

RAVI RAJPUT

CYBER SECURITY MANAGER · SECURITY AUTOMATION & AGENTIC AI · AI SECURITY & RED TEAMING

Eleven years of breaking things on purpose — networks, infrastructure, cloud, web, APIs, SaaS, thick clients, hardware and plant floors — and security products shipped, including the AI that now does the breaking.

Hyderabad, India (Open to Remote / Global) | +91 940 928 1655 | rajputravi645@gmail.com
infosecravi.com | linkedin.com/in/frustratedresearcher | github.com/frustratedresearcher

PROFESSIONAL SUMMARY

Cyber Security Manager and offensive security leader with **11+ years of continuous, hands-on penetration testing** across network, infrastructure and cloud, covering external and internal network testing, **Active Directory and Windows exploitation**, and cloud configuration and architecture review across **Azure, AWS and GCP**, alongside deep application and product security, web and API testing to **OWASP Top 10**, Software as a Service (SaaS) multi-tenancy and authorization testing, thick client assessment and **manual secure code review** across Python, Java, JavaScript and Node.js, PHP and Go. **Still testing hands-on today.**

Security product builder who has shipped multiple security products, including **Xalon**, a production agentic SOC of 22 agents handling **916,000 detections at 78% auto-resolution** and **\$110K in annual cost reduction**; **SecAI**, a SaaS LLM vulnerability scanner that anchored **\$1.2M in annual client revenue** and cut critical AI application risk by **50%**; an AI-enabled automated hardware pentest device delivered as a working MVP; and **open-source security tools** spanning LLM penetration testing, machine learning supply-chain security, vehicle intrusion detection and agentic AI threat modeling.

Works AI security in both directions, **building it and breaking it**, architecting production agentic systems on **AutoGen** with Claude and Gemini in adversarial reasoning, and red teaming AI against **MITRE ATLAS and the OWASP Top 10 for LLM Applications**, covering prompt injection, jailbreaks, tool abuse, RAG poisoning and excessive agency, exercised with **PyRIT and Garak**. Found **30+ critical vulnerabilities** across client estates and disclosed **zero-day findings in a production vehicle platform** to the vendor with **direct CEO acknowledgement**. Speaker at **DEF CON 33, Hack In The Box, Black Hat Asia, HITCON and NULLCON**. Open to Security Leadership and AI Security roles.

WORK EXPERIENCE

Manager, Cyber Security, XBP Global (formerly SourceHOV LLC), India, Remote

Nov 2025 – Present

- Architected and shipped **Xalon**, a production agentic SOC platform on AKS, ingesting **10–12K alerts/day**, auto-resolving **78% of volume** and delivering **\$110K in annual operating cost reduction**.
- Engineered a five-lane severity-tiered model routing scheme across **22 specialized agents** using **AutoGen 0.4, Claude and Gemini** adversarial reasoning, achieving a **30× per-alert cost differential** and reducing daily LLM spend from **\$500 to \$40**.
- Developed per-agent AI threat models mapped to **MITRE ATLAS and the OWASP Top 10 for LLM Applications**, covering prompt injection, jailbreaks, tool abuse, RAG poisoning and excessive agency.
- Executed recurring **AI red team exercises** using **PyRIT and Garak** against production Claude and Gemini pipelines.
- Delivered network, infrastructure and cloud penetration testing across **Azure, AWS and GCP**, including Active Directory attack path review.
- Owled application and product security covering web and API testing to **OWASP Top 10**, SaaS multi-tenancy and authorization testing, thick client assessment, **manual secure code review** and vulnerability triage.
- Led a cross-functional team of **11–20 engineers**, SOC analysts and shift roster managers through a **post-acquisition transition**, retaining Oracle, AIDO and LLA partnerships.

Subject Matter Expert, Hardware Security and Applied AI (Contract), Independent, India

Mar 2025 – Oct 2025

- Led end-to-end research and development for an **AI-enabled automated hardware pentest device**, owning research direction and prototype architecture.
- Delivered a **working MVP** with on-device reasoning that autonomously fingerprints targets, selects attack chains and generates structured findings reports.

