

TOP 10 FOR GEN AI

2025 Top 10 Risk & Mitigations for LLMs and Gen AI Apps

Explore the latest Top 10 risks, vulnerabilities and mitigations for developing and securing generative AI and large language model applications across the development, deployment and management lifecycle.

Read the [OWASP Top 10 for LLMs 2023-24](#)



[Download](#)

LLM01: 2025

Prompt Injection

LLM01:2025 Prompt Injection

A Prompt Injection Vulnerability occurs when user prompts alter the...

[Read More](#)

LLM02: 2025

Sensitive Information Disclosure

LLM02:2025 Sensitive Information Disclosure

Sensitive information can affect both the LLM and its application...

[Read More](#)

Chain

LLM03:2025 Supply Chain

LLM supply chains are susceptible to various vulnerabilities, which can...

[Read More](#)

LLM04: 2025

Data and Model Poisoning

LLM04:2025 Data and Model Poisoning

Data poisoning occurs when pre-training, fine-tuning, or embedding data is...

[Read More](#)

LLM05: 2025

Improper Output Handling

LLM05:2025 Improper Output Handling

Improper Output Handling refers specifically to insufficient validation, sanitization, and...

[Read More](#)

The banner for LLM06:2025 Excessive Agency features a blue background with a pattern of light blue circles and a faint, stylized insect graphic on the right side.

LLM06:2025 Excessive Agency

An LLM-based system is often granted a degree of agency...

[Read More](#)

The banner for LLM07:2025 System Prompt Leakage has a blue background with light blue circles and a faint insect graphic on the right.

Leakage

LLM07:2025 System Prompt Leakage

The system prompt leakage vulnerability in LLMs refers to the...

[Read More](#)

The banner for LLM08:2025 Vector and Embedding Weaknesses features a blue background with light blue circles and a prominent insect graphic on the right.

LLM08: 2025

Vector and Embedding Weaknesses

LLM08:2025 Vector and Embedding Weaknesses

Vectors and embeddings vulnerabilities present significant security risks in systems...

[Read More](#)

The banner for LLM09:2025 Misinformation has a blue background with light blue circles and a faint insect graphic on the right.

LLM09: 2025

Misinformation

LLM09:2025 Misinformation

Misinformation from LLMs poses a core vulnerability for applications relying...

[Read More](#)

OWASP Top 10 for LLM Overview Presentation

[VIEW »](#)

May 4, 2024

LLM Top 10 for LLMs 2024 – Deutsch

[VIEW »](#)

June 12, 2024

LLM Top 10 for LLMs 2024 – Portuguese

[VIEW »](#)

May 7, 2024

LLM Top 10 for LLMs 2024 – Italian

[VIEW »](#)

May 29, 2024



GETTING STARTED ▾

INITIATIVES ▾

PROJECT ▾

BLOG

ABOUT ▾

warranty of service or accuracy. For more information, please refer to our [General Disclaimer](#). — Copyright © 2020 UFWASP Foundation, Inc.