KOMPARASI KERENTANAN FORM REGISTRASI WEB TERHADAP SERANGAN BOT OTOMATISASI MENGGUNAKAN METODE OWASP RISK RATING

SKRIPSI

untuk memenuhi salah satu syarat mencapai derajat Sarjana

Program Studi Teknik Komputer

disusun oleh

ALAN BAYU EKA SATRIA

21.83.0648

Kepada

FAKULTAS ILMU KOMPUTER

UNIVERSITAS AMIKOM YOGYAKARTA

YOGYAKARTA

2026

KOMPARASI KERENTANAN FORM REGISTRASI WEB TERHADAP SERANGAN BOT OTOMATISASI MENGGUNAKAN METODE OWASP RISK RATING

SKRIPSI

untuk memenuhi salah satu syarat mencapai derajat Sarjana

Program Studi Teknik Komputer

disusun oleh

ALAN BAYU EKA SATRIA

21.83.0648

Kepada

FAKULTAS ILMU KOMPUTER

UNIVERSITAS AMIKOM YOGYAKARTA

YOGYAKARTA

2026

HALAMAN PERSETUJUAN

SKRIPSI

KOMPARASI KERENTANAN FORM REGISTRASI WEB TERHADAP SERANGAN BOT OTOMATISASI MENGGUNAKAN METODE OWASP RISK RATING

yang disusun dan diajukan oleh

Alan Bayu Eka Satria

21.83.0648

telah disetujui oleh Dosen Pembimbing Skripsi
pada tanggal 20 Februari 2026

Dosen Pembimbing,

Rina Pramitasari, S.Si., M.Cs
NIK. 190302335

HALAMAN PENGESAHAN

SKRIPSI

KOMPARASI KERENTANAN FORM REGISTRASI WEB TERHADAP SERANGAN BOT OTOMATISASI MENGGUNAKAN METODE OWASP RISK RATING

yang disusun dan diajukan oleh

Alan Bayu Eka Satria

21.83.0648

Telah dipertahankan di depan Dewan Penguji
pada tanggal 20 Februari 2026

Susunan Dewan Penguji

Nama Penguji	Tanda Tangan
Joko Dwi Santoso, S.Kom., M.Kom. **NIK. 190302181**	
Senie Destya S.T., M.Kom. **NIK. 190302312**	
Jeki Kuswanto S.Kom., M.Kom. **NIK. 190302456**	

Skripsi ini telah diterima sebagai salah satu persyaratan
untuk memperoleh gelar Sarjana Komputer
Tanggal 20 Februari 2026

DEKAN FAKULTAS ILMU KOMPUTER

Prof. Dr. Kusrini, M.Kom.
NIK. 190302106

HALAMAN PERNYATAAN KEASLIAN SKRIPSI

Yang bertandatangan di bawah ini,

Nama mahasiswa : ALAN BAYU EKA SATRIA
NIM : 21.83.0648

Menyatakan bahwa Skripsi dengan judul berikut:

KOMPARASI KERENTANAN FORM REGISTRASI WEB TERHADAP SERANGAN BOT OTOMATISASI MENGGUNAKAN METODE OWASP RISK RATING

Dosen Pembimbing : Rina Pramitasari, S.Si., M.Cs.

1. Karya tulis ini adalah benar-benar ASLI dan BELUM PERNAH diajukan untuk mendapatkan gelar akademik, baik di Universitas AMIKOM Yogyakarta maupun di Perguruan Tinggi lainnya.
2. Karya tulis ini merupakan gagasan, rumusan dan penelitian SAYA sendiri, tanpa bantuan pihak lain kecuali arahan dari Dosen Pembimbing.
3. Dalam karya tulis ini tidak terdapat karya atau pendapat orang lain, kecuali secara tertulis dengan jelas dicantumkan sebagai acuan dalam naskah dengan disebutkan nama pengarang dan disebutkan dalam Daftar Pustaka pada karya tulis ini.
4. Perangkat lunak yang digunakan dalam penelitian ini sepenuhnya menjadi tanggung jawab SAYA, bukan tanggung jawab Universitas AMIKOM Yogyakarta.
5. Pernyataan ini SAYA buat dengan sesungguhnya, apabila di kemudian hari terdapat penyimpangan dan ketidakbenaran dalam pernyataan ini, maka SAYA bersedia menerima SANKSI AKADEMIK dengan pencabutan gelar yang sudah diperoleh, serta sanksi lainnya sesuai dengan norma yang berlaku di Perguruan Tinggi.

