BAB V
PENUTUP

5.7 Kesimpulan

Berdasarkan hasil penelitian mengenai analisis kerentanan form registrasi web terhadap serangan bot otomatisasi pada OWASP Juice Shop dan id.hm.com menggunakan metode OWASP Risk Rating, diperoleh beberapa kesimpulan sebagai berikut.

1. Kedua objek penelitian memiliki tingkat kerentanan tinggi terhadap serangan bot otomatisasi. Seluruh parameter keamanan yang diuji—ketiadaan CAPTCHA, lemahnya validasi email, API endpoint yang terbuka, dan tidak adanya mekanisme rate limiting—menunjukkan nilai Likelihood dan Impact sebesar 3, sehingga menghasilkan skor risiko 9 (risiko tinggi). Kondisi ini menunjukkan bahwa kedua sistem tidak memiliki kontrol proteksi dasar untuk mencegah pendaftaran otomatis.

2. OWASP Juice Shop dan id.hm.com memiliki pola kerentanan yang serupa, meskipun berasal dari dua konteks berbeda (simulatif dan sistem produksi). Juice Shop menampilkan kelemahan bawaan sebagai aplikasi latihan keamanan, sementara id.hm.com menunjukkan kelemahan nyata pada proses registrasi yang tetap memproses input tanpa verifikasi manusia maupun pembatasan permintaan. Kedua objek memungkinkan bot mengirim request secara cepat, berulang, dan dalam jumlah besar.

3. Form registrasi id.hm.com terbukti tidak memiliki kontrol adaptif, seperti CAPTCHA, reputasi email, pemblokiran domain disposable, autentikasi API, maupun rate limiting. Hal ini memungkinkan terbentuknya akun palsu yang dapat berdampak pada operasional sistem, seperti penyalahgunaan program loyalti, analitik pelanggan, maupun beban server akibat request

otomatis.

4. Evaluasi risiko melalui OWASP Risk Rating memberikan gambaran objektif mengenai tingkat ancaman pada kedua sistem. Dengan seluruh parameter berada pada kategori risiko tinggi, maka penelitian memastikan bahwa serangan otomatisasi dapat dilakukan dengan tingkat keberhasilan yang signifikan, terutama pada sistem tanpa mekanisme verifikasi tambahan.

5. Rekomendasi mitigasi diperlukan untuk meningkatkan keamanan registrasi, terutama pada aspek verifikasi pengguna, pengamanan API endpoint, validasi email, dan pembatasan permintaan. Temuan ini menunjukkan bahwa pencapaian keamanan yang memadai memerlukan pendekatan multi-lapis, bukan hanya mengandalkan validasi dasar atau pemeriksaan format input.

5.8 Saran

Berdasarkan temuan dan analisis yang dilakukan, beberapa saran yang dapat diberikan untuk pengembangan sistem maupun penelitian selanjutnya adalah sebagai berikut.

1. Penerapan CAPTCHA atau challenge-based verification

   Sistem registrasi perlu dilengkapi dengan CAPTCHA modern (behavior-based atau adaptive CAPTCHA) untuk menghambat otomatisasi. Mekanisme tradisional seperti gambar statis sebaiknya diberi pembaruan karena telah terbukti mudah dilewati oleh bot modern.

2. Memperkuat validasi email

   Sistem sebaiknya menerapkan filter domain disposable email, pemeriksaan MX record, serta verifikasi email melalui tautan (email verification). Pendekatan berbasis machine learning juga dapat dipertimbangkan untuk membedakan email asli dan sementara.

3. Penerapan autentikasi API dan pembatasan akses

   Endpoint registrasi harus dilindungi dengan token-based authentication (misalnya JWT atau OAuth2) serta input sanitization pada sisi server. Hal ini mencegah bot melakukan panggilan langsung ke endpoint tanpa melewati antarmuka yang sah.

4. Implementasi mekanisme rate limiting adaptif

   Penerapan algoritma seperti Sliding Window atau Token Bucket dapat mengurangi risiko request berulang dalam waktu singkat. Pendekatan adaptif berbasis beban server akan lebih efektif dalam menahan serangan otomatisasi.

5. Pengembangan sistem monitoring aktivitas

   Sistem perlu dipadukan dengan analitik perilaku (behavior analysis) untuk mengidentifikasi pola interaksi abnormal seperti kecepatan pengisian form, frekuensi request, atau pola IP yang mencurigakan.

6. Penelitian lanjutan dapat memperluas cakupan objek dan metode

   Penelitian selanjutnya dapat menguji:

   - lebih banyak situs produksi,
   - efektivitas CAPTCHA tertentu,
   - perbandingan mekanisme rate limiting,
   - atau model deteksi bot berbasis machine learning untuk interaksi

7. Implementasi mitigasi secara bertahap

   Mengingat beberapa kontrol memerlukan integrasi teknis yang kompleks, pengembang dapat memulai dari mekanisme dasar seperti validasi email dan rate limiting, sebelum menerapkan sistem autentikasi API dan CAPTCHA adaptif.