BAB I

PENDAHULUAN

1.1 Latar Belakang

Industri 4.0 atau revolusi industri keempat merupakan istilah yang umum digunakan untuk tingkatan perkembangan industri teknologi di dunia. Pada tingkatan keempat ini, dunia memang fokus kepada teknologi-teknologi yang bersifat digital, oleh karena itu teknologi informasi sangat-sangat menjadi tumpuan untuk industri yang bertujuan untuk mempermudah dan mempercepat proses-proses untuk membuat produk.

Pandemi *covid*-19 secara tidak lansung mempercepat revolusi industri 4.0, dimana banyak kegitan dilakukan tidak dengan bertatap muka secara lansung, melainkan melalui pertemuan *online* melalui *gadget* masing-masing. Begitu juga dengan pencarian informasi, semua dilakukan dengan cepat melalui internet. Dengan faktor tersebut, banyak industri dan instansi berpacu untuk melakukan pembaharuan terhadap layanan informasi mereka yang agar pengiriman data dan informasi meningkat. Disamping keuntungan tersebut, tingkat resiko dan ancaman penyalahgunaan teknologi informasi juga menjadi semakin meningkat (Bustami dan Bahri, 2020).

Perubahan yang sangat cepat, kadang kala meluputkan *developer* dalam melakukan pengujian terhadap aplikasi yang dibangun. Pengujian merupakan proses yang sangat penting didalam pengembangan perangkat lunak yang berkualitas tinggi, karena dari beberapa kesalahan yang dianggap tidak penting beresiko sangat berbahaya hal ini menjadi celah (*vulnerability*) bagi *attacker* untuk memanfaatkan informasi yang di curi melalui serangan kepada aplikasi. Kebutuhan akan *vulnerability assessment* selama ini biasanya dipandang sebelah mata, karen hanya dianggap sebagai kegiatan formalitas dan sedikit orang yang melakukan kegiatan ini (Goel dan Mehtre, 2015). Salah satu sistem yang umumnyamenjadi sasaran *hacker*

dan *cracker* adalah aplikasi berbasis *website*. Hal tersebut dikarenakan pemanfaatan aplikasi mengalami pertumbuhan yang sangat pesat saat ini (Al Fajar, 2020). Serangan yang dilakukan dapat berupa *Cross Site Scripting* (XSS), *Cross Site Request Forgeri* (CSRF), SQL *injection* dan lain sebagainya (Riadi et al, 2020). Serangan SQL *injection* merupakan sebuah aksi *hacking* yang dilakukan di aplikasi *client* dengan cara memodifikasi perintah SQL yang ada di memori aplikasi *client* dan mengekploitasi aplikasi menggunakanh basis data untuk penyimpanan data (Ade Bastian et al, 2020). Penelitian lainya juga mendapatkan hasil jenis serangan seperti *Local File Inclusio*n (LFI) dan parameter tampering (Gupta et al, 2020).

Vulnerability testing banyak digunakan untuk meningkatkan kesadaran tentang pentingnya keamanan informasi (Riadi et al, 2021). Penilaian kerentanan bisa mendeteksi hampir semua celah kerentanan yang biasanya terjadi pada sebuah sistem (Pohan, 2021). Beberapa faktor dari dari celah keamanan bisa terjadi karena kurangnya sistem pengamanan *website* dan kekeliruan *programmer* ketika melakukan *coding* (Syarifudin, 2018).

Salah satu cara untuk melakukan evaluasi keamanan *website* menggunakan perangkat lunak yang khusus dirancang untuk mengetahui kerentanan yang ada pada suatu sistem yaitu *acunetix vulnerability scanner* (Mayasari et al, 2020), Pentest-tools.com, *acunetik* WVS, *vulnerability scanner*, OWASP ZAP (Irawadi Alwi dan Umar, 2020). Pengujian ini juga tidak terbatas pada aplikasi yang di kustom sendiri, aplikai CMS (*Content Management System*) seperti OJS juga menjadi target uji (Wibowo dan Purwo Wicaksono, 2019). Pengujian *vulnerability* dilakukan untuk pengukuran atau *assessment* yang mutlak dilakukan untuk mendapatkan peningkatan kualitas dan salah satu cara pengukuran terhadap keamanan sistem. Hasil dari *assesment* menjadi bahan pertimbangan bagi *developer* untuk mengambil tindakan pencegahan dan mengetahui cara kerja dari *attackers* (Orisa dan Ardita, 2021).