Yogyakarta, 20 Februari 2026

Yang Menyatakan,

Alan Bayu Eka Satria

HALAMAN PERSEMBAHAN

Skripsi ini dipersembahkan dengan rasa hormat dan penuh syukur kepada:

1. Ibu dan kaka saya

   Atas kasih sayang, dukungan, dan doa yang tak pernah henti mengiringi setiap langkah saya.
2. Guru dan Dosen

   Yang telah memberikan ilmu, bimbingan, dan inspirasi selama perjalanan akademik saya.
3. Rekan-rekan dan Sahabat

   Yang senantiasa memberikan motivasi, dukungan moral, dan semangat untuk terus maju.

Semoga skripsi ini dapat memberikan manfaat dan menjadi kontribusi yang berarti bagi semua pihak.

KATA PENGANTAR

Puji syukur saya panjatkan ke hadirat Allah SWT yang telah memberikan rahmat, karunia, dan kemudahan sehingga saya dapat menyelesaikan skripsi ini dengan baik. Skripsi yang berjudul "Komparasi Kerentanan Form Registrasi Web Terhadap Serangan Bot Otomatisasi Menggunakan Metode Owasp Risk Rating" ini disusun sebagai salah satu syarat untuk memperoleh gelar Sarjana Teknik di Universitas Amikom Yogyakarta.

Saya ingin mengucapkan terima kasih yang sebesar-besarnya kepada:

1. Rina Pramitasari, S.Si., M.Cs. ,selaku Dosen Pembimbing, yang dengan sabar memberikan arahan bimbingan, dan motivasi selama proses penyusunan skripsi ini.
2. Tim Dosen Penguji, yang telah memberikan masukan konstruktif dan kritik yang membangun untuk perbaikan kualitas skripsi ini
3. Keluarga saya, yang selalu memberikan dukungan moral, doa, dan kasih sayang sepanjang perjalanan studi ini.
4. Rekan-rekan dan Sahabat, yang telah memberikan dukungan dan semangat yang tak ternilai harganya dalam proses penyelesaian skripsi ini.

Akhir kata, saya berharap skripsi ini dapat memberikan manfaat bagi semua pihak yang berkepentingan, terutama dalam mengembangkan keamanan form register. Saya juga menyadari bahwa skripsi ini masih jauh dari sempurna, oleh karena itu saya sangat mengharapkan kritik dan saran yang membangun demi perbaikan di masa mendatang.

Yogyakarta, 7 Januari 2026

Penulis

DAFTAR ISI

HALAMAN PERSETUJUAN ii
HALAMAN PENGESAHAN iii
HALAMAN PERNYATAAN KEASLIAN SKRIPSI iv
HALAMAN PERSEMBAHAN v
KATA PENGANTAR vi
DAFTAR ISI vii
DAFTAR TABEL xi
DAFTAR GAMBAR xii
DAFTAR LAMPIRAN xiii
DAFTAR LAMBANG DAN SINGKATAN xiv
DAFTAR ISTILAH xv
INTISARI xvi
ABSTRACT xvii
BAB I PENDAHULUAN 1
1.1 Latar Belakang 1
1.2 Rumusan Masalah 3
1.3 Batasan Masalah 3
1.4 Tujuan Penelitian 4
1.5 Manfaat Penelitian 4
1.6 Sistematika Penulisan 4
BAB II TINJAUAN PUSTAKA 6
2.1 Studi Literatur 6
2.2 Dasar Teori 16

2.2.1 Serangan Bot dan Validitas Data Survei Daring.....16
2.2.2 Ekosistem Bot Pendaftaran dan Layanan Bypass.....16
2.2.3 Verifikasi Identitas dan Pembatasan Akses Anonim.....16
2.2.4 OWASP Risk Rating.....16
2.2.5 Keterbatasan Sistem CAPTCHA Konvensional.....17
2.2.6 Eksploitasi CAPTCHA oleh Sistem Otomatis Murah.....17
2.2.7 Deteksi Bot dengan Pembelajaran Mesin.....17
2.2.8 Temporary Email.....17
BAB III METODE PENELITIAN.....18
3.1 Objek Penelitian.....18
3.2 Alur Penelitian.....19
3.3 Tahapan Penelitian.....20
3.3.1 Studi Literatur.....20
3.3.2 Penentuan objek penelitian.....20
3.3.3 Observasi non-invasif.....21
3.3.4 Pengolahan data observasi.....26
3.3.5 Evaluasi risiko dengan metode OWASP Risk Rating.....27
3.3.6 Analisis komparatif.....30
3.3.7 Perumusan rekomendasi mitigasi.....31
3.3.8 Penarikan kesimpulan.....31
3.4 Alat Dan Bahan.....32
3.4.1 Data Penelitian.....32
3.4.2 Alat/instrumen.....32
BAB IV HASIL DAN PEMBAHASAN.....34
4.1 Gambaran Umum Objek Penelitian.....34

