BAB I

PENDAHULUAN

1.1 Latar Belakang

Perkembangan teknologi informasi berkembang pesat seiring dengan pertumbuhan penggunanya. Contoh dari perkembangan teknologi adalah penggunaan *website* untuk mendukung kegiatan pembelajaran. *Website* merupakan kumpulan halaman *web* yang dapat diakses secara publik. *Website* dapat terdiri dari teks, gambar, video, dan media suara lainnya. Namun dengan berkembangnya suatu teknologi, maka perkembangan kerentanan atau serangan terhadap teknologi tersebut juga bertambah. Berdasarkan laporan tahunan monitoring keamanan siber tahun 2021 oleh Badan Siber dan Sandi Negara (BSSN), terdapat lebih dari 1,6 miliar serangan siber yang telah terjadi di Indonesia (Putra, Budiono dan Septo, 2023).

SQL Injection adalah aksi *hacking* yang dilakukan di aplikasi *client* dengan memodifikasi perintah *SQL* yang ada di memori aplikasi *client* dan merupakan teknik mengeksploitasi *web* aplikasi yang didalamnya menggunakan *database* untuk penyimpanan data. Metode *SQL injection* digunakan untuk memasukan perintah *SQL* sebagai input pada suatu *website* untuk mendapatkan akses ke dalam basis data. Jika basis data *website* dapat diakses, maka seorang *hacker* dapat dengan mudah mencuri berbagai data rahasia, bahkan dapat memanipulasi atau merusak data pada *website* tersebut (Pratama, Songida dan Gunawan, 2022). Dan dari penelitian sebelumnya yang lain *SQL Injection* merupakan perintah yang memiliki resiko tinggi menyerang *database website*. Tanpa langkah keamanan yang kuat, serangan injeksi *SQL* dapat menembus pertahanan situs *web*. Mengingat *website* ini banyak digunakan, maka dipandang perlu untuk memperhatikan keamanan *website*. Injeksi *SQL* dapat terjadi ketika penyerang mampu memanipulasi kueri *SQL* (*Structured Query Language*) yang

diarahkan melalui aplikasi dan terpapar kerentanan di situs *web*. Berdasarkan penelitiannya, dia menyimpulkan bahwa *tool SQLMap* di *Kali Linux* sangat bagus dan dapat dengan mudah menembus keamanan situs *web* yang dia serang. *SQLMap* ini memiliki fungsi bawaan untuk mendeteksi jenis *database* yang digunakan oleh korban dan data yang diterima, sehingga konten dapat dilihat, diselesaikan, dan dimodifikasi. Selain itu, alat *SQLSUS* dapat mengisi *database* sepenuhnya, tetapi beberapa paket harus diinstal terlebih dahulu dan terakhir sehubungan dengan pin atau pembatas parameter yang digunakan oleh situs (Adinata *et al.*, 2022).

Serangan Cross-Site Scripting (XSS) juga biasa digunakan untuk mengubah situs *web*. Dalam serangan ini, pelaku menyisipkan kode skrip berbahaya ke dalam halaman *web*, yang kemudian dijalankan oleh *browser* pengguna. Ini memungkinkan peretas mencuri informasi sensitif, mengarahkan pengguna ke halaman palsu, atau mengubah tampilan dan nuansa situs (Aji, 2023). Berdasarkan hasil penelitian yang lain dilakukan pada *website* servio diperoleh kerentanan – kerentanan seperti *HTML* tanpa perlindungan *CSRF*, *clickjacking*, dan beberapa *web alert informational*. Hasil yang ditemukan Acunetix berada pada *level medium*, yang berarti kerentanan terjadi karena kesalahan konfigurasi dan *site coding* yang lemah (Kristianto, Rahman dan Bahri, 2022).

