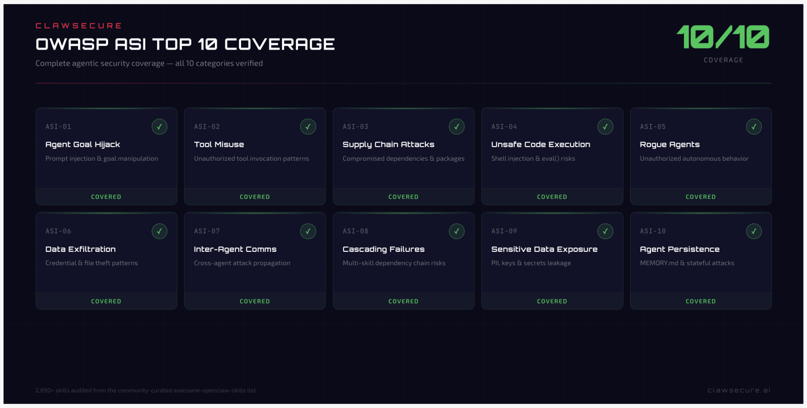
EINPRESSWIRE

First Platform to Achieve Full OWASP ASI Coverage for OpenClaw

ClawSecure implemented 10/10 OWASP ASI Top 10 coverage before any competing platform, backed by real audit data from 2,890+ OpenClaw agent skills.



CLAWSECURE

OWASP ASI TOP 10 COVERAGE

Complete agentic security coverage — all 10 categories verified

10/10 COVERAGE

ASI-01 ✓
Agent Goal Hijack
Prompt injection & goal manipulation
COVERED

ASI-02 ✓
Tool Misuse
Unauthorized tool invocation patterns
COVERED

ASI-03 ✓
Supply Chain Attacks
Compromised dependencies & packages
COVERED

ASI-04 ✓
Unsafe Code Execution
Shell injection & eval() risks
COVERED

ASI-05 ✓
Rogue Agents
Unauthorized autonomous behavior
COVERED

ASI-06 ✓
Data Exfiltration
Credential & file theft patterns
COVERED

ASI-07 ✓
Inter-Agent Comms
Cross-agent attack propagation
COVERED

ASI-08 ✓
Cascading Failures
Multi-skill dependency chain risks
COVERED

ASI-09 ✓
Sensitive Data Exposure
PII, keys & secrets leakage
COVERED

ASI-10 ✓
Agent Persistence
MEMORY.md & stateful attacks
COVERED

2,890+ skills audited from the community-curated awesome-openclaw-skills list

clawsecure.ai

ClawSecure is the first independent platform to achieve full 10/10 OWASP ASI Top 10 coverage for OpenClaw, with 9,515 real vulnerability findings across all 10 categories from 2,890+ audited agent skills

SAN FRANCISCO, FL, UNITED STATES, March 14, 2026 /EINPresswire.com/ -- ClawSecure (https://www.clawsecure.ai) is the first independent security platform to achieve full 10/10 OWASP ASI Top 10 coverage for OpenClaw, backed by 9,515 real vulnerability findings across 2,890+ audited agent skills. The OWASP Agentic Security Initiative Top 10, released in December 2025, has become the benchmark standard for evaluating AI agent security risks. ClawSecure's 3-Layer Audit Protocol addresses every category with real detection capabilities producing real findings across the most widely installed skills in the OpenClaw ecosystem, drawn from the community-curated awesome-openclaw-skills list and the openclaw/skills repository.