4.2 Hasil Observasi Non-Invasif 34
4.2.1 Hasil Observasi pada OWASP Juice Shop 35
4.2.2 Hasil Observasi pada id.hm.com 39
4.3 Evaluasi Risiko.....43
4.3.1 Penilaian Likelihood 43
4.3.2 Penilaian Impact.....44
4.3.3 Perhitungan Risiko (Risk Score).....45
4.4 Analisis Kerentanan 48
4.4.1 Analisis Kerentanan pada OWASP Juice Shop 48
4.4.2 Analisis Kerentanan pada id.hm.com 51
4.5 Analisis Komparatif Antar Objek 53
4.5.1 Perbandingan Pola Kerentanan 54
4.5.2 Perbandingan Tingkat Risiko.....56
4.5.3 Faktor Penyebab Perbedaan Tingkat Kerentanan 57
4.6 Keterkaitan dengan Penelitian Terdahulu 58
4.6.1 Perbandingan dengan Penelitian Terdahulu (Research Gap).....58
4.6.2 Keterbaruan yang Dihasilkan (Novelty) 59
4.7 Rekomendasi Mitigasi.....59
4.7.1 Dasar Penyusunan Rekomendasi 60
4.7.2 Tabel Rekomendasi Mitigasi 60
4.7.3 Pembahasan Rekomendasi.....62
BAB V PENUTUP 63
5.7 Kesimpulan.....63
5.8 Saran.....64
REFERENSI 66

LAMPIRAN.....68

DAFTAR TABEL

Tabel 2.1 Keaslian Penelitian 11
Tabel 3.1 Penilaian Likelihood 28
Tabel 3.2 Penilaian Impact 29
Tabel 3.3 Nilai Resiko 29
Tabel 3.4 Perangkat Keras dan Spesifikasi 32
Tabel 3.5 Perangkat Lunak Dan Versi 33
Tabel 4.1 Ringkasan Hasil Pengujian OWASP Juice Shop 38
Tabel 4.2 Ringkasan Hasil Pengujian id.hm.com 42
Tabel 4.3 Hasil Evaluasi Risiko OWASP Juice Shop 46
Tabel 4.4 Hasil Evaluasi Risiko id.hm.com 47
Tabel 4.5. Rekomendasi Mitigasi Keamanan Form Registrasi 61

DAFTAR GAMBAR

Gambar 2.1 Captcha 16
Gambar 3.1 Alur Penelitian 19
Gambar 3.2 Alur Observasi non-invasive 21
Gambar 3.3 Alur Evaluasi Kontrol CAPTCHA 22
Gambar 3.4 Alur uji penggunaan email sementara 23
Gambar 3.5 Alur Analisis proses registrasi melalui tab Network 24
Gambar 3.6 Alur Pengujian Rate Limiting 25
Gambar 3.7 Evaluasi risiko dengan metode OWASP Risk Rating 27
Gambar 4.1 Tampilan form registrasi OWASP Juice Shop tanpa CAPTCHA 35
Gambar 4.2 Pengujian Form Registrasi Menggunakan Email Sementara 36
Gambar 4.3 Network Request Ke Endpoint /Api/Users Tanpa Autentikasi 37
Gambar 4.4 Pengujian Pengiriman Permintaan Berulang. 38
Gambar 4.5 Tampilan form registrasi id.hm.com tanpa CAPTCHA 39
Gambar 4.6 Pengujian validasi email dengan domain sementara 40
Gambar 4.7 Api Endpoint 41
Gambar 4.8 Rate Limiting 42

DAFTAR LAMPIRAN

Lampiran 1. Profil obyek Penelitian 68

DAFTAR LAMBANG DAN SINGKATAN

CAPTCHA	Completely Automated Public Turing test to tell Computers and Humans Apart
OWASP	Open Web Application Security Project
API	Application Programming Interface
DOS	Denial of Service
TLD	Top-Level Domain
OCR	Optical Character Recognition
ML	Machine Learning
ANN	Artificial Neural Network
SVM	Support Vector Machine
RF	Random Forest
k-NN	k-Nearest Neighbor
TF-IDF	Term Frequency-Inverse Document Frequency
HTML	HyperText Markup Language
IP	Internet Protocol
OWASP	Open Web Application Security Project

