BAB I
PENDAHULUAN

1.1 Latar Belakang

Perkembangan layanan berbasis web menjadikan formulir registrasi sebagai gerbang utama pembentukan identitas digital pengguna. Namun, kemajuan teknologi otomatisasi telah melahirkan bot pendaftaran akun yang mampu melakukan pembuatan akun massal, penyalahgunaan layanan, manipulasi data, serta pelanggaran kebijakan sistem dalam skala besar. Penelitian [1] menunjukkan bahwa serangan bot dan spam secara langsung merusak integritas data dan melemahkan proses verifikasi karena mekanisme yang ada belum mampu membedakan aktivitas manusia dan bot secara konsisten. Selanjutnya, [2] mengungkap bahwa ekosistem bot pendaftaran akun telah berkembang menjadi sistem terorganisasi yang mampu menembus berbagai mekanisme pengamanan seperti CAPTCHA, verifikasi SMS, dan pembatasan alamat IP.

Dari sisi mekanisme pertahanan, penelitian [4] menyatakan bahwa sebagian besar skema CAPTCHA konvensional telah berhasil dilewati oleh teknik kecerdasan buatan dan kelemahan desain. Penelitian [5] membuktikan bahwa sistem hCaptcha dapat dibypass dengan tingkat keberhasilan tinggi menggunakan sumber daya komputasi yang relatif rendah. Pada aspek identitas pengguna, [7] menunjukkan bahwa email sementara banyak dimanfaatkan dalam pembuatan akun palsu dan sulit dideteksi apabila sistem hanya mengandalkan validasi format. Sementara itu, pada lapisan layanan, penelitian [9] dan [10] menegaskan bahwa API tanpa autentikasi kuat dan tanpa mekanisme rate limiting sangat rentan terhadap penyalahgunaan otomatis dalam skala besar.

Meskipun berbagai penelitian tersebut telah membahas bypass CAPTCHA, penyalahgunaan email sementara, serta kelemahan API dan rate limiting, belum terdapat penelitian yang secara khusus menganalisis kerentanan

form registrasi akun secara komprehensif dan membandingkannya antara sistem simulatif dan sistem produksi dalam satu kerangka evaluasi risiko yang terstruktur. Sebagian besar studi terdahulu masih bersifat parsial, berfokus pada satu mekanisme keamanan, serta menggunakan pendekatan deskriptif atau persentase keberhasilan serangan [4], [5], [7], tanpa melakukan pemetaan tingkat risiko yang mempertimbangkan keterkaitan antara kemungkinan eksploitasi dan dampaknya terhadap sistem. Kondisi ini menunjukkan adanya research gap berupa ketiadaan analisis risiko terintegrasi yang mampu menggambarkan tingkat kerentanan form registrasi secara menyeluruh, terukur, dan komparatif.

Sebagai respons terhadap keterbatasan tersebut, penelitian ini memiliki perbedaan mendasar dibandingkan studi terdahulu yang umumnya berfokus pada deteksi multi-vulnerability aplikasi web, seperti *SQL Injection, XSS, RCE,* dan *fingerprinting backend*, [8] maupun penelitian yang menelaah dampak aktivitas bot pada survei daring *(online survey)* [1] tanpa pemetaan risiko keamanan form registrasi secara spesifik. Berbeda dengan pendekatan tersebut, penelitian ini secara khusus memusatkan perhatian pada kerentanan form registrasi web terhadap serangan bot otomatisasi serta melakukan komparasi tingkat risiko pada dua lingkungan berbeda menggunakan metode *OWASP Risk Rating*. Pendekatan ini menegaskan kontribusi utama penelitian, yaitu penyajian analisis komparatif berbasis risiko dalam konteks serangan otomatisasi pada form registrasi, bukan sekadar pemetaan kerentanan aplikasi web secara umum atau analisis gangguan bot pada survei daring.

Urgensi penelitian ini muncul dari meningkatnya intensitas dan kecanggihan serangan bot otomatisasi pada sistem registrasi web, sementara pengelola sistem belum memiliki dasar evaluatif yang sistematis untuk menentukan mekanisme keamanan mana yang paling lemah dan paling prioritas untuk diperkuat [3]. Tanpa pemetaan kerentanan berbasis risiko, strategi pengamanan cenderung bersifat parsial, reaktif, dan tidak berorientasi pada prioritas mitigasi, sehingga kurang efektif dalam menghadapi pola serangan

otomatis yang semakin terorganisasi.

