

Stalin S

Security Researcher | Agentic AI Systems | Ethical Hacker

stalin78830@gmail.com | +919655293238 | Chennai, Tamil Nadu
linkedin.com/in/stalin-s | github.com/0x5t41n | stalin.engineer

OBJECTIVE

AI and Cybersecurity student skilled in ethical hacking, penetration testing, vulnerability assessment, and AI-driven security solutions. Experienced in vulnerability research, responsible disclosure, and securing modern digital systems.

EDUCATION

St. Joseph's Institute of Technology

B.Tech Artificial Intelligence and Data Science | CGPA: 7.7/10

Present
Chennai, India

EXPERIENCE

Project Lead — OWASP Foundation

Aug 2026 – Present

OWASP HUniting

Remote

- Project Lead for OWASP HUniting, coordinating project development, security research, documentation, and contributor activities.
- Lead technical initiatives focused on application security, security testing, and modern cybersecurity research.

Artificial Intelligence Engineer — IdeaBoxAI

Aug 2026 – Present

Internship

Remote

- Develop automation workflows for AI/ML engineering and security-testing use cases.
- Work on Agentic AI security-testing agents, including testing, evaluation, and benchmarking.
- Perform LLM and Agentic AI benchmarking and evaluation for security-oriented tasks.
- Use Langfuse for LLM observability, tracing, evaluation, and performance analysis.

PROJECTS

DataOracle – Agentic AI Platform for Autonomous ML & Predictive Analytics

React, FastAPI, LangChain, Python, Scikit-learn, XGBoost, Supabase, MCP, Multi-LLM | [GitHub](#)

- Architected a dynamic multi-agent orchestration system that converts natural-language business questions into executable ML workflows – routing through intent classification, sandboxed code generation/execution, self-healing retries, and model inference to deliver automated insights.
- Built a stage-wise multi-LLM routing framework and engineered 20+ specialized AI agents with 70+ modular MCP-integrated skills for extensible, enterprise-scale autonomous data science workflows.
- Secured 2nd place (Rs. 15,000 prize) at HackIndia 2026, Open Stack Track, qualifying for the national grand finale.

OpenLearnX – Decentralized Learning & Blockchain Certification Platform

Next.js, React, Flask, Solidity, Web3.py, MongoDB, IPFS, TensorFlow | [GitHub](#)

- Built a decentralized adaptive-learning and assessment platform issuing tamper-proof, blockchain-verified NFT certificates for completed courses and skill assessments.
- Designed the full stack – Next.js/TypeScript frontend, Flask backend, and Solidity smart contracts (ERC-721) – with IPFS-based decentralized storage and MetaMask wallet authentication.
- Implemented a secure multi-language code execution sandbox (8+ languages) and an AI-driven adaptive quiz engine with real-time feedback and peer-review bias detection.

SKILLS

Agentic AI & LLM Systems: Multi-Agent Orchestration, LangChain, MCP, Multi-LLM Routing

Programming: Python, MySQL, Bash Scripting

Soft Skills: Social Engineering, Leadership, Emotional Intelligence

ACHIEVEMENTS

- Top 5 Global & #1 India on TryHackMe (May 2025).
- Top 10 Winner, TN Police Hackathon 2025.
- Finalist, Indian Army Terrier Cyber Quest.
- Won 10+ CTF competitions.
- Hall of Fame recognition from Sony, IBM, and ZOHO (OpenMage, TomTom, ELAN, Zerodha, Max Healthcare + major platforms).
- Open-source contribution – NextTOR IP Changer (AUR).

CERTIFICATIONS

eJPT – Junior Penetration Tester | Certified Network Security Practitioner (CNSP) | Certified AppSec Practitioner v2 (CAP)