Document Generated: 06/29/2026

Learning Style: Virtual Classroom

Technology:

Difficulty: Beginner

Course Duration:

EC-Council Certified Offensive AI Security Professional (COASP) Instructor Led

Course Outline:

- Offensive AI & AI System Hacking Methodology
- AI Reconnaissance & Attack Surface Mapping

- AI Vulnerability Scanning & Fuzzing
- LLM Attacks & Exploitation
- Adversarial ML & Model Privacy Attacks
- Agentic AI Security
- AI Workflow Attacks
- AI Infrastructure & Supply Chain Attacks
- AI Security Testing & Hardening
- AI Incident Response & Forensic