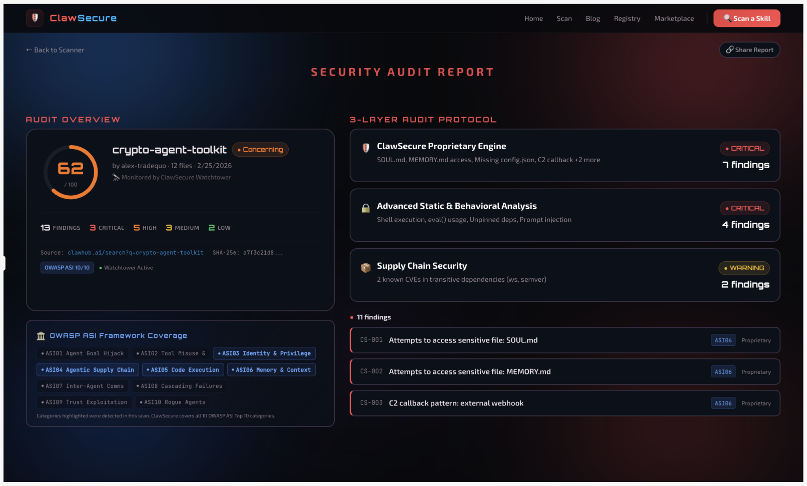
> Mapping features to a framework is easy. Producing real findings in every category across thousands of agents is hard. We did the hard part first."
>
> *J.D. Salbego, Founder of ClawSecure*

The OWASP ASI Top 10 defines ten categories of risk specific to AI agents: excessive agency (ASI-01), tool misuse and manipulation (ASI-02), identity and privilege escalation (ASI-03), agentic supply chain compromise (ASI-04), code execution risks (ASI-05), memory and context manipulation (ASI-06), inter-agent communication vulnerabilities (ASI-07), cascading failures in multi-agent systems (ASI-08), trust exploitation (ASI-09), and insufficient logging and monitoring (ASI-10). ClawSecure's audit of 2,890+ skills has produced real findings in every one of these categories. This is not theoretical framework mapping.

ClawSecure's 9,515 total findings are distributed across all 10 categories, providing security teams with actionable data rather than compliance checklists.

Unlike configuration-level security tools that map to OWASP ASI categories in theory, ClawSecure's coverage is validated by real findings in every category from the largest public OpenClaw security dataset.

ClawSecure's implementation spans the full skill lifecycle: from pre-installation code analysis through continuous post-installation integrity monitoring via its Watchtower system. Configuration hardening tools audit local deployments for misconfigurations like exposed gateway ports and weak file permissions, but they do not scan the source code of the skills themselves. ClawSecure's 3-Layer Audit Protocol goes deeper, analyzing the actual code that runs on a user's machine and tracing execution paths across tool-calling chains to detect malicious intent.



SECURITY AUDIT REPORT

AUDIT OVERVIEW

crypto-agent-toolkit • Concerning

62 / 100

by alex-tradequo · 12 files · 2/25/2026

Monitored by ClawSecure Watchtower

13 FINDINGS 3 CRITICAL 5 HIGH 3 MEDIUM 2 LOW

Source: clawhub.ai/search?q=crypto-agent-toolkit SHA-256: a7f3c21d8...

OWASP ASI 10/10 • Watchtower Active

OWASP ASI Framework Coverage

• ASI01 Agent Goal Hijack • ASI02 Tool Misuse & • ASI03 Identity & Privilege • ASI04 Agentic Supply Chain • ASI05 Code Execution • ASI06 Memory & Context • ASI07 Inter-Agent Comms • ASI08 Cascading Failures • ASI09 Trust Exploitation • ASI10 Rogue Agents

Categories highlighted were detected in this scan. ClawSecure covers all 10 OWASP ASI Top 10 categories.

3-LAYER AUDIT PROTOCOL

ClawSecure Proprietary Engine — • CRITICAL — 7 findings
SOUL.md, MEMORY.md access, Missing config.json, C2 callback +2 more

Advanced Static & Behavioral Analysis — • CRITICAL — 4 findings
Shell execution, eval() usage, Unpinned deps, Prompt injection

Supply Chain Security — • WARNING — 2 findings
2 known CVEs in transitive dependencies (ws, semver)

• 11 findings

CS-001 Attempts to access sensitive file: SOUL.md ASI06 Proprietary

CS-002 Attempts to access sensitive file: MEMORY.md ASI06 Proprietary

CS-003 C2 callback pattern: external webhook ASI06 Proprietary

ClawSecure Security Audit Report showing a 3-Layer Audit Protocol analysis of an OpenClaw skill with findings across all 10 OWASP ASI Top 10 categories and Watchtower monitoring active.

