BAB I

PENDAHULUAN

1.1 LATAR BELAKANG

Perkembangan teknologi informasi dan komunikasi yang semakin pesat telah mendorong pemanfaatan website sebagai sarana utama dalam penyampaian informasi, layanan, serta komunikasi secara digital [1]. *Website* tidak hanya digunakan oleh perusahaan komersial, tetapi juga oleh organisasi, lembaga pendidikan, dan komunitas sebagai media publikasi dan interaksi dengan masyarakat luas. Kemudahan akses dan jangkauan yang luas menjadikan *website* sebagai aset penting yang harus dikelola dengan baik, terutama dari sisi keamanan sistem informasi [2].

Seiring dengan meningkatnya penggunaan website, ancaman terhadap keamanan sistem informasi juga semakin beragam dan kompleks [3]. Serangan *siber seperti SQL Injection, Cross-Site Scripting (XSS), Brute Force, Web Application Potentially Vulnerable to Clickjacking dan Common Directory* menjadi ancaman nyata yang dapat menyebabkan kebocoran data, perubahan informasi tanpa izin, hingga gangguan layanan [4]. Lemahnya sistem keamanan website dapat dimanfaatkan oleh pihak yang tidak bertanggung jawab untuk mengeksploitasi celah keamanan yang ada.

Salah satu aturan dasar dalam menentukan keamanan suatu sistem ada 3 yaitu *Confidentiality* (kerahasiaan) menjaga rahasia informasi dari orang-orang yang tidak berhak, *Integrity* (integritas) menjaga perubahan informasi dari

orang yang tidak berhak, dan *Availability* (ketersediaan) data harus dapat diakses dan dapat dipertanggungjawabkan [5]. Jika 3 faktor dasar dalam keamanan informasi itu tidak dapat terpenuhi maka suatu sistem dapat dikategorikan tidak aman dan rawan tersusupi oleh pihak yang tidak bertanggung jawab. Dalam mengatasi masalah ini salah satu langkah yang dapat ditempuh adalah dengan melakukan analisis terhadap sistem dan jaringan yang terdapat pada web.

Website almudaya.or.id merupakan website yang digunakan sebagai media informasi dan publikasi kegiatan organisasi. Sebagai website yang dapat diakses secara publik, almudaya.or.id berpotensi menjadi target serangan siber apabila tidak dilengkapi dengan sistem keamanan yang memadai. Hingga saat ini, belum diketahui secara pasti tingkat keamanan website tersebut terhadap berbagai jenis serangan, sehingga diperlukan suatu analisis untuk mengetahui potensi kerentanan yang ada pada sistem.

Salah satu metode yang dapat digunakan untuk mengevaluasi tingkat keamanan website adalah *penetration testing (pentest)* [6]. *Penetration testing* merupakan metode pengujian keamanan dengan cara mensimulasikan serangan yang biasa dilakukan oleh penyerang untuk menemukan celah keamanan pada sistem. Metode ini bertujuan untuk mengidentifikasi kerentanan, menilai tingkat risiko, serta memberikan rekomendasi perbaikan agar sistem menjadi lebih aman [7]. Agar pengujian dilakukan secara terstruktur dan sesuai standar internasional, diperlukan acuan klasifikasi kerentanan, salah satunya adalah *OWASP Top* 10 [8].

Selain itu, dalam penelitian ini pengujian keamanan dilakukan menggunakan pendekatan *black box penetration testing*. Pendekatan black box dipilih karena pengujian dilakukan tanpa akses terhadap kode sumber, database, maupun konfigurasi internal dari website yang diuji. Dengan metode ini, peneliti melakukan simulasi serangan dari sudut pandang pengguna eksternal atau pihak yang tidak memiliki hak akses terhadap sistem internal. Pendekatan tersebut dianggap relevan karena website almudaya.or.id merupakan website publik yang dapat diakses secara terbuka melalui internet, sehingga potensi serangan juga umumnya berasal dari pihak eksternal. Melalui pendekatan black box penetration testing, penelitian ini diharapkan mampu menggambarkan kondisi keamanan website secara lebih realistis berdasarkan perspektif serangan yang mungkin terjadi di lingkungan nyata [9].

Berdasarkan uraian tersebut, penelitian ini dilakukan untuk menganalisis keamanan website almudaya.or.id menggunakan metode *penetration testing*. Hasil penelitian diharapkan dapat memberikan gambaran mengenai tingkat keamanan website serta menjadi bahan evaluasi dan rekomendasi perbaikan guna meningkatkan keamanan sistem dan meminimalkan risiko serangan siber di masa mendatang. Oleh karena itu, penelitian ini diangkat dengan judul **"ANALISIS KEAMANAN *WEBSITE* ALMUDAYA.OR.ID BERBASIS *OWASP TOP* 10 MENGGUNAKAN METODE *PENETRATION TESTING*"**.

