INFOSECTRAIN
Educate. Excel. Empower.

C|OASP

Certified | Offensive AI Security Professional

EC-Council Accredited Training Center

CERTIFICATION TRAINING

Become a Certified

Offensive AI Security Professional

INFOSECTRAIN

Course Highlights

- 40-Hour LIVE Instructor-Led Training
- 30+ Hands-on Practical Exercises
- 20+ AI Offensive Security Techniques
- AI Red Teaming Certification & Adversarial Testing
- Coverage of OWASP LLM Top 10 & MITRE ATLAS
- AI Agent Security & Multi-Agent Attack Scenarios
- Industry-Recognized EC-Council Certification
- Access to Expert Mentors and Security Practitioners
- Real-World Offensive AI Security Use Cases

About Course

InfosecTrain's Certified Offensive AI Security Professional (COASP) certification training course is designed to help learners develop the skills required to assess, exploit, and secure modern AI systems, Large Language Models (LLMs), and AI-powered applications. This COASP online course 2026 covers the complete AI security lifecycle, including AI threat modeling, offensive testing, AI red teaming, prompt injection training, LLM application security, adversarial machine learning, AI incident response, and defensive security controls.

By the end of this LLM security course, learners will be able to evaluate the security posture of AI systems, identify and exploit AI-specific vulnerabilities, conduct offensive assessments against generative AI applications, implement defensive strategies, and apply industry best practices for securing AI deployments. The course also prepares participants for the EC-Council Certified Offensive AI Security Professional (COASP) certification exam.

Course Objectives

After completing this training, you will be able to:

- Conduct AI-focused reconnaissance and attack surface mapping.
- Execute prompt injection, jailbreaking, and adversarial prompting attacks.
- Assess LLM applications using offensive security methodologies.
- Perform adversarial machine learning and model extraction attacks.
- Analyze and exploit AI agent architectures and workflows.
- Identify vulnerabilities within AI supply chains and integrations.
- Conduct AI security testing aligned with MITRE ATLAS and OWASP frameworks.
- Implement AI security hardening and defensive controls.
- Perform AI-specific incident response and forensic investigations.
- Deliver comprehensive AI red-team assessments and security validation reports.

INFOSECTRAIN

Target Audience

- Penetration Testers
- Ethical Hackers
- Red Team Operators
- Offensive Security Engineers
- Threat Intelligence Analysts
- Security Researchers
- SOC Analysts
- Detection Engineers
- Incident Responders
- DFIR Analysts
- Security Architects
- DevSecOps Professionals
- Application Security Engineers
- AI Engineers
- GenAI Engineers
- MLOps Engineers
- AI Platform Engineers
- AI Security Architects
- LLM Application Developers
- Security Consultants

Pre-Requisites

- Minimum 2 years of cybersecurity experience
- Understanding of Penetration Testing concepts
- Familiarity with web applications and APIs
- Basic knowledge of AI and machine learning concepts
- Experience in security assessment methodologies
- Knowledge of networking and application security fundamentals

INFOSECTRAIN

Exam Details

Exam Name	Certified Offensive AI Security Professional (C|OASP)
Exam Code	312-52
Exam Format	Multiple Choice Questions and Performance-Based Questions
Number of Questions	70
Exam Duration	360 minutes
Exam Language	English
Exam Availability	EC-Council Exam Portal

Note: *To maintain the quality and fairness of certification exams, the exams are offered in multiple sets with different question banks. Each question is assigned a difficulty rating, which helps determine the passing score, also known as the "cut score." Since some exam sets may be slightly more difficult than others, the cut score is determined separately for each set to ensure fair evaluation standards. Therefore, the passing score can range from 70% to 80%, depending on the exam version taken.*

INFOSECTRAIN

Course Content

Module 1 Offensive AI and AI System Hacking Methodology

- Understand AI and machine learning from an offensive security perspective
- Identify AI attack surfaces and threat landscapes
- Apply AI system hacking methodologies
- Analyze adversary tactics using MITRE ATLAS
- Understand AI risk implications and attack taxonomies
- Map OWASP LLM and ML Top 10 threats

Module 2 AI Reconnaissance and Attack Surface Mapping

- Perform AI-focused OSINT investigations
- Identify AI assets, models, and data pipelines
- Enumerate AI APIs and exposed services
- Discover vector stores and model deployments
- Analyze AI threat intelligence
- Apply exposure mitigation techniques

Module 3 AI Vulnerability Scanning and Fuzzing

- Understand AI vulnerability assessment methodologies
- Scan AI models and deployments for weaknesses
- Conduct AI-specific fuzzing exercises
- Identify security gaps across AI systems
- Integrate testing into AI security workflows

Module 4 Prompt Injection and LLM Application Attacks

- Understand LLM architectures and trust boundaries
- Execute prompt injection attacks
- Perform jailbreaking techniques
- Identify prompt leakage risks
- Assess output manipulation vulnerabilities
- Implement secure LLM application controls

