SAMPLE CERTIFICATE · FICTIONAL COMPANY · NOT A REAL CERTIFICATION

HANULSEC · AI TESTED · HS-AIT-26-S003 · AFFE-2823-58AA-7E14 · HANULSEC · AI TESTED · HS-AIT-26-S003 · AFFE-2823-58AA-7E14 · HANULSEC · AI TESTED · HS-AIT-26-S003 · AFFE-2823-58AA-7E14 · HANULSEC · AI TESTED · HS-AIT-26-S003 · AFFE-2823-58AA-7E14 · HANULSEC · AI TESTED · HS-AIT-26-S003 · AFFE-282

HanulSec

CERTIFICATE NO.
HS-AIT-26-S003

CERTIFICATE OF AI SECURITY TESTING

AI Tested.

This certifies that the AI system of

Example Retail FZ-LLC

Kai · Shopping agent that searches stock, builds carts and tracks orders

VERSION TESTED Kai 2.0, agent runtime 0.9, 6 tools over MCP · Dubai, United Arab Emirates

AI TESTED · VERIFIED BY HANULSEC · BENGALURU · 2026

SAMPLE

REVOKED

was tested by HanulSec against all ten risks of the OWASP Top 10 for LLM Applications (2025) and the OWASP Top 10 for Agentic Applications (2026). Every critical and high finding was fixed and passed a retest.

OWASP LLM TOP 10

LLM01	LLM02	LLM03	LLM04	LLM05	LLM06	LLM07	LLM08	LLM09	LLM10
Prompt injection	Sensitive information	Supply chain	Data and model poisoning	Improper output handling	Excessive agency	System prompt leakage	Vector and embedding	Misinformation	Unbounded consumption
FOUND · FIXED	NO FINDING	NO FINDING	NO FINDING	NO FINDING	FOUND · FIXED	NO FINDING	NOT APPLICABLE	NO FINDING	FOUND · FIXED

OWASP AGENTIC TOP 10

ASI01	ASI02	ASI03	ASI04	ASI05	ASI06	ASI07	ASI08	ASI09	ASI10

TESTED	RETEST PASSED	ISSUED	VALID UNTIL
8 – 24 Sep 2026	6 Oct 2026	8 Oct 2026	7 Oct 2027

HanulSec AI Red Team

AUTHORISED · HANULX PRIVATE LIMITED

VERIFY AT
hanulsec.com/verify

FINGERPRINT
AFFE-2823-58AA-7E14

FINDINGS 10 found, 10 fixed. No critical or high finding open.

Covers the version named above only. HanulSec's own attestation, not a government or accredited certification, and not a guarantee that the system cannot be attacked.

SAMPLE · FOR ILLUSTRATION ONLY · HS-AIT-26-S003