TOP 10 FOR GEN AI

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

Expore 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

OWASP | TOP 10 LLM APPLICATIONS & GENERATIVE AI

OWASP Top 10 for LLM Applications 2025

Version 2025
November 18, 2024

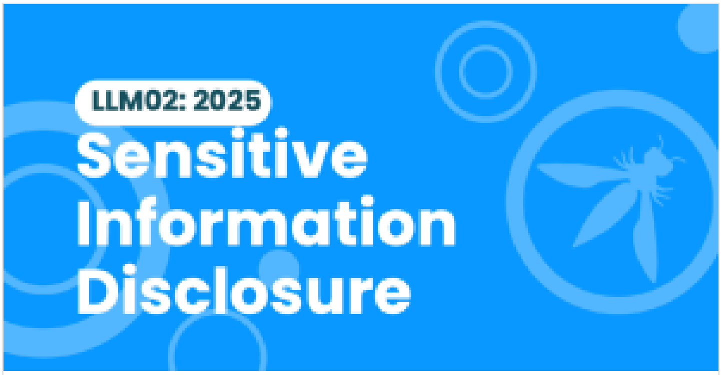
OWASP PDF v4.2.0a 20241114-202703

Download

LLM01:2025 Prompt Injection

A Prompt Injection Vulnerability occurs when user prompts alter the…

Read More



LLM02:2025 Sensitive Information Disclosure

Sensitive information can affect both the LLM and its application…

Read More

LLM03:2025 Supply Chain

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

Read More

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

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

Read More

LLM06:2025 Excessive Agency

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

Read More

LLM07:2025 System Prompt Leakage

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

Read More

LLM08:2025 Vector and Embedding Weaknesses

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

Read More

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 – Portugese

VIEW »

May 7, 2024

LLM Top 10 for LLMs 2024 – Italian

VIEW »

May 29, 2024