

SAURABH SINGH

Mirzapur, Uttar Pradesh

+919555641793 [✉ saurabhsingh881888@gmail.com](mailto:saurabhsingh881888@gmail.com) [in Saurabh singh](https://www.linkedin.com/in/Saurabh singh) [G Saurabh21](https://github.com/Saurabh21) [🌐 Discover my portfolio](#)

Education

Polaris School of Technology

Bachelor of Science in Computer Science

Aug. 2023 – present

Gurugram , Haryana

Experience

Detoxio AI | AI Intern

March 2025 - June 2026

- Built **AI agent** using Browser-Use to automate CVE enumeration and security intelligence gathering, identifying **50+ potential vulnerabilities** and reducing manual reconnaissance effort.
- Built AI agent to automate vulnerability reconnaissance and exploit correlation across internal security data, cutting manual research time and surfacing actionable attack paths for the red team.
- Engineered a **full-stack security dashboard** using React.js and Node.js to visualize attack paths and red-team metrics, improving incident response efficiency by **30%**.

Projects

Exploithub RAG application | LangChain, Python, Fastapi

Dec 2025 [🔗 Project link](#)

- Built a high-performance **RAG pipeline** to index and query over **46,000+ exploits** from ExploitDB , utilizing **ChromaDB** and **HuggingFace embeddings** for sub-second semantic retrieval.
- Developed a sophisticated backend using FastAPI and GPT-4o-mini featuring an Intent Classifier and Hallucination Validator to improve response reliability and reduce hallucinated output in AI-generated pentesting responses.
- Implemented a **conversation manager** allowing for context-aware follow-up questions, enabling users to customize exploits for specific target environments.

Drug discovery agent | LangGraph, MCP, Python

Feb 2026 [🔗 Project link](#) | [🌐 Demo Link](#)

- Built an autonomous **Multi-Agent drug discovery system** using **langGraph**, coordinating specialized AI agents to automate drug target research across **biomedical databases**.
- Developed an **agentic memory and validation framework** that combined LLM reasoning with structured verification, achieving **0.91+ evidence support scores** for target analysis.
- Integrated **MCPs** and multi-model support, enabling flexible data retrieval and automated generation of pharmaceutical research reports.
- Built an automated evidence aggregation pipeline that analyzed **50+ biomedical evidence records** per run, generating comprehensive research dossiers for **cancer-related drug targets**.

Nirdesh AI: Multilingual Voice Agent | LangGraph, FastAPI, WebSockets, Sarvam AI Aug 2026 [🔗 Project link](#)

- Built a real-time **multilingual voice assistant** that converts speech to text, processes it with an **AI agent**, then converts the response back to speech, all in under 3 seconds.
- Implemented local **Voice Activity Detection** for silence filtering and barge-in, letting users interrupt the AI mid-response.
- Added **LangGraph** tool-calling for web search , with per-session memory and **JWT**-secured sessions.
- Benchmarked latency across **120+ voice calls**, achieving **p50 2.96s** and **p95 3.99s** with **99%+ success rate**.

Technical Skills

Languages: JavaScript, TypeScript, Python, c++

Web Development: React.js, Next.js, Node.js, FastAPI

Databases: MongoDB, MySQL, Supabase

CS Fundamentals: DSA, DBMS, OOPs, OS, System Design

AI: LangGraph, Agents, RAG, LLMs, Vector DBs, MCPs

Developer Tools: Git, GitHub, Docker, Postman, GH Actions

Achievements

- Contributed to **open-source software** with **10+ merged pull requests** across community-driven projects and developer tools.
- Built and delivered **5+ client projects** as a freelancer, ranging from automation solutions to full-stack web applications.
- Solved **100+ LeetCode** problems and actively participated in competitive programming and technical communities.