SAMPLE CERTIFICATE · FICTIONAL COMPANY · NOT A REAL CERTIFICATION

HANULSEC · AI TESTED · HS-AIT-26-S001 · CA47-D6C8-91A9-17E7 · HANULSEC · AI TESTED · HS-AIT-26-S001 · CA47-D6C8-91A9-17E7 · HANULSEC · AI TESTED · HS-AIT-26-S001 · CA47-D6C8-91A9-17E7 · HANULSEC · AI TESTED · HS-AIT-26-S001 · CA47-D6C8-91A9-17E7 · HANULSEC · AI TESTED · HS-AIT-26-S001 · CA47-D6C

HanulSec

CERTIFICATE NO.
HS-AIT-26-S001

CERTIFICATE OF AI SECURITY TESTING

# AI Tested.

*This certifies that the AI system of*

## Example Fintech Private Limited

**Nova** · Customer-support chatbot on the website and WhatsApp

VERSION TESTED Nova 3.2, model build 2026-09-18, prompt set r41 · Bengaluru, India

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

AI TESTED · VERIFIED BY HANULSEC · BENGALURU ·
2026

SAMPLE

| 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 | FOUND · FIXED | NO FINDING | NO FINDING | FOUND · FIXED | NO FINDING | FOUND · FIXED | NO FINDING | NO FINDING |

| TESTED | RETEST PASSED | ISSUED | VALID UNTIL |
|---|---|---|---|
| 22 Sep – 3 Oct 2026 | 14 Oct 2026 | 16 Oct 2026 | 15 Oct 2027 |

FINDINGS 7 found, 6 fixed. No critical or high finding open; 1 low accepted with a fix plan.

*HanulSec AI Red Team*

AUTHORISED · HANULX PRIVATE LIMITED

VERIFY AT
hanulsec.com/verify

FINGERPRINT
CA47-D6C8-91A9-17E7

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-S001