Information Security Manager, SourceHOV LLC, Chennai, India

Mar 2023 – Feb 2025

- Built and delivered **SecAI**, a proprietary SaaS LLM vulnerability scanner implementing the **OWASP Top 10 for LLM Applications 2024**.
- Generated **\$1.2M in annual client revenue** across Oracle, AIDO and LLA accounts and reduced critical AI application risk by **50%** within six months of launch.
- Redesigned the Security Operations Center and Red Team operating model, reducing incident response time by **40%** across **20+ enterprise clients**.

- Led network, infrastructure and cloud security assessments covering segmentation, privilege escalation, **Active Directory attack paths**, IAM and misconfiguration review.
- Performed **manual secure code review** across **Python, Java, JavaScript and Node.js, PHP and Go** codebases, identifying authentication, access control, injection, deserialization and secrets handling defects.
- Operated vulnerability intake and triage including reproduction, severity scoring, duplicate adjudication and remediation tracking.

Lead Engineer, Automotive Security, BlueBinaries Engineering and Solutions, Pune, India

Oct 2022 – Mar 2023

- Built and led the **Automotive Security practice** from inception, operationalizing **ISO/SAE 21434** compliance programs and executing **TARA** for OEM and Tier 1 clients.
- Led penetration testing across **infotainment systems, Android Automotive operating system** and supporting cloud and network infrastructure.

Lead Security Researcher, AmynaSec Research Lab, Pune, India

Jan 2022 – Sep 2022

- Discovered a **zero-day Chromium browser exploit**, an Android companion application vulnerability and a cloud-side backend defect in a production vehicle platform, reported under **coordinated disclosure with direct CEO acknowledgement** from the vendor.
- Published the research at **Hack In The Box (HITB) 2024**.
- Delivered penetration tests and Threat Analysis and Risk Assessment across **20+ vehicle communication protocols**.
- Extended testing into industrial OT environments, assessing **Modbus** and adjacent **ICS** and **SCADA** protocols for plant floor clients.

Senior Security Researcher, 8 Bit Digital Solution, Bhopal, India

Sep 2019 – Jun 2021

- Fuzzed proprietary protocols and Windows and Linux thick client binaries, leading **zero-day research and exploit development** adopted across client engagements.
- Automated application security testing for web and Android pipelines, reducing cycle time by **40%**.

Penetration Tester, Innovador Infotech, Lucknow, India

Aug 2015 – Sep 2019

- Delivered network, infrastructure, web application, API and Android penetration tests protecting **millions of user accounts**.
- Identified and remediated **30+ critical vulnerabilities** across wireless and RF systems.
- Developed Windows user mode exploits against desktop applications, increasing client patch adoption by **25%**.

SKILLS & TECHNOLOGIES

AI and Machine Learning Security: Agentic AI, Multi-Agent Systems, AutoGen, MCP, Claude, Gemini, Azure OpenAI, MITRE ATLAS, OWASP Top 10 for LLM Applications, PyRIT, Garak, promptfoo, DeepTeam, RAG Security, AI Threat Modeling, AI Red Teaming, NIST AI RMF, ISO 42001

Security Operations: SOC Modernization, CrowdStrike Falcon, Sentinel, Splunk, MITRE ATT&CK, MITRE D3FEND, Threat Hunting, Incident Response, Red Team, Purple Team

Cloud and Infrastructure Security: Azure, AKS, ACR, AWS, GCP, Active Directory (AD), IAM, Cloud Security Architecture

Offensive Security and Penetration Testing: Network Penetration Testing, Infrastructure Penetration Testing, Cloud Penetration Testing, Web Application Penetration Testing, API Testing, Burp Suite, Thick Client Testing, Wireless and RF, Firmware Analysis, Reverse Engineering, Exploit Development, Fuzzing, Zero-Day Research

Application and Product Security: OWASP Top 10, Manual Secure Code Review, SAST, SaaS Security, Multi-Tenancy Testing, Authorization Testing, Vulnerability Management and Triage, SARIF, CI/CD Security

Programming Languages: Python, Java, JavaScript, Node.js, PHP, Go, Bash

Operational Technology and Automotive Security: Modbus, SCADA, IEC 62443, CAN bus, ISO/SAE 21434, TARA, Android Automotive

Leadership: Team Leadership, P&L Ownership, Security Strategy and Roadmap, Product Management, Stakeholder Management, Mentoring

PROJECTS

Xalon, Production Agentic Security Operations Center

Built a 22-agent agentic SOC using AutoGen 0.4, Claude, Gemini, MCP, ChromaDB, Playwright, Azure Kubernetes Service and CrowdStrike Falcon, enabling automated triage of **916K detections at 78% auto-resolution** and **\$110K annual cost reduction**.

SecAI, SaaS Large Language Model Vulnerability Scanner

Built an LLM vulnerability scanner implementing the OWASP Top 10 for LLM Applications 2024, enabling enterprise AI application assessment, generating **\$1.2M annual revenue** and reducing critical AI risk by **50%**.

AI-Enabled Automated Hardware Penetration Testing Device

Developed an AI-driven hardware pentesting device with on-device reasoning for autonomous target fingerprinting, attack chain selection and structured reporting; delivered **working MVP**.

Trustmap, Agentic AI Threat-Modeling Lab (Open Source)

Built and published a **free, browser-based threat-modeling lab for agentic AI systems** that maps agents, tools, data stores and the handoffs between them, then surfaces the dangerous ones, shared identity, excessive agency and handoffs that transfer implicit authority, and proposes a secure blueprint. Backed by a **168-control readiness library** across six worked example domains; **runs fully client-side with no data sent to any language model**. infosecravi.com/trustmap

LLM-PT, Autonomous LLM Penetration Testing Suite

Built a Python command line interface orchestrating promptfoo, Garak and DeepTeam against LLM-backed web applications, APIs and websockets, automatically detecting prompt fields from Burp Suite exports and emitting **SARIF for CI/CD**.

github.com/frustratedresearcher/LLM_PT

MLSec-Analyzer, Machine Learning Model File Vulnerability Scanner

Developed a static scanner detecting pickle remote code execution, **Keras Lambda remote code execution (CVE-2024-3660)**, GGUF overflow, zip slip, embedded secrets and backdoored weights across **seven model formats**, securing the machine learning supply chain.

github.com/frustratedresearcher/MLSec-Analyzer

LSTM Automotive Security, CAN Bus Intrusion Detection

Implemented LSTM Autoencoder and Variational Autoencoder (VAE) models detecting replay attacks, fuzzing, timing deviations and entropy anomalies on raw CAN telemetry without proprietary decoding. Presented at **DEF CON 33 Creator Stage 2025**.

AutoHackOS, Open Source Vehicle Penetration Testing Operating System

Built a bootable Linux distribution integrating CAN, BLE, SDR, firmware and network tooling, eliminating multi-virtual-machine friction for vehicle security teams. Presented at **Black Hat Asia 2023 Arsenal**.

E D U C A T I O N

Bachelor of Engineering

A D Patel Institute of Technology, Anand, India

2011 – 2015

C E R T I F I C A T I O N S

Certified AI Security Expert (MSEC-CAIS) — ModernSecurity.io

Issued Sep 2026 · Credential ID trz0fzpakg

OWASP Top 10 for LLM Applications — CyberWarFare Labs

Issued Sep 2026 · Credential ID 95344643-ed24-4391-92b3-50cfc78bcd8b

AI Red Team Analyst (AI-RTA) — CyberWarFare Labs

Issued Oct 2026 · Credential ID 6ad12ff1b6d122ea6a92ba7a

Certified Multi-Cloud Red Team Analyst (MCRTA) — CyberWarFare Labs

Issued Oct 2026 · Credential ID 6ad12e20b6d122ea6a92b85a

S P E A K I N G , P U B L I C A T I O N S A N D P R O F E S S I O N A L D E V E L O P M E N T

Featured Speaker: **DEF CON 33** Creator Stage and Workshop, Las Vegas, 2025 · c0c0n Telecom Village, Kochi, 2025 · CSAxCON, 2025 · **Hack In The Box** Security Conference, Bangkok, 2024 · BSides Mumbai, 2024 · **Black Hat Asia** Arsenal, Singapore, 2023 · **HITCON**, Taipei, 2023 · **NULLCON**, Goa, 2023 · BSides Indore, 2023 · BSides Maharashtra, 2020 · Bounty Bash, Nepal, 2019

Publications and Community: Course Author, AutoSec Pro Vehicle Cybersecurity Mastery W52, Pentest Magazine, 2024 · Co-organizer, DEF CON Telecom Village, 2023 – Present · Chapter Lead, NULL Ahmedabad, 2017 – 2020