Abhishek Chayadri Vaidya

Dallas, Texas | 945.367.2111 | abhishekcv.us@gmail.com | LinkedIn | GitHub | Portfolio | Blog

CompTIA Security+ | ISC2 Certified in Cybersecurity (CC) | TryHackMe Top 1% (Global)

PROFESSIONAL SUMMARY

Cybersecurity M.S. student (GPA 3.89) with enterprise security experience on Boeing's HR platform at TCS: RBAC, API hardening, secure CI/CD gates. 5× TCS award recipient; TryHackMe Top 1%; HIPAA manuscript in preparation with faculty.

EDUCATION

University of Texas at Dallas | M.S., Cybersecurity, Technology and Policy **Expected May 2027**

Dallas, TX | GPA: 3.89 | Founder, Pixelora (product studio, active)

- Coursework: Cyber Security Essentials, Data Security & Privacy, Digital Forensics & Incident Mgmt, Conflict in Cyberspace

Visvesvaraya Technological University | B.E., Electronics and Communications **June 2023**

SKILLS

- **Security:** SIEM (Elastic), Threat Detection, Alert Analysis, Threat Hunting, Incident Response, Vulnerability Assessment, Log Analysis, Digital Forensics
- **Frameworks & Compliance:** OWASP Top 10, NIST CSF, Zero Trust Architecture, HIPAA, RBAC, IDS/IPS, Firewalls, Linux
- **Networking & Tools:** TCP/IP, DNS, HTTP/S, Wireshark, Nmap, Snort, SpiderFoot, Burp Suite, OWASP ZAP, Postman, Nessus, SonarQube
- **Cloud / DevSecOps:** Azure, AWS, Docker, Kubernetes, CI/CD, Supabase | Python, TypeScript, Node.js, Java, SQL, MongoDB

PROFESSIONAL EXPERIENCE

University of Texas at Dallas | Student Assistant Developer **Nov 2025 – Present**

Dallas, TX

- Independently built an inventory management application (Next.js, Supabase/PostgreSQL) consolidating fragmented device datasets into one searchable scanning/tracking platform; adopted team-wide and recognized by university staff.
- Secured the platform with Supabase authentication and role-based access control (alert-list export restricted to the supervisor role), enforced server-side through PostgreSQL Row-Level Security policies.
- Implemented input validation on user-facing forms and remediated over-permissive API endpoints application-wide.

Tata Consultancy Services | Full Stack Developer (Security Focus) **Feb 2024 – May 2025**

Maharashtra, India | Boeing Program | 5× TCS Award Recipient

- Implemented role-based access control across Boeing's core HR application: enforced role checks on restricted pages, filtered API responses to return only role-authorized fields, and gated UI actions by permission across 40+ REST endpoints, closing 6+ authorization gaps spanning frontend and backend (React, Spring Boot, SQL).
- Remediated legacy API endpoints that over-exposed data, redesigning responses to return minimal, role-scoped payloads; introduced lazy loading on data-heavy HR tables so only in-view, authorized records are retrieved.
- Enforced a SonarQube security quality gate (90%+ required) in the CI/CD pipeline for every production branch, identifying and remediating code vulnerabilities and security hotspots before release.
- Closed 120+ development and production tickets (Jira, ServiceNow) across change packages valued at $5K–$30K each; earned 2× Star of the Month for delivery leadership and an On-the-Spot Award for production support.

EduSkills (Palo Alto Networks) | Cybersecurity Virtual Intern **Mar 2022 – May 2022**

Remote

- Completed hands-on labs in network security, IDS/IPS, and vulnerability assessment; monitored traffic with Wireshark and Snort, detecting 8 simulated intrusions via packet-level analysis.

PROJECT EXPERIENCE

HIPAA-Compliant Hospital Management System **2026**

- Co-developed a HIPAA-aligned hospital platform (Next.js, Supabase/PostgreSQL, TypeScript) in a 4-person team on a Zero-Trust, six-portal architecture isolating PHI by role; manuscript in preparation with UT Dallas faculty.
- Owned the database and encryption layer: designed the complete PostgreSQL schema, built the core hospital management APIs, and implemented AES-256-GCM application-level encryption so PHI remains unreadable even if the database is compromised.
- Contributed to PostgreSQL Row-Level Security (RLS) and a doctor-initiated referral module with time-bound (72-hour) encrypted links; validated enforcement via OWASP ZAP, Burp Suite, and Postman API fuzzing.

Azure Honeypot & Threat Detection Lab **2025**

- Deployed a T-Pot honeypot on Azure, generating 200+ SIEM events and identifying 22+ unique IOCs from SSH brute-force and port-scan campaigns via log correlation, network traffic analysis, and OSINT-based attribution (WHOIS, geolocation).

AWARDS, RECOGNITION & WRITING

- **5× TCS Awards (2024–2025):** Star of the Month ×2 (individual), Best Team ×2, On-the-Spot (emergency production support)
- **Technical Writing:** 3 published Medium articles: Azure Honeypot/SIEM, Secure E-Commerce, CompTIA Security+ (2025)