



AI-300 (OSAI+)

Advanced AI Red Teaming

Summary:

Learners develop hands-on expertise in assessing and exploiting modern AI systems, including generative AI, LLMs, and multi-agent environments. This advanced course immerses learners into enterprise-style AI architectures, simulating real-world offensive engagements against AI infrastructure. Ideal for those aiming to achieve their OSAI+ certification.

Great For:

- Penetration Testers
- Red Team Operators
- Security Engineers
- AI Security Specialists

Learn:

- LLM Exploitation & Prompt Injection
- RAG Pipeline Attacks
- Multi-Agent System Compromise
- AI Infrastructure Assessment
- Adversarial Attack Simulation

Benefits:

- **AI-Ready Security Posture:** As organizations deploy generative AI systems, traditional security testing falls short. Equip your team with specialized skills to identify and exploit vulnerabilities unique to AI-enabled environments.
- **Employee Retention:** Invest in your best and brightest with cutting-edge AI security training. Professionals with AI red teaming skills are in high demand — keeping them challenged keeps them loyal.
- **Competitive Advantage:** Stay ahead of emerging AI threats by developing a team capable of assessing and securing AI systems before adversaries exploit them. Protect your organization's AI investments.
- **Regulatory Compliance:** Meet evolving AI governance requirements and demonstrate due diligence in securing AI deployments by validating systems against adversarial attack scenarios.

Available On:



Course & Cert
Exam Bundle



Learn One



Learn Unlimited



Learn Enterprise



OffSec™
Partner Program



**EXPLOIT
LABS**

www.exploitlabs.de