Gaurav Mendse

Senior Full-Stack & AI Engineer | Secure Development & AI Security | Angular · React/Next.js · Python · PowerBuilder Modernization

+91 9921600018 | gaurav.mendse@outlook.com | Amravati, India (Remote) | LinkedIn | GitHub | Portfolio

SUMMARY

Full-stack engineer with 20+ years on banking, insurance, mortgage and SaaS products, now focusing on AI security. Early on, as a developer and team lead on an HSBC credit-card product, also took on QA coordination and security audit duties, reviewing code and removing malicious code before release. Since then has built web apps and AI features with security built in (input validation, server-side authorization, guardrails, audit logging, human-in-the-loop approval) and evaluated LLMs for safety failures such as sensitive-data exposure and jailbreaks.

Currently training in cybersecurity with a focus on AI security (OWASP Top 10 for LLMs, prompt injection, AI risk frameworks). Looking for a long-term remote or hybrid role in AI security, application security or secure AI engineering, and open to full-stack and PowerBuilder modernization work. W-8BEN available for US contracts.

PROFICIENCY

- PowerBuilder — Advanced ●●●●○
- Angular — Advanced ●●●●○
- React / Next.js (JS & TS) — Proficient ●●●○○
- Python (FastAPI, LangChain) — Proficient ●●●○○
- Java (Spring Boot) — Proficient ●●●○○
- Secure code review & QA — Proficient ●●●○○
- AI / LLM & Agentic (LangChain, LangGraph, MCP) — Working ●●○○○
- AI safety evaluation & red-teaming — Working ●●○○○
- AI security (OWASP LLM Top 10, prompt injection) — In training ●○○○○

TECHNICAL SKILLS

- **Frontend:** Angular, React, Next.js, TypeScript, RxJS, NgRx, Redux, Tailwind CSS, MUI
- **Backend & Data:** NestJS, Node.js, FastAPI, Spring Boot, GraphQL, Python, SQL, PostgreSQL, Oracle, SQL Server
- **Security & QA:** secure code review, OWASP Top 10, input validation, auth & access control, dependency vulnerability fixes, audit logging, AI red-teaming, QA coordination, Playwright, Vitest
- **Cloud & Tools:** AWS Lambda, Firebase, Vercel, GitHub, Figma
- **AI Engineering:** GitHub Copilot, Antigravity, Claude Code daily; LangChain, LangGraph, MCP, Vercel AI SDK

CURRENT FOCUS

Cybersecurity & AI Security Training (Career break – professional development) Nov 2026 – Present

- Retraining in cybersecurity from the foundations (networking, Linux, web application security, OWASP Top 10) toward AI security: OWASP Top 10 for LLM Applications, prompt injection, data leakage, insecure tool use, MITRE ATLAS and the NIST AI Risk Management Framework.

EXPERIENCE RECENT

Founder & Full-Stack Engineer — Masala Recipe Jul 2026 – Oct 2026

- Built a website where food manufacturers, startups and cloud kitchens buy ready-to-produce spice recipes (20+) with manufacturing rights, plus tools to scale recipes to production and calculate cost per kg.
- Includes an AI assistant for ingredient substitutions and cost savings within food-safety rules, online payments and subscriptions, and automatic GST invoices.
- Built security in from the start: server-side authorization on every action, input validation, payment webhook signature checks, bot protection, and guardrails on the AI assistant.
- Designed, built, tested and launched the complete product, including 52 bilingual recipe pages for organic search traffic; project completed Oct 2026.

Stack: Next.js 16, React 19, TypeScript, PostgreSQL, Drizzle ORM, Razorpay, Vercel AI SDK, Zod, Playwright.

AI Evaluator & Trainer (Freelance) — Outlier AI, DataAnnotation May 2026 – Aug 2026

- Evaluated AI LLM answers for safety failures (sensitive-data exposure, prohibited actions, jailbreak attempts) as well as made-up facts and sycophancy, and documented how each failure happened.
- Wrote requirement documents that teach AI models how real software features should work.

Stack: Python, LLM evaluation tools, AI agents.

