



Lohith Kumar M D

Staff Application Security Engineer

Profile

Staff Application Security Engineer with 7+ years of hands-on experience in:

- **AI Red Teaming:** LLM, MCP, agentic AI security, and AI governance
- **Supply chain security:** SCA, SBOM, package firewalls, CI/CD gates
- **API, Web/Mobile and Cloud Security:** iOS & Android, AWS, GCP
- **Architecture reviews,** risk assessments, STRIDE Threat Modeling
- **Code Reviews (SAST)** and Black/White/Grey Box Pen Testing (DAST)
- **Compliance:** PCI DSS, SOC 2, HIPAA, and ISO 27001
- **Industries:** B2B SaaS, FinTech, and InsurTech

I set up **security programs from scratch** and run them end to end, across **AI, application, and cloud security**, from AI Red Teaming and LLM security reviews to CI/CD security gates and WAF (AWS, Cloudflare, Akamai) rules. Passionate about Ethical Hacking and discovering new vulnerabilities, with responsible disclosures recognized by **Amazon**, **Cursor**, **Cloudflare**, **Google**, **Loom**, and **WeWork**.

Employment History

Staff Application Security Engineer at **Atomicwork**, Bengaluru

January 2026 - Present

- Establishing the **security program** from scratch across **application, cloud, and AI**
- Leading the security function; managing a Security Engineer and reporting to the Head of Engineering
- Performing **AI Red Teaming** and **MCP** security testing across **agentic workflows**, identifying critical **prompt injection**, **authentication bypass**, and **authorization bypass** vulnerabilities
- Centralizing **MCP** and internal **AI tool governance**, defining how teams onboard, review, and use AI integrations securely
- Conducting **API security** assessments, **security architecture reviews**, and **threat modeling** across services, including **AI and LLM** features
- Securing the build and **CI/CD pipeline** for our **Bazel-based Java monorepo**, with automated scanning, security gates, and a **package firewall** for malicious open-source packages
- Fixing vulnerabilities found in internal assessments and external reports by raising PRs with the engineering team
- Managing the external **bug bounty** program on **BugBase** and **HackerOne**, and triaging reported issues

Sr. Security Engineer at **Acko**, Bengaluru

June 2025 - January 2026

- Built a **supply chain firewall** and **SBOM dashboard**, integrating **GitHub Dependabot** and **Dependency Graph** for real-time dependency and vulnerability visibility across repositories, with **Slack** alerts for malware and critical findings
- Performed **AI Red Teaming** on Acko's customer-facing **AI support chatbot**, testing for **prompt injection** and **jailbreaks**
- Led **DevSecOps** adoption and embedded security controls in the **CI/CD pipeline**
- Conducted internal **VAPT** for web and mobile applications (Android & iOS), and evaluated and managed **third-party security vendors** for external engagements
- Led cloud security improvements across **AWS** and **GCP** infrastructure
- Managed and mentored a Security Engineer; reported directly to the CISO
- Launched the external **bug bounty** program on **BugBase** from scratch and triaged reported issues

Contact Details

contact@lohigowda.in
Bengaluru, India

Links

[LinkedIn](#)
[GitHub](#)
[Blog](#)
[Talks](#)
[HackerOne](#)
[BugBase](#)

Certification

[Certified Ethical Hacker \(CEH\)](#)

Sr. Security Engineer at **Plivo**, Bengaluru

June 2023 - June 2025

- Implemented automated **Dependency Scanning (SBOM)** pipelines, generating consolidated vulnerability reports and streamlining remediation workflows
- Initiated and developed a **package firewall** to block malicious open-source packages at install time
- Identified **OWASP Top 10** vulnerabilities, including **SSRF**, **IDOR**, and **XSS** in web applications and APIs, and collaborated with development teams to implement security fixes
- Reduced **AWS Inspector** scan review from days to hours by automating result aggregation and flagging critical RCEs
- Managed a Compliance Engineer; reported to the Security Manager
- Led structured **security risk assessments** and **STRIDE Threat Modeling** sessions, reducing production vulnerabilities
- Migrated from **Akamai** to **AWS WAF** and set up Lambda-based alerts for **WAF**, **GuardDuty**, and **CloudTrail** security events
- Introduced AI into security operations, building **AI-driven CloudTrail alerting** and starting **agentic AI security reviews**
- Rolled out **secret detection** with pre-commit scanning, plus **API** and **code** scanning in CI/CD pipelines, and automated **GitHub** activity monitoring for organization-wide visibility

Sr. Security Engineer at **Airmeet Networks Pvt Ltd**, Bengaluru

May 2021 - June 2023

- Established end-to-end API, mobile (**Frida**, **MobSF**, **Burp Suite**), and cloud security testing from scratch, including pre-release testing
- Created a **Vulnerability Disclosure Program (VDP)** from scratch and triaged external reports
- Led **STRIDE Threat Modeling** sessions and configured custom **Cloudflare WAF** rules for external threat mitigation
- Owned **ISO 27001** and **SOC 2** compliance end to end as the only security engineer, covering control implementation, evidence collection, and auditor coordination

Security Engineer at **Reward360 Global Services Pvt Ltd**, Bengaluru

July 2019 - May 2021

- Performed internal and external penetration testing (web, mobile, network, and API)
- Managed OS patching and **vulnerability remediation** cycles, log reviews, and pre- and post-patch verification reports
- Collaborated with engineering and DevOps teams to identify and remediate security issues in production

✦ Vulnerability Research & Disclosures

- **CVE-2024-0953** - Firefox (Mozilla) iOS QR Code Scanner navigated users to the scanned URL without prompting, potentially directing them to unwanted content
- **GHSA-g4ff-54cv-h6f9** - Any **Cursor** team member could open the **Stripe billing portal**, view the billing admin's address and last 4 card digits, and cancel the plan
- **Brave iOS** - Reported a **Face ID lock** bypass on private tabs via deep links; **fixed** and **credited** by Brave
- Featured on **TechCrunch** for discovering an API vulnerability in **Naukri's** mobile apps that exposed recruiter email addresses to phishing and spam risks
- Found two IDORs (Critical & High) in a video-sharing platform exposing PII of **1.2M+ users** - **\$8,000** bounty
- Discovered a KYC bypass vulnerability in a Bangalore-based banking application - **\$1,000** bounty
- Discovered a Face Lock bypass vulnerability in a leading fintech mobile application - **\$500** bounty
- Bypassed fare logic in **Bangalore Namma Metro's** QR system to enable **₹1** travel - **Blog**

🏆 Open Source, Talks & Hall of Fame

- **Open Source**: **E2B** - Merged PRs adding **BTF** and **eBPF** tracing to Firecracker sandbox kernels - **#26**, **#27**
- **Talk**: **AI in Cloud Security** at the **Razzify Cybersecurity Meetup**, Bangalore - **Talk**
- **Hall of Fame**: **Google**, **Amazon**, **LinkedIn**, **Uber**, **BMW Group**, **1Password**, **Cloudflare**, **Robinhood**, **Automattic**, **Flipkart**, **Swiggy**, **PhonePe**, **Zomato**, **Blinkit**, **Groww**, **BigBasket**, **Hostinger**, **Adafruit**, **Sorare**, **Soundtrack**