Automated Cognitive DAST

The Problem

Traditional DAST (Dynamic Application Security Testing) is rigid. Automated scanners lack context—they don't know *how* our organization tests, which logic flows are critical, or how to navigate complex authentication. Conversely, manual PenTesting is thorough but unscalable. We need a solution that bridges this gap.

The Solution

Automated Cognitive DAST is an AI-driven security agent that wraps the industry-standard **ZAP Proxy** in the **Model Context Protocol (MCP)**. It orchestrates security scans using natural language, enriched by our organization's specific testing methodologies (RAG), and analyzes results for genuine exploitability.

Key Innovations

1. **MCP-Native Architecture:** By wrapping ZAP in an MCP Server, we allow any MCP-compliant client (Gemini CLI, Claude Code) to interact with the scanner directly. The LLM acts as the "driver," making real-time decisions on scan depth and strategy.
2. **Organizational Alignment (RAG):** Before scanning, our agent queries a vector database containing the organizations's "VA Team Playbooks." It learns that "Company123 requires JWT manipulation tests on all Finance APIs," and dynamically instructs ZAP to perform these specific attacks.
3. **Hybrid AI Intelligence:**
    - **Orchestrator (Cloud LLM):** Handles complex logic, report generation, and exploitability reasoning.
    - **Privacy Layer (Ollama):** Processes sensitive header data or performs offline logic checks to ensure PII doesn't leak to public models.
4. **Universal Authentication Config:** A standardized JSON configuration allows our agent to script ZAP's authentication (OAuth2, scripting-based auth) automatically, solving the #1 pain point in automated DAST: losing the session.

Value Proposition

We are moving from "Static Scanning" to "Agentic Security Testing." Automated Cognitive DAST doesn't just run a script; it reads our policy, understands the target, executes the scan, and tells us what actually matters.
