BAB I

PENDAHULUAN

1.1. Latar Belakang

Seiring dengan perkembangan internet dan teknologi membawa dampak yang sangat besar bagi peradaban. Internet telah mengubah tatanan hidup masyarakat dunia. Pencarian informasi, semua dilakukan dengan cepat melalui internet. Faktor tersebut menyebabkan banyak industri dan instansi berpacu untuk melakukan pembaharuan terhadap layanan informasi mereka agar pengiriman data dan informasi meningkat. Disamping keuntungan tersebut, tingkat resiko dan ancaman penyalahgunaan teknologi informasi juga menjadi semakin meningkat (Bustami,dkk 2020). Keamanan aplikasi *web* adalah komponen utama dari setiap bisnis berbasis *web*. Karena sifat internet ini, aplikasi *web* dapat diserang dari lokasi yang berbeda pada berbagai tingkat skala dan kompleksitas. Sejumlah besar teknik pengujian, pendekatan, alat dan kerangka kerja telah diusulkan oleh praktisi dan peneliti selama beberapa dekade terakhir untuk secara efektif dan efisien menguji keamanan aplikasi *web* (Aydos, dkk 2021).

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 menggunakan basis data untuk penyimpanan data (Ade Bastian,dkk 2020). Penelitian lainnya juga mendapatkan hasil jenis serangan seperti *Local File Inclusion* (LFI) dan parameter *tampering* (Ujjwal Gupta dkk, 2020). Helsinki University Press melaporkan bahwa setiap tahun hampir 43% peningkatan pendaftaran kerentanan dari berbagai sumber organisasi di dunia (Sharma, dkk 2022).

Pada salah satu sumber yang ditulis oleh peneliti lain telah dikatakan bahwa tidak ada aplikasi *website* tanpa adanya risiko kerentanan terhadap serangan siber (Md Moniruzzaman,dkk 2019). Oleh karena itu, informasi yang tersedia didalam *website* perlu dilakukan pengamanan secara komprehensif agar tidak

mengakibatkan pelanggaran integritas atau pencurian data. Dalam mengetahui celah kerentanan keamanan tersebut dapat dilakukan dengan memanfaatkan metode *Penetration Testing* yang merupakan bagian dari proses pengujian sistem dengan harapan dapat mengetahui celah keamanan yang tersedia (Devi, 2020; Goutam dan Tiwari, 2019; Nagpure dan Patel, 2019). *Vulnerability testing* banyak digunakan untuk meningkatkan kesadaran tentang pentingnya keamanan informasi (Riadi,dkk 2021). Penilaian kerentanan bisa mendeteksi hampir semua celah kerentanan yang biasanya terjadi pada sebuah sistem (Pohan, 2021).

Tersedia beberapa alat yang dapat dioptimalkan dalam kegiatan *vulnerability scanning* didalam implementasinya seperti Acunetix, OWASP ZAP, Vega, dan lainnya (Tsani, 2021). 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,dkk 2020), Pentest-tools.com, acunetix WVS, *vulnerability scanner*, OWASP ZAP (Irawadi Alwi dan Umar, 2020). Pengujian ini juga tidak terbatas pada aplikasi yang di kustom sendiri, aplikasi CMS (*Content Management System*) seperti OJS juga menjadi tujuan pengujian (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 pengembang untuk mengambil tindakan pencegahan dan mengetahui cara kerja dari penyerang (Orisa dan Ardita, 2021).

Aspek keamanan sering diabaikan dalam penerapan Teknologi Informasi. Kerentanan biasanya disebabkan oleh kelalaian pengembang yang menyebabkan kerusakan pada sistem yang digunakan. Serangan SQL *Injection*, *Cross Site Scripting* dan tidak tersedianya penggunaan saluran terenkripsi menyebabkan terpaparnya pengguna terhadap data sensitif. Tujuan dari penelitian ini adalah untuk melakukan audit dan analisis aspek keamanan terhadap *Web* Yayasan Pendidikan Beerseba. Audit dan analisis keamanan adalah langkah pencegahan sehingga kerentanan yang ditemukan tidak menjadi pintu masuk bagi peretas sistem. Hasil dari penelitian ini dalam bentuk laporan audit keamanan yang memuat tentang kerentanan *Web* Yayasan Pendidikan Beerseba. Laporan tersebut akan digunakan

sebagai referensi bagi pengembang (*developer*) aplikasi *online*. Metode yang dilakukan pada pengujian ini akan menggunakan *tool* berupa perangkat lunak dan cara-cara tertentu yang digunakan untuk menguji keamanan sebuah Aplikasi *Web*.

