

Ishaani Prashant

AI/ML Security Engineer | LLM Security | Application Security

Mumbai, India | +91 9967351936 | ishaanii.prashant@gmail.com | portfolio.ishaani.tech | linkedin.com/in/ishaani-prashant
| github.com/mindxflayer

Professional Summary

AI/ML Security and Application Security researcher with experience in LLM threat modeling, prompt injection, adversarial ML, API security, vulnerability research, and offensive security. Discovered and responsibly disclosed vulnerabilities through Bugcrowd, CERT-In and NCIIPC; built AI security tooling and CTF infrastructure supporting 3,200+ participants.

Technical Skills

AI/ML Security: Prompt Injection, Adversarial ML, LLM Threat Modeling, OWASP Top 10 for LLMs, MITRE ATLAS

AppSec: API Security, Penetration Testing, Vulnerability Assessment, Threat Modeling, SSRF, IDOR, XSS, SQLi

Tools: Burp Suite, OWASP ZAP, Postman, Docker, Linux, Git, JWT, OAuth2

Languages: Python, SQL, Java

Databases: MySQL, PostgreSQL, SQLite

Soft Skills: Technical Writing, Analytical Thinking, Communication, Leadership, Collaboration

Experience

Independent Security Researcher | Freelancer

2025 – Present

- Conducted security assessments across **5 web applications** and **7 API endpoints** spanning **4 government portals**, testing **11 attack classes** and identifying **14 vulnerabilities**, including **4 Critical** and **4 High-severity** findings such as **RCE, IDOR, and sensitive data exposure**.
- Responsibly disclosed vulnerabilities through **Bugcrowd, CERT-In, NCIIPC, and independent programs**, also validating exploitability, and reproducibility while providing remediation guidance for web and API security issues.

CTF Developer

2025 – 2026

HackZero'26 CTF & Advitya 2026 CTF

- Designed and deployed **AI/ML and OSINT security challenges** for two inter-college CTFs with **800+ participating teams**, developing challenge logic, automated flag validation, scoring, and supporting infrastructure.
- Engineered challenge infrastructure for **3,200+ participants across concurrent sessions**, ensuring reliable challenge execution and automated flag validation during live competitions.

Projects

FlightZone Red Labs | AI/ML CTF Platform

ishaani.tech

- Engineered and deployed** a gamified AI/ML security CTF platform covering the **OWASP Top 10 for LLMs** across **10 security tracks**, including insecure output handling, data poisoning, model theft, and supply chain attacks.

PasteGuard | Zero-Server AI DLP Extension

github.com/mindxflayer/proj2 | JS, Python, Scikit-learn

- Developed** an ML-based AI DLP guardrail using **TF-IDF** and **Logistic Regression** to detect and redact sensitive data from AI chatbot inputs in real time, incorporating **negation-aware intent classification**.

Adaptive LLM Red Team Scanner

github.com/mindxflayer/llm-redteam-scanner | Python, AsyncIO

- Engineered** an automated LLM red-team framework using **Python/AsyncIO** for prompt injection, jailbreak, and evasion attacks across **REST/SSE/WebSocket APIs**, with genetic fuzzing and **LLM-as-a-Judge validation**.

Blockade | MCP Security Proxy

github.com/mindxflayer/blockade | Python, MCP, SQLite, Docker

- Built** a policy-enforcing proxy for AI coding assistants with **LLM risk scoring, taint tracking, tool-schema pinning, and Docker sandboxing**.

Achievements

- Competitive Security:** Achieved **Top 4/200** at **IIITB CTF**, **Top 10** at **Eschaton CTF**, and **Top 20** at **Illuminate and CREST CTF**; ranked in the **top 5%** across web, OSINT, cryptography, and forensics.
- Security Leadership:** **Vice President, OWASP Student Chapter, VIT Bhopal**, leading events, workshops, and CTFs reaching **3,000+ students**.

Education

VIT Bhopal University

2023 – 2027

B.Tech, Computer Science (AI/ML)

CGPA: 8.6/10

Smt. Sulochanadevi Singhania School, Thane

2021 – 2023

Class XII, CISCE

81.5%

Universal High School, Thane

2020 – 2021

Class X, CISCE

91.8%

Certifications

- Certified API Security Analyst (CASA) — APISEC University, 2026
- API Security Certified Professional (ACP) — APISEC University, 2026
- CAPIJ — The XSS RAT, 2026