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*, *Pentest-tools.com*, *vulnerability scanner*, *OWASP ZAP*. Pengujian ini juga tidak terbatas pada aplikasi yang di kustom sendiri, aplikai CMS (*Content Management System*) seperti OJS juga menjadi target uji. 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* (Zirwan, 2022).

Beberapa penelitian sebelumnya adalah: Analisis Keamanan Website Sman 1 Sumbawa Menggunakan Metode *Vulnerability Assement* oleh Mulyanto, Haryanti dan Jumirah (2021). Penelitian ini fokus dengan kerentanan pada situs *web*. Menggunakan

metode *vulnerability assessment* dengan bantuan *software Open Web Application Security Project* (OWASP), *Network Mapper* (NMAP), hasil pengujian yang dilakukan ditemukan beberapa kerentanan salah satunya *SQL Injection* dimana kerentanan tersebut memudahkan penyerang mengakses seluruh *database*. Penelitian berikutnya yaitu: Audit Keamanan dan Manajemen Risiko pada *e-Learning* Universitas Sangga Buana oleh Sangga, Sandy dan Solihin (2021). Menggunakan *Framework NIST SP 80-26* sebagai yang menjelaskan tentang level keamanan teknologi informasi dan *tool Acunetix* untuk menguji kerentanan *website E-learning* Universitas Sangga Buana, Metode penelitian yang digunakan adalah metode kuantitatif, yaitu suatu proses dengan menggunakan sekumpulan angka-angka yang digunakan untuk dapat menganalisis apa yang ingin diketahui, secara struktur dari awal hingga akhir proses perhitungan. Hasil dari penelitian ini berupa tingkat keamanan dan manajemen risiko yang terdapat pada sistem *e-Learning*.

Penelitian berikutnya, *Website Security* Test At the University of Mataram Using *Vulnerability Assessment* oleh Adha, KWA dan Muhammad (2023). Web site yang menjadi sasaran adalah unram.ac.id milik Universitas Mataram yang digunakan untuk operasional Perusahaan dengan menggunakan beberapa *tools* pengujian yaitu *Hosted Scan, OWASP*, dan *OpenVAS* dalam pencarian ulang dan pengujian keamanan *website* sebelumnya. Langkah-langkah yang dilakukan adalah dengan memulai dengan menerapkan metode *penetration test* untuk mengetahui kerentanan pada *website*. Berdasarkan hasil proses VA pada *website* Universitas Mataram berjalan dengan baik dan menghasilkan temuan dari kelemahan atau kerentanan. *Owasp ZAP* menemukan 14 kerentanan data, sedangkan *OpenVAS* menemukan 2 kerentanan data. dengan perbandingan waktu *scanning* yang relatif lama yaitu *Owasp ZAP* membutuhkan waktu 40 menit sedangkan *OpenVAS* membutuhkan waktu 145 menit. Data yang lemah ini dapat dijadikan masukan bagi tim sistem informasi Universitas Mataram untuk segera menutup atau memperbaiki celah keamanan yang ada.

Dari penjelasan pada latar belakang diatas maka dilakukan penelitian untuk menerapkan Pengujian dan Audit Keamanan *Website* SMK Muhammadiyah 3 Terpadu Pekanbaru Menggunakan *Acunetix*, karena dengan menggunakan aplikasi *Acunetix Web Vulnerability Scanner* adalah salah satu aplikasi *scanner web* terkemuka

yang sangat baik sebagai solusi untuk memecahkan masalah keamanan situs *web* dan dalam penelitian ini penulis mengusulkan penelitian berupa tesis **Audit Keamanan Website Menggunakan Acunetix Web Vulnerability (Studi Kasus di SMK Muhammadiyah 3 Terpadu Pekanbaru).**

1.2 Rumusan 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 keamanan terhadap *website* dengan menggunakan *tools Acunetix WVS* dapat mengetahui celah keamanan ?
2. Bagaimana melakukan tahapan perbaikan kerentanan keamanan *website* yang ditemukan dari hasil pindai dengan menggunakan *Acunetix WVS* dapat mengidentifikasi keamanan ?
3. Bagaimana hasil pengujian kerentanan keamanan *website* setelah dilakukan perbaikan dari hasil pindai ?

