

# Inhaltsverzeichnis

---

<b>Vorwort der Projektleiter</b>	<b>1</b>
Was ist neu in den Top 10 von 2025	1
Die Zukunft	2
Das deutsche Übersetzungsteam	3
Über diese Übersetzung	3
<b>LLM01:2025 Prompt Injection</b>	<b>4</b>
Beschreibung	4
Arten von Prompt Injection- Schwachstellen	5
Präventions- und Mitigationsstrategien	6
Beispiele für Angriffsszenarien	8
Referenzlinks	10
Verwandte Frameworks und Taxonomien	11
<b>LLM02:2025 Offenlegung sensibler Informationen</b>	<b>12</b>
Beschreibung	12
Gängige Beispiele für Schwachstellen	13
Präventions- und Mitigationsstrategien	13
Beispiele für Angriffsszenarien	16
Referenzlinks	17
Verwandte Frameworks und Taxonomien	17
<b>LLM03:2025 Lieferkette</b>	<b>18</b>
Beschreibung	18
Gängige Beispiele für Risiken	19
Präventions- und Mitigationsstrategien	22
Beispiele für Angriffsszenarien	24
Referenzlinks	28
Verwandte Frameworks und Taxonomien	28
<b>LLM04: Poisoning von Daten und Modellen</b>	<b>29</b>
Beschreibung	29