Vishnu Kosuri

Bangalore, India | +91 7842829009 | kvr.vishnu23@gmail.com | linkedin.com/in/vishnu-kosuri | github.com/VISHNU0906 | vishnu.aresredteam.com

EDUCATION

B.Tech, Cyber Security, Jain (Deemed-to-be) University, FET 2023 - 2027

WORK EXPERIENCE

Founder & CEO, ARES RED TEAM Bangalore | Dec 2025 - Present

- Building an AI for continuous penetration testing on production web, API, and infrastructure targets; persistent memory layer reuses attack patterns from prior engagements.
- Architected human-in-the-loop validation that gates every AI-generated finding before a customer report ships.
- Selected: 1752 Ventures Accelerator (2026), Y Combinator Startup School India (Bangalore, Apr 2026).

Security Lead, Founder's Office, Vahini Technologies Bangalore | Dec 2024 - Dec 2025

- Led firmware and IoT security for an IMU-based handwriting device for accessibility; reverse engineered BLE, NFC, and SPI protocols using Ghidra; identified hardcoded credentials in shipping firmware.
- Filed Patent No. 584433 (Government of India, granted Mar 2026): *Handwriting Recognition with an Intelligent Ballpoint Pen Using IMU Sensors*; deployed as a pilot across 5 schools.
- Led GTM and product strategy: pricing model, school pilot rollout, and hiring across firmware, app, and web teams.

Security Consultant, Tapnex (NexGen FC) Remote | Jul - Oct 2025

- Audited NFC cashless event platform; identified 11 vulnerabilities including MFA bypass, reflected XSS, and IDOR-based privilege escalation.
- Designed the secure NFC wristband payment workflow that shipped to production for live events.

Penetration Testing Intern, ISAC, National Security Database India | Jun - Aug 2024

- Conducted web application penetration tests on 2 commercial production sites; reported 18 vulnerabilities (5 rated critical) with CVSS v3 scoring.
- Standardized the team's client reporting workflow using a templated CVSS+remediation format; reduced average report turnaround by 30%.
- Earned the Professional Ethics Certification on completion of the 15-week structured industry program.

Cybersecurity Intern, iHUB DivyaSampark, IIT Roorkee & Diginique TechLabs Roorkee | Jul - Sep 2024

- Built an Nmap-based reconnaissance scanner in Python; performed OWASP Top 10 analyses on 2 live production websites.
- Surveyed 41 active bug bounty programs across HackerOne, Bugcrowd, and Intigriti; produced a comparative report on scope and payout structures.

ACHIEVEMENTS

- **29+ production vulnerabilities** disclosed across government, enterprise, and fintech systems (5 rated critical).
- **$20,000+ bug bounty payouts** on HackerOne, Bugcrowd, and via direct disclosure programs.
- **154 merged pull requests across 88 open-source projects**: NumPy, Django, FastAPI, SciPy, Pandas, Scikit-learn, OWASP Nettacker, Impacket, Scapy, NetworkX, Starlette, Celery, Scrapy.
- **$25,000 SANS Cyber Academy scholarship**: 3rd of 3,000+ participants in a SANS Capture-the-Flag (2025).
- **Patent No. 584433** (Government of India, 2026): IMU-sensor handwriting recognition pen; deployed across 5 schools in pilot.

COMPETITIONS

- **SANS NetWars Tournament Core Champion**, 1st place (2026).
- **OWASP AppSec Bangalore BeSec CTF**, 1st place, Web Application Security track (2025).
- **SANS Capture-the-Flag**, 3rd place of 3,000+ participants (2025); converted to the SANS Cyber Academy scholarship listed above.
- **SANS Veterans Day CTF**, 6th place (2026).

PROGRAMS AND FELLOWSHIPS

- **Y Combinator Startup School**, India cohort, Bangalore (April 2026).
- **1752 Ventures Accelerator** (2026): going through the program with ARES RED TEAM.
- **Founder Inc.** alumnus (2025): selected fellow of the program for student founders.
- **McKinsey Forward Program** (2025): completed cohort.

CERTIFICATIONS

GIAC GFACT, 99th percentile, SANS Institute (2024) | **CEH v12**, EC-Council (2024) | **eJPT**, INE Security (2025) | **GSEC**, SANS Institute (2026) | **GCIH**, SANS Institute (2026).

PROJECTS

ARES RED TEAM 2025 - Present | aresredteam.com

- AI-driven continuous penetration testing platform built on a custom agent loop with persistent memory across engagements, MCP-style tool registry over 150+ security utilities, and human-in-the-loop validation gating every finding before it ships.
- Targets web applications, REST/GraphQL APIs, internal infrastructure, and AI/LLM application surfaces; multi-model ensemble (Anthropic Claude, OpenAI GPT, local Llama) chooses tools and chains exploits.

