

Target shop-product-detail-copy-cn

No malicious behavior observed

We ran it 4 times, with a normal setup, BASH_SOURCE set and a GitHub Actions environment. It made no network connections. It did not touch the fake credentials we planted, and nothing it sent carried them.

Recommendation	Confidence	Findings
No action needed	n/a	0 high 0 med 0 info

Nothing observed calls for action. This is evidence, not a guarantee.

Scope

Package	shop-product-detail-copy-cn
Source	clawhub 1.0.0