# Kartik Jain

Security Engineer | VAPT & Penetration Testing

Mumbai, India | career@jkartik.in | jkartik.in | linkedin.com/in/kartikjain1410 | github.com/KartikJain14

## Summary

Security engineer focused on web application VAPT: found 2 high-severity flaws in a banking portal as an intern, earned a $1,500 Meta bug bounty, and reported vulnerabilities to Microsoft (MSRC) and CERT-In.

## Education & Leadership

**B.Tech, Information Technology** | *SVKM's NMIMS MPSTME, Mumbai* | **CGPA: 8.34/10.0** Expected Apr 2028

- **Chairperson**, ACM MPSTME (~250 members); ex-Technical Head: Taqneeq, Mumbai MUN, Social Conclave, Sattva.
- Set problems for and mentored at CyberCypher, Taqneeq's cybersecurity hackathon; designed a CTF for freshers.

## Experience

**VisionRise Technosoft Pvt. Ltd.** | *Software Engineer Intern* Apr 2026 – Oct 2026

- Built the API behind two Google Play apps (Rise Academy, eGuru): Node.js, TypeScript, 276 routes, PostgreSQL, with JWT authentication, role-based access control and audit logs.
- Secured paid video with AES-128-encrypted HLS, per-session playback tokens and signed cloud-storage URLs.
- Hardened the production Linux server (Ubuntu 24.04 LTS: key-only SSH, firewall, auto security updates) and administered the GitHub org (15 repos) and Google Workspace (35+ accounts).

**R.U.D.R.A Cybersecurity Pvt. Ltd.** | *Security Engineer Intern* May 2025 – Jul 2025

- Found 2 high-severity vulnerabilities (Local File Inclusion, broken access control) in a banking client's web portal through manual code review, then wrote custom Nuclei templates to detect them automatically.
- Automated external attack-surface monitoring with BBOT, saving ~$20,000/year of manual reconnaissance.
- Deployed and operated the Sliver C2 framework for purple-team exercises emulating real-world intrusions.
- Developed a custom Semgrep (SAST) module with Neo4j graph visualization for large-scale code analysis.

**Freelance** | *Backend & Security Engineer* May 2025 – Jun 2025

- Led ransomware incident response for a 16,000+ user platform: restored it from backups and hardened its servers.

## Security Research

- Awarded a **$1,500 bug bounty by Meta** for a privilege-escalation vulnerability in WhatsApp.
- Reported access-control and information-disclosure flaws in Microsoft Intune and Exchange Admin to MSRC.
- Responsibly disclosed a stored XSS on the Mumbai Police website in coordination with CERT-In.
- Reported exposed staging infrastructure (The Souled Store) and a code and credential leak (Belgian Waffle Co.).
- **1st place** (global), chat.win AI Jailbreakathon: LLM prompt attack and defense, won with the fewest tokens.
- Participated in CSAW LLM Attack Challenge (LLMAC) '25, NYU.

## Projects

**Fool The LLM** | prompt-injection contest | *TypeScript, Next.js, Express, PostgreSQL, Gemini* Write-up

- Built and ran a contest for ~70 participants: guarded Gemini levels, an organizer console with live logs, and per-player token budgets.

**GhostShare** | end-to-end-encrypted file sharing | *TypeScript, Next.js, Fastify, PostgreSQL, Redis, Docker* Live

- Zero-knowledge design: keys are derived in-browser (Argon2id) and data is sealed with AES-256-GCM, so the server stores only ciphertext; the API adds rate limiting and security headers (helmet).

**Event & Payment Backends** | NMIMS student events | *TypeScript, Python, PostgreSQL* Check-in | Payments

- Co-led paid registration on Cashfree where tickets issue only on HMAC-verified webhooks; built QR access control for 500+ delegates, with check-ins made race-free by a Postgres unique constraint.

## Skills

**Security:** Web Application Penetration Testing, VAPT, OWASP Top 10, Burp Suite, Nmap, SAST/DAST (Semgrep, Nuclei), Dependency Scanning (SCA), BBOT, Sliver C2, Code Review, Responsible Disclosure, Incident Response, LLM Red Teaming, Prompt Injection
**Languages:** Python, Bash, TypeScript, JavaScript, SQL, Java
**Backend & Infra:** Node.js, FastAPI, REST APIs, JWT/OAuth 2.0, PostgreSQL, Docker, Linux, CI/CD (GitHub Actions)