Pranit Garud

Senior Product Security Engineer

Senior Product Security Engineer with 10+ years across offensive security, product security and AI security. Leads product security for Crusoe's AI Inference Cloud Platform, the infrastructure behind large-scale AI workloads, and threat models and security-reviews every new AI/ML service, partner service and customer-facing API before it ships. Builds the agentic AI security workflows that make that possible: AI-SAST, penetration testing, and infrastructure security automation. A decade of hands-on offensive security runs through all of it, from vulnerability discovery and rapid Proof of Concept development to bug bounty work, with 300+ applications secured and 20+ Hall of Fame placements.

info@pranitgarud.com | United States | pranitgarud.com | linkedin.com/in/pranit-garud

WORK EXPERIENCE

Sr. Product Security Engineer
Crusoe.ai

2025 - Present

- Lead Product Security for Crusoe's AI Inference Cloud Platform, powering large-scale ML training and inference workloads.
- Developed Agentic AI workflows for AI-SAST, Pentesting, Infrastructure Security.
- Secured GCP Kubernetes infrastructure powering thousands of GPUs and datacenter workloads, hardening cluster configuration and workload isolation.
- Drive threat modeling and secure design reviews for new AI/ML services, partner services, and customer-facing APIs before they ship.
- Architect secure-by-default patterns for multi-tenant GPU isolation, model serving, and data pipelines.

Offensive Security Engineer II
Amazon

10/2023 - 2025

- Responsible for conducting Red & Purple Team engagements, simulating advanced adversary tactics.
- Conducted Pentesting with source code analysis and secure SDLC integration.
- Performed cloud security assessments, identifying and mitigating risks in cloud infrastructures.
- Executed hardware pentesting for Robotics and IoT systems, uncovering vulnerabilities in embedded devices.

Security Engineer
Apple

06/2023 - 10/2023

- Performed threat modeling techniques to enhance the security posture of software applications, assisting developers in effectively mitigating potential risks.
- Conducted comprehensive source code analysis, penetration testing, and contributed to the implementation of secure software development practices, ensuring adherence to industry standards.
- Strengthened cloud security through comprehensive assessments and implemented strategies to safeguard critical infrastructure.

Lead Pentester
Hackerone/Cobalt

07/2022 - 05/2023

- Responsible for leading & performing pentests and communicating with stakeholders.
- Conducted Pentesting engagements for clients in various industries such as Blockchain, Fintech, Cryptocurrency, Healthcare, and Finance.
- Conducted security audits and penetration testing on HSM (Hardware Security Module) infrastructure.
- Executed security assessments for various systems including web and mobile applications, APIs, internal and external networks, and cloud.

SKILLS

AI & AGENTIC SECURITY

Agentic AI Security Workflows, AI-SAST, LLM Security, LLM Council, Offensive Harness, Prompt Engineering, Inference Security, GPU Security, VMR, DPU Security, CI/CD Security, Patch Drift Detection, AI Supply Chain Security, ML Adversarial Attacks, Side-Channel Attacks

OFFENSIVE SECURITY

Penetration Testing, Network VAPT, RedTeam, Web AppSec, Reverse Engineering, Exploit Development, Binary Exploitation, Wi-Fi Hacking, IoT Hacking, OT Security, Adversary Simulation, Blockchain Security, Smart Contract Audit, Zero-day Research, AI Red Teaming, ML Adversarial Attacks

THREAT MODELING & DESIGN

Threat Modeling, Design Review, Architecture Review, Code Review, MITRE, Secure SDLC

APPLICATION & API SECURITY

SAST, DAST, API Testing, Active Directory, Mobile AppSec, Container Security

CLOUD & PLATFORM

Cloud Security, AWS, GCP, Azure, Oracle Cloud, Kubernetes, GPU Isolation, NVIDIA InfiniBand Security, RDMA Security, Confidential Computing

TOOLS & LANGUAGES

Python, Go (Golang), Rust, Bash, Shell Script, LangChain, LangGraph, Pydantic, Burp Suite, Nuclei, Metasploit

PROJECTS EXECUTED

Runtime Detection and Response Bypass Research

- Conducted independent EDR-style research into layered runtime detection and blocking controls, developing three novel techniques to bypass application-layer, network-layer, behavioural-profiling, and workload-layer defences.

Reconator: Attack Surface Management (ASM) Platform

- Built Reconator, an AI-powered reconnaissance and Attack Surface Management platform for bug bounty hunters and security professionals, featuring AI-guided analysis, attack path prediction, distributed fleet scanning, IP rotation, and comprehensive attack surface discovery.
- Deployed it as a distributed system on AWS Fargate and Lambda, running parallel scanning pipelines for continuous, organization-scale ASM.
- Mapped and continuously monitored 100K+ subdomains, remediated the issues surfaced by continuous ASM and vulnerability scanning, and reused the platform for external red-team engagements.