Untuk menjawab celah tersebut, penelitian ini menggunakan metode *OWASP Risk Rating* sebagai kerangka evaluasi kualitatif dengan menentukan parameter likelihood dan impact guna menghitung tingkat risiko setiap kerentanan. Pendekatan ini memungkinkan pemetaan kerentanan secara sistematis serta penentuan prioritas mitigasi yang objektif. Dibandingkan pendekatan deskriptif, *OWASP Risk Rating* lebih unggul karena konsisten antar-parameter dan mampu mengonversi temuan kerentanan menjadi skor risiko numerik yang terukur, sehingga mendukung pengambilan keputusan berbasis tingkat keparahan dan potensi dampak.

Novelty (kebaruan) penelitian ini terletak pada penerapan kerangka OWASP Risk Rating sebagai alat analisis kualitatif untuk membandingkan kerentanan form registrasi pada dua lingkungan berbeda, yaitu sistem simulatif dan sistem produksi, dengan fokus pada empat parameter inti: CAPTCHA, validasi email, keamanan API endpoint, dan rate limiting. Berbeda dari penelitian terdahulu yang menelaah mekanisme keamanan secara terpisah, penelitian ini menyajikan pemetaan risiko terstruktur berbasis likelihood dan impact yang menghasilkan klasifikasi tingkat risiko serta prioritas mitigasi secara komparatif dan terintegrasi dalam satu kerangka evaluasi yang konsisten.

1.2 Rumusan Masalah

1. Bagaimana tingkat risiko kerentanan form registrasi web terhadap serangan bot otomatisasi berdasarkan OWASP Risk Rating?
2. Bagaimana hasil perbandingan risiko antara OWASP Juice Shop dan id.hm.com serta rekomendasi mitigasi yang dapat diusulkan?

1.3 Batasan Masalah

1. Penelitian hanya difokuskan pada form registrasi akun pada dua objek, yaitu OWASP Juice Shop dan id.hm.com.
2. Pengumpulan data dilakukan secara observasi non-invasif melalui Inspect Element dan tab Network tanpa eksploitasi aktif.

3. Fokus hanya pada elemen form registrasi, tidak termasuk fitur lain seperti login atau reset password, kecuali terkait langsung.
4. Evaluasi risiko menggunakan metode OWASP Risk Rating dan rekomendasi mitigasi disusun secara konseptual tanpa implementasi langsung.

1.4 Tujuan Penelitian

1. Menganalisis kerentanan form registrasi terhadap serangan bot pada dua objek penelitian menggunakan OWASP Risk Rating.
2. Membandingkan hasil evaluasi risiko kedua objek penelitian
3. menyusun rekomendasi mitigasi untuk meningkatkan keamanan form registrasi web.

1.5 Manfaat Penelitian

1. Memberikan gambaran tingkat kerentanan form registrasi terhadap serangan bot berdasarkan evaluasi risiko.
2. Menyediakan perbandingan pola dan tingkat risiko keamanan antara sistem simulatif dan situs web publik.
3. Memberikan acuan bagi pengembang dalam merancang mekanisme registrasi yang lebih aman.

1.6 Sistematika Penulisan

Sistematika penulisan skripsi ini terdiri dari lima bab utama, yaitu:

1. BAB I PENDAHULUAN
   Berisi latar belakang, rumusan masalah, tujuan, manfaat, batasan masalah, dan sistematika penulisan.
2. BAB II TINJAUAN PUSTAKA
   Berisi studi literatur, tabel keaslian penelitian, dan dasar teori.
3. BAB III METODE PENELITIAN
   Menjelaskan metode penelitian, objek penelitian, alur penelitian, teknik pengumpulan data, serta alat dan bahan yang digunakan.

4. BAB IV HASIL DAN PEMBAHASAN

   Menampilkan hasil observasi dan analisis kerentanan formulir registrasi, serta pembahasan mengenai strategi mitigasi.

5. BAB V PENUTUP

   Berisi kesimpulan dari penelitian dan saran untuk pengembangan selanjutnya.