Karan Bansal

+919821974890 | karanb192@gmail.com | linkedin.com/in/karanb192 | github.com/karanb192 | @karanb192

Summary

Engineering leader with 9+ years building AI-powered security products at scale. Architected agentic AI systems serving Fortune 500 enterprises. Built open-source MCP servers with 340+ GitHub stars. Track record of 0-to-1 product builds, startup acquisition (6 months to exit), and scaling teams to 25+ engineers. Speaker at DEFCON and OWASP.

Experience

Head of AI Dec 2023 – Present
ArmorCode (Series B, ASPM Leader) *Gurugram*

- Led AI strategy and 7-engineer team building Anya, ArmorCode's agentic AI security champion, delivering 80% MTTR reduction for Fortune 500 customers through intelligent vulnerability triage and remediation
- Architected enterprise MCP server enabling Claude/GPT/Copilot to query 40B+ security findings across 320+ integrations with OAuth 2.0, typed schemas, and least-privilege RBAC
- Designed RAG pipelines and multi-step agentic workflows for automated VAPT report interpretation, vulnerability correlation, and context-aware remediation prioritization
- Championed AI-assisted development with Claude Code: 100% AI-generated code in AI team, 90% org-wide adoption

Engineering Manager Apr 2021 – Jul 2023
Urban Company (Unicorn, $2.8B valuation) *Gurugram*

- Led 12-engineer security org covering product security, privacy (GDPR), and IPO readiness; built team from scratch
- Drove core platform initiatives achieving 99.999% uptime: auto-failover, rate limiting, load shedding, canary reverts, disaster recovery, and multi-region architecture
- Implemented "Crypto Shredding" privacy solution encrypting all PII with per-user keys for GDPR compliance

Founding Engineer → Engineering Manager Jul 2018 – Apr 2021
Avid Secure (acquired by Sophos, Jan 2019) *Gurugram*

- First engineer; built MVP in 6 months leading to acquisition. Scaled team to 25 engineers post-acquisition
- Re-architected platform from 10 to 10K customers: distributed systems, HA, multi-tenancy, security hardening
- Established engineering excellence: SSDLC, external pen-tests, and launched bug bounty program

Sr. Software Engineer May 2016 – Jul 2018
NTRO (National Technical Research Organisation) *New Delhi*

- Built secure software systems for critical information infrastructure protection

Open Source & Community

- **reddit-mcp-buddy** (340★, 52 forks): Most popular Reddit MCP server for Claude/AI assistants
- **awesome-claude-skills** (30★): Curated collection of 50+ verified Claude skills for Claude Code
- Contributor: vLLM (67k★), find-sec-bugs (2k★) | AWS case study
- Speaker: DEFCON/OWASP '16 (Applied Crypto), c0c0n '14 (Distributed Fuzzing), GCCS '17 (Blockchain)
- Internships: **FireEye** '15 (vulnerability scanner, PPO) | **Citrix** '14 (distributed fuzzer)

Education

IIT Kanpur Kanpur, UP
B.Tech. in Computer Science & Engineering (IITJEE AIR 192) *2012 – 2016*

Technical Skills

AI/ML: LLMs (Claude, GPT-5, Gemini), AI Agents, Agent Orchestration, RAG, MCP, Context Engineering, LangGraph
AI Tools: Claude Code, Windsurf, GitHub Copilot, Cursor
AI Security: LLM Red Teaming, Prompt Injection, OWASP Top 10 for LLMs, AI Guardrails
Infrastructure: AWS, Kubernetes, Kafka, Redis, Cassandra, Docker, Terraform, CI/CD
Security: VAPT, Threat Modeling, SAST/DAST, OWASP Top 10, Cryptography, Secure SDLC
Languages: Python, Java, Go, TypeScript, Node.js, Spring Boot