DAFTAR ISTILAH

FORM REGISTRASI	Komponen pada website atau aplikasi yang digunakan pengguna untuk membuat akun baru dengan mengisi data seperti nama, email, dan password.
BOT ATTACK	Aktivitas jahat yang dilakukan oleh program otomatis (bot), seperti pembuatan akun palsu secara massal, spamming, atau eksploitasi API tanpa interaksi manusia.
CAPTCHA	Mekanisme keamanan yang dirancang untuk membedakan antara pengguna manusia dan bot dengan memberikan tantangan yang sulit dipecahkan oleh mesin.
EMAIL SEMENTARA	Layanan email sekali pakai yang biasanya digunakan untuk pendaftaran tanpa identitas tetap, dan tidak dapat diverifikasi kembali. Rentan disalahgunakan untuk membuat akun anonim.
RATE LIMITING	Teknik keamanan yang membatasi jumlah permintaan ke server dalam periode waktu tertentu untuk mencegah penyalahgunaan oleh bot.
OWASP JUICE SHOP	Aplikasi web simulasi yang dikembangkan oleh OWASP sebagai platform edukatif untuk menguji dan mempelajari berbagai kerentanan keamanan web secara legal dan etis.

INTISARI

Serangan bot otomatisasi pada form registrasi web semakin meningkat dan berpotensi menyebabkan pembuatan akun palsu massal, penyalahgunaan sumber daya sistem, serta penurunan integritas data. Penelitian ini bertujuan menganalisis tingkat kerentanan form registrasi terhadap serangan bot otomatisasi dengan membandingkan OWASP Juice Shop sebagai aplikasi simulatif dan id.hm.com sebagai platform layanan nyata. Metode pengumpulan data dilakukan secara observasi non-invasif melalui Inspect Element, analisis Network Request, uji validasi email, serta pengujian batas permintaan. Evaluasi risiko menggunakan metode OWASP Risk Rating dengan parameter Likelihood dan Impact untuk mengukur tingkat ancaman pada setiap kerentanan.

Hasil penelitian menunjukkan bahwa kedua objek memiliki empat kerentanan utama, yaitu tidak adanya CAPTCHA, lemahnya validasi email, API endpoint yang terbuka, serta tidak diterapkannya rate limiting. Seluruh parameter memperoleh nilai Likelihood dan Impact sebesar 3 sehingga menghasilkan skor risiko 9 (risiko tinggi). Kondisi ini menunjukkan bahwa kedua sistem sangat rentan terhadap otomatisasi, memungkinkan bot melakukan pendaftaran massal tanpa hambatan teknis. Penelitian ini merekomendasikan penerapan mekanisme verifikasi berbasis tantangan, pemblokiran email sementara, autentikasi API, serta rate limiting adaptif untuk memperkuat keamanan form registrasi web.

Kata kunci: Registrasi Web, Serangan Bot, OWASP Risk Rating, Kerentanan, Mitigasi Keamanan.

ABSTRACT

Automated bot attacks on web registration forms have increasingly become a critical threat, enabling the creation of large-scale fake accounts, resource exhaustion, and degradation of data integrity. This study aims to analyze the vulnerabilities of web registration forms against automated bot attacks by comparing OWASP Juice Shop, a security training application, with id.hm.com, an active production platform. Data were collected through non-invasive observation using Inspect Element, Network Request analysis, temporary email testing, and rate-limit probing. Risk evaluation was performed using the OWASP Risk Rating method by assessing Likelihood and Impact for each identified vulnerability.

The findings indicate that both systems exhibit four major vulnerabilities: absence of CAPTCHA, weak email validation, exposed API endpoints, and lack of rate limiting. Each parameter received a Likelihood and Impact score of 3, resulting in a total risk score of 9 (high risk). These results demonstrate that both systems are highly susceptible to automation, allowing bots to perform mass registrations without significant barriers. This study recommends implementing challenge-based verification, temporary email filtering, authenticated API access, and adaptive rate limiting to enhance the security of web registration forms..

Keyword**:** *Web Registration, Bot Attacks, OWASP Risk Rating, Vulnerabilities, Security Mitigation.*