perbaikan untuk layanan berbasis web. *Vulnerability Assessment* adalah proses untuk mengidentifikasi risiko dan ancaman yang mungkin timbul [3]. Biasanya, ini termasuk penggunaan alat pengujian otomatis seperti pemindaian keamanan jaringan. Hasil dari proses ini dicatat dalam laporan *Vulnerability Assessment* [2].

Peneliti mengungkapkan bahwa metode *Vulnerability Assessment* dapat digunakan untuk mengidentifikasi masalah keamanan sistem web, hal ini dibuktikan oleh penelitian sebelumnya oleh Hermanto, dalam jurnalnya yang berjudul "Analisis Celah Keamanan *E-Learning* Perguruan Tinggi Menggunakan *Vulnerability Assessment*". Dengan menggunakan *vulnerability assessment* dan *tools OWASP Zap*, hasil pemeriksaan menunjukkan adanya 15 kerentanan yang diidentifikasi setelah diuji, yang terbagi ke dalam 10 kategori yang berbeda. Namun, menurut standar *OWASP*, tidak ada celah risiko kerentanan yang tergolong tingkat tinggi. Dengan demikian, hasil penelitian menunjukkan bahwa tidak ada kerentanan yang memiliki risiko tinggi yang paling dominan [3].

Penelitian yang dilakukan oleh Yulia Taryana dan Nono Heryana, yang berjudul "Analisis Keamanan *Website* BPJS Kesehatan Menggunakan Metode *Vulnerability Asesement*". Penelitian ini memanfaatkan *OWASP ZAP* versi 2.11.0 untuk memindai keamanan *website* BPJS Kesehatan. Penelitian ini menunjukkan bahwa situs web aman untuk diakses, dan *OWASP ZAP* terbukti efektif dalam mengidentifikasi kerentanan [4].

Penelitian yang dilakukan oleh Ardita, dalam jurnalnya "Analisis Kerentanan Keamanan *Website* Menggunakan Metode *OWASP (Open Web Application Security Project)* Pada Dinas Tenaga Kerja". Penelitian ini menerapkan Metodologi *OWASP Risk Rating* pada dua contoh aplikasi berbasis web dengan karakteristik yang berbeda. Ditemukan 8 risiko, terdapat 3 risiko dengan tingkat keparahan tinggi, 3 risiko dengan tingkat keparahan sedang, dan 2 risiko dengan tingkat keparahan rendah [5].

Dari permasalahan diatas, maka penelitian ini dilakukan dengan tujuan mengumpulkan informasi tentang masalah keamanan dan kerentanan yang terkait dengan *e-learning* yang telah digunakan di perguruan tinggi negeri khusus nya di

Aceh. Ada 4 *e-learning* perguruan tinggi negeri di Aceh yang penulis akan lakukan pengujian, yaitu Universitas Malikussaleh (UNIMAL), Universitas Syiah Kuala (USK), Politeknik Negeri Lhokseumawe (PNL), Institu Seni Budaya Indeonesia Aceh (ISBI Aceh). Metode yang digunakan pada penelitian ini adalah *Vulnerability Risk* A*ssessment* dan penggunaan *tools OWASP*, yang ditujukan khusus untuk situs web, yang memungkinkan penulis untuk menemukan masalah keamanan dalam *e-learning* dengan benar. Penulis menambah judul dengan memperhatikan konteks yang disebutkan di atas dengan judul **"*Vulnerability Risk Assessment* Menggunakan Metode *Open Web Application Security Project (OWASP)* Pada *E-Learning* Perguruan Tinggi Negeri di Aceh"**.

1.2.Rumusan Masalah

Berdasarkan latar belakang diatas, permasalahan yang dapat dirumuskan adalah sebagai berikut:

1. Bagaimana cara menemukan celah keamanan yang ada pada *e-learning* perguruan tinggi negeri di Aceh?
2. Bagaimana menentukan besar tingkat risiko terkait kerentanan keamanan yang ada pada masing-masing *e-learning* perguruan tinggi negeri di Aceh?
3. Bagaimana solusi perbaikan sistem untuk meningkatkan keamanan masing-masing aplikasi *e-learning* perguruan tinggi negeri di Aceh?

1.3.Batasan Masalah

Beberapa hal yang dibatasi dalam penelitian ini adalah sebagai berikut:

1. Penelitian ini dilakukan pada *e-learning* 4 perguruan tinggi negeri di Aceh.
2. *Social Engineering* tidak termasuk dalam penelitian ini.
3. Penelitian ini menggunakan *tools OWASP ZAP* dan mengacu pada kerangka kerja *Vulnerability Risk Assessment*.
4. Kesimpulan dari hasil pengujian berupa solusi yang dapat dipertimbangkan untuk perbaikan sistem dan peringkat keamanan pada masing-masing *e-learning* perguruan tinggi negeri di Aceh.
5. Penelitian ini menghasilkan laporan tertulis.

1.4. Tujuan Penelitian

Tujuan dari penelitian ini adalah sebagai berikut:

1. Menganalisis keamanan pada *e-learning* perguruan tinggi negeri di Aceh menggunakan *Open Web Application Security Project (OWASP)*.
2. Mengukur *Vulnerability Risk Assessment* untuk mengetahui peringkat keamanan pada masing-masing *e-learning* perguruan tinggi negeri di Aceh.
3. Memberikan rekomendasi perbaikan yang dapat diterapkan pada sistem untuk meningkatkan keamanan.

1.5.Manfaat Penelitian

Adapun manfaat dari penelitian ini adalah sebagai berikut:

1. Digunakan sebagai referensi untuk sumber pengetahuan dan studi penelitian selanjutnya yang menggunakan metode dan studi kasus yang sama.
2. Memberikan informasi tambahan dan rekomendasi perbaikan untuk meningkatkan keamanan.
3. Kesadaran terkait keamanan sistem informasi.