

Inhaltsverzeichnis

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