BAB 1 PENDAHULUAN

1.1. Latar Belakang

Kemunculan berbagai teknologi baru di era digital saat ini memudahkan segala aspek kehidupan, termasuk akses dan pengumpulan informasi oleh Masyarakat [1]. Tentu saja, teknologi jika digunakan dengan cara yang positif, dapat memberikan banyak keuntungan dalam kehidupan manusia [2]. Penggunaan teknologi elektronik telah membuat hampir semua kegiatan masyarakat menjadi lebih efisien dan nyaman. Namun, jika tidak digunakan dengan bijak, teknologi digital bisa berdampak negatif pada kehidupan Masyarakat [3]. Belakangan ini, beberapa dampak negatif dari teknologi telah muncul dalam aktivitas digital, termasuk penipuan, perjudian, penyebaran berita bohong atau hoaks, dan kejahatan *cyber* [4].

Kejahatan siber adalah rangkaian tindakan kriminal yang dilakukan dengan memanfaatkan teknologi komputer dan jaringan internet [5]. Internet sebagai bentuk dari inovasi teknologi telah berhasil menghilangkan hambatan yang selama ini membatasi akses informasi dan komunikasi dalam Masyarakat [6], khususnya dalam pesantren. Seiring dengan peningkatan penggunaan internet setiap hari, keamanan menjadi aspek penting dalam dunia online. Hal ini disebabkan oleh pertukaran informasi yang sangat sensitif melalui situs online salah satunya adalah website, menjadikannya sasaran bagi penjahat siber yang berusaha mencuri atau memanipulasi data untuk tujuan jahat [7]. Dengan semakin luasnya penggunaan situs website, dampak dari tindakan kriminal terhadap situs website juga terus berkembang, termasuk pencurian dan manipulasi data oleh pihak yang tidak bertanggung jawab [8].

Pertumbuhan teknologi di pondok pesantren, seperti di banyak organisasi lainnya, semakin mengandalkan komputer dan jaringan untuk mengelola informasi, menjalankan kegiatan administratif, dan menyebarkan ilmu pengetahuan. Oleh karena itu, keamanan siber menjadi sangat penting untuk melindungi data, infrastruktur, dan aktivitas pendidikan. Peluang dan ancaman digital yang muncul di era ini membawa manfaat besar dalam pembelajaran, administrasi, dan penyebaran ajaran agama. Namun, ancaman serius seperti peretasan data, pencurian

identitas, dan serangan siber juga meningkat, mengancam kelangsungan pendidikan dan keamanan di pondok pesantren.

Pondok Pesantren X, yang menggunakan metode pembelajaran jarak jauh (PJJ) berbasis website, mengalami serangan peretasan pada 24 Maret 2021. Peretasan ini berupa defacement website, di mana penyerang mengganti konten situs dengan pesan mereka sendiri, menyebabkan gangguan PJJ selama empat hari. Pesan tersebut dapat berisi pesan politik, agama, sumpah serapah, atau konten tidak pantas yang mempermalukan pemilik situs atau mengumumkan bahwa situs telah diretas oleh kelompok tertentu [9].

Perlindungan data santri sangat penting karena pondok pesantren menyimpan informasi sensitif seperti catatan pendidikan, data pribadi, dan data keuangan. Oleh karena itu, penting untuk memastikan data ini aman dari akses yang tidak sah. Kesadaran keamanan siber tidak hanya menjadi tanggung jawab administrator IT; santri dan pengajar juga harus memiliki kesadaran dan keterampilan dasar untuk melindungi diri mereka sendiri dan data yang mereka Kelola [10].

Website Yayasan Pondok XYZ adalah platform digital yang dibentuk dan dikelola oleh Yayasan Pondok XYZ untuk menyediakan berbagai informasi penting kepada masyarakat umum. Website ini mencakup informasi mengenai persyaratan pendaftaran, pengumuman, nilai, rapor, data santri, serta pendaftaran santri baru. Selain itu, website ini juga mencakup informasi untuk Pondok Pesantren, Madrasah Formal, dan Sekolah Tinggi yang berada di bawah naungan Yayasan Pondok XYZ. Pengujian keamanan pada salah satu website Yayasan Pondok XYZ sangat penting dilakukan untuk memastikan perlindungan data dan menjaga agar website dapat digunakan dengan aman oleh seluruh pengunjung dan pengguna.

Dalam menghadapi pengujian skala besar dan data yang masif, metode yang digunakan dalam security assessment tidak mampu memenuhi kebutuhan aktual dalam hal representasi dan penalaran pengetahuan karena memerlukan waktu yang cukup lama untuk diterapkan [11]. Namun dalam penelitian ini memberikan gambaran tingkat keamanan yang komprehensif, sehingga dalam penelitian tersebut mengesampingkan kelemahan *security assessment*. Sehingga dalam

penelitian ini, hanya menggunakan pendekatan dari *security assessment*, Salah satu dari metode security assessment yaitu *OWASP Web Security Testing Guide*.