Purple Team TTP Dashboard

- Created Red/Blue team dashboard via CrowdStrike + Splunk to AWS QuickSight
- Improved real-time TTP tracking & detection engineering

Web Application Exploitation

- Bypassed Antivirus and security checks to gain shell on target server via malicious apk
- Successfully exploited file upload to gain shell on target server
- Created Malicious JavaScript for post exploitation

Security Consultant
Varutra Consulting Pvt. Ltd.
12/2017 - 12/2021

- Performed Application Security including Security Life Cycle, SDLC, Penetration Testing, Threat Modeling and Vulnerability Assessment using OWASP, NIST and CWE/SANS Special Publications
- Performed & Lead Red Team Assessment for Multiple Client
- Performed SAST/DAST Security Assessment using OWASP/NIST Security Standards for over 200+ customers
- Performed Onsite Engagements such as Wi-Fi Hacking, Red Teaming, Cloud Audit (AWS, GCP, Azure, Oracle Cloud (OCI))
- Expertise in penetration testing using various tools like Burp Suite, OWASP ZAP Proxy, Kali, SQLmap, Nmap, Nessus, Nexpose, Acunetix, Metasploit

CERTIFICATIONS

AI Red Team: Attacking AI
Arcanum Information Security, Issued Mar 2026

SEC565 Red Team Operations & Adversary Emulation
SANS, 12/2024

CREST Registered Penetration Tester (CRT)
CREST, 04/2024

CREST Practitioner Security Analyst (CPSA)
CREST, 04/2024

OSCP: Offensive Security Certified Professional
Offensive Security, 2021

AWS Security Fundamentals
Amazon Web Services Certified, 2020

HacktheBox Dante ProLabs
Completed HacktheBox Prolabs, 2021

CEH v9: Certified Ethical Hacker
EC Council, 2016

EDUCATION

Master of Engineering in Cyber Security
University of Maryland, College Park

Bachelor of Engineering in Computer Engineering
Pune Institute of Computer Technology

PROJECTS EXECUTED

IoT Security Assessment

- Performed Security Assessment on Client's IoT Ecosystem gaining access to critical devices and API Servers resulting in identification of major data and source code leak
- Performed Exploitation for MQTT protocol to dump sensitive data
- Developed BadUSB using Digispark Attiny85 for Red teaming and Social engineering attacks

ACHIEVEMENTS

Vulnerability Research on Open-Source AI Infrastructure Projects
Reported 12+ CVEs and vulnerabilities to open-source AI libraries and products including Harbor, VictoriaMetrics, VictoriaLogs, vLLM, and SGLang.

Reconator v2: AI-Powered Reconnaissance with Adaptive Pipeline Orchestration
Published May 2, 2026 | Version v1

Presented Talk on Mastering Smart Contract Security
Presented a talk covering topics such as Introduction to Blockchain, Smart Contracts, Security gaps, Exploits, and Mitigation techniques for smart contract bugs.

Research on Crucial Cyber Security Services
Developed and implemented IoT security testing, malware analysis, Indicator of Compromise (IoC), and Open-Source Intelligence (OSINT) services within the organization.

Employee of the Quarter
Recognized twice for dedicated and quality work

Advanced Attack Surface Management: Automated External Reconnaissance Using Modular Tool Orchestration
Published June 15, 2021 | Version v1 | Preprint | Open

Hall of Fame/ CVE-2019-20058
Achieved Hall of Fame on TripAdvisor, Unilever, HealthifyMe, GM

PUBLICATIONS AND WRITING

How I Nearly Accessed Millions of Maruti Suzuki Customer Records
Collaborated with fellow security researcher on exposed Swagger UI endpoints exposing customer records for roughly 25 million customers.

From Vibe Coding to Threat Hunting: How I Built a Honeypot That Caught the Mirai Botnet
Built a honeypot that caught the Mirai botnet in the wild.

How I Pwned a Phishing Campaign: Hacking the Hackers
Took over a phishing campaign by attacking the attackers' own infrastructure.

Bug Bounty Recon: Perform Faster Port Scan
A faster port-scanning approach for bug bounty reconnaissance.

LANGUAGES

English
Full Professional Proficiency

Hindi
Native or Bilingual Proficiency

Marathi
Native or Bilingual Proficiency

INTERESTS

Music | Cryptocurrency | Bug Bounty | Travelling