Pengujian Penetrasi Web Menggunakan Multi-Agen Kolaboratif dan Pelaporan Terintegrasi

Rizki Juliadi[1], Parman Sukarno[2], Aulia Arif Wardana[3]

Fakultas Informatika, Universitas Telkom, Bandung
rizkijuliadi@student.telkomuniversity.ac.id,
psukarno@telkomuniversity.ac.id,
aulia.wardana@pwr.edu.pl,

Abstrak

Kemunculan ancaman dunia maya yang semakin cepat menggaris bawahi perlunya langkah-langkah keamanan aplikasi web yang kuat. Pengujian penetrasi konvensional sering kali terbukti tidak memadai saat dihadapkan dengan vektor serangan kontemporer. Studi ini membahas kekurangan ini dengan mengusulkan kerangka kerja pengujian penetrasi multiagen kolaboratif yang meningkatkan deteksi kerentanan. Kerangka kerja ini menggunakan alat seperti OWASP ZAP, Nikto, dan Wapiti, yang diintegrasikan dengan ELK Stack, untuk mensimulasikan skenario serangan yang kompleks dan menghasilkan laporan yang dapat ditindaklanjuti bagi para pemangku kepentingan. Solusi ini menggunakan pembelajaran penguatan yang mendalam untuk beradaptasi dengan ancaman yang berkembang secara dinamis. Pengujian mengungkapkan 41 kerentanan, dengan OWASP Juice Shop menyumbang 26 (63,41%) dan DVWA 15 (36,59%), yang sebagian besar diidentifikasi melalui OWASP ZAP. Hasilnya menyoroti peningkatan yang signifikan dalam pendeteksian dan pelaporan dibandingkan metode tradisional, mendorong keamanan aplikasi web yang lebih kuat melalui pengujian yang dinamis dan terkoordinasi.

Kata Kunci : Collaborative Multi-Agent, Deep Reinforcement Learning, ELK Stack, Penetration Testing, Web Application Security.