Swetha B

https://swethab.dev/

Email : swethab@terpmail.umd.edu

Summary

OSCP-certified Security Architect with hands-on experience in **threat modeling**, **secure-by-design architecture**, & **cloud-native SaaS security**. Proficient in **Python** & **Terraform** for security automation, with deep expertise in **zero-trust architecture**, **DevSecOps**, & integrating **AI-powered tooling** into vulnerability triage & CI/CD pipelines.

Experience

YSecurity.io — San Francisco, CA, USA
Security Consultant — *February 2026 - Present*

- Delivered **penetration testing** & **application security assessments** across client environments, identifying **OWASP Top 10** vulnerabilities, performing threat modeling, & producing actionable remediation roadmaps that improved client compliance posture.
- Supported **SOC 2 & ISO 27001 audit readiness** for multiple clients by collecting & managing evidence, maintaining **GRC platform hygiene** (Drata/Vanta), & executing ongoing control operations including access reviews & vendor risk assessments.
- Drove **secure SDLC adoption** by configuring & triaging SAST/DAST tooling, integrating security scanning into **CI/CD pipelines**, & coordinating vulnerability remediation with client engineering teams to prevent high-severity findings from reaching production.

Swecure.inc — San Francisco, CA, USA
Penetration Tester — *September 2025 - Present*

- Spearheaded **web application security enablement** across multiple startups; performed **penetration tests**, attack surface mapping & secure code reviews, remediating critical findings & elevating compliance posture by **40%**.
- Integrated **DevSecOps security controls** into CI/CD pipelines, including SAST/DAST, dependency scanning & appsec reviews; reduced misconfigurations by **25%** & prevented **20+ high-severity vulnerabilities** pre-production.

University of Maryland Police Department — College Park, MD, USA
Application Security Engineer — *December 2024 - May 2025*

- Built an **offensive security pipeline** to emulate **attacker reconnaissance** on public **apps/APIs**, eliminating visibility gaps & accelerating **vulnerability discovery** by **10%** across the organization in high-traffic environments.
- Engineered a **real-time detection & mitigation engine** using **Python** & **Terraform/Terragrunt**, preventing subdomain takeovers; integrated **Wiz CSPM** to auto-prioritize alerts, strengthening the overall **cloud security posture.**
- Designed & deployed a **centralized DNS asset management framework** to resolve limited **visibility & control** across org & portfolio companies; enabled targeted recon, secure backups & deeper insight into external-facing cloud infra.

Wipro Technologies — Bangalore, India
Security Engineer — *July 2022 - August 2023*

- Improved **AWS CSPM compliance** in **PCI-regulated environments** from 80% to 96% by leading **Zero Trust** cross-team architectural reviews, automating patching, & partnering cross-functional teams to close cloud security gaps & reduce audit risk.
- Addressed critical container security gaps by embedding end-to-end **CI/CD hardening workflows** via Jenkins; enforced runtime protections that minimized attack surface & enhanced visibility into overall risk exposure.
- Enhanced **Kubernetes (ECS, EKS) security** by defining org-wide **security baselines** & developing a comprehensive **incident response playbook**, ensuring **PCI** & **SOC2** compliance & reducing incident resolution time by **40%** across cloud deployments.

Ignited Sparks — Visakhapatnam, India
Security Engineer — *July 2020 - December 2021*

- Directed & grew the security function from the ground up, spearheading **Red Team & Purple Team operations** across cloud infrastructure & a responsible disclosure program; hardened **Kubernetes** for microservices, shrinking external attack surface by **60%**.
- Embedded **SAST/DAST checks** in CI/CD using OWASP ZAP & **executed secure code reviews** for **PHP/Go**, protecting web & &roid apps used by 30M+ users; **engineered a Go package** to eliminate common security flaws.

Certifications & Accomplishments

OSCP(PEN-200) OSID 57183028: Expertise in Active Directory, Red Teaming — *September 2025*
AWS Cloud Solutions Architect: Proficient in designing & deploying secure, scalable AWS cloud architectures. — *July 2024*
CompTIA Security+ (SY0-701): Strong foundation in risk management, & threat mitigation strategies. — *June 2024*
INE Junior Penetration Tester(eJPTv2): Proficient in vulnerability assessment & penetration testing. — *December 2024*
AWS Cloud Practitioner: Solid understanding of AWS core services & foundational architecture principles. — *March 2023*

Skills Summary

Application Security: Secure SDLC, Threat Modeling(STRIDE), Secure Code Review, Vulnerability Management, SAST & DAST, OWASP Top 10, MITRE ATT&CK, IDOR & BOLA, Auth Security (SAML 2.0, OAuth)
AI Security Integration: LLM-powered vulnerability analysis (Claude/GPT-4), automated exploit generation, intelligent SAST triage, context-aware remediation
Offensive Security Tools: Burp Suite, Caido, Metasploit, Nmap
Programming & Scripting: Python, GoLang, Bash, SQL, Javascript

Security Research & Projects

AASRT (AI Agent Security Reconnaissance Tool): Engineered a **CVSS-scored reconnaissance platform** targeting exposed AI infrastructure; enforced **defense-in-depth** via parameterized queries, credential redaction, **0600 file permissions**, & SSL pinning — achieving **zero injection vectors** across 63 passing unit tests. Shipped with **GitHub Actions CI/CD gates**, Pydantic schema validation, & OWASP-aligned **Secure SDLC** controls from design to deployment. *Stack: Python, SQLAlchemy, Pydantic, Pytest, Docker, Streamlit, GitHub Actions.*

AI-Enhanced Vulnerability Management Platform: Developed a **FastAPI** service embedding **Claude API** to autonomously triage SAST/DAST findings — generating exploit scenarios, scoring real-world exploitability, & emitting **framework-specific patches** (Django ORM, React DOMPurify) per CVE. Cut false-positive investigation overhead via **LLM-driven code-context analysis**, reducing manual triage time across multi-service architectures. *Stack: Python, FastAPI, Claude API, Elasticsearch, React.*

Education

University of Maryland, College Park — College Park, MD
Master of Engineering Graduate student in Cyber Security, Minor-Cloud Engineering — *August 2023 - May 2025*
Courses: *Hacking of C programs & Unix binaries, Network Security, Information Assurance, Cloud Security, Security Tools.*