Subadevan C

Security Researcher | Web & API Penetration Tester (VAPT)

Chennai, India | +91 86376 07481 | subadevanc@gmail.com | linkedin.com/in/subadevan | hackerone.com/subadevan

PROFESSIONAL SUMMARY

Security researcher and final-year B.E. Computer Science and Engineering (Cybersecurity) student specializing in web application and API security testing. Experienced in identifying and responsibly disclosing vulnerabilities to Vercel, Instacart, Sony, JPMorgan Chase, WHO, UNESCO, Porsche and ZKTeco. Earned bug bounty rewards from Vercel ($400), Instacart ($250) and ZKTeco (INR 18,000). First-place finishes in six cybersecurity competitions, including CTF and bug bounty events. Hands-on with Burp Suite, Nmap, Nessus, Qualys, CVSS-based risk assessment and technical security reporting.

TECHNICAL SKILLS

- **Web & API VAPT:** OWASP Top 10 (Web), XSS, SQL Injection, IDOR / Broken Access Control, Authentication Bypass, Information Disclosure
- **Tools:** Burp Suite, OWASP ZAP, Metasploit, Nmap, sqlmap, Nikto, Wireshark, Nessus, Qualys
- **Methodologies & Reporting:** PTES, CVSS, Recon & Attack Surface Mapping, Code Review, Security Reporting, Responsible Disclosure
- **Cloud Security:** AWS IAM, VPC & Security Groups, AWS Security Hub, Network Hardening, Security Audits
- **Scripting & OS:** Python, Linux (Kali, Ubuntu)

SECURITY RESEARCH & BUG BOUNTY

- **Vercel (Open Source) – Flags SDK ($400 bounty):** Identified a stateful regular-expression flaw that leaked state across evaluations; recommended a fix; report accepted.
- **Instacart – API Security Vulnerability ($250 bounty, May 2026):** Reported through the bug bounty program; triaged and resolved by Instacart.
- **Sony – DOM-based XSS and Broken Access Control (May 2026):** Reported two vulnerabilities through Sony's VDP; both confirmed and remediated.
- **ZKTeco – Authentication Bypass (INR 18,000 reward):** Reported an authentication bypass vulnerability; recognized with a cash reward.
- **Additional responsible disclosures:** JPMorgan Chase, WHO and UNESCO (exposed .git data) and Porsche (authentication bypass).

EXPERIENCE

DevSecOps Intern, TechForce Services (Salesforce ecosystem) Chennai, India | Jun 2025 – Jul 2025

- Served as the security team member on a project migrating the open-source Kimai application to a containerized AWS and GCP deployment.
- Designed 3 least-privilege IAM roles (Jenkins, App Server, Bastion), each scoped strictly to its service's requirements.
- Hardened the network architecture: application and database in private subnets, bastion-only key-based SSH, inbound traffic restricted to ports 22 and 80, and an encrypted RDS instance.
- Verified network exposure before deployment using Nmap port scans and AWS Security Hub audits.

COMPETITIONS

- **First-Place Finishes (6):** ISACA Thiruvananthapuram CTF; TEXUS'25 Bug Bounty Hunt (SRM-RMP); Boot2Root (VIT); Hack With Jolu 2026 (JGEC); CyberHant CTF (Sai Ram Institute of Technology); JCE CTF
- **Runner-up (2nd Place):** Network Security CTF, CEG Anna University (ISEA-III); CipherCase 24-hour CTF (Cycoms, VIT); ZYVERSE / ARCADIA / WTF 3.0 CTFs (SRM-KTR); Bastion Boot2Root (Chat-Club)
- **Podium and Finalist:** 3rd, Multiverse Breach CTF (LICET); Top 3, Cybershield Hackathon (Amrita Vishwa Vidyapeetham); Top 5, HackathonX Semi-Finals (NCSRC); Top 12, DCG Coimbatore CTF 2026; Top 15, Kalchakara'26 CTF Finals (NFSU Goa)

LEADERSHIP

- **President, CyberNexus Club, JCE (Feb 2025 – Present):** Organized 10+ cybersecurity events, including inter-college CTFs, workshops and technical sessions.
- **Co-Founder, Flaggers United (Apr 2024 – Present):** Design CTF challenges and onboard new players.

EDUCATION

Jerusalem College of Engineering, Chennai, India: B.E. Computer Science and Engineering (Cybersecurity) Nov 2023 – May 2027

CERTIFICATIONS

Certified Cybersecurity Educator Professional, CCEP (Red Team Leaders, Dec 2025) | Junior Penetration Tester and Pre Security (TryHackMe, 2025) | Google Cybersecurity (2024) | Cisco Networking (2025)

LANGUAGES

Tamil | English