Web Penetration Testing Using Collaborative Multi-Agents and Integrated Reporting

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,

Abstract

The accelerated emergence of cyber threats underscores the necessity for robust web application security measures. Conventional penetration testing frequently proves inadequate when confronted with contemporary attack vectors. This study addresses these deficiencies by proposing a collaborative multiagent penetration testing framework that enhances vulnerability detection. The framework utilizes tools such as OWASP ZAP, Nikto, and Wapiti, integrated with the ELK Stack, to simulate complex attack scenarios and generate actionable reports for stakeholders. It employs deep reinforcement learning to adapt to evolving threats dynamically. Testing revealed 41 vulnerabilities, with OWASP Juice Shop accounting for 26 (63.41%) and DVWA for 15 (36.59%), primarily identified via OWASP ZAP. The results highlight significant improvements in detection and reporting over traditional methods, promoting stronger web application security through dynamic and coordinated testing.

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