BAB I
PENDAHULUAN

1.1. Latar Belakang

Era digitalisasi yang kita alami saat ini menghadirkan perubahan transformasional yang mencakup segala aspek kehidupan, terutama di dunia bisnis. Inovasi teknologi tidak hanya menjadi pendorong perkembangan, tetapi juga menjadi hal utama yang mampu mempercepat setiap proses (Putriana, 2023), meningkatkan efisiensi operasional, dan memperbesar peluang baru yang belum pernah terjadi sebelumnya. Dalam paradigma bisnis modern, kehadiran teknologi menjadi kunci utama untuk menjawab tuntutan zaman. Transformasi digital bukan sekadar opsi, tetapi suatu keharusan agar bisnis dapat beradaptasi, bertahan, dan bahkan unggul di tengah dinamika pasar yang semakin kompleks.

Digital marketing adalah strategi pemasaran yang memanfaatkan kemajuan teknologi digital untuk memasarkan produk dan jasa secara *online*. Salah satu teknik populernya adalah *e-commerce,* model penjualan produk dan jasa secara *online* melalui *website* perusahaan, *email*, atau media sosial.

Di era transformasi digital yang pesat, aplikasi berbasis *website* telah menjadi tulang punggung berbagai aktivitas, mulai dari bisnis, pemerintahan, hingga layanan publik. Kemudahan akses dan skalabilitas yang ditawarkan oleh *platform website* telah mendorong adopsi yang meluas. Namun, pertumbuhan aplikasi berbasis *website* juga diiringi dengan peningkatan risiko keamanan. Serangan *cyber* seperti *Sql Injection*, *Cross-site scripting* (*XSS*), dan serangan *brute force* menjadi ancaman serius yang dapat mengakibatkan kerugian finansial, kebocoran data sensitif, dan kerusakan reputasi.

Kompleksitas arsitektur aplikasi *website* modern, yang seringkali melibatkan integrasi dengan berbagai layanan pihak ketiga dan penggunaan kerangka kerja perangkat lunak yang beragam, semakin memperluas permukaan serangan. Celah keamanan yang tidak terdeteksi atau tidak ditangani dengan tepat dapat dieksploitasi oleh pelaku kejahatan *cyber* (Hoshmand dkk., 2023). Oleh karena itu, analisis keamanan aplikasi berbasis *web* menjadi kebutuhan krusial untuk memastikan integritas, kerahasiaan, dan ketersediaan layanan.

Pada penelitian berjudul "Analisa Celah Keamanan Pada *Website* Pemerintah Kabupaten Kediri Menggunakan Metode *Penetration Testing* Melalui *Kali Linux*" (Firda dkk., 2023). Hasil pengujian penetrasi pada *website* Pemerintah Kabupaten Kediri menemukan beberapa *port* ditemukan beberapa *port* terbuka yang memiliki akses 200. Kemudian setelah dilakukan *attacking* untuk masuk ke *directory environment* ditemukan *Exposure of Sensitive Information* (*DBCredentials*) *to Unauthorized Actor* yang memungkinkan untuk mengekspos data *sensitive* berupa *username* dan *password* yang bisa digunakan untuk akses *login* ke halaman *cpanel* admin.

Salah satu metode yang efektif untuk mengidentifikasi dan mengevaluasi celah keamanan dalam aplikasi berbasis *website* adalah *penetration testing* (*pentest*). *Penetration testing* melibatkan simulasi serangan dunia nyata oleh profesional keamanan yang terlatih untuk mengungkap kerentanan yang mungkin terlewatkan dalam proses pengembangan atau pengujian biasa. Dengan melakukan *pentest* secara berkala, organisasi dapat memperoleh pemahaman yang lebih mendalam tentang risiko keamanan yang mereka hadapi, serta mengambil langkah-langkah proaktif untuk memperkuat pertahanan aplikasi mereka.

Penelitian ini bertujuan untuk menganalisis keamanan aplikasi berbasis *website* menggunakan metode *penetration testing*. Dengan mengidentifikasi kerentanan yang ada dan memberikan rekomendasi perbaikan, penelitian ini diharapkan dapat berkontribusi dalam meningkatkan keamanan aplikasi berbasis *website*, melindungi data pengguna, dan menjaga kepercayaan terhadap layanan digital.

1.2. Rumusan masalah

Adapun rumusan masalah dari penelitian ini adalah sebagai berikut:

1. Bagaimana tingkat keamanan aplikasi *e-commerce* Assakinahmart terhadap berbagai jenis serangan *cyber* ?
2. Kerentanan apa saja yang dapat diidentifikasi dalam aplikasi *e-commerce* Assakinah melalui metode *penetration testing* ?
3. Seberapa efektif metode *penetration testing* dalam mengungkap kelemahan keamanan pada aplikasi *e-commerce* Assakinahmart ?

1.3. Tujuan Penelitian

Adapun rumusan masalah dari penelitian ini adalah sebagai berikut:

1. Mengidentifikasi kerentanan keamanan dalam aplikasi *e-commerce* Assakinahmart melalui metode *penetration* testing.
2. Menilai tingkat risiko dari kerentanan yang ditemukan selama proses *penetration testing*.
3. Tujuan utama untuk memberikan rekomendasi perbaikan berdasarkan hasil *penetration testing* untuk meningkatkan keamanan aplikasi berbasis *website*.

1.4. Batasan Penelitian

Adapun batasan dari penelitian ini adalah sebagai berikut:

1. Penelitian ini hanya mencakup aplikasi Assakinahmart sebagai sampel studi kasus.
2. Hanya kerentanan yang diidentifikasi dan dieksploitasi selama pengujian yang akan dianalisis, tidak termasuk kerentanan yang memerlukan *patch* atau pembaruan dari vendor.
3. Hanya *e-commerce* As-sakinahmart saja yang diuji.
4. Penelitian ini hanya memfokuskan 3 pada beberapa kerentanan umum yang tercantum dalam *OWASP TOP* 10-2021, *Injection*,*Security Misconfiguration* dan *Broken Access Control*.

1.5. Manfaat Penelitian

Adapun manfaat dari penelitian ini sebagai berikut:

1. Meningkatkan kesadaran tentang pentingnya keamanan aplikasi *website* dan potensi risiko yang dapat dihadapi.
2. Menyediakan data dan analisis yang bisa digunakan untuk mengembangkan standar keamanan aplikasi *e-commerce* yang lebih baik.