Parakh Shinde

Cybersecurity | AI Security & Security Engineering | Early-Career Candidate

Bengaluru, India | parakhshinde15@gmail.com | github.com/Parakh-Shinde | linkedin.com/in/parakh-shinde | parakh-shinde.github.io

PROFESSIONAL SUMMARY

Early-career cybersecurity candidate transitioning from IT technical support. Builds Python security tooling for AI/LLM security, static application security testing (SAST), and Google Cloud identity and access management (IAM); four public projects with automated tests and CI. Seeking security engineering and application security internships or entry-level roles.

TECHNICAL SKILLS

AI / LLM Security: prompt-injection detection, adversarial evaluation corpora, RAG source inspection, agent tool-use policy checks

Application Security & Tooling: Python AST static analysis, SARIF 2.1.0 reporting, authentication, MFA, scoped API tokens, audit logging, dependency auditing (pip-audit)

Cloud / Identity Security: Google Cloud IAM policy analysis (allow/deny inheritance, impersonation, escalation paths)

Detection Engineering: atomic detections, multi-stage attack-chain correlation, versioned telemetry, holdout precision/recall evaluation

Programming & Engineering: Python, FastAPI, Pydantic, SQLAlchemy, TypeScript, React, PostgreSQL, Redis, Docker Compose, pytest, Ruff, MyPy, GitHub Actions, Git

Lab Exposure: Splunk and Microsoft Sentinel labs; MITRE ATT&CK and NIST 800-61 (foundational)

SELECTED SECURITY PROJECTS

AegisForge *(personal project, v0.10.0)* github.com/Parakh-Shinde/AegisForge

- Built a lab-safe CLI and API that simulates a poisoned-document RAG, agent tool request, and cross-tenant API access chain; compares vulnerable and secure modes and produces correlated attack-chain alerts with JSON/Markdown reports carrying SHA-256 provenance.
- Implemented prompt-injection inspection with Unicode, confusable-character, and bounded Base64 normalization; evaluated on tuning, regression, and untouched holdout corpora and documented that tuning scores did not generalize to the fresh holdout set. 136 automated tests pass; CI on Python 3.11 and 3.12 with benchmark gates.

AegisAI *(personal project, local lab, active development)* github.com/Parakh-Shinde/aegisai

- Developing an AI security evaluation workbench with versioned adversarial suites (prompt injection, RAG injection, agent tool safety), evidence capture, analyst triage, baseline comparison, and release-gate policy.
- Implemented authentication with MFA, scope-limited API tokens, organization-scoped data, and audit logging; added static inspection of file inputs, RAG sources, and proposed agent actions. 131 backend tests pass; CI runs Ruff, MyPy, pytest, pip-audit. Documented as not production-certified.

GCP IAMGraph *(personal project, v0.2.0)* github.com/Parakh-Shinde/GCP-IAMGraph

- Built a Google Cloud IAM analyzer that models resource hierarchy, inherited allow and deny policies, custom roles, and multi-hop service-account impersonation, returning ALLOW, DENY, or UNKNOWN decisions with structured evidence.
- Implemented 8 detection rules for privilege-escalation paths and exposure; exports JSON, Markdown, SARIF 2.1.0, and Graphviz attack graphs. On included synthetic environments it reports 8 findings (vulnerable) and 0 (hardened). 74 tests pass with 91% coverage and a CI coverage gate.

AST Auditor *(personal project)* github.com/Parakh-Shinde/ast-auditor

- Built an AST-based Python static security scanner with 5 rules (`eval`, `exec`, `pickle`, `shell=True/os.system`, `yaml.load`) and import-alias tracking; outputs text, JSON, and SARIF 2.1.0 with CI-friendly exit codes.
- 66 tests pass and lint is clean; CI runs on Python 3.10 to 3.14. Documents its limitations (no full data-flow analysis).

PROFESSIONAL EXPERIENCE

Technical Support Engineer, Swastik Engineering Pvt. Ltd.

- Diagnosed and resolved Windows and Linux software and hardware issues, including onsite support.
- Troubleshot network and router connectivity problems.
- Provided technical support in Windows/Linux infrastructure and Active Directory environments.

EDUCATION

MCA, Cyber Security and Cyber Forensics, VIT *In progress*
BCA, RNTU

CERTIFICATIONS & TRAINING

- Red Team Leaders: Introduction to Offensive Security with Artificial Intelligence (completed Aug 2026)
- CEH v13 and CHFI training programs, APC Hacking University, Bangalore (completed)
- Advanced Cybersecurity Program, IIT Guwahati / AccioJob (in progress)