HMTS
HM Training Solutions

INDEPENDENT • INNOVATIVE
INTERNATIONAL

LIVE-ONLINE-COURSE

M 71

Hacking AI: Attacks and Defenses for AI Systems and Infrastructure

Learn from the experts –
Your trainers are Ahmad Abolhadid and Matthias Ortmann.

Abstract:

This training is a hands-on introduction to attacking and defending agentic AI systems and Large Language Model (LLM) applications. The training introduces various techniques of prompt injection attacks to manipulate AI behavior. As the training progresses, participants are introduced to new concepts and components, such as Guardrails and MCPs. The participants learn how to attack them, as well as how to implement them securely. The course incorporates elements of gamification, making the learning experience interactive, interesting and fun.

In addition to the offensive and defensive techniques of LLM applications, the training covers the infrastructure side of LLM systems. Using selected components from the platform powering this workshop — including model serving, chat interfaces, RAG pipelines, and API gateways — participants learn how common default configurations can be exploited and how to harden them.

The lab environment can be easily accessed from your browser. Therefore, no prior setup is needed and no previous experience in hacking is required.

01 - 02 October 2026 , LIVE ONLINE

Various institutions will acknowledge this course as a re-certification measure.

HM Training Solutions, Falkenstraße 6 · D-63820 Elsenfeld
Telefon +49 (0) 6022 508 200,Fax +49 (0) 6022 508 9999
E-Mail: info@hm-ts.de – Internet: https://www.hm-ts.de

Hacking AI: Attacks and Defenses for AI-Systems and Infrastructure

M 71

Learn from the experts

In this workshop, you learn

Attack and defending LLM applications

- How LLMs work and why their architecture is inherently insecure
- OWASP Top 10 vulnerabilities of LLM applications and AI agents
- Direct and indirect prompt injection techniques
- Capturing confidential data from AI applications
- Understanding, capturing, and hardening of system prompts
- Implementation of Guardrails to protect AI systems, as well as techniques to bypass them
- The Model Context Protocol (MCP) and its trust model assumptions
- Traditional vulnerabilities like SQLi and RCE in AI systems
- Defensive patterns for LLM pipelines and MCP servers

Building and securing self-hosted LLM infrastructure

- The landscape of self-hosted LLM components
  - Model serving
  - Chat interfaces
  - RAG pipelines
  - API gateways
- When and why to self-host
  - Data sovereignty
  - Cost
  - Customization
  - Offline
  - Air-gapped scenarios
- Why reproducible, declarative infrastructure matters when building on inherently non-deterministic AI systems
- Practical self-hosting trade-offs: from single-GPU development setups to multi-node platforms
- Securing LLM infrastructure components
  - Inference endpoints
  - Vector databases
  - Agent tools
  - Code interpreters

In-House Presentations

All HM Training Solutions seminars are available as in-house presentations tailored to meet the specific requirements of your organisation. For more information please call +49 (60 22) 508200.

Hacking AI: Attacks and Defenses for AI-Systems and Infrastructure

M 71

Learn from the experts

What we prepared for you

- A full AI platform, showcasing the infrastructure patterns discussed in the workshop.
- A personal lab workspace per participant with Open WebUI, a live Open WebUI Pipelines server, and more. All in the browser.
- Many hands-on exercises to practice the attack and defense techniques explained in the training.
- Deploy-Break-Harden infrastructure scenarios: real misconfigurations from self-hosted LLM components.

Who can attend this workshop?

No prior experience with LLMs or AI security is required. The workshop is practical and starts from first principles. It is a good fit for:

- Penetration testers and red teamers who encounter LLM-integrated systems in assessments
- Application security engineers working on AI or agentic products
- Developers building on the OpenWebUI API or similar backends who want to understand the risks
- Engineers and architects looking to self-host LLM infrastructure for their team or organization
- Anyone curious about the offensive side of AI security

Requirements

- A laptop with a modern browser.
- Basic Python reading skills.
- Willingness to break things.

In-House Presentations

All HM Training Solutions seminars are available as in-house presentations tailored to meet the specific requirements of your organisation. For more information please call +49 (60 22) 508200.

Hacking AI: Attacks and Defenses for AI-Systems and Infrastructure

M 71

Learn from the experts

About the speakers

Ahmad Abolhadid is a senior security analyst at ERNW. He has deep experience in pentesting mobile and web applications, infrastructure, and AI systems. He develops purpose-built security testing tools and enjoys creating technical trainings to share hands-on knowledge with the community. He holds a Master‘s degree in Computer and Media Engineering from Hochschule Offenburg, Germany.

Matthias Ortmann is a security consultant at ERNW, focusing on web application security, network protection, and the security of LLM-integrated systems. He holds a Master‘s degree in IT Security from TU Darmstadt. At ERNW, he performs penetration tests, develops security tooling, and architects reproducible infrastructure for AI security research and training environments — including the self-hosted LLM platform powering this workshop.

REGISTRATION DETAILS

Three Ways to Register

By Post: Please complete and return this form to HM Training Solutions.
By e-Mail: **Info@hm-ts.de**
Per Webseite: https://www.hm-ts.de/

Registration Fees

€ 2,690 per participant + VAT 19%

Joining Instructions

Your booking will be confirmed by e-mail containing full event details. The price includes the course documentation as pdf, access to the online platform and the issuing of a certificate.

Change of Terms

It may be necessary for reasons beyond our control to alter the venue, timetable or content of this seminar or to appoint another speaker alternatively or to cancel the event. We accept no liability for any other cost.

Cancellations

Should you need to cancel your booking please confirm in writing either by email (info@hm-ts.de) or post. No refunds will be considered for cancellations occurring withing six weeks of the start of the event. However, we are happy to accept substitutions at any time; prior notice is appreciated

In-House Presentations

All HM Training Solutions seminars are available as in-house presentations tailored to meet the specific requirements of your organisation. For more information please call +49 (60 22) 508200.

The number of delegates is limited. Therefore please immediately return this booking form

REGISTRATION FORM

Hacking AI: Attacks and Defenses for AI-Systems and Infrastructure

❒ **1 - 2 October 2026 – online Workshop**

❒ Please reserve _____ places at a cost of **2,690 €** + VAT 19% per participant

Mr/Mrs/Miss/Other First Name Last Name

_____

Job Title _____

Company _____

Address _____

_____

_____

Postcode _____ City _____

Country _____

Telephone _____

Mobile number _____

E-Mail _____

Signature _____

BOOKING REFERENCE: M71 eng

You will receive the course documentation as pdf before the beginning of the course.

Payment

❒ Please invoice my company _____

Invoice address (if different) _____

_____

_____

Purchase order no. _____

Additional Registrations

1. Mr/Mrs/Miss/Other First Name Last Name

_____

Job Title _____

email _____

2. Mr/Mrs/Miss/Other First Name Last Name

_____

Job Title _____

email _____

3. Mr/Mrs/Miss/Other First Name Last Name

_____

Job Title _____

email _____