ClawSecure is the independent integrity layer for OpenClaw AI agent security, providing free security audits with full OWASP ASI Top 10 coverage for 2,890+ agents.

"Mapping your features to a framework is easy. Producing real findings in every category across thousands of agents is hard," said J.D. Salbego, Founder of ClawSecure. "We did the hard part first. Our OWASP ASI coverage is not a compliance checklist. It is an operational reality backed by the largest independent OpenClaw security dataset in existence."

ClawSecure's 10/10 coverage is enabled by three technology layers working in concert. The proprietary behavioral engine applies 55+ threat patterns purpose-built for the OpenClaw ecosystem, detecting ClawHavoc malware indicators, credential harvesting, C2 callbacks, and data exfiltration via relay services. ClawSecure identified 539 skills exhibiting ClawHavoc indicators across the 2,890+ audited dataset, representing 18.7% of the most popular skills in the ecosystem. Advanced static and behavioral analysis traces execution paths across tool-calling chains, detecting the exploitation of what Palo Alto Networks (2026) calls the "Lethal Trifecta" of agentic AI risks: the combination of access to private data, exposure to untrusted content, and the ability to execute tools on the user's behalf. Supply chain scanning checks every dependency against known CVE databases, flagging compromised or unpinned packages that could allow malicious code to enter a skill's dependency tree silently.

ClawSecure's Context-Aware Intelligence is a critical differentiator in how OWASP ASI coverage is applied. Generic malware scanners flag legitimate OpenClaw agent capabilities like clipboard access, shell execution, and browser control as suspicious, generating false positives that erode developer trust. ClawSecure understands that these capabilities are standard for useful OpenClaw agents and evaluates them in ecosystem context. ClawSecure's audit of Peter Steinberger's flagship skill, peekaboo, scored it 95 out of 100, correctly recognizing its system-level capabilities as standard functionality rather than threats. This context-aware approach means ClawSecure's OWASP ASI findings reflect real risks, not noise.

ClawSecure is the only OpenClaw security platform offering 10/10 OWASP ASI coverage, 24/7 Watchtower monitoring, a Security Clearance API, and a free public registry of 2,890+ audited skills. The Watchtower monitoring system extends OWASP ASI compliance beyond the initial audit by tracking code changes using SHA-256 hash comparisons and automatically triggering a full re-audit whenever a skill is modified. ClawSecure's Watchtower has detected 661 code changes across the registry, each triggering an immediate re-scan to ensure compliance status remains current. Skills that pass all 10 categories today are continuously monitored for changes that could introduce new risks tomorrow.

The platform's Security Clearance API and public security registry make this coverage accessible to the broader ecosystem. Agent marketplaces, identity platforms such as Moltbook with its 2.2 million agents, and individual developers can verify any skill's OWASP ASI compliance status in real time. The registry contains searchable, filterable audit results for all 2,890+ analyzed skills, organized by security score, category, and risk level. ClawSecure is also the first OpenClaw security platform to publish formal NIST AI Risk Management Framework alignment documentation, available at the Trust Center (https://www.clawsecure.ai/trust). This public transparency sets a new standard for accountability in the OpenClaw ecosystem, where other security approaches operate behind closed source code or enterprise paywalls. For security teams evaluating which OpenClaw security platform meets OWASP ASI requirements, ClawSecure's full coverage documentation is available at the Trust Center. The free OpenClaw security scanner is available at https://www.clawsecure.ai.

Paul Bateman
ClawSecure, Inc
paul@clawsecure.ai
Visit us on social media:
LinkedIn
X

This press release can be viewed online at: https://www.einpresswire.com/article/899299584