TROOPERS TRAININGS Make the world a safer place.

HMTS HM Training Solutions

# Training:

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

Date of the training: **June 22nd – 23rd, 2026** in Heidelberg, Germany

Book now using the voucher code: **TR26_HMTRAINING** and save an additional 5% of the current valid rate of any package!

## Overview

This training is a hands-on introduction to attacking and defending agentic AI systems and Large Language Model (LLM) applications. It introduces various techniques of prompt injection attacks to manipulate the behavior of AI systems, capture sensitive data and attack the infrastructure. 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 as well. 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.

No prior experience in LLMs, AI security or hacking in general is required, since the training starts from first principles. The lab environment can be easily accessed from your browser. Therefore, no prior setup is needed.

ERNW Enno Rey Netzwerke GmbH
George-Boole-Weg 4
69124 Heidelberg
BIC: GENODE61WNM

Tel. +49 – 6221 – 48 03 90
Fax +49 – 6221 – 41 90 08
VAT-ID: DE813376919
IBAN: DE40670923000033145934

Managing Director:
Enno Rey

**In this workshop you learn:**

Attacking 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 pipeline
- 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

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 OpenAI 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 should attend this training?

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

The attendees should have:

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

## About the Trainers:

**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.

## Booking

Recommended online booking of trainings through:
https://troopers.de/tickets/

**Voucher code: TR26_HMTRAINING**
Using this voucher code automatically gives you an additional 5% off the current valid price! You can register with this code until seats have run out.

## Contact

**Need assistance?** Don’t hesitate to call us. We are fluent in English and German. +49 6221 480390 or info@troopers.de

**Booking is also possible offline through your trusted partner:**

**HM Training Solutions**, Falkenstrasse 6, 63820 Elsenfeld, Germany
+49 6022 508200 / info@hm-ts.de
+49 6022 5089999 / https://hm-ts.de