AJMAL M S

Cybersecurity Specialist | Penetration Tester | Red Team Operator (CRTA) | Application Security | CTF Developer

Pathanamthitta, Kerala, India | +91 85905 08376 | hireajmal@gmail.com | linkedin.com/in/ajmalms | github.com/AjmalX0 | ajmalx0.dev

Also a software engineer – see my Software Engineer resume (attached inside this PDF): ajmalx0.dev/assets/resume-engineering.pdf

PROFESSIONAL SUMMARY

Cybersecurity engineer, penetration tester and CTF developer, doing freelance cybersecurity and software development work since 2019 through multiple platforms and direct referrals. Performed web, API and infrastructure security assessments in production as a Cyber Security Engineer at RzQuick.app and is listed in the NASA Vulnerability Disclosure Program Hall of Fame. Certified Red Team Analyst (CRTA) and CNSP, top 1% on TryHackMe, experienced in Active Directory compromise, Kerberos abuse, pivoting, lateral movement and post-exploitation mapped to MITRE ATT&CK. Designs CTF challenges and platforms, and builds security tooling in Rust, Python and TypeScript: an eBPF runtime threat-detection and blocking sensor, a cryptographic chain-of-custody engine for digital forensics and a vulnerability intelligence graph. Years of full-stack development make findings and remediation advice precise and code-level. Maintains 368 GitHub repositories (public and private), almost all original projects.

TECHNICAL SKILLS

Security Tools: Burp Suite Professional, Metasploit Framework, BloodHound, Impacket, NetExec (CrackMapExec), Mimikatz, Rubeus, Responder, Ligolo-ng, Chisel, sqlmap, ffuf, Nuclei, Hashcat, John the Ripper, OWASP ZAP, Nmap, Wireshark

Offensive Security: Penetration testing (VAPT), web application and API pentesting, OWASP Top 10 and API Security Top 10, red team operations, adversary simulation, exploitation, post-exploitation, privilege escalation, reconnaissance and OSINT

Active Directory & Infrastructure: AD enumeration and attack paths, Kerberoasting, AS-REP roasting, pass-the-hash and pass-the-ticket, lateral movement, network pivoting and tunneling, Living Off the Land (LOLBAS), Linux and Windows privilege escalation

Defense, Detection & Forensics: eBPF runtime detection, detection engineering (MITRE ATT&CK), Splunk, Wazuh, Sysmon, log analysis and incident triage, Volatility, Autopsy, Ghidra (reverse engineering), vulnerability management, CVSS risk rating, secure code review, threat modeling, cloud and configuration review

Operating Systems: Kali Linux, BlackArch Linux, Parrot OS, Arch Linux, Ubuntu/Debian servers, Windows Server and Active Directory, Windows 10/11

Programming: Python, Bash, Rust, C, PowerShell, TypeScript, JavaScript, SQL, PHP; React, Next.js, Node.js, FastAPI, Django, PostgreSQL, Docker, Kubernetes basics

PROFESSIONAL EXPERIENCE

Freelance Cybersecurity & Software Development **2019 – Present**

Self-employed (multiple freelance platforms and direct clients), Remote

- Freelancing since 2019 in both cybersecurity and software development. Closed and delivered cybersecurity engagements including web and API penetration tests, vulnerability assessments, configuration reviews and remediation guidance with re-testing.
- Delivered software development projects end to end for clients: web platforms, admin dashboards, mobile apps, WhatsApp bots and CRM automation, built secure by default.

Cyber Security Engineer – Application Security & Pentesting **Oct 2025 – Nov 2026**

RzQuick.app, Kochi, India

- Conduct web application and API penetration tests aligned with OWASP Top 10 and API Top 10, finding and exploiting SQL injection, XSS and broken authentication before deployment.
- Run API attacks including authentication bypass, JWT forgery and manipulation, rate-limit abuse and parameter tampering.
- Perform vulnerability assessments with CVSS-based risk ratings and written reports; re-test to confirm each patch works after remediation.
- Review cloud infrastructure and system configurations for misconfigurations; assess access control and data-handling practices.
- Monitor the security posture of applications and systems, review logs for incident triage, and help developers adopt secure coding practices.

CTF Developer **Jul 2025 – Present**

Cyber Club, College of Engineering Kallooppara, Kerala, India

- Design and build Capture-The-Flag events for colleges: challenges in web exploitation, cryptography, forensics, OSINT and reverse engineering, plus the platform and infrastructure that host them.

Technical Lead (2025–26 term); now Vice Chair **Jul 2025 – Apr 2026**

Cyber Club, College of Engineering Kallooppara, Kerala, India

- Led the club's technical activities, conducted multiple online and offline cybersecurity sessions and hands-on workshops, and mentored students in ethical hacking and CTFs; Vice Chair since Jul 2026.

Full Stack Developer **Jan 2025 – Jul 2026**

Coxdo Solutions, Kochi, India (Hybrid)

- Built full-stack applications (Django, React, Next.js, MERN) with secure REST APIs, authentication flows and backend logic on PostgreSQL and MongoDB, applying input validation and access control by default.

