BAB I
PENDAHULUAN

1.1 Latar Belakang

E-commerce atau perdagangan elektronik adalah gabungan dari teknologi, aplikasi, dan kegiatan bisnis yang memungkinkan perusahaan maupun individu sebagai konsumen untuk melakukan transaksi secara digital. Transaksi ini meliputi jual beli barang serta pertukaran informasi yang dilakukan melalui internet, televisi interaktif, situs web (WWW), atau berbagai jaringan komputer lainnya [1]. *E-commerce* menjadi semakin rentan terhadap berbagai ancaman *cyber*, termasuk pencurian data, penipuan transaksi, dan serangan *malware*. *Platform* seperti Shopee, Tiktok *Shop* dan Facebook *Marketplace* menjadi target utama bagi penjahat *cyber*, karena menangani *volume* transaksi begitu besar. Oleh karena itu, penting untuk memiliki sistem keamanan yang kuat dan terus diperbarui untuk menghadapi ancaman-ancaman ini [2].

Penelitian terdahulu mengenai penerapan *Dynamic Application Security Testing (DAST)* pada aplikasi berbasis Android menunjukkan bahwa metode DAST mampu mengidentifikasi celah keamanan (*vulnerability*) yang tidak terdeteksi oleh SAST. DAST dapat secara otomatis melakukan pengujian terhadap setiap *activity* dalam aplikasi, yang dibuktikan dengan ditemukannya kerentanan pada *activity Insecure Data Storage*, termasuk celah keamanan seperti XSS dan *Database Breach*. Adapun penelitian lain, yaitu Pemindaian Aplikasi Web Otomatis dengan Wapiti, Selenium, dan SQLMap menunjukkan hasil bahwa Alat Wapiti merupakan pilihan optimal untuk otomatisasi awal proses pemindaian aplikasi web karena akurasinya yang tinggi dalam mendeteksi berbagai kerentanan dan laporan komprehensif serta rekomendasi perbaikan yang dihasilkannya.

Metode ***Dynamic Application Security Testing*** **(DAST)** merupakan salah satu pendekatan yang dapat digunakan untuk menganalisis celah keamanan pada aplikasi web. Dengan fokus pada Shopee, Tiktok *Shop* dan Facebook *Marketplace* untuk pengujian celah keamanan terhadap ancaman, peneliti baru menetapkan judul "Analisis Perbandingan Keamanan Aplikasi Web pada *Platform E-commerce*: Studi Kasus Shopee, TikTok *Shop*, dan Facebook *Marketplace* Menggunakan *Dynamic Application Security Testing* (DAST)" dan memperdalam cakupan

penelitian sebelumnya dengan menyoroti *platform e-commerce* yang lebih spesifik. Dengan metode pengumpulan data kualitatif (Studi Kasus: *Website* Shopee, Tiktok *Shop* dan Facebook *Marketplace*), penelitian ini diharapkan dapat memanfaatkan hasil temuan studi sebelumnya untuk melakukan analisis lebih mendalam dan spesifik terhadap celah keamanan di Shopee, Tiktok *Shop* dan Facebook *Marketplace*. Peneliti berharap ketiga *platform* tersebut *c*ukup aman terhadap ancaman *cyber*, mengingat fitur transaksi dan data pribadi pengguna yang merupakan isu kritis dalam konteks keamanan *cyber* saat ini [3].

1.2 Rumusan Masalah

1. Apa saja jenis kerentanan keamanan yang terdeteksi pada aplikasi web Shopee, Tiktok *Shop* Dan Facebook *Marketplace*?
2. Bagaimana hasil perbandingan keamanan dari *platform* shopee, Tiktok *Shop*, dan Facebook *Marketplace*?
3. Bagaimana kinerja metode DAST dalam mengidentifikasi dan mengevaluasi celah keamanan yang berpotensi terhadap serangan pada ketiga *platform* tersebut?
4. Langkah-langkah apa yang dapat direkomendasikan untuk memperkuat sistem keamanan guna mengurangi risiko serangan?

1.3 Tujuan Penelitan

Penelitian ini bertujuan untuk:

1. Menganalisis kerentanan dan menemukan celah keamanan pada *website* Shopee, Tiktok *Shop*, dan Facebook *Marketplace*
2. Menganalisis perbandingan keamanan dari *platform* Shopee, Tiktok *Shop*, dan Facebook *Marketplace*
3. Mengetahui kemampuan metode DAST dalam mendeteksi dan mengevaluasi celah keamanan terhadap ancaman
4. Memberikan langkah-langkah rekomendasi upaya perbaikan keamanan untuk memperkuat sistem dan meminimalisir risiko serangan

1.4 Batasan Penelitian

1. Penelitian ini hanya berfokus pada analisis celah keamanan dan perbandingandari *website* Shopee, Tiktok *Shop*, dan Facebook *Marketplace*
2. Metode DAST yang digunakan adalah *Vulnerability Scanning*, dan pelaporan hasil
3. Alat pengujian yang digunakan adalah Wapiti

1.5 Manfaat Penelitian

Penelitian ini memiliki beberapa manfaat bagi berbagai pihak yang terlibat, antara lain:

1. Bagi Pengembang Aplikasi:

   Memberikan pengetahuan yang lebih mendalam tentang celah keamanan yang ada dalam aplikasi web dan solusi perbaikannya. Membantu pengembang dalam memperkuat perlindungan pada potensi celah yang ditemukan melalui pengujian DAST
2. Bagi Pengguna:

   Meningkatkan keamanan data pribadi pengguna dengan mengurangi risiko kebocoran data akibat serangan atau gangguan. Meningkatkan kepercayaan pengguna terhadap *platform* seperti Shopee, Tiktok *Shop*, dan Facebook *Marketplace*.
3. Bagi Perusahaan:

   Menurunkan risiko kerugian finansial akibat serangan yang dapat merusak reputasi atau mengganggu operasional perusahaan.
4. Bagi Peneliti:

   Memberikan pengetahuan tambahan mengenai teknik pengujian dinamis (DAST) dan bagaimana metode ini dapat diterapkan untuk mendeteksi kerentanannya dalam konteks aplikasi web besar. Menjadi referensi untuk pengembangan metodologi baru dalam pengujian aplikasi berbasis web dari sudut pandang keamanan teknis.