

BAB I

PENDAHULUAN

1.1 LATAR BELAKANG

Perkembangan teknologi informasi dan komunikasi telah mendorong perusahaan untuk memanfaatkan website sebagai media utama dalam penyampaian informasi, layanan, dan aktivitas bisnis [1]. Website tidak hanya berfungsi sebagai sarana promosi, tetapi juga sebagai sistem yang menyimpan dan mengelola data penting perusahaan [2]. Seiring dengan meningkatnya ketergantungan terhadap website, risiko terhadap ancaman keamanan siber juga semakin meningkat, seperti pencurian data, perusakan sistem, dan penyalahgunaan akses oleh pihak yang tidak bertanggung jawab [3].

Karkoon Group Asia sebagai sebuah perusahaan yang memanfaatkan website untuk mendukung aktivitas bisnisnya memiliki potensi risiko terhadap berbagai ancaman keamanan siber. Serangan terhadap website, seperti pencurian data, perusakan sistem, maupun penyalahgunaan akses, dapat menimbulkan kerugian baik dari segi finansial, reputasi, maupun kepercayaan pengguna. Ancaman ini semakin meningkat seiring dengan berkembangnya teknik dan metode serangan yang dilakukan oleh pihak tidak bertanggung jawab [4].

Salah satu upaya yang dapat dilakukan untuk mengetahui dan meminimalkan celah keamanan pada website adalah dengan melakukan *penetration testing* [5]. *Penetration testing* merupakan metode pengujian keamanan yang dilakukan dengan mensimulasikan serangan terhadap sistem untuk mengidentifikasi kelemahan yang

berpotensi dieksploitasi oleh penyerang. Metode ini membantu pengelola sistem dalam memahami tingkat keamanan website secara nyata dan menyeluruh [6].

Dalam pelaksanaannya, *penetration testing* perlu mengacu pada standar yang diakui secara luas agar hasil pengujian lebih terstruktur dan dapat dipertanggungjawabkan [7]. OWASP Top 10 merupakan salah satu standar internasional yang berisi daftar sepuluh kerentanan keamanan aplikasi web paling kritis dan sering terjadi [8]. Standar ini banyak digunakan sebagai acuan dalam analisis dan pengujian keamanan website karena relevan dan selalu diperbarui mengikuti perkembangan ancaman keamanan [9].

Berdasarkan permasalahan tersebut, penelitian ini bertujuan untuk menganalisis tingkat keamanan website Karkoon Group Asia menggunakan metode *penetration testing* berdasarkan OWASP Top 10. Hasil dari penelitian ini diharapkan dapat mengidentifikasi potensi kerentanan yang terdapat pada website serta memberikan rekomendasi perbaikan guna meningkatkan keamanan sistem dan melindungi data serta layanan yang disediakan. Dengan demikian, penelitian ini diangkat dengan judul **“ANALISIS KEAMANAN WEBSITE KARKOON GROUP ASIA MENGGUNAKAN METODE *PENETRATION TESTING* BERDASARKAN OWASP TOP 10.”**

1.2 RUMUSAN MASALAH

Berdasarkan latar belakang tersebut, rumusan masalah dalam penelitian ini adalah:

1. Bagaimana tingkat keamanan website Karkoon Group Asia berdasarkan hasil pengujian menggunakan metode *penetration testing*?
2. Kerentanan apa saja yang terdapat pada website Karkoon Group Asia berdasarkan standar OWASP Top 10?
3. Rekomendasi perbaikan apa yang dapat diberikan untuk meningkatkan keamanan website Karkoon Group Asia berdasarkan hasil *penetration testing* dan OWASP Top 10?

1.3 BATASAN MASALAH

Untuk menghindari terjadinya pembahasan di luar dari topik dan agar tidak menyimpang dari permasalahan maka batasan permasalahannya sebagai berikut:

1. Penelitian ini hanya membahas keamanan website Karkoon Group Asia dari sisi aplikasi web. Penelitian ini tidak membahas aspek keamanan jaringan, server fisik, maupun kebijakan internal organisasi.
2. Metode pengujian keamanan yang digunakan adalah *penetration testing* dengan acuan standar OWASP Top 10 menggunakan tools Arachni.
3. *Proof of Concept* (PoC) dilakukan secara terbatas, yaitu hanya satu kerentanan yang mewakili masing-masing tingkat severity, dengan tujuan pembuktian risiko tanpa mengeksploitasi seluruh temuan secara menyeluruh.

1.4 TUJUAN PENELITIAN

Tujuan dari penelitian ini adalah sebagai berikut:

1. Menganalisis tingkat keamanan website Karkoon Group Asia menggunakan metode *penetration testing* berdasarkan standar OWASP Top 10.
2. Mengidentifikasi jenis kerentanan pada website Karkoon Group Asia yang termasuk dalam kategori OWASP Top 10.
3. Memberikan rekomendasi perbaikan untuk meningkatkan keamanan website Karkoon Group Asia.

1.5 MANFAAT PENELITIAN

Manfaat yang diharapkan dari penelitian ini adalah sebagai berikut:

1. Memberikan gambaran tingkat keamanan website Karkoon Group Asia berdasarkan *penetration testing* mengacu pada OWASP Top 10.
2. Menjadi dasar rekomendasi perbaikan untuk meningkatkan keamanan website Karkoon Group Asia.
3. Menambah referensi akademis di bidang keamanan aplikasi web dan *penetration testing*.

1.6 SISTEMATIKA PENULISAN

Untuk mempermudah dalam memahami isi laporan tugas akhir ini, penulis menyusun sistematika penulisan sebagai berikut:

BAB I : PENDAHULUAN

Dalam bab ini berisi penjelasan mengenai latar belakang masalah, rumusan masalah, batasan masalah, tujuan dan manfaat penelitian, serta sistematika penulisan.

BAB II : LANDASAN TEORI

Bab ini membahas teori-teori yang relevan dengan penelitian, yang diperoleh dari buku, jurnal ilmiah, standar keamanan, dan referensi lainnya. Pembahasan meliputi konsep dasar keamanan website, *penetration testing*, *information gathering*, *vulnerability scanning*, *vulnerability analysis*, OWASP Top 10, serta jenis-jenis kerentanan yang umum ditemukan pada aplikasi web.

BAB III : METODOLOGI PENELITIAN

Bab ini menjelaskan metode dan pendekatan penelitian yang digunakan, objek penelitian, serta tahapan penelitian yang mengacu pada alur kerja *penetration testing*. Tahapan tersebut meliputi proses pengumpulan informasi (*Information Gathering*), pemindaian kerentanan (*Vulnerability Scanning*), analisis kerentanan (*Vulnerability Analysis*), pembuktian kerentanan melalui *Proof of Concept* (PoC), hingga penyusunan laporan hasil pengujian. Selain itu, bab ini juga menjelaskan tools yang digunakan serta acuan standar keamanan OWASP Top 10.

BAB IV : ANALISIS DAN PEMBAHASAN

Bab ini menyajikan hasil pelaksanaan setiap tahapan penelitian. Pembahasan dimulai dari hasil pengumpulan informasi terhadap website Karkoon Group Asia, hasil pemindaian kerentanan, analisis jenis dan karakteristik kerentanan berdasarkan OWASP Top 10, pembuktian kerentanan melalui *Proof of Concept* (PoC), analisis perbandingan *vulnerability scanning* dan PoC serta rekomendasi perbaikan dari kerentanan yang ditemukan.

BAB V : PENUTUP

Bab ini berisi kesimpulan yang diperoleh dari hasil penelitian serta saran untuk meningkatkan keamanan website Karkoon Group Asia.