Web Security Testing Guide (WSTG) adalah alat untuk melakukan pengujian keamanan pada situs website, bertujuan mengevaluasi dan menganalisis aplikasi untuk mengidentifikasi setiap kelemahan, baik teknis maupun kerentanan. WSTG mencakup berbagai teknik, termasuk Pengumpulan Informasi, Pengujian Konfigurasi dan Manajemen Penerapan, Pengujian Manajemen Identitas, Pengujian Otentikasi, Pengujian Otorisasi, Pengujian Manajemen Sesi, Pengujian Validasi Input, Pengujian Penanganan Kesalahan, Pengujian Kriptografi Lemah, Pengujian Logika Bisnis, Pengujian Sisi Klien, dan Pengujian API[12].

Sehingga penelitian ini dilakukan dengan menggunakan metode *OWASP Web Security Testing Guide* untuk mengukur keamanan dari *website* Intitusi Yayasan Pondok XYZ.

1.2. Rumusan Masalah

Penelitian ini dilatarbelakangi oleh maraknya serangan siber terhadap *website* pondok pesantren, yang diakibatkan oleh kelemahan keamanan *website* dan kurangnya kesadaran atas serangan siber. Kurangnya kesadaran serangan siber di kalangan pondok pesantren membuat mereka rentan terhadap serangan yang mana mereka menyimpan informasi sensitif. Oleh karena itu, penelitian ini bertujuan untuk mengembangkan metode pengujian keamanan *website* yang efisien dan meningkatkan kesadaran serangan siber di kalangan pondok pesantren.

1.3. Tujuan dan Manfaat

Tujuan dari penelitian ini adalah untuk menganalisis hasil pengujian keamanan pada *website* Yayasan Pondok XYZ dengan menggunakan metode *OWASP Web Security Testing Guide*. Melalui pengujian ini, penelitian ini bertujuan untuk memberikan gambaran menyeluruh mengenai potensi kerentanannya dan upaya yang diperlukan untuk memperkuat sistem keamanan di platform digital tersebut.

Manfaat dari penelitian ini diharapkan dapat memberikan kontribusi penting, baik bagi pihak pesantren maupun bagi perkembangan keamanan siber di kalangan masyarakat secara umum. Hasil dari penelitian ini dapat digunakan

sebagai bahan pertimbangan untuk evaluasi dan perbaikan sistem keamanan data yang ada pada *website* tersebut. Dengan begitu, pesantren dapat lebih waspada terhadap ancaman penyusupan oleh pihak yang tidak bertanggung jawab, yang dapat merusak tampilan situs *website* atau bahkan menyebabkan kebocoran data sensitif. Selain itu, penelitian ini diharapkan dapat meningkatkan kesadaran dan pemahaman tentang pentingnya keamanan siber, khususnya di kalangan santri, pengajar, dan staf administrasi pesantren, agar mereka dapat lebih siap dalam menghadapi tantangan dunia digital yang semakin kompleks.

1.4. Batasan Masalah

Batasan dalam suatu masalah digunakan untuk menghindari adanya sebuah penyimpangan dan pelebaran dalam pokok masalah. Dalam penelitian ini dibatasi oleh beberapa hal berikut:

1. Penelitian pengujian keamanan dilakukan pada *website* Institusi Perguruan Tinggi dalam Yayasan Pondok XYZ.
2. Pengujian menggunakan tahapan dari *OWASP Web Security Testing Guide* dengan fokus pada beberapa area penting, yaitu: *Information Gathering, Testing for Reflected Cross Site Scripting, SQL Injection Testing, Testing for Clickjacking, dan Testing for Weak Lockout Mechanism,*
3. Seluruh tahapan pengujian dilakukan secara menyeluruh sesuai panduan *OWASP*, namun informasi sensitif dan hasil rinci terkait *website* tidak dipublikasikan demi menjaga kerahasiaan.
4. Rekomendasi diberikan berdasarkan temuan kerentanan sesuai dengan standar keamanan *OWASP* dan BSSN untuk meningkatkan tingkat keamanan *website*.

1.5. Metode Penelitian

Penelitian ini menggunakan pendekatan *security assessment* dengan mengacu pada standar *OWASP Web Security Testing Guide* untuk menguji keamanan *website* Yayasan XYZ. Proses pengujian dilakukan melalui tiga tahapan utama, yaitu:

1. *Information Gathering*

Tahap ini dilakukan dengan mengumpulkan informasi mengenai struktur dan konfigurasi *website*, teknologi yang digunakan, serta potensi titik lemah yang dapat menjadi sasaran serangan.

2. *Vulnerability Analysis*

Analisis kerentanan dilakukan untuk mengidentifikasi dan memetakan celah keamanan yang mungkin ada berdasarkan informasi yang telah dikumpulkan pada tahap sebelumnya.

3. *Exploitation*

Pada tahap ini, pengujian eksploitasi dilakukan menggunakan teknik-teknik pengujian keamanan yang tercantum dalam *OWASP Web Security Testing Guide*, meliputi:

a. *Testing for Reflected Cross Site Scripting (XSS)*
b. *SQL Injection Testing*
c. *Testing for Clickjacking*
d. *Testing for Weak Lockout Mechanism*