TUGAS RISET INFORMATIKA

RUMUSAN MASALAH

Dosen Pengampu

Dr. Basuki Rahmat, S.Si. MT.

Disusun Oleh :

Muhammad Fattah Ziidan

NPM 22081010149

PROGRAM STUDI INFORMATIKA

FAKULTAS ILMU KOMPUTER

UNIVERSITAS PEMBANGUNAN NASIONAL "VETERAN" JAWA TIMUR

SURABAYA

2025

Gap Research

No	Judul Penelitian	Nama dan Publiser	Persamaan dan perbedaan	Hasil Penelitian
1	Analisis Keamanan Website Global Academic Information System menggunakan OWASP ZAP dan Model AI Lokal	Asep Rio Saputra, et al. (2025). *JTIM : Jurnal Teknologi Informasi dan Multimedia*.	**Persamaan:** Mengintegrasikan OWASP ZAP dengan model AI (kecerdasan buatan) untuk otomatisasi analisis dan pembuatan laporan. Menggunakan Python sebagai skrip otomasi. **Perbedaan:** Menggunakan model AI *lokal* (Mistral via Ollama) dengan fokus pada privasi data. Penelitian yang diusulkan menggunakan model AI *cloud-based* (Gemini) yang berpotensi memiliki basis pengetahuan lebih luas dan kemampuan penalaran yang lebih canggih, serta menargetkan secara spesifik *developer pemula* sebagai pengguna akhir.	Berhasil mengembangkan sistem otomatis yang memindai kerentanan dengan ZAP, menganalisisnya dengan AI lokal, dan menghasilkan rekomendasi mitigasi teknis. Sistem ini terbukti efektif dalam menyederhanakan audit keamanan dan menjaga privasi karena tidak ada data yang dikirim ke layanan cloud. Menemukan 193 kerentanan (4 tinggi, 8 medium).

2	Analisis Keamanan Web Samsat Menggunakan Metode Owasp (Open Web Application Security Project)	Zarifah Aina, et al. (2025). *JOURNAL OF COMPUTER SCIENCE AND INFORMATICS ENGINEERING (COSIE)*.	**Persamaan:** Menggunakan OWASP ZAP sebagai alat utama untuk pemindaian kerentanan otomatis dan mengacu pada kerangka OWASP untuk analisis. **Perbedaan:** Merupakan penerapan standar OWASP ZAP tanpa integrasi AI. Laporan yang dihasilkan bersifat teknis (daftar *alerts* dan level risiko), tidak ada mekanisme untuk menerjemahkan hasil bagi audiens non-spesialis.	Teridentifikasi total 18 celah keamanan pada website SAMSAT, yang terdiri dari 2 tingkat ancaman tinggi, 4 menengah, 7 rendah, dan 5 informatif. Penelitian ini memberikan rekomendasi perbaikan teknis berdasarkan temuan standar dari OWASP ZAP.
3	IMPLEMENTASI SISTEM KEAMANAN SIBER BERBASIS ARTIFICIAL INTELLIGENCE UNTUK MENGATASI SERANGAN PHISHING	Maria Rosanti, et al. (2025). *Aisyah Journal Of Informatics and Electrical Engineering (A.J.I.E.E)*.	**Persamaan:** Menerapkan Kecerdasan Buatan (AI) dalam domain keamanan siber di Indonesia. **Perbedaan:** Fokus AI adalah untuk *deteksi ancaman* (*phishing*) secara *real-time* menggunakan model *machine learning* (SVM, Random Forest), bukan untuk *analisis post-scan* dan *interpretasi laporan kerentanan*. Ini menunjukkan spektrum penerapan AI yang berbeda dalam keamanan siber.	Sistem berbasis AI yang dikembangkan mampu mendeteksi email dan situs web phishing dengan akurasi 97%. Penelitian ini membuktikan efektivitas AI dalam memberikan solusi keamanan siber yang proaktif dan mengurangi *false positive*, memperkuat argumen umum bahwa AI dapat meningkatkan postur keamanan.

4	IMPLEMENTASI OWASP TOP 10 DALAM PENGUJIAN PENETRASI WEBSITE: MENGIDENTIFIKASI CELAH KEAMANAN DALAM SISTEM PENGELOLAAN VOTING INDONESIA	Zora Zairina, et al. (2025). *Jurnal Teknologi Informasi, Komputer, dan Aplikasinya (JTIKA)*.	**Persamaan:** Menggunakan kerangka OWASP Top 10 sebagai acuan utama untuk kategorisasi kerentanan, sesuai dengan rancangan konseptual skripsi. **Perbedaan:** Fokus pada proses *penetration testing* manual dan semi-otomatis menggunakan berbagai *tools* (subfinder, nuclei, dll.), bukan otomatisasi penuh dari pemindaian hingga pelaporan. Tidak ada komponen AI untuk interpretasi hasil.	Dari 10 subdomain yang diuji, 9 di antaranya memiliki kerentanan yang terkait dengan kategori OWASP Top 10, seperti Broken Access Control (paling umum), Injection, dan Security Misconfiguration. Penelitian ini memberikan bukti empiris tentang relevansi OWASP Top 10 pada sistem kritis di Indonesia.