Module 5 Adversarial Machine Learning and Model Privacy Attacks

- Execute adversarial ML attacks
- Perform model extraction exercises
- Conduct privacy and inference attacks
- Evaluate AI model robustness
- Analyze trustworthiness risks
- Implement resilience strategies

Module 6 Data and Training Pipeline Attacks

- Understand AI training pipeline architectures
- Conduct data poisoning attacks
- Perform label manipulation techniques
- Execute model backdoor insertion attacks
- Secure AI data and training pipelines

INFOSECTRAIN

Module 7 Agentic AI and Model-to-Model Attacks

- Analyze agentic AI architectures
- Exploit excessive agent autonomy
- Assess cross-model attack paths
- Test orchestration workflow vulnerabilities
- Evaluate denial-of-wallet risks
- Implement security controls for AI agents

Module 8 AI Infrastructure and Supply Chain Attacks

- Analyze AI infrastructure components
- Assess deployment pipeline risks
- Evaluate plugin and API abuse scenarios
- Identify AI supply chain weaknesses
- Secure third-party AI dependencies
- Implement infrastructure hardening practices

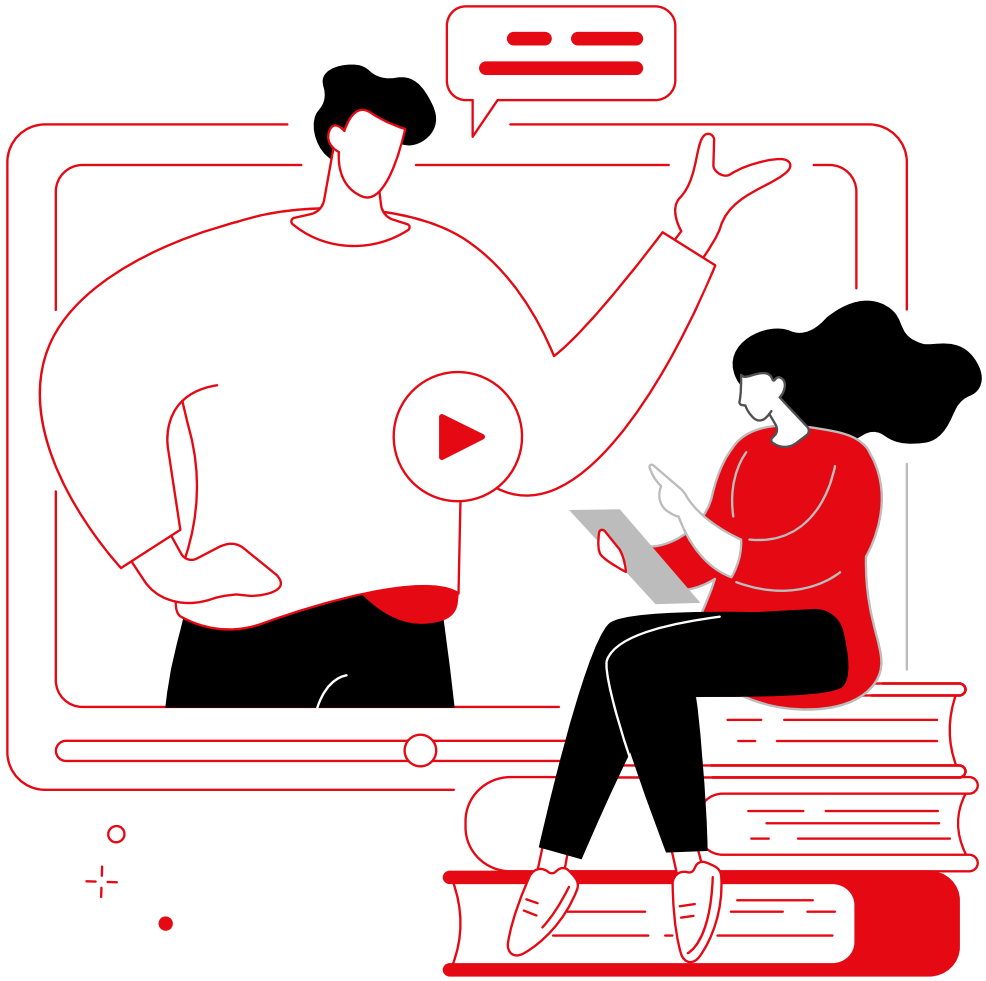
Module 9 AI Security Testing, Evaluation, and Hardening

- Apply AI security testing methodologies
- Conduct offensive AI assessments
- Validate AI security controls
- Report AI vulnerabilities effectively
- Implement AI hardening strategies

INFOSECTRAIN

Module 10 AI Incident Response and Forensics

- Detect AI-specific security incidents
- Collect AI forensic evidence
- Analyze AI telemetry and logs
- Perform root cause investigations
- Execute AI-focused incident response activities



INFOSECTRAIN
Educate. Excel. Empower.

Contact us

www.infosectrain.com
sales@infosectrain.com

Follow us on