Devang Jain

devangjain239@gmail.com | devangjain.com
linkedin.com/in/djrobin17 | github.com/djrobin17 | djrobin17.medium.com

WORK EXPERIENCE

Applied Intuition, Security Engineer, Sunnyvale, CA, USA **Sep 2026 - Present**

- Drive offensive (purple-team) security across Applied's Vehicle OS, Self-Driving System (SDS), and OTA / remote command-center backends, conducting penetration testing, code review, and hands-on security testing of embedded, firmware, and connected-vehicle systems using manual analysis and automated tooling.
- Lead security verification and validation (V&V) initiatives as the point of contact for security V&V, standing up hardware benches for penetration tests and risk assessments in an automotive environment.
- Recommend and implement defensive techniques and secure-design improvements, coordinating with core software teams to drive long-term remediation of high-impact vulnerabilities across connected and autonomous vehicle architectures.
- Perform threat modeling and formal risk assessments to prioritize threats and mitigations by risk, partnering across business units and with software, safety, and systems engineering to develop secure automotive products aligned with ISO/SAE 21434 and UN R155.

Harbor Labs, Senior Research Scientist, Baltimore, MD, USA **Feb 2024 - Aug 2026**

- Led 30+ end-to-end security assessments, penetration tests, and code reviews for medical device manufacturers, spanning web and mobile applications, cloud infrastructure, connected and embedded systems, firmware, hardware, software, and protected health information (PHI), directly enabling client products to obtain FDA regulatory clearance.
- Partnered with 15+ client teams across engineering, product, regulatory, and quality compliance functions to risk-assess and remediate 200+ critical and high-severity vulnerabilities and drive shift-left architectural and design changes across the SSDLC, while mentoring 4+ junior researchers on vulnerability triage, exploit validation, V&V, and client-facing communication.
- Authored and owned cybersecurity compliance documentation, including eSTAR pre-market submissions, post-market surveillance processes, SBOMs, and threat models (Attack Trees, STRIDE, Attack Chains), aligned with FDA guidance, AAMI TIR57, AAMI/ISO 14971, IEC-62304, and IEC 81001-5-1, for multiple Class I, II, and III medical devices.
- Spearheaded internal tooling and team-wide assessment playbooks, architecting AI-augmented workflows with locally-hosted LLMs (Ollama) for privacy-preserving analysis of sensitive client data, alongside automated triage and report-generation pipelines that improved engagement consistency and reduced repeat findings.

EDUCATION

Johns Hopkins University, Baltimore, MD, USA **Aug 2022 - Dec 2023**

- Degree: Master of Science in Security Informatics | GPA: 3.99/4 | TA: Security and Privacy in Computing (Fall 2023)

Indian Institute of Technology (IIT) Goa, India **Aug 2018 - July 2022**

- Degree: Bachelor of Technology in Computer Science and Engineering | GPA: 3.64/4

RESEARCH

Industrial Research Advisor, Johns Hopkins University **Jan 2026 - Present**

- Advising a team of 5 graduate student researchers on "Sweet Targets: A Security Analysis of Regulated Diabetes Monitoring Devices," leading threat modeling, methodology design, and hands-on security evaluation of FDA-regulated CGMs and BGMs across BLE, NFC, companion mobile apps, and backend infrastructure.
- Mentoring students on offensive security techniques and guiding coordinated vulnerability disclosure, CVE submission to MITRE, and open-sourcing of research artifacts to advance medical device security.

TECHNICAL SKILLS

- **Programming:** Python, C/C++, Bash, Rust
- **Operating Systems & Architectures:** Linux, macOS, Windows, Android, iOS, FreeRTOS; ARM, AArch64, x86/x86-64
- **Application & Product Security:** SAST, DAST, SCA, OWASP Top 10, Threat Modeling, SSDLC, DevSecOps, Code Review, API Security, VAPT
- **Hardware & Firmware Security:** JTAG, SWD, UART, Serial Console, Chip Enumeration, Firmware Extraction, Secure Boot, Fuzzing
- **Hardware Hacking:** GreatFET One, J-Link Segger, Ubertooth One, Chameleon Ultra DevKit, USB-to-TTL, JTAGulator, Binwalk, Ghidra
- **Mobile & Wireless:** BLE, NFC, RFID, Wi-Fi, LightBlue, nRF Connect, jadx, MobSF, Frida, ADB
- **Penetration Testing:** Kali, Burp Suite, Charles Proxy, OWASP ZAP, Nmap, Wireshark, Nessus, TestSSL, SonarQube, Dependency-Track, CycloneDX, Syft
- **Cloud & Infrastructure:** AWS, Azure, GCP, Docker, Kubernetes, CI/CD, IAM, TLS/mTLS, PKI, HSM, KMS
- **Standards & Frameworks:** NIST CSF, MITRE ATT&CK, FDA Premarket Cybersecurity, IEC-62304, AAMI/ISO 14971, AAMI TIR57, IEC 81001-5-1, ISO 27001, HIPAA
- **AI/ML Security:** OWASP Top 10 LLM, Adversarial ML, Prompt Injection, Ollama, Claude, Cursor, Copilot
- **Certifications:** CompTIA Security+, CNSS

PUBLICATIONS

- "ScottCare Aermos™: Secure By Design Whitepaper," 2026 - Link available upon request.
- Acknowledged contributor for IEEE publication, "Compliance without Completeness: A Case Study on SBOMs in Light of FDA Premarket Cybersecurity Guidance," 2025 - https://ieeexplore.ieee.org/document/11418023.
- Devang Jain and Sharad Sinha, "SolSec Labs: Virtual Labs for Learning Smart Contracts Security," IEEE Potentials, Nov 2022 - https://ieeexplore.ieee.org/document/9935793.