Senior Consultant / Product Manager — Veerappa Software Solutions and Services Jun 2024 – Apr 2026

- Built AI chat assistants that answer customer questions in 6 languages (manual support tickets −60%) and an AI insights assistant that summarizes accounts, stock and entries into profit/loss trends and inventory risks.
- Put guardrails around the AI features: rate-limited and validated APIs, secure endpoints, human approval of AI decisions and audit logs.
- Built a multilingual clinic website with online appointments that collect patient history, instant alerts and a virtual receptionist bot; added data checks (quality +50%) and faster dashboards (response time −40%).

•As Product Manager (Jun 2024 – Jun 2025), set the vision and roadmap for an accounting web app, including security and privacy requirements as acceptance criteria, and owned QA sign-off; feature delivery +35%, adoption +25%.

Stack: Python, FastAPI, LangChain, OpenAI, Gemini, Next.js, Angular, NestJS, Java, Spring Boot, Firebase.

Senior Consultant — Infosys Jun 2025 – Aug 2025

•Consulted on moving a live insurance product from PowerBuilder to the web; reviewed the large legacy codebase and wrote plain-language guides for analysts and engineers (documentation work 40% more efficient, rework −35–50%), flagging embedded SQL and access-control logic to carry over safely.

•Engagement ended early when the client moved the project to another vendor; the full 35-person team was released.

Stack: PowerBuilder, Angular, Java.

Consultant (Part-time) — Centriqe.AI Nov 2023 – Mar 2024

•Maintained three web apps (Angular SaaS, React survey, Next.js help app); made the main app 30% faster, cut duplicate code by 35% and production problems by 25%, partly by fixing vulnerable dependencies and removing unused code.

Stack: Angular 15, React 18, Next.js, RxJS, Redux, MUI, Tailwind CSS.

Consultant — mimik Technology Inc. Apr 2023 – Nov 2023

•Stabilized an existing Angular app (bugs −85%), including dependency upgrades to clear known vulnerabilities; built an admin app prototype and turned Figma designs into working screens.

Stack: Angular 14/16, RxJS, NgRx, SCSS, TypeScript.

Lead Frontend Developer — Centriqe Inc. Jan 2021 – Apr 2023

•Led the Angular/React team and built three web apps from scratch; a coding standard and review checklist with secure-coding checks (input sanitization, auth guards) raised team speed by 25%.

•Built a Help System (support efficiency +15%) with parameterized data access, and the first mobile prototypes in Flutter and React Native.

Stack: Angular 12/14, React 18, Next.js, RxJS, Redux, MUI, Flutter, React Native, .NET Core, SQL Server.

EARLIER CAREER

Technical Lead — Hot Desk Consultancy (Wellington, NZ) Nov 2014 – May 2015

•Government land-records system (LINZ): helped evaluate and replace a third-party map component under government change-control requirements.

Project Lead — SunGard Feb 2010 – Oct 2014

•Led a reinsurance product with teams in India and the USA; cleared the defect backlog through root-cause analysis and set release quality gates.

Systems Analyst — Fiserv Sep 2007 – Feb 2010

•Mortgage-lending product handling borrower financial data: requirements, code reviews and regression testing; trained the .NET team on a PowerBuilder-to-C# migration.

Consultant — Kanbay International (acquired by Capgemini) Nov 2004 – Aug 2007

•Developer and team lead on an HSBC credit-card product. Also took on QA coordination and security audit duties: reviewed code before release, found and removed malicious code, and tracked audit findings to closure. On-site client coordinator in Chicago, USA.

Also: web and Angular developer roles at RikArena and Braincranx; founded and exited a food-products business (2017–2019); software trainee on a government town-planning system (2003–2004).

SELECTED PROJECTS

•**Masala Recipe** — B2B marketplace for ready-to-produce spice formulas with a batch-scaling cost calculator, AI formulation assistant and GST invoicing. masalarecipe.in

•**Insurance Portal Prototype** — Angular 21, NestJS, LangChain. Turns PowerBuilder DataWindows into role-aware web UIs with AI risk scoring, fraud detection and claim triage; JWT auth, human-in-the-loop approval and full audit logging, designed with the EU AI Act in mind. Live demo

EDUCATION & CERTIFICATIONS

•MCA and B.Sc. (Computer Applications), Amravati University

•Certifications: Agentic AI – Risk & Cybersecurity Masterclass (2026); Ethical Hacking with JavaScript; NestJS: The Complete Developer's Guide; GraphQL Bootcamp; Complete Python Developer