V8-Scanner: Adaptive AI-Assisted Vulnerability Detection System

Abouelmaaty, Khaled (School: We Alexandria For Applied Technology)
Abohatab, Ibrahim (School: We Alexandria For Applied Technology)

Modern web vulnerability scanners often generate high noise, miss Application Programming Interface (API) and dynamic application paths, or fail under defensive controls. We developed V-8 Scanner to improve practical detection quality by combining asynchronous scanning, adaptive evasion, dynamic discovery, and AI-based validation. We implemented V-8 in Python with a modular architecture. The system includes dynamic endpoint discovery (HTML crawl, JavaScript analysis, and API schema discovery), multi-module testing (SQL injection, XSS (Cross-Site Scripting), command injection, Local File Inclusion (LFI), Server-Side Request Forgery (SSRF), Insecure Direct Object Reference (IDOR), Cross-Site Request Forgery (CSRF), open redirect, and information disclosure), and a Smart Client that classifies responses and adapts request techniques against Web Application Firewall (WAF) and rate-limit behavior. also implemented an optional AI Brain and Cortex pipeline for scan planning, payload refinement, autonomous follow-up probing, finding deduplication, and narrative risk summarization. In authorized tests on an intentionally vulnerable local web target, one full run reported 100 raw findings. After Cortex validation, output was reduced to 41 validated findings, with 53 duplicates removed, and 6 false positives dismissed, corresponding to 59.0% noise reduction. The validated set included high-impact categories, like SQL injection, command injection, SSRF, IDOR, and reflected XSS, with evidence-rich JSON reporting for reproducibility. V-8 Scanner improved actionable signal quality by reducing duplicate and false-positive noise, while preserving critical findings. The results support adaptive scanning with AI validation enables faster, higher-confidence web security assessments.

Awards Won: