

MOHIT SHARMA

Delhi NCR, India • github.com/index-oss • linkedin.com/in/mohit-sharma-143271330

PROFESSIONAL SUMMARY

Offensive Security & Systems Engineer with strong experience in building automated threat intelligence pipelines, security analysis tools, and autonomous agent frameworks. Specialized in web application security, stealth recon engines, and vulnerability management. Skilled in Python, Linux systems engineering, and LLM automation to build tools that discover, analyze, and remediate real-world security vulnerabilities under operational constraints.

EDUCATION

YMCA University (JC Bose UST)

Faridabad, Delhi NCR | 2024 – 2028

**Bachelor of Technology (B.Tech) in Computer Engineering /
Technical Studies**

Relevant Coursework: Computer Networks, Operating Systems, Web Application Security, Data Structures & Algorithms, Object-Oriented Programming

TECHNICAL SKILLS

Languages: Python, JavaScript (ES6+), HTML5, CSS3, Bash/Shell Scripting

Security & Testing: Web Application Security, Red Teaming, WAF Fingerprinting, Logic Flow Analysis (IDOR/BOLA), Penetration Testing, OWASP Top 10

Automation & Systems: Linux Systems, Real-Time Log Analysis, LLM Integration (OpenRouter/Local LLMs), REST APIs, Telegram Bot API

Developer Tools: Git, GitHub, VS Code, Linux CLI, Apache, NGINX

TECHNICAL PROJECTS

SecureStack v7.0 – Hybrid Security Intelligence Engine

Python, Web Security, OWASP, Red Teaming

- Architected a stealth recon and logic vulnerability detection engine to identify complex security flaws like IDOR and BOLA in web applications.
- Engineered custom bypass capabilities for Web Application Firewalls (WAFs) and mapped client-side JavaScript attack surfaces.
- Applied taint analysis and automated exploit simulation to prioritize high-severity exploitable vulnerabilities over minor misconfigurations.

CVEStrike – Automated Threat Intelligence Pipeline

Python, LLM Automation, REST APIs, Telegram API

- Developed an end-to-end threat intelligence bot that continuously ingests CISA security advisories and vulnerability feeds.
- Integrated local LLMs via OpenRouter to automatically summarize raw CVE data into actionable, prioritized threat reports.
- Built dynamic notification workflows to stream real-time alert updates directly to operational Telegram channels.

Self-Heal AI – Autonomous Linux Security & Recovery Agent

Python, Linux Systems, Log Analysis, AI Systems

- Implemented an autonomous security monitoring agent for Linux servers that inspects NGINX and Apache logs in real time.
- Designed real-time anomaly detection routines to automatically block malicious IP addresses and mitigate unauthorized access attempts.
- Automated service recovery mechanisms to detect and restart crashed system services without requiring manual administrative intervention.

Spiderweb Crawler – Controlled Web Reconnaissance Engine

Python, Web Scraping, Penetration Testing, HTML

- Built a recursive web crawler for penetration testers to map web application endpoints and attack surfaces.
- Implemented strict cycle prevention, deduplication algorithms, and configurable traversal depth to prevent infinite loops during scans.
- Discovered hidden parameters, endpoints, and common security misconfigurations across target environments.

LEADERSHIP & EXTRACURRICULAR ACTIVITIES

Offensive Security & Web Application Security Researcher

- Published open-source security tools on GitHub focusing on vulnerability research, WAF evasion, and red team automation.
- Authored technical breakdowns and impact-focused security analyses on web application security methodologies.