Begitu juga dengan Institut Teknologi Padang (ITP), baru saja meluncurkan *website* resmi versi ke 3. Alasan ITP meluncurkan versi ialah untuk menutupi celah keamaan yang terjadi pada versi 2 dimana pada versi ini masih menggunakan teknolgi *scripting* yang masih lama dimana rentan menjadi target serangan oleh *attacker*. Kerentanan pada keamanan *website* merupakan hal yang harus diperhatikan bagi setiap institusi agar terhindar dari tindakan kejahatan di dunia

maya (*cyber crime*) (Irawadi Alwi dan Umar, 2020). Oleh karena itu pengujian *vulnerability* penting dilakukan, yang hasilnya bukan menggaransi sistem akan bebas dari resiko serangan, tetapi dapat meminimalisir serangan yang dapat disalahgunakan, karena untuk menjelajahi semua aspek harus dilakukan pengujian tingkat lanjut (T dan Sasikala D, 2019).

Berdasarkan paparan diatas, penulis ingin melalukan analisa dan pengujian serta terhadap versi 3 dari *website* ini, dengan tujuan agar dapat memberikan saran perbaikan dan peningkatan dari kemanan *webisite* ini. Berdasarkan uraian diatas, penulis mengangkat permasalahan diatas sebagai judul penelitian yang berjudul "**Pengujian dan Analisis Keamanan *Website* Institut Teknologi Padang Menggunakan *Acunetix Vulnerability Scanner***".

1.2 Perumusan Masalah

Berdasarkan permasalahan yang ada, agar tesis ini sesuai dengan tujuan yang ingin dicapai, maka penulis merumuskan beberapa permasalahan sebagai berikut :

1. Bagaimana melakukan pengujian kemanan terhadap *website* ITP dengan menggunakan *tools* Acunetix WVS.
2. Bagaimana menganalisis celah keamanan yang ditemukan.
3. Bagaimana memberikan solusi dari permasalahan yang ditemukan.

1.3 Batasan Masalah

Agar pembahahasan pada penelitian ini tidak menyimpang maka penulis membatasi ruang lingkup objek penelitian. Adapun ruang lingkup penelitian antara lain:

1. Penelitian ini digunakan untuk mengetahui celah keamanan dari *website* ITP.
2. Penelitian ini menggunakan *tools* Acunetix WVS untuk pengujian,
3. Penelitian dilakukan demgan prinsip keamanan sistem informasi yaitu *confidentiality* (Kerahasiaan) dan *integrity* (Kesatuan).

1.4 Tujuan Penelitian

Tujuan yang ingin diperoleh dari penelitian ini agar lebih bermanfaat kedepannya adalah:

1. Melakukan pengujian terhadap keamanan *website* ITP dengan menggunakan *tools* Acunetix WVS.
2. Melakukan analisa terhadap kemanan yang ditemukan.
3. memberikan saran peningkatan keamanan dan perbaikan *website* ITP.

1.5 Manfaat Penelitian

Penelitian ini diharapkan memberikan manfaat kedepannya, yang beberapa diantaranya adalah:

1. ITP dapat mengetahui celah kemanan yang terdapat pada *website*.
2. Meningkatkan sistem keamanan dari *website* ITP.
3. Dapat menjadi konsultan keamanan sistem informasi bagi ITP.

1.6 Sistematika Penulisan

Sistematika yang digunakan dalam penyusunan tesis ini adalah sebagai berikut:

Bab I PENDAHULUAN

Bab ini berisikan tentang latar belakang, perumusan masalah, batasan masalah, tujuan penelitian, manfaat penelitian, dan sistematika penelitian

Bab II TINJAUAN PUSTAKA

Bab Ini berisikan tentang *vulnerability*, *vulnerability assesment*, Serangan Dalam Keamanan Komputer dan *tools* Acunetix WVS.

Bab III METODOLOGI PENELITIAN

Bab ini menjelaskan jenis penelitian 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 analisa sistem yang akan diuji, bagaimana *tools* Acunetix WVS bekerja dan mengelompokkan hasil *assesment* dan cara pengujian serta analisa perbaikan dari hasil *assesment*.

Bab V IMPLEMENTASI DAN HASIL

Bab ini berisi tentang implementasi perancangan yang telah dilakukan serta detail perbaikan dan hasil dari pengujian yang dilakukan.

Bab VI KESIMPULAN DAN SARAN

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