AI Vulnerability Scanner NCIIPC AI Grand Hackathon 2024 | github.com/VISHNU0906/vulnerability-scanner

- Multi-language SAST scanner aggregating 6 static-analysis tools (Semgrep, Bandit, Flawfinder, Cppcheck) with retrieval-augmented LLM enrichment using locally-hosted CodeLlama and DeepSeek.
- Implemented multi-model voting consensus to reduce false positives; auto-generates Excel reports with CVSS v3 scores, CWE/CVE mappings, and OWASP category labels for Python, Java, C/C++, and PHP codebases.

AI-Nova Wellness Assistant University Project 2024 - 2025 | Flutter, Python, MySQL, IoT

- Cross-platform health monitoring application integrating IoT wearable sensor data with a Python backend and MySQL persistence; features authentication, hydration / workout / symptom logging, mental wellness tracking, and personalized health recommendations.
- Demonstrated as AI-Nova prototype at university hackathons; delivered Phase-2 project report with UML diagrams, pseudocode, and implementation walkthroughs.

Automated Pentest Recon Framework 2024 | Python, Nmap, Metasploit API

- Modular pentest automation tool that chains Nmap host discovery, vulnerability scanning, and Metasploit exploit suggestions; cuts initial reconnaissance time on a 24-host environment from ~6 hours to under 90 minutes.

POSITIONS OF RESPONSIBILITY

- **Founder, Salus Cybersecurity Club**, Jain University (2023 - Present): grew chapter to 200+ active members; ran 3 inter-college CTFs. Hosted 5+ industry-expert workshops and mentored 50+ students in offensive security and penetration testing; multiple alumni now disclose vulnerabilities on production bug bounty programs.
- **Research Analyst, CSAI R&D Cell** (2024 - 2026): contributed to research under Lt. Gen. (Dr) Rajesh Pant, India's former National Cyber Security Coordinator at the Prime Minister's Office. Authored explainers on IoT, embedded, and BLE side-channel threats for the team's industry-advisory output.
- **AWS Cloud Captain** (2025 - 2026): built campus cloud-security community; delivered 4 workshops to 150+ students on AWS IAM, S3 misconfigurations, and infrastructure hardening. Authored hands-on lab guides and maintained the campus AWS security learning-resource set used by Jain University FET.
- **Cyber Security Facilitator, Google Developer Groups On Campus**, FET, Jain University (2025 - 2026). Led web application pentesting and OWASP Top 10 sessions for the developer community; promoted secure-by-default coding practices in student hackathon teams.

TECHNICAL SKILLS

AI / ML: LLM operations across Anthropic Claude, OpenAI GPT, and open-weights models (Llama, Qwen, DeepSeek, CodeLlama); retrieval-augmented generation (RAG) with vector stores; multi-model ensemble voting for triage; prompt evaluation and red-teaming; offensive-security agents for vulnerability discovery, fuzz target generation, and exploit-chain reasoning; sensor-data ML (Kalman filters, CNN+RNN hybrids) for IMU handwriting recognition.
Agent Engineering: agent harness design (single-loop and dispatcher patterns); REPL and CLI tool development on top of pexpect / Typer / Rich; multi-agent systems with orchestrator and specialist roles, hand-off and shared context patterns; tool registry over Model Context Protocol (MCP); persistent memory layers combining FTS5, vector indices, and graph stores; evaluation harnesses with regression testing.
Languages: Python, JavaScript / TypeScript, Bash, C, SQL, Dart (Flutter), HTML / CSS.
Penetration Testing: web application, REST / GraphQL APIs, NFC and embedded systems, IoT firmware, BLE / SPI protocol analysis, Active Directory, OWASP Top 10, PTES.
Security Tools: Burp Suite, Nmap, Metasploit, Impacket, OWASP Nettacker, OWASP ZAP, Ghidra, Wireshark, sqlmap, ffuf, Nuclei, Nikto, John the Ripper, Hashcat, Aircrack-ng, Semgrep, Bandit.
Cloud and Infrastructure: AWS (IAM, S3, EC2, security misconfiguration audits), Google Cloud Platform, Docker / Docker Compose, GitHub Actions, CI/CD pipelines, Linux system administration.
Frameworks and Data: Flutter, React, FastAPI, Django, Node.js; PostgreSQL, MySQL, MongoDB, Firestore.
Reporting and Compliance: CVSS v3 scoring, SARIF, OWASP Testing Guide, structured client penetration test reports, security.txt and disclosure-policy advisory.

LANGUAGES

English (Fluent, Professional Working Proficiency) | **Telugu** (Native).