Analisis keamanan aplikasi *web ini menggunakan software* Acunetix *Web Vulnerability scanner*. Hasil dari pengujian dapat ditemukan berbagai level kerentanan dari level kerentanan *low* sampai level kerentanan *high* pada *domain* beerseba.sch.id. Dari hasil analisis yang diperoleh dan dapat dilihat berbagai *web alerts* yang terdapat pada sebuah aplikasi *web* tersebut. Adapun berbagai *web alerts* yang berhasil ditemukan berupa SQL *Injection*, *Cross Site Scripting* dan berbagai *web alerts* lainnya. Untuk mendukung permasalahan terhadap bahasan, peneliti berusaha melacak berbagai literatur dan penelitian terdahulu yang masih relevan terhadap masalah yang menjadi objek penelitian saat ini. Selain itu yang menjadi syarat mutlak bahwa dalam penelitian ilmiah menolak yang namanya plagiarisme atau mencontek secara utuh hasil karya tulisan orang lain. Berdasarkan hasil eksplorasi terhadap penelitian-penelitian terdahulu, peneliti menemukan beberapa penelitian terdahulu yang relevan dengan penelitian ini. Meskipun terdapat keterkaitan pembahasan, penelitian ini masih sangat berbeda dengan penelitian terdahulu.

Adapun beberapa penelitian terdahulu tersebut yaitu: Analisa Serangan Vulnerabilities Terhadap Server Selama Periode WFH di Masa Pandemi Covid-19 Sebagai Prosedur Mitigasi oleh K. Subandi (2021). Penelitian ini berfokus terhadap *scanning* IP *address*. Dilakukan metode *vulnerability assesment* menggunakan *penetration testing* menggunakan *footprinting, finger printing* dan *enumeration*, kemudian hasil penilaian kerentanan dan tes penetrasi yang dilakukan dapat menemukan dan mengevaluasi sebagian besar kerentanan yang diketahui. Penelitian selanjutnya yaitu Uji Vulnerability Pada *Website* Jurnal Ilmiah Universitas Muhammadiyah Purwokerto Menggunakan OpenVAS dan Acunetix WVS oleh Feri Wibowo, Wicaksono (2019). Penelitian ini menggunakan OpenVAS dan Acunetix WVS untuk menguji kerentanan pada *website* jurnal ilmiah Universitas Muhammadiyah Purwokerto, metode yang digunakan adalah penelitian terapan yang berfokus pada analisis hasil evaluasi sehingga diharapkan dapat menghasilkan informasi yang dijadikan masukan atau pengambilan

keputusan tertentu sesuai urgensi sasaran. Secara teknis penelitian ini dilakukan dengan menggunakan 3 tahapan inti dari proses *Vulnerability Assesment* (VA) yaitu penentuan batasan proyek, implementasi *Vulnerability Asessment*, dan analisis hasil *Vulnerability Asessment*. Proses VA terhadap *website* jurnal ilmiah UMP berbasis OJS versi 2.4.8.0 berjalan dengan baik dan menghasilkan temuan kelemahan atau kerentanan. OpenVAS menemukan celah kelemahan sejumlah 9 data, sedangkan Acunetix WVS menemukan celah kelemahan sejumlah 166 data. Penelitian selanjutnya, Analisis Keamanan Aplikasi *Web* Prodi Teknik Informatika UIKA Menggunakan Acunetix *Web Vulnerability* oleh Febri Al Fajar (2020). Metode yang dilakukan pada pengujian ini akan menggunakan *tool* berupa perangkat lunak dan cara-cara tertentu yang digunakan untuk menguji keamanan sebuah aplikasi *web*. Tujuan dari penelitian ini adalah untuk melakukan audit dan analisis aspek keamanan terhadap Aplikasi *Web* Prodi Teknik Informatika UIKA. Hasil dari pengujian dapat ditemukan berbagai level kerentanan dari level kerentanan *low* pada *domain* ti.ft.uika-bogor.ac.id sampai level kerentanan *high* pada sub *domain* lainnya yang berupa sub *domain* fakultas. Dari hasil analisis yang diperoleh dan dapat dilihat berbagai *web alerts* yang terdapat pada sebuah aplikasi *web* tersebut. Adapun berbagai *web alerts* yang berhasil ditemukan berupa SQL *Injection*, *Cross Site Scripting* dan berbagai *web alerts* lainnya. Penelitian selanjutnya Analisis Vulnerability Pada Website Universitas Singaperbangsa Karawang Menggunakan Acunetix Vulnerability oleh Rini Mayasari,dkk (2020). Penelitian ini menggunakan metode kualitatif dengan memanfaatkan perangkat lunak Acunetix *Web Vulnerability*, yang dimulai dari tahap inisiasi, investigasi, pengujian dan verifikasi. Hasil dari penelitian ini, tingkat kerentanan *website* Universitas Singaperbangsa Karawang berada pada level 2 yaitu *medium*, sehingga kemungkinan untuk mengakses dan mengumpulkan informasi sensitif, karena dengan informasi tersebut penyusup bisa dengan mudah mengeksploitasi kelemahan yang ada. Penelitian yang relevan selanjutnya adalah *Vulnerability Asessment* Untuk Meningkatkan Kualitas Keamanan *Web* oleh Orisa,Ardita (2021). Metode *vulnerability assessment* yang digunakan ini adalah cara terbaik saat ini untuk membantu pihak-pihak tertentu dalam menjaga keamanan aplikasi *web* mereka. Dengan melakukan *vulnerability assessment* dapat mengidentifikasi

