PARTH BHATT

Faridabad, India | +91 8920948990 | paarthbhatt37@gmail.com

Portfolio | GitHub | LinkedIn

TECHNICAL SKILLS

Security & Research: LLM Security, Prompt Injection Mitigation, Autonomous Reconnaissance, Threat Intelligence, SOC Operations, Penetration Testing, OSINT.
Tools & Platforms: Linux (Debian/Kali), Nmap, Metasploit, Burp Suite, Wireshark, Docker, Git, Bun, PostgreSQL, Redis.
Languages & Frameworks: Python, TypeScript, JavaScript, C++, Next.js 15, React 19, Three.js, Tailwind CSS 4, Zustand.
Specialized: Model Context Protocol (MCP), Agentic Workflows, 3D Physics Engines, Real-time HUD Architectures.

ACHIEVEMENTS & TROPHIES

2nd Place – Hackfest 2.0 | GDG Cloud New Delhi & Turgon AI | Feb 2026
Secured Top 3 among 500+ innovators in a 24-hour rapid development hackathon.

Top 1% Rank (Global) | TryHackMe | 2024–2025
Verified Top 1% ranking on a global cybersecurity training platform; completed SOC Level 1 and Junior Pentester pathways.

9x Technical Certifications Verified | Portfolio Scan | 2025
Authenticated credentials across Cybersecurity, Cloud Infrastructure, and Full-Stack Development.

Standout Tech Innovator | University Recognition | 2024
Recognized for initiative in high-agency projects and open-source contributions.

TECHNICAL PROJECTS

Entropy Firewall (Open-Source LLM Security) | Python, AI Security
• Architected a production-ready firewall to intercept and analyze LLM requests/responses in real-time.
• Implemented 28+ regex patterns across 8 OWASP-aligned categories for prompt injection and jailbreak detection.
• Engineered a Redis-backed rate limiter and PII redaction engine with sub-millisecond latency.

ROBIN (Autonomous Security Research Agent) | TypeScript, Bun, Agentic AI
• Developed a Reconnaissance & Operations Bot for Intelligence Networks (ROBIN) built on autonomous task planning.
• Integrated GitHub CLI and NVD database for deep repository analysis and real-time CVE correlation.
• Designed a self-validating agentic loop for automated technical intelligence gathering.

USS Enterprise NCC-1701 Flight Simulator | Next.js 16, Three.js, TypeScript
• Built a 16,000+ line immersive 3D flight simulator featuring Newtonian physics and real-time planetary rendering.
• Engineered a custom LCARS-inspired HUD architecture with warp drive mechanics and destructible planet systems.
• Implemented a high-performance First-Person bridge interior using complex state management (Zustand)..

MRP-OPT-97 (High-Efficiency Token Framework) | Python, Orchestration
• Designed a performance framework achieving 97% token efficiency in multi-agent communication.
• Reduced API overhead and operational costs for autonomous agent handoffs.

EDUCATION

B.Tech in Computer Science & Engineering | Expected 2028
Faridabad, India | Focusing on Cybersecurity and Advanced Autonomous Systems.