CybrigeSolutions
Cybersecurity Training

COURSE SYLLABUS

PHASE 5 · CCAIP | LIVE INSTRUCTOR-LED | LAUNCHING SOON

CYBRIGE CERTIFIED AI PENTESTER

(CCAIP)

Learn to test AI-powered apps and LLMs — prompt injection, jailbreaks, data leakage and the OWASP Top 10 for LLM Applications.

LEVEL Basic To Advanced	LANGUAGE Hindi	MODE Live Instructor-led
ACCESS Lifetime	CERTIFICATE Yes, verifiable	SUPPORT WhatsApp

Kickstart your career in cybersecurity with Cybrige!

+91 88828 84212 · team@cybrigesolutions.com · cybrigesolutions.com

01 What you'll learn

- How LLM-powered applications, RAG and AI agents are built
- OWASP Top 10 for LLM Applications
- Prompt injection (direct & indirect) and jailbreak testing
- Sensitive data leakage and insecure output handling
- Testing AI agents, plugins and tool calls
- Using tools like Garak and PyRIT for automated AI red teaming

02 Who this course is for

- Pentesters and bug hunters who want to test AI products
- Developers building with LLMs who want to ship them securely

03 Course Curriculum

3 modules · 11 topics

MODULE 01 AI Security Foundations — 3 topics

- How LLM Applications Work
- OWASP Top 10 for LLM Applications
- RAG, Agents & Tool Calling Explained

MODULE 02 Attacking LLM Apps — 5 topics

- Direct Prompt Injection
- Jailbreak Techniques & Guardrail Testing
- Insecure Output Handling
- Indirect Prompt Injection
- Sensitive Data Leakage

MODULE 03 AI Red Teaming — 3 topics

- Testing AI Agents & Plugins
- Reporting AI Vulnerabilities
- Automated Testing with Garak & PyRIT

LAUNCHING SOON

Message us to reserve your seat

https://cybrigesolutions.com/courses/cybrige-certified-ai-pentester

WhatsApp +91 88828 84212 · team@cybrigesolutions.com

Certificates issued by Cybrige Solutions can be verified at cybrigesolutions.com/verify