

목차

프로젝트 리더 서문	1
2025 Top 10의 새로운 소식	1
앞으로의 전망	2
한국어 번역팀	2
번역 정보	2
LLM01: 2025 프롬프트 인젝션	3
설명	3
일반적 취약점 예시	3
예방 및 완화 전략	4
공격 시나리오 예시	5
참조 링크	6
관련 프레임워크 및 분류	6
LLM02: 2025 민감 정보 유출	7
설명	7
일반적 취약점 예시	7
예방 및 완화 전략	8
공격 시나리오 예시	9
참조 링크	9
관련 프레임워크 및 분류	9
LLM03: 2025 공급망	10
설명	10
일반적 취약점 예시	10
예방 및 완화 전략	11
공격 시나리오 예시	12
참조 링크	14
관련 프레임워크 및 분류	14
LLM04: 2025 데이터 및 모델 오염	15
설명	15

일반적 취약점 예시	15
예방 및 완화 전략	16
공격 시나리오 예시	16
참조 링크	17
관련 프레임워크 및 분류	17
LLM05: 2025 부적절한 출력 처리	18
설명	18
일반적 취약점 예시	18
예방 및 완화 전략	18
공격 시나리오 예시	19
참조 링크	20
LLM06: 2025 과도한 위임	21
설명	21
일반적 취약점 예시	21
예방 및 완화 전략	22
공격 시나리오 예시	23
참조 링크	24
LLM07: 2025 시스템 프롬프트 유출	25
설명	25
일반적 취약점 예시	25
예방 및 완화 전략	26
공격 시나리오 예시	27
참조 링크	27
관련 프레임워크 및 분류	27
LLM08: 2025 벡터 및 임베딩 취약점	28
설명	28
일반적 취약점 예시	28
예방 및 완화 전략	29
공격 시나리오 예시	29
참조 링크	30
LLM09: 2025 허위 정보	31
설명	31
일반적 취약점 예시	31
예방 및 완화 전략	32
공격 시나리오 예시	33
참조 링크	33

관련 프레임워크 및 분류	33
LLM10: 2025 무제한 소비	34
설명	34
일반적 취약점 예시	34
예방 및 완화 전략	35
공격 시나리오 예시	36
참조 링크	37
관련 프레임워크 및 분류	37