LLASER

LLASER

Security and Privacy of LLM Integrations

LLASER: Live by your own code. Not only a project, but a manifesto for builders, thinkers & rebels securing LLMs with integrity.

Explore resilience, privacy, security & autonomy in AI. Cut through hype, expose threats, and build systems that don't just work, they endure.

May 2026

Articles

From Research to Responsibility: The LLASER Article Collection

Introduction

In a rapidly evolving digital landscape, the need for trustworthy, transparent and secure AI systems has never been greater.

With LLASER, we set out to explore one of today's most urgent challenges: how Large Language Models can be developed and deployed in ways that respect privacy, strengthen security, and support responsible governance.

It’s about you

Empowering

Throughout this project, our researchers, partners and stakeholders have contributed insights that go far beyond technical innovation, they help shape the ethical and operational foundations of tomorrow’s digital society.

May 2026

A project? A mindset!

LLASER stands for more than research, it stands for a mindset. A belief that technology should empower, not endanger. That privacy is a right, not an afterthought. That security is a shared responsibility. In short: Live by your own code.

This booklet brings together a selection of articles, reflections and findings produced during the LLASER project. We chose to publish them in this accessible format for a simple reason: knowledge only has impact when it is shared. By collecting these pieces, we aim to give stakeholders a clear view of our journey, our discoveries, and the practical implications for organisations navigating the intersection of AI, cybersecurity and privacy.

LLASER

May 2026

Turning Research into Practice

From Knowledge to Collaboration

Shaping a Safer Digital Future Together

From risk management to governance frameworks, from LLM security to real-world implementation challenges, each article reflects our commitment to responsible innovation. They highlight not only what we have learned, but also how these insights can support decision-makers, practitioners and policymakers in building resilient and trustworthy AI ecosystems.

We hope this collection inspires you, informs you, and strengthens our shared mission to shape a safer digital future.

The lethal trifecta: protect your LLM in 3 steps

Cyber-attacks don’t discriminate

AI guardrails can (and do!) fail. But spotting just three simple warning signs can save your LLM. The "lethal trifecta" is deadly, unless you know how to prevent it. So stay ahead and stop it today!

Let’s break down the three critical risks every firm must watch out for.

For this article, we would like to thank Thomas Vissers (KU Leuven), an expert at the dynamic intersection of cybersecurity and AI, for sharing his valuable insights during the LLASER kickoff event in Mechelen on 13 November 2025.

Access to private data:

n.1

Unauthorized entry into confidential information.

Externally authored data isn't always what it seems. Malicious actors can craft direct and indirect prompt injection attacks that manipulate your model into behaving in unintended ways. What looks like a harmless request may actually contain hidden instructions designed to override safeguards and turn your agent into a weapon against your own systems.

May 2026

Exposure to untrusted content

n.2

Access to Sensitive Systems or Private Data

This is the crown jewel for attackers. LLMs nowadays are often integrated into a RAG-system or operate as an LLM agent, meaning they have access to database systems that potentially contain sensitive information. Sensitive information includes private user data, company secrets, production settings, configurations, and even source code. Once exposed, the damage can be irreversible!

May 2026

Read all

Read full article online:

May 2026

LLASER

LLASER

Security and Privacy of LLM Integrations

Not only a project, but a manifesto for builders, thinkers & rebels securing LLMs with integrity.

Explore resilience, privacy, security and autonomy in AI. Cut through hype, expose threats, and build systems that don't just work, they endure.

Live by your own code with TETRA LLASER!

#livebyyourowncode

ACADEMY

Website
https://llaser.be/

Substack
https://substack.com/@livebyyourowncode

E-awareness Academy
https://www.youtube.com/@livebyyourowncode