macam-macam celah yang memungkinkan masuknya serangan. Metode ini dapat membantu pihak-pihak tertentu untuk mengambil tindakan pencegahan terhadap serangan atau suatu kerusakan akibat kejahatan dunia maya. *Network mapping* atau dikenal dengan Nmap dapat membantu para *master web* untuk melakukan *vulnerability assessment*. Hasilnya dapat melakukan pengecekan terhadap serangan *denial of service*, dapat menemukan *vulnerability* xss pada file php, dan dapat menemukan *vulnerability* terhadap serangan SQL *Injection*.

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 (Simran T dan Sasikala D, 2019).

Berdasarkan paparan diatas, penulis ingin melakukan analisa dan pengujian serta perbaikan terhadap *website* ini, dengan tujuan agar dapat memberikan saran perbaikan dan peningkatan dari keamanan *website* ini. Berdasarkan uraian di atas, penulis mengangkat permasalahan diatas sebagai judul penelitian yang berjudul "Audit Keamanan Web Menggunakan Acunetix Web Vulnerability (Studi Kasus di Yayasan Pendidikan Beerseba Pekanbaru)".

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 menerapkan Acunetix *Web Vulnerability* untuk pengujian keamanan terhadap *website*?
2. Bagaimana proses melakukan perbaikan dari kerentanan yang ditemukan?
3. Bagaimana hasil pengujian kerentanan setelah dilakukan perbaikan?

1.3 Batasan Masalah

Agar penelitian tetap terarah dan tidak menyimpang dibutuhkan adanya batasan masalah, yaitu sebagai berikut:

1. Batasan masalah dalam penelitian ini adalah *website* yang di analisa beerseba.sch.id milik Yayasan Pendidikan Beerseba.
2. Penelitian ini untuk mengetahui celah keamanan pada *website* Beerseba.sch.id dengan menggunakan tool Acunetix *Web Vulnerability*.
3. Pada penelitian ini dilakukan perbaikan kerentanan pada tingkat risiko *high* dan *low* yang ditemukan.
4. Dilakukan *vulnerability scanning* ulang untuk mengetahui perbandingan celah kerentanan sebelum dan sesudah dilakukan perbaikan.

1.4 Tujuan Penelitian

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

1. Menemukan kerentanan (*vulnerability*) yang ada pada *website* beerseba.sch.id milik Yayasan Pendidikan Beerseba.
2. Melakukan Analisa terhadap keamanan yang ditemukan.
3. Merancang sistem untuk memperbaiki kerentanan pada tingkat kerentanan paling tinggi hingga terendah yang ditemukan pada hasil deteksi pemindaian (*scanning*).

1.5 Manfaat Penelitian

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

1. Yayasan Pendidikan Beerseba dapat mengetahui celah keamanan yang terdapat pada *website*.

2. Meningkatkan sistem keamanan dari *website* Yayasan Pendidikan Beerseba.
3. Menjadi konsultan keamanan sistem informasi bagi Yayasan Pendidikan Beerseba.

1.6 Sistematika Penulisan

Sistematika penulisan dilakukan agar lebih mudah untuk dibaca dan dimengerti, maka penulis berusaha membuat pembahasan lebih rinci dalam penyusunan tesis ini, sistematika penulisan dibagi atas beberapa bab 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

Pada bagian ini berisi berbagai teori yang digunakan sebagai landasan untuk menyelesaikan permasalahan yang diangkat pada penelitian ini. Bahasan dalam bagian ini, di antaranya pembahasan teori dasar dan penerapannya terkait *vulnerability*, *vulnerability assessment*, Serangan Dalam Keamanan Komputer, SQL *Injection*, *Cross-Site Scripting* (XSS) dan *tool* Acunetix *Web Vulnerability*.

BAB III METODOLOGI PENELITIAN

Bab ini berisi tentang objek dan jenis penelitian, teknik pengumpulan data, analisis terhadap kebutuhan aplikasi yang akan dibangun, dan perancangan alur aplikasi.

BAB IV ANALISA DAN PERANCANGAN

Bab ini berisi tentang analisa sistem yang akan diuji, bagaimana *tool*

Acunetix WVS bekerja dan mengelompokkan hasil *assesment* dan cara pengujian serta analisa perbaikan dari hasil *assessment*.

BAB V IMPLEMENTASI DAN HASIL

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

BAB VI KESIMPULAN DAN SARAN

Pada bagian ini berisi kesimpulan dan saran untuk pengembangan selanjutnya juga menjelaskan tujuan penelitian dapat tercapai.