Ansh Raj

Security Engineer — Application & Infrastructure Security

+91 9155452233 | theanshchaurasiya@gmail.com | linkedin | Github | Portfolio

About

Security Engineer with 1+ year of hands-on experience in penetration testing, vulnerability management, and DevSecOps across production systems. Proven track record of uncovering critical security weaknesses in real-world applications and infrastructure, and engineering controls to eliminate them. Recognised in the Hall of Fame by NASA, Air Canada, and Village Roadshow for responsible disclosure. Combines offensive security expertise with defensive engineering to deliver measurable, end-to-end risk reduction.

Experience

Security Engineer I **Sep 2025 – Present**
Hashira Works Pvt. Ltd. *Hyderabad, India*

- Performed application and infrastructure penetration testing across production systems (Garden Finance and internal services), identifying and validating vulnerabilities including IDOR/BOLA, access control issues, and critical misconfigurations.
- Led attack surface discovery and asset enumeration using Amass, Subfinder, ffuf, and Nmap to uncover externally exposed services and hidden endpoints.
- Designed and implemented Zero Trust access controls using Cloudflare Tunnel and Access policies, eliminating direct exposure of backend infrastructure (origin cloaking).
- Developed a container security pipeline using Trivy with SBOM generation and centralized ingestion into Wazuh SIEM for continuous vulnerability visibility.
- Engineered detection and monitoring pipelines using Wazuh, Suricata, and Falco, enabling real-time alerting and improved threat detection across infrastructure and containers.

Security Engineer Intern **Feb 2025 – Aug 2025**
Hashira Works Pvt. Ltd. *Hyderabad, India*

- Executed application security testing across APIs and web services, identifying vulnerabilities such as IDOR, authentication bypass, and input validation flaws.
- Performed structured reconnaissance and enumeration using Subfinder, ffuf, and Nmap to map attack surfaces and identify potential entry points.
- Assisted in deployment and configuration of Wazuh SIEM for centralized log collection, alerting, and initial detection rule tuning.
- Integrated Trivy-based container vulnerability scanning into development workflows to enable early detection of high and critical CVEs.
- Analyzed alerts, validated vulnerabilities through proof-of-concepts, and collaborated with engineering teams to support remediation and security hardening.

Penetration Tester Intern **Jun 2024 – Jul 2024**
CFSS *Remote*

- Conducted web application and network penetration testing using Burp Suite, Nmap, and Metasploit in controlled lab and simulated environments.
- Identified and exploited vulnerabilities including SQL Injection, IDOR, and authentication flaws aligned with OWASP Top 10.
- Performed reconnaissance and enumeration to map application logic, endpoints, and network attack surfaces.
- Executed exploitation and post-exploitation techniques including privilege escalation and lateral movement.
- Documented findings with detailed proof-of-concepts and actionable remediation recommendations following industry best practices.

Certifications

- **CEH (Certified Ethical Hacker)** – **EC-Council**
- **eJPT (eLearnSecurity Junior Penetration Tester)** – **INE**
- **Jr Penetration Tester (PT1)** – **TryHackMe**
- **OSCP (Offensive Security Certified Professional)** – *Offensive Security · In Progress*
- **OSWP (Offensive Security Wireless Professional)** – *Offensive Security · In Progress*

Projects

Syntr1x — Autonomous Pentesting Agent **Apr 2026 – Present**
AI Security · Automation

- Built an MCP (Model Context Protocol) server to enable AI agents to perform automated bug bounty workflows through structured tool execution.
- Designed a modular architecture integrating TypeScript-based MCP server with Python agents for reconnaissance, vulnerability scanning, exploitation, and reporting.
- Implemented end-to-end pipelines covering subdomain enumeration, service discovery, vulnerability detection, exploit validation, and report generation.
- Developed session-based workflow management and centralized findings storage to support repeatable and scalable security assessments.
- Enabled integration with AI agents (Claude, GPT) for autonomous decision-making and adaptive security testing workflows.

Wazuh-Based Security Monitoring Platform **Dec 2025 – Feb 2026**
Open Source XDR · SIEM

- Built and operated a centralized security monitoring platform using Wazuh to provide unified XDR and SIEM capabilities across infrastructure and workloads.
- Integrated host, container, and network-level telemetry to enable real-time threat detection and log analysis.
- Developed and tuned detection rules to identify suspicious activity, brute-force attempts, and anomalous system behavior.
- Configured log ingestion, alerting, and correlation workflows to improve visibility and reduce noise in security events.
- Enabled continuous monitoring and incident visibility across systems, supporting proactive threat detection and response.

Git Security Automation — Branch Protection System **Nov 2025 – Dec 2025**
DevSecOps · Security Automation

- Built a webhook-driven automation system to enforce secure repository workflows on repository creation.
- Implemented automated branch creation and protection policies, including pull request requirements, access control, and merge restrictions.
- Designed approval workflows with role-based permissions to ensure controlled and auditable code changes.
- Integrated event logging and monitoring for audit visibility and debugging of repository-level security events.
- Standardized secure development practices across repositories by applying consistent policy enforcement at scale.

ShadowDNS Spy — DNS Reconnaissance & Analysis Tool **Jun 2025 – Jul 2025**
Open Source · Security Tooling

- Developed a DNS reconnaissance and analysis tool to automate domain intelligence gathering for security assessments.
- Implemented multi-record resolution and validation to analyze domain configurations and identify misconfigurations.
- Integrated email security checks including SPF, DKIM, and DMARC to assess domain security posture.
- Enabled structured reporting with export support (JSON, CSV, XLSX) for repeatable and shareable security analysis.
- Designed optional reporting views to visualize DNS data and improve analysis during reconnaissance workflows.

Technical Skills

Offensive Security: Web & API Pentesting, VAPT, OWASP Top 10, BOLA/IDOR
Security Engineering: Application Security, Infrastructure Security, System Hardening
DevSecOps: CI/CD Security, Secure Workflows, Automation
Detection Engineering: SIEM, Log Analysis, Threat Detection, Alert Tuning
Cloud & Infrastructure: Zero Trust, WAF, Linux Systems, Virtualized Environments
Identity & Endpoint: Access Control, RBAC, MDM, Endpoint Security
Compliance: SOC 2, GDPR, Policy & Evidence Handling
Programming: Python, Bash, Rust

Achievements / Extracurricular

- Hall of Fame From **NASA, Air Canada, Village Roadshow**
- Secured **Global Rank Top 1%** TryHackMe
- CTF competition **Indian Cyber Security Solution**

Education

Lovely Professional University **Aug 2021 – May 2025**
Bachelor of Technology in Computer Science and Engineering *Phagwara, Punjab*