KHONAIN SULTAN KHAN (KK)

Founder of ForgeGuard AI | AI Engineer | Full-Stack Security Engineer
Karachi, Pakistan | +92 312 3583827 | khonainkhan.dev@gmail.com | github.com/kkcyber2

PROFESSIONAL SUMMARY

Security engineer and full-stack builder specializing in production LLM applications, self-verifying multi-agent RAG pipelines, and adversarial security evaluations. Founder of ForgeGuard AI. Author of 61 public repositories with 3,125 passing automated tests across full-stack and AI workloads.

FEATURED PRODUCTION PROJECTS

ForgeGuard AI - Founder & Lead Engineer (https://www.forgeguard-ai.com)

- Architected multi-tenant AI security & red-teaming platform for automated adversarial stress-testing.
- Designed deterministic evaluation engine covering prompt injection, jailbreaks, and sensitive data leakage.
- Full-stack Next.js, TypeScript, Python backend with containerized microservices and automated CI/CD.

Sentinel-RAG - Self-Verifying Multi-Agent Architecture (github.com/kkcyber2/sentinel-rag)

- Built closed-loop RAG pipeline with LangChain, LangGraph, ChromaDB, and local Ollama inference.
- Developed dual-agent audit cycle: Researcher agent drafts answers, Verifier agent validates claims against source chunks with automatic revision loops to prevent hallucination.
- FastAPI asynchronous backend with Streamlit interactive validation console and Docker deployment.

Calvin & Stitch - Bespoke Brand & Tailoring E-Commerce (kelvarinstitches.com)

- Designed and shipped custom e-commerce web platform for bespoke luxury tailoring client.
- High-contrast brutalist aesthetic, responsive design, fast SSR, and zero-downtime hosting.

TECHNICAL SKILLS

Languages: Python, TypeScript, JavaScript, SQL, Bash
AI & Agents: LangChain, LangGraph, ChromaDB, Ollama, Llama 3, RAG Architectures, Vector Search
Security: Adversarial Red-Teaming, Prompt Injection Defense, Cloud Security, OWASP Top 10
Full-Stack & Cloud: Next.js, React, Node.js, FastAPI, PostgreSQL, Docker, Git, Linux / Parrot OS