MAYUR DUSANE

Application Security Analyst — Platform Engineering, Applied AI & Security

Jersey City, NJ • mayurdusane1@gmail.com • 201-423-0463 • mayurdusane.com • linkedin.com/in/mayur19

SUMMARY

Application security and platform engineer with 7+ years securing web applications, CI/CD pipelines, and cloud-native systems — now focused on securing AI/LLM and agentic systems. I build production internal platforms and Model Context Protocol (MCP) tooling while embedding security directly into agentic and LLM-assisted development: AI-generated code review, prompt-injection and data-leakage defense, and PII redaction — grounded in OWASP LLM Top 10, OWASP Agentic/MCP, MITRE ATLAS, and the NIST AI RMF.

CORE SKILLS

AI / LLM Security: OWASP LLM Top 10 · OWASP Agentic & MCP Top 10 · prompt-injection & jailbreak defense · AI-generated code review · LLM data-leakage prevention · PII detection & redaction · secure MCP tool-calling & agentic workflows · MITRE ATLAS · NIST AI RMF

Application Security: secure code review · threat modeling · OWASP Top 10 / CWE · SAST/DAST (SonarQube, Veracode) · penetration testing (Burp Suite, OWASP ZAP, Nmap) · authN/authZ (JWT, OAuth, SSO) · vulnerability management

Platform & Engineering: Python · JavaScript/TypeScript · Flask · Vue.js · REST APIs · Docker · AWS S3 · CI/CD · MCP · Claude Code · Codex · internal platform & tooling development

PROFESSIONAL EXPERIENCE

Applause | *Application Security Analyst — Platform, Applied AI & Security* Mar 2025 – Present · Jersey City, NJ

- Designed and shipped a self-serve data platform for secure multi-type data collection and labeling, removing per-use-case developer dependency.
- Built MCP workflows around internal platforms so teammates extend systems with agentic tools (Claude Code, Codex) while preserving secure review, PII handling, and deployment controls.
- Review AI-generated code before merge for injection, insecure-dependency, authentication, and prompt-injection-adjacent risks; lead secure code review across Python, JS, Flask, and Vue.js.
- Integrated PII detection and redaction to prevent data leakage across AI pipelines; hardened containers and secured CI/CD; cut critical vulnerabilities 30% in Q1.
- Lead threat modeling and OWASP Top 10 / CWE remediation; triage and validate external vulnerability disclosures from security researchers.

Applause | *Application Security Intern* May 2024 – Aug 2024 · New York, NY

- Ran manual and automated security assessments across internal web platforms, finding 50+ vulnerabilities; built Flask/Vue.js middleware preventing XSS, RCE, SQLi, CSRF, and path traversal.
- Contributed to threat modeling and provided secure-coding guidance aligned with NIST and ISO 27001.

uTest (Applause) | *Software Engineer — Data Platforms & Security* Mar 2019 – Aug 2023 · India

- Replaced manual data-collection workflows with a dedicated collection & labeling platform supporting AI data pipelines; added auto-labeling and human-in-the-loop reduction on a revenue-critical system.
- Ran secure code reviews across 50+ web applications (−40% reported issues); designed JWT/OAuth/SSO authentication; led threat modeling and CI/CD security improvements.
- Built automation frameworks improving test accuracy 60% and delivery efficiency 20% across 25+ cross-functional projects.

PROJECTS

- **Flask-Sanitize-Escape / Vue-Sanitize-Escape —** Server- and client-side security libraries mitigating XSS, SQL injection, open redirect, and injection attacks.
- **WASM (Attack Surface Monitor) —** Discovers and monitors externally exposed domains, APIs, and open ports.
- **S3-Etag-Generator —** Concurrent hashing utility validating integrity of multipart uploads to AWS S3.

EDUCATION, CERTIFICATIONS & RECOGNITION

M.S., Cybersecurity — Yeshiva University (Katz), New York, NY (2024) · Adv. Certificate in Cybersecurity — IIIT Bangalore (2023)

B.E., Information Technology — NDMVP's KBTCOE, Nashik (2017)

ISC2 Certified in Cybersecurity (CC) · Google Cybersecurity Specialization · ISACA NYM Moisey Levin Memorial Scholarship

3rd Place, 2024 ISACA NYM Cybersecurity Case Study Competition (supply-chain / SolarWinds analysis)