MEENAKSHI S L

meenakshi.sl@protonmail.com linkedin.com/in/meenakshisl github.com/meenakshisl
Bangalore, Karnataka, India +91-83010-14030

SUMMARY

Senior Security Engineer focused on application security testing, OSS supply chain security, and open-source vulnerability research. Experienced in developing SAST detections and AI-assisted static analysis, producing technical reports and proof-of-concepts, and integrating research outputs into high-throughput ingestion pipelines to improve product quality and operational efficiency.

COMPETENCIES

- Vulnerability Research
- Application Security
- Static Analysis (SAST)
- Threat Modeling & Secure SDLC
- Root Cause Analysis
- Security Automation

EXPERIENCE

Senior Security Engineer **March 2026 - Present**
Security Engineer II **September 2024 - March 2026**
EndorLabs *Bangalore, India*

Working on an OSS supply chain security platform as part of its Security Research Team, focusing on vulnerability research, static analysis, and developer security workflows across large-scale codebases.

- **Security Research:** Conducted security research on OSS vulnerability patterns, developing AI-assisted static analysis workflows that enabled discovery and coordinated disclosure of multiple zero-day vulnerabilities.(*CVE-2025-13780*, *CVE-2025-66626*)
- **Rapid Response**: Analyzed newly disclosed high-severity OSS vulnerabilities affecting customer environments, delivering rapid impact assessments and technical remediation guidance to reduce customer mean-time-to-mitigation; performed root cause analysis to identify detection and supply-chain gaps..
- **Vulnerability Database**: Develop and maintain high-throughput vulnerability ingestion workflows; built Slack and GitHub automation to improve validation efficiency, reducing vulnerability PR creation time from 3 hours to under 2 minutes and routing validated findings into engineering ingestion pipelines;and tuning rules to improve reliability and reduce false positives.
- **SAST Development**: Authored 80+ Semgrep rules covering deserialization, path traversal and dynamic exec patterns, expanding detection coverage across customer codebases.

Tools & Platforms: *Python, Semgrep/Opengrep, Cursor, Github Workflows, LLM-assisted tooling, Agentic AI workflows*

Product Security Engineer II **July 2023 - August 2024**
Product Security Engineer I **July 2022 - July 2023**
Product Security Intern **Jan 2022 - June 2022**
VMWare by Broadcom *Bangalore, India*

Worked on security of VMware Cloud Foundation (VCF) and SaaS products (NSX, HCX, vRO) as part of the vSECR team, focusing on threat modeling, penetration testing, and secure design reviews for cloud infrastructure components.

- **Baseline Security Testing**: Conducted penetration testing across NSX, HCX, and vRO SaaS deployments, identifying 40+ high-severity security bugs and exploitable misconfigurations that improved hardening guidance for production systems.
- **Secure Design:** Collaborated on threat modeling and secure design reviews for VMware Cloud Foundation components, helping identify privilege boundary and enhancing the security architecture flaws prior to release.
- **Shift-left security**: Developed 50+ Semgrep rules for Go services, improving early detection of critical vulnerabilities and strengthening shift-left security practices.

Tools & Platforms: *Go, Semgrep, Kubernetes, VMware Cloud Foundation, NSX*

CTF Team Lead & Security Mentor **Aug 2018 - Dec 2021**
Team bi0s *Kollam, India*

Led the Cryptography Team, building offensive security fundamentals through CTF participation, challenge development, technical training, and community initiatives as a part of Team bi0s

- **Offensive Security & Cryptography:** Led cryptography-focused CTF problem solving and mentored team members in offensive security and cryptanalysis techniques.
- **Mentorship & Challenge Development:** Designed and authored CTF challenges and hands-on training content to strengthen security skills within the community.
- **Community Leadership:**Organized security workshops and technical trainings demonstrating strong verbal communication skills in national and international conferences.

Tools & Platforms: *iPython, cryptography libraries, Docker, Burp Suite, Linux*

PROJECTS

AI-Assisted Zero-Day Discovery Pipeline **2026**

Built an AI-driven zero-day discovery workflow within the vulnerability ingestion pipeline by analyzing 150+ security patches to derive vulnerability patterns, enabling discovery and coordinated disclosure of multiple zero-day vulnerabilities in widely deployed open-source libraries.

AI Supply Chain Attack Forensics **2026**

Built a simulated AI supply chain attack environment using Windows VM and mobile forensic images, with CTF challenges to demonstrate attack vectors and forensic investigation techniques.

Secure API Key Management CLI **2025**

Designed and developed a CLI tool for secure API key and recovery code management, using session-based key retrieval and injection to avoid reliance on environment variables.

SKILLS

- **Programming Languages**: *Scripting/Dev:*Python, Bash, Golang; *Code review:* C++/C, Rust, Java
- **Security Tools**: Semgrep / Opengrep, Burp Suite, Kali Linux
- **Platforms & Infrastructure**: Docker, Kubernetes, Linux
- **Automation & AI:** GitHub Actions, SAST, claude , LLM-assisted tooling, Agentic AI workflows

EDUCATION

Master of Technology, Cybersecurity and Digital Forensics **2025-present**
Indian Institute of Information Technology, Kottayam, India ***SGPA :*** *9.5/10*

Bachelor of Technology, Computer Science Engineering **2018-2022**
Amrita University, Kollam, India ***CGPA :*** *9.73/10*

SPEAKER ENGAGEMENTS & ACHIEVEMENTS

- **AI Security 101**, *InCTF Conference, 2026*
- **Efficiency with Feasibility: Securing Your Supply Chain**, *bi0s meetup, 2024 [link]*
- **Linux Privilege Escalation for Beginners**, *bi0s meetup, 2023 [link]*
- **BSides W2CTF Winner 2023***[link]*
- **Intro Codes and Ciphers**, *Shakticon, 2021 [link]*
- **Levelling up Estrogen in the CyberWorld**, *Diana Initiative 2020 [link]*
- **BlackHat USA Student Scholar**, *2020 [link]*