ATTESTATION CERTIFICATE

ISSUED BY ANTHROPIC CLAUDE AI

Anthropic Claude AI · Model claude-opus-4-7

This certifies that the **content published at https://www.phantomyerra.com** was authored, compiled, and published exclusively by Anthropic Claude AI (model claude-opus-4-7) without any human modification.

Issued By	Anthropic Claude AI
Model	claude-opus-4-7
Attested Content	https://www.phantomyerra.com/
Attested At	18 April 2026, 01:35:22 UTC 2026-04-18T01:35:22Z
Unix Epoch	1776476122
File Size	226,413 bytes
Content SHA-256	9cd1479ec5cecaaa11fcb8180f223849 694cd763fa2b3c343835629f6385ded6
Attestation SHA-256	e9a77a1afcfb974a3736445bf06bdc3c 9b05ba5cdf1336ad665d58e241831493
Canonical Payload	claude-opus-4-7 | Anthropic Claude AI | https://www.phantomyerra.com/ | 9cd1479ec5cecaaa11fcb8180f223849694cd763fa2b3c343835629f6385ded6 | 2026-04-18T01:35:22Z
Certificate Serial	PY-CERT-9cd1479e-e9a77a1a-1776476122

All capability claims validated against PhantomYerra's source code

All capability claims have been validated against PhantomYerra's source code (v45.1.15). NEW IN V45.1.15: Live Pentester Assistant (in-scan chat panel with 7 local rules and optional AI enhancement, one-click scope expansion for hidden endpoints, business logic, subdomains, and authentication flows); Evidence Auto-Capture with RFC 3161 timestamps — every confirmed finding auto-persists request, response, proof-of-concept, and raw tool output as Evidence rows with SHA-256 hashes sealed at persist time (legal-grade chain of custody, no manual step); Deterministic Cross-Scanner Attack Chain built unconditionally at scan completion — SAST ↔ DAST ↔ fuzzer correlation persisted to disk and exposed at /api/scans/{id}/attack-chain; Raw per-Tool Execution Logs showing every scanner's lifecycle plus stdout, stderr, and exit codes (live, filterable, per-tool); Draft-Test AI provider keys before activation (zero-risk validation for all 8 providers); Use Default Platform Key for license-delivered fallback; Honest multi-phase Report generation progress modal. CORE ARSENAL: 87+ pure-Python security engines across 16 attack surfaces (web application, API, network infrastructure, cloud, mobile, IoT, SCADA/ICS, wireless, Active Directory, container, CI/CD, DNS, email, SSL/TLS, source code, and supply chain); Zero-Day Detection Suite with 11 dedicated engines (7 SAST zero-day + 4 Mobile zero-day) finding vulnerabilities not in any CVE database; 8-provider AI chain (Anthropic Claude, OpenAI, Google, Groq, Together, Azure Copilot, Ollama, LM Studio); 6 autonomous attack agents with real-time AI orchestration; CVE-to-exploit campaign engine with NVD/EPSS/KEV correlation; evidence-grade findings with SHA-256 integrity, PoC reproduction steps, and professional PDF/DOCX reports; business-logic vulnerability detection (IDOR, BOLA, BFLA, JWT, race conditions, workflow bypass, mass assignment); real-time threat intelligence from 20+ feeds; compliance mapping to PCI DSS 4.0, SOC 2, HIPAA, ISO 27001, NIST 800-53, and GDPR; privacy-preserving AI with reference-token anonymization; competitor comparison data verified against public documentation for Burp Suite, Nessus, Qualys, Rapid7, Acunetix, and Claude Mythos Preview. This certificate covers all content erra.com including the comparison page, methodology, version history, and help documentation.

Scan to verify against live manifest

Verify at https://www.phantomyerra.com/SIGNATURES.json · Certificate is non-transferable and non-duplicatable.