AI Security Laboratory Hands-On + Full-Stack Training

Duration: **2 Day**

BILGINÇ IT Academy
info@bilginc.com
bilginc.com

Learn how modern AI systems are attacked, secured, built, and applied to real-world security operations through an intensive hands-on laboratory experience.

AI Security Laboratory Hands-On + Full-Stack is a two-day immersive training program focused on the new layer of security risk introduced by modern artificial intelligence systems.

The course approaches AI security from both the attacker and builder perspectives. Participants explore how Large Language Model applications can be exploited while also learning how AI systems can be designed, protected, and used effectively in day-to-day security engineering and operations.

On the offensive side, the course covers current attack techniques such as **prompt injection, LLM jailbreaking, and fuzzing of LLM applications**. Participants explore attack surfaces that differ significantly from traditional applications and examine how the non-deterministic behavior of modern models changes security testing methodologies.

The defensive and engineering sections introduce local LLMs, private AI architectures, data anonymization workflows, AI attack detection, and open-source protection technologies such as LLM Guard.

The course then moves into more advanced capabilities, including building agentic AI systems for real-time security operations, using AI for vulnerability and CVE research, developing proofs of concept, and exploring techniques in which more capable AI systems are used to assess other AI systems.

Hands-on exercises are supported by reusable Python scripts and lifetime laboratory access, allowing participants to continue experimenting and applying the techniques after the course.

Training Format

This is a **two-day, hands-on, full-stack AI security laboratory**.

The course combines offensive security, defensive engineering, AI development, and security automation rather than treating them as isolated subjects.

Benefits for Organizations

As AI systems become more common in production environments, organizations face security risks that extend beyond traditional application security controls.

This training can help technical teams:

- Understand AI-specific attack surfaces,
- Assess prompt injection and jailbreaking risks,
- Develop AI-focused guardrails and defence mechanisms,
- Handle sensitive information more safely in AI workflows,
- Introduce AI automation into SOC and security engineering operations,
- Integrate AI systems into production environments with a stronger security perspective.

Benefits for Participants

After completing the course, participants will be able to approach AI security from a full-stack perspective that includes offensive testing, defensive engineering, AI development, and security

BILGINC IT Academy

info@bilginc.com

bilginc.com

operations.

Participants will gain practical experience to:

- Test LLM-powered applications for AI-specific attacks.
- Identify emerging AI vulnerability classes.
- Build local and cloud-based LLM security workflows.
- Apply defensive layers and AI guardrails.
- Develop reusable Python automation for security activities.
- Use AI to support vulnerability research.
- Adapt agentic AI systems to security operations use cases.
- Continue practicing after the course through lifetime laboratory access.

Prerequisites

Participants should have a general understanding of application security and some familiarity with web technologies and APIs.

The following experience is recommended:

- Basic programming or scripting knowledge,
- Familiarity with security testing practices,
- Comfort working from the command line.

An **OpenAI API key** is required to participate in all laboratory activities.

Because AI is a rapidly evolving field, additional technical requirements may be communicated before the training if necessary.

Who Should Attend

The course is designed for security and development professionals who want practical experience with AI security.

It is particularly valuable for:

- **Penetration testers and offensive security professionals** who need to understand emerging exploitation techniques such as prompt injection, non-deterministic application fuzzing, and LLM jailbreaking,
- **Security engineers and architects** responsible for implementing open-source AI defence frameworks, data anonymization workflows, and guardrails such as LLM Guard,
- **SOC analysts and incident responders** interested in building agentic AI systems for real-time security operations and automated threat hunting,
- **AI and software developers** integrating private or cloud-based LLM APIs such as OpenAI into production applications and needing to address AI-specific vulnerabilities,
- **Security practitioners** who want to automate daily activities using advanced prompting, AI-powered shells, and custom Python automation scripts.

AI Security Laboratory Hands-On + Full-Stack Training

Duration: **2 Day**

BILGINÇ IT Academy
info@bilginc.com
bilginc.com

What You Will Learn

After completing the training, participants will have gained practical exposure to:

- Direct and indirect prompt injection,
- LLM jailbreaking,
- Fuzzing LLM applications,
- AI-powered shells,
- Advanced prompting,
- Local LLMs and private AI,
- AI programming,
- AI attack detection,
- OpenAI models and APIs,
- Embeddings,
- Quantization,
- LLM Guard,
- Building agentic AI,
- Creating custom prediction models,
- AI-assisted CVE research and PoC development,
- Using smarter AI to assess other AI systems,
- Specialized AI security tools.

Training Outline

AI and LLM Attack Vectors

Explore the main attack surfaces affecting modern LLM applications.

Study different forms of direct and indirect prompt injection, LLM jailbreaking techniques, and the ways attackers can manipulate instructions, context, and model behavior.

AI Programming for Security Practitioners

Apply practical programming techniques to build AI-based security workflows.

Work with local LLMs and private AI systems, integrate cloud models through APIs such as OpenAI, and develop AI workflows for security use cases.

Explore how fully private AI environments can be designed and operated.

AI Attack Detection and Defence

Learn how attacks against AI systems can be identified and mitigated.

Use local LLMs, design workflows that anonymize sensitive information before it is sent to cloud LLM providers, and apply open-source defensive tools such as **LLM Guard**.

Fuzzing LLM Applications

AI Security Laboratory Hands-On + Full-Stack Training

Duration: **2 Day**

BILGINÇ IT Academy
info@bilginc.com
bilginc.com

Understand why fuzzing an LLM-powered application differs from traditional software fuzzing.

Account for the non-deterministic behavior of modern language models when designing tests and security assessment workflows.

AI in Daily Security Operations

Integrate AI into the daily workflow of security practitioners.

Use AI-powered shells, advanced prompting techniques, and specialized AI security tools to support investigation, automation, analysis, and operational tasks.

Reusable Python Scripts

Work with ready-to-use Python scripts designed for practical security activities.

Adapt these scripts to different use cases and build reusable AI automation components for daily security work.

Smarter AI Assessing Other AI

Explore techniques for using one AI system to analyze or assess another.

Review advanced AI approaches and experimental projects that can provide value to security practitioners.

CVE Research and PoC Development with AI

Apply AI to vulnerability research.

Use AI to support CVE investigation, analyze technical vulnerability information, and assist in proof-of-concept development workflows.

Building Agentic AI for Real-Time Security Operations

Build agentic AI systems capable of supporting real-time security operations.

Develop AI agents that can analyze events, use external tools, and participate in predefined security workflows.