CERTIFICATIONS

- **Certified Red Team Analyst (CRTA)** – CyberWarFare Labs, Jan 2026. 6-hour hands-on practical exam: Active Directory, Kerberos attacks, pivoting, lateral movement, MITRE ATT&CK. Credential ID 695a712c350a0624a438152e
- **Certified Network Security Practitioner (CNSP)** – The SecOps Group, Nov 2025. Credential ID 10776026
- **Certified Cybersecurity Educator Professional (CCEP)** – Red Team Leaders, Nov 2025

SECURITY PROJECTS

K-Guard – eBPF Runtime Security Sensor for Linux and Kubernetes
Tech: Rust, eBPF (CO-RE), BPF LSM, C, Kubernetes, Helm, Prometheus, OpenTelemetry

- Built a single-binary kernel sensor that watches process, file, network and privilege activity, with 32 MITRE ATT&CK-mapped detection rules (reverse shells, container escapes, credential access, Kubernetes service-account token theft, cryptominers), each with a replayable attack simulation.
- Blocks malicious actions in the kernel through BPF LSM policy maps (monitor → audit → enforce rollout); learn mode generates allowlist policies; outputs ECS JSON, Slack, OpenTelemetry and Prometheus; 48 tests plus fuzz targets; Helm DaemonSet.

ProofTrail – Verifiable Digital Evidence and Chain-of-Custody Engine
Tech: Rust, Python, SHA-256/SHA3-256, RSA signatures, RFC 6962 Merkle trees

- Hashes evidence in one streaming pass, seals it in an encrypted store, logs every action in an append-only hash chain and anchors Merkle batch roots to a ledger with warrant-scope enforcement; exports signed court packages verifiable offline with Rust, Python or sha256sum/OpenSSL, pinpointing any tampered record.

VulnGraph – Vulnerability Intelligence & Application-Security Graph
Tech: Python, FastAPI, Celery, PostgreSQL, Neo4j, Next.js, Docker

- Correlates CVE, NVD, OSV, GitHub Advisory, CISA KEV and EPSS data with lockfile dependencies across 15+ ecosystems, ranks findings with an explainable risk model and proposes minimal safe upgrades; its AI investigator has prompt-injection defenses and verified citations.

Cyber Club CTF Portal – Secure Capture-The-Flag Platform
Tech: Next.js 15, TypeScript, Supabase (PostgreSQL RLS), Vitest

- Zero-trust design: every rule enforced by Row-Level Security and SECURITY DEFINER functions, flags never readable by players, no service-role key in the app, advisory-locked rate-limited submissions; 70+ database tests including concurrency.

SentriUI – Security-First React UI Framework (in development)
Tech: React, TypeScript, DOMPurify, Zod

- Secure forms (sanitization, Unicode normalization, javascript: URL and DOM-clobbering protection, CSRF tokens), RBAC-aware dashboard, MFA/OTP auth kit, signed-request API client with replay nonces, and an XSS/JWT/CSRF testing playground.

CyberSahayi – Cyber-Fraud Victim Response Assistant
Tech: TypeScript, Node.js, Next.js, Supabase, Claude API

- WhatsApp assistant that guides fraud victims in Malayalam and English through the golden-hour response, collects evidence safely (masks OTPs and PINs) and generates police-ready complaint packs.

More: 368 GitHub repositories (public and private), almost all original projects, including CTF challenge sets and security tools, at github.com/AjmalX0; private client work available on request.

RESEARCH & ACHIEVEMENTS

- NASA Vulnerability Disclosure Program Hall of Fame (via Bugcrowd) for a responsibly disclosed vulnerability, 2026.
- NASA International Space Apps Challenge 2025 (local event): Best Use of Science award (Senior category) and Top 10 of 500+ teams.
- Published an analysis of CVE-2025-55184: pre-authentication denial of service through unsafe deserialization in React Server Components / Next.js (CWE-502, CVSS 7.5), covering affected versions, patches and mitigations.
- Top 1% on TryHackMe; completed all 24 challenges of TryHackMe Advent of Cyber 2025.
- Chaitanya CTF 2025 (500+ teams): 5th overall and 2nd on server with team 3NDP01NT (17,866 points) across web exploitation, forensics, OSINT, reverse engineering and cryptography.

EDUCATION

Bachelor of Technology (B.Tech), Computer Science and Engineering (Cyber Security) **Sep 2024 – Jun 2028 (Expected)**
College of Engineering Kallooppara, APJ Abdul Kalam Technological University (KTU), Kerala

LEADERSHIP & COMMUNITY

- **Speaker** – Conducted multiple online and offline cybersecurity and ethical hacking sessions, including SKILLFORGE 2.0 (ISTE SC RIT), Jun 2026
- **Mentor** – Hackathon mentor at Tech Thrive 2.0 (24-hour hackathon, RIT Kottayam) and mentor to students in CTFs and security
- **Finance Lead (Jan 2026 – Present)** – IEDC, College of Engineering Kallooppara

LANGUAGES

English (professional working proficiency – speaking, reading, writing), Malayalam (native), Hindi (professional working proficiency)