1.3 Batasan Masalah

Adapun beberapa batasan masalah dalam penelitian ini untuk tidak melebar dan lebih terarah dari tema yang diangkat, maka peneliti mencantumkan batasan masalah sebagai berikut:

1. Penelitian ini dalam pengujian celah keamanan *website* SMK Muhammadiyah 3 Terpadu Pekanbaru.
2. Penelitian ini menggunakan *tools Acunetix WVS* untuk menemukan kerentanan keamanan *website* SMK Muhammadiyah 3 Terpadu Pekanbaru.
3. Penelitian ini dalam memindai kerentanan ulang dengan menggunakan *tools Acunetix WVS* guna untuk mengetahui perubahan dan perbandingan celah kerentanan sebelum dan sesudah dilakukan perbaikan.

1.4 Tujuan Penelitian

Tujuan Penelitian ini dengan tema *audit* keamanan *website* SMK Muhammadiyah 3 Terpadu Pekanbaru menggunakan alat bantu *Acunetix WVS* sebagai berikut:

1. *Acunetix* WVS dapat melakukan pemindaian secara otomatis terhadap website dan pengujian terhadap berbagai kerentanan keamanan *website*.
2. Diperlukan komitmen untuk menjaga keamanan *website* secara terus-menerus dan mengambil langkah-langkah proaktif untuk mengatasi dan mencegah kerentanan yang mungkin muncul.
3. Hasil pengujian kerentanan keamanan sebuah *website* setelah dilakukan perbaikan dari hasil pindai dapat bervariasi tergantung pada sejumlah faktor, termasuk jenis kerentanan yang ditemukan, tindakan perbaikan yang dilakukan, dan tingkat keamanan yang diinginkan.

1.5 Manfaat Penelitian

Pada penelitian ini diharapkan dapat memberikan manfaat kedepannya, beberapa diantaranya yaitu:

1. Administrator system dan SMK MUTI dapat mengetahui celah keamanan yang terdapat pada *website*.
2. Meningkatkan sistem keamanan dengan melakukan *audit* mandiri terhadap *website* SMK MUTI.

1.6 Sistematika Penulisan

Penulisan yang sistematis digunakan untuk memudahkan pembacaan dan pemahaman, oleh karena itu penulis dalam menyusun tesis memuat beberapa bab tergantung bagaimana permasalahan yang disajikan. Sebagai berikut:

BAB I PENDAHULUAN

Bab ini membahas latar belakang penelitian, perumusan masalah, batasan masalah, tujuan penelitian, manfaat penelitian, dan sistematika penulisan.

BAB II LANDASAN TEORI

Pada bab ini berisi tentang teori-teori yang berkaitan dengan permasalahan yang diteliti pada penelitian ini. Diantaranya terkait *vulnerability*, *vulnerability assessment*, *SQL Injection*, *Cross-Site Scripting* (XSS) dan *tool Acunetix Web Vulnerability Scanner*.

BAB III METODOLOGI PENELITIAN

Bab ini menjelaskan tentang jenis penelitian yang dilakukan, objek penelitian, sumber data, pendekatan yang digunakan, metode dan analisa pengumpulan data yang dilakukan secara sistematis dan tepat sasaran.

BAB IV ANALISA DAN PERENCANAAN

Bab ini berisi Analisa sistem yang akan diuji, bagaimana *tool Acunetix WVS* bekerja dan mengelompokkan hasil *assessment* 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 PENUTUP

Bab ini berisi tentang kesimpulan dari penelitian yang telah dilakukan serta keterbatasan dan saran yang bisa digunakan dalam pengembangan penelitian selanjutnya dengan topik pembahasan yang sama.