

Samir Jani

junior cybersecurity engineer, prompt engineer, junior AI Engineer

github.com/samirjani03 | candidates.intervues.club/u/samir-jani

SUMMARY

Junior Cybersecurity Engineer, Prompt Engineer, and Junior AI Engineer with hands-on experience in offensive security workflows and community leadership. Demonstrated background in red teaming labs, vulnerability scanning, and designing web security CTF challenges. Skilled in leveraging emerging AI tools, Model Context Protocols, and threat analysis frameworks.

EXPERIENCE

Cybersecurity Intern

Gujarat Technological University (GTU)

Mar 2026 – May 2026

- Executed red teaming labs, reconnaissance, vulnerability scanning, and exploitation procedures.
- Explored and implemented artificial intelligence applications within offensive security workflows.

CTF Competition Organizer

College

Sep 2025 – Sep 2025

- Organized a college-level Capture The Flag (CTF) competition.
- Designed hands-on CTF challenges focused on web security, cryptography, and OSINT.

Technical Manager

Univyn Hub

Apr 2025 – Present

- Delivered technical insights to the community regarding key updates in cybersecurity and artificial intelligence.
- Analyzed AI trends, security tools, AI agents, emerging cyber attacks, and practical threat breakdowns.

EDUCATION

Shree Swaminarayan Institute of Technology · Bachelor of Engineering (BE) · 2023 – 2026

Government Polytechnic Ahmedabad · Diploma in Engineering · 2020 – 2023

SKILLS

Languages and Frameworks: Bash, Batchfile, Core Java, CSS, HTML, Javascript, PHP, Python, SQL, TypeScript, YARA, Bootstrap, LangChain, MCP, ReactJS, Tailwind CSS, Wowjs

Databases: MongoDB, PostgreSQL

Tools: Docker, Git, GitHub, Kali Linux, Local RAG, Ollama, WordPress

PROJECTS

RedTeamMCP

AI-powered penetration testing MCP server connected with Kali Linux Docker containers. Integrated 50+ offensive security tools with Cursor, Claude, and MCP-compatible IDEs.

Kali Linux, Docker, Cursor, Claude, MCP

[View Project](#)

Local RAG Using Ollama

Built a local AI RAG system for answering questions from uploaded documents. Implemented private offline document querying utilizing Ollama.

Ollama, Local RAG

[View Project](#)

URL Shield

Developed a URL and IP analysis tool for reconnaissance and threat analysis. Integrated DNS, SSL/TLS, port scanning, and technology detection features.

DNS, SSL/TLS

[View Project](#)

Additional projects: CyberShield, URLShield, RedTeamMCP, Local RAG Using Ollama, Local LLM Chatbot – Ollama + Llama 3.1 (8B), Latest Cyber Attacks Blog

AWARDS

Model Context Protocol: Advanced Topics, Cybersecurity 101, Introduction to Ethical Hacking, Introduction to Large Language Models, LangChain for LLM Application Development, Open-source models with huggingface, Speaker at Null Ahmedabad, Workshop Lead, Introduction to Model Context Protocol, Open Source Models with Hugging Face, Introduction to Ethical hacking: Beginner's guide to cybersecurity