1.2 RUMUSAN MASALAH

Berdasarkan latar belakang yang telah diuraikan, maka rumusan masalah dalam penelitian ini adalah sebagai berikut:

1. Bagaimana tingkat keamanan website almudaya.or.id berdasarkan hasil pengujian menggunakan metode *penetration testing* ?
2. Jenis kerentanan keamanan apa saja yang terdapat pada website almudaya.or.id ?
3. Bagaimana tingkat risiko dari setiap kerentanan yang ditemukan pada website almudaya.or.id ?
4. Rekomendasi perbaikan apa yang dapat diberikan untuk meningkatkan keamanan website almudaya.or.id ?

1.3 BATASAN MASALAH

Agar penelitian ini lebih terarah dan tidak menyimpang dari tujuan yang ditetapkan, maka batasan masalah dalam penelitian ini adalah :

1. Objek penelitian hanya difokuskan pada website almudaya.or.id.
2. Pengujian terhadap web almudaya.or.id mengacu pada *Open Web Application Security Project (OWASP) Top* 10.
3. Penelitian ini tidak membahas seluruh sepuluh kategori kerentanan dalam *OWASP Top* 10, melainkan hanya memfokuskan pembahasan pada beberapa jenis kerentanan yang ditemukan untuk dianalisis secara lebih mendalam.

1.4 TUJUAN PENELITIAN

Adapun tujuan penelitian ini antara lain :

1. Menguji keamanan dari website almudaya.or.id yang bertujuan untuk menemukan kerentanan diwebsite tersebut.
2. Menganalisis kerentanan yang ditemukan berdasarkan standar internasional salah satunya adalah *OWASP* Top 10.
3. Memberikan rekomendasi perbaikan terhadap website almudaya.or.id.

1.5 MANFAAT PENELITIAN

Adapun manfaat penelitian ini antara lain :

1. Implementasi ilmu pengetahuan yang telah dipelajari terkait *cybersecurity.*
2. Mengetahui kerentanan yang terdapat dalam website almudaya.or.id.
3. Menyediakan laporan serta masukan untuk website almudaya.or.id untuk meningkatkan keamanan dimasa yang akan datang.

1.6 SISTEMATIKA PENULISAN

Untuk memberi gambaran umum mengenai keseluruhan penulisan ilmiah, dapat dilihat melalui sistematika penulisan yang meliputi:

BAB I : PENDAHULUAN

Bab ini berisi tentang latar belakang masalah yang menjadi dasar dilakukannya penelitian, perumusan masalah yang akan dikaji, batasan masalah untuk memperjelas ruang lingkup penelitian, tujuan penelitian, manfaat penelitian baik secara teoritis maupun praktis, serta sistematika penulisan yang

menjelaskan susunan dari isi penelitian.

BAB II : LANDASAN TEORI

Dalam bab landasan teori ini terdiri dari konsep-konsep teoritis yang digunakan sebagai dasar penelitian, meliputi konsep keamanan website, *penetration testing, OWASP Top* 10, dan jenis-jenis kerentanan aplikasi web.

BAB III: METODOLOGI PENELITIAN

Bab ini menjelaskan metode penelitian yang digunakan, meliputi jenis penelitian, tahapan penetration testing, penggunaan *OWASP Top* 10 sebagai acuan analisis kerentanan, *tools* pengujian keamanan yang digunakan, skema pengujian website, serta teknik analisis dan penilaian risiko keamanan sistem.

BAB IV : ANALISIS DAN PEMBAHASAN

Bab ini membahas hasil analisis keamanan website berdasarkan data yang diperoleh dari proses *penetration testing*. Analisis dilakukan terhadap jenis kerentanan yang ditemukan, tingkat risiko keamanan, serta pemetaan kerentanan berdasarkan *OWASP Top* 10. Selain itu, dilakukan pembahasan mengenai kontribusi konfigurasi sistem dan komponen website terhadap tingkat keamanan secara keseluruhan.

BAB V : PENUTUP

Bab ini berisi kesimpulan yang diperoleh dari seluruh rangkaian penelitian serta memberikan saran-saran perbaikan yang relevan untuk meningkatkan keamanan website. Saran yang diberikan ditujukan bagi pemilik atau pengelola website dalam upaya mitigasi resiko dan peningkatan keamanan ke depannya dan juga menjadi acuan untuk penelitian selanjutnya.