CERT NO.**RCAAP**

PROFESSIONAL CERTIFICATION PROGRAM

REDSPECTOR

Redspector Certified Advanced AI Pentester

PROFESSIONAL

// RCAAP · ADVANCED AI PENTESTING

A hands-oncertification forsecurityprofessionalsmoving into LLMinternals,RAG engineering, agentic systems, and enterprise AI red teaming.

```
~/redspector/rcaap

redspector ~$ pentest_llm --target gpt-agent --mode adversarial

> prompt-injection & agent exploit chain verified.
```

ENROLL NOW →

WWW.REDSPECTOR.COM · TEAM@REDSPECTOR.COM · +91 80783 28520

"BEYOND CERTIFICATIONS. TOWARD EXPERTISE."

ABOUT THE PROGRAM

Course Overview

TheRedspectorCertifiedAdvancedAIPentester (RCAAP) program is an elite, hands-on training track that transforms security professionalsandengineers intofrontier AIred teamers. Students master LLM internals, RAG pipelines, agentic systems,andadversarialAI— learning to attack, defend, and architect production-grade AI systems end-to-end.

18	05	08	01
CORE MODULES	CAPSTONE BUILDS	BONUS MODULES	CERTIFICATION

Who Should Join?

Cybersecurity Pros

Penetration testers and red teamers pivoting into AI security.

AI Engineers

Practitioners securing LLM apps, RAG systems, and agent stacks.

Software Developers

Engineers shipping AI features who need production-grade security.

Security Researchers

Researchers exploring adversarial ML and LLM threat models.

Startup Founders

Founders building AI products who must own risk end-to-end.

Advanced Students

Graduates targeting elite AI-security roles and specialization.

LEARNING JOURNEY

Learning Path

Astructured,six-stageprogressionfromLLMinternals to production red teaming.

01

LLM INTERNALS

Transformers,attention,tokenization, training & fine-tuning

02

RETRIEVAL & AGENTS

Embeddings,RAG,vectorDBs,LangGraph, CrewAI, MCP

03

AI SECURITY

OWASPLLMTop10,prompt injection, jailbreaks, agent security

04

ADVERSARIAL AI

Modelpoisoning,backdoors,evasion & robustness engineering

05

AI INFRASTRUCTURE

Ollama,vLLM,GPUoptimization,APIs, monitoring & scaling

06

CAPSTONE

Shipproduction-grade RAG, agents, MCP servers & assessments

PROGRAM CURRICULUM

Modules 01–04

Comprehensive,hands-ontrainingacrossthefulladvanced AI pentesting stack.

MOD 01 ADVANCED TRANSFORMERS

- Attention Mechanisms
- Multi-Head Attention
- KV Cache
- Context Windows
- Mixture of Experts (MoE)
- Reasoning Models

MOD 02 LLM TRAINING & FINE-TUNING

- Tokenization Internals
- Dataset Engineering
- Pretraining
- Supervised Fine-Tuning (SFT)
- RLHF
- DPO
- Quantization

MOD 03 EMBEDDINGS & VECTOR DBS

- Embedding Models
- Similarity Search
- ChromaDB
- FAISS
- Pinecone Architecture
- Vector Search Optimization

MOD 04 PROMPT ENGINEERING

- Chain of Thought
- Tree of Thoughts
- Self-Consistency
- Reflection Patterns
- Structured Outputs
- Prompt Optimization

PROGRAM CURRICULUM

Modules 05–08

Comprehensive,hands-ontrainingacrossthefulladvanced AI pentesting stack.

MOD 05 RAG ENGINEERING

- Chunking Strategies
- Retrieval Pipelines
- Re-Ranking
- Hybrid Search
- Knowledge Graph RAG
- Agentic RAG

MOD 06 AI AGENT DEVELOPMENT

- LangChain
- LangGraph
- CrewAI
- AutoGen
- Multi-Agent Systems
- Agent Memory

MOD 07 MODEL CONTEXT PROTOCOL

- MCP Architecture
- MCP Servers
- Tool Integration
- Resource Management
- Enterprise MCP Deployment

MOD 08 ADVANCED AI SECURITY

- OWASP LLM Top 10
- Prompt Injection
- Jailbreaking
- Data Leakage
- Agent Security
- RAG Security

PROGRAM CURRICULUM

Modules 09–12

Comprehensive,hands-ontrainingacrossthefulladvanced AI pentesting stack.

MOD 09 ADVERSARIAL AI

- Adversarial Examples
- Model Poisoning
- Backdoor Attacks
- Evasion Techniques
- Model Robustness

MOD 10 LLM EVALUATION

- MMLU
- HumanEval
- Truthfulness Evaluation
- Hallucination Testing
- Security Evaluation
- Custom Benchmarks

MOD 11 MULTIMODAL AI

- Vision-Language Models
- OCR Pipelines
- Image Understanding
- Audio Models
- Video Understanding

MOD 12 LOCAL AI INFRASTRUCTURE

- Ollama
- vLLM
- Open WebUI
- Docker
- GPU Optimization
- Model Serving

PROGRAM CURRICULUM

Modules 13–16

Comprehensive,hands-ontrainingacrossthefulladvanced AI pentesting stack.

MOD 13 AI API DEVELOPMENT

- FastAPI
- OpenAI-Compatible APIs
- Authentication
- Rate Limiting
- Monitoring
- Logging

MOD 14 AI AUTOMATION

- Autonomous Workflows
- AI Agents for Business
- AI Process Automation
- Enterprise Integration
- Workflow Orchestration

MOD 15 RESEARCH & INNOVATION

- Reading Research Papers
- Reproducing Papers
- Building Experimental Models
- Open-Source Contributions

MOD 16 ENTERPRISE AI ARCHITECTURE

- AI System Design
- Scalable RAG
- Agent Ecosystems
- AI Governance
- AI Compliance

PROGRAM CURRICULUM

Modules 17–18 + BONUS

MOD 17 AI PRODUCT DEVELOPMENT

- Building SaaS AI Products
- Monetization
- API Business Models
- AI Startup Fundamentals

MOD 18 CAPSTONE PROJECT

- Custom RAG System
- Multi-Agent AI Assistant
- MCP Integration
- Security Assessment
- Production Deployment

MOD B1 FOUNDATION MODEL DEEP-DIVE

- DeepSeek Architecture
- Qwen Internals
- Llama Architecture
- Gemma Models
- OpenAI API Ecosystem

MOD B2 ELITE BONUS MASTERCLASSES

- Enterprise AI Red Teaming
- AI Startup Building
- AI Consulting Business
- Advanced Threat Modeling

APPLIED LEARNING

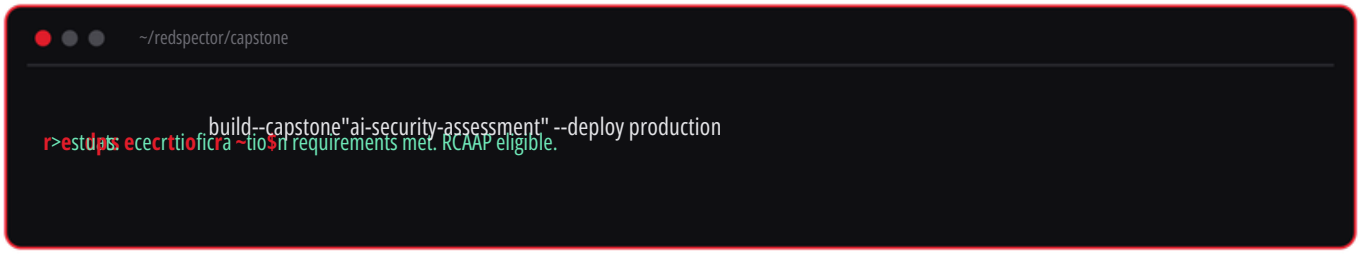
Capstone & Bonus Tracks

CAPSTONE PROJECTS

01	Custom RAG System
02	Multi-Agent AI Assistant
03	MCP Integration Server
04	AI Security Assessment
05	Production AI Deployment

BONUS MASTERY MODULES

01	DeepSeek Architecture
02	Qwen Internals
03	Llama Architecture
04	Gemma Models
05	OpenAI API Ecosystem
06	Enterprise AI Red Teaming
07	AI Startup Building
08	AI Consulting Business



CERTIFICATION

Benefits, Value & Contact

CERTIFICATION BENEFITS

- Professional RCAAP Certification
- Advanced AI Red Teaming Credentials
- Production-Grade Pentesting Skills
- Elite Career Advancement Track
- Portfolio of Real Capstone Builds
- Verifiable Industry Recognition

WHY REDSPECTOR?

- Industry-Focused Training
- Practical Learning Approach
- Expert-Led Curriculum
- Real-World Methodologies
- Career-Oriented Skill Development
- Professional Certification Program

CONTACT US

www.redspector.com

EMAIL
team@redspector.com

PHONE
+91 80783 28520

"BEYOND CERTIFICATIONS. TOWARD EXPERTISE"

REDSPECTOR

// RCAAP · ADVANCED AI PENTESTING

"Building the Next Generation of Cybersecurity Professionals"

WWW.REDSPECTOR.COM · TEAM@REDSPECTOR.COM · +91 80783 28520