Manan Shah

Arlington, TX | mananshah237@gmail.com | github.com/Mananshah237 | linkedin.com/in/mananshah237

Education

University of Texas at Arlington — Arlington, TX
B.S. Computer Science & Engineering — *Expected May 2026*
Coursework: Information Security, Software Engineering, Database Systems, Computer Networks, Operating Systems

Technical Skills

Languages: Python, C, C++17, Java, TypeScript, JavaScript, SQL, Bash
Cloud & DevOps: Docker, AWS (EC2/S3/IAM/CloudTrail), GCP, Linux, Git, CI/CD
Security Tools: Trivy, Grype, Snyk, Burp Suite, Nmap, Wireshark, OWASP ZAP, SIEM
Domains: Container/Cloud Security, Penetration Testing, Incident Response, DevSecOps, AppSec

Experience

Research Assistant — Container & Cloud Security | *UTA, Dept. of CSE* — *Jan 2025 – Present · Arlington, TX*

- Spearheaded **original security research** on container vulnerability reduction, constructing an automated multi-scanner pipeline (Docker, AWS, Trivy, Grype, Snyk) that systematically identified and eliminated CVEs across production-grade image datasets.
- Architected **multi-threaded C++17 modules and Bash automation scripts** for real-time vulnerability detection and image debloating, significantly accelerating triage and remediation workflows.
- Translated research into **DevSecOps-ready integration playbooks** with faculty; findings selected for **submission to SCRF 2025**.

Software Engineering Intern — Application Security | *TCN Investments* — *Aug – Dec 2025 · Remote*

- Identified and remediated **critical OWASP Top 10 vulnerabilities** — injection flaws, broken authentication, and insecure direct object references — across production systems via rigorous security-focused code reviews.
- Redesigned **authentication and session management controls**, eliminating credential-based attack vectors and enforcing least-privilege access patterns across internal services.
- Instrumented **granular observability pipelines** to surface anomalous authentication events in real time; embedded automated **security validation gates into CI/CD**, shifting detection left and reducing post-deployment risk.

Software Engineer Intern — Cloud-Native AppSec | *IncuseHR, Hire-to-Retire HRMS* — *May – Aug 2025 · Bengaluru, India*

- Hardened a **cloud-deployed SaaS HRMS platform** protecting enterprise-scale HR data by implementing OWASP controls — input validation, authentication flows, session management, and secure error handling.
- Secured **REST API integrations and compliance-driven workflows**, eliminating data exposure vectors and aligning platform behavior with enterprise privacy mandates.
- Elevated **codebase security posture** through structured peer code reviews enforcing secure coding standards across JavaScript and React production systems.

Projects

PhishNet — AI Phishing Detection & Safe Rewrite Engine | *Python, BERT, NLP, Scikit-Learn*

- Engineered an **end-to-end phishing neutralization system** with fine-tuned BERT classification (94%+ accuracy), an NLP rewrite engine that defangs malicious URLs and strips live payloads, and a secure analyst preview interface — enabling SOC teams to safely dissect active phishing campaigns without direct threat exposure.

AegisScan — Automated Container Scanning & Debloating | *Python, Docker, Trivy, Grype, Snyk*

- Architected a **layered CVE detection and debloating framework** fusing Trivy, Grype, and Snyk; slashed container attack surface by **30–40%** and deployed severity-ranked dashboards that halved remediation triage time, integrated as a pre-release CI/CD security gate.

Cloud-IR-Lab — Cloud Incident Response Laboratory | *Python, AWS, GCP, IAM, CloudTrail*

- Engineered and executed **adversarial cloud attack simulations** (privilege escalation, IAM abuse, S3 exfiltration) across AWS and GCP; developed automated IR playbooks with Python-driven evidence collection and containment, **cutting simulated MTTR by 60%**.

Log-Aggregator & Rate Limiter — Systems Security Libraries | *C, C++17, POSIX, Multithreading*

- Built a **high-throughput multi-source log aggregation engine in C** for real-time security event correlation; paired with a **production-grade C++17 rate limiting library** (token bucket + sliding window) defending APIs against brute-force and application-layer DoS attacks.

Certifications & Interests

Pursuing: CompTIA Security+, AWS Cloud Practitioner **Interests:** CTF Competitions, Open-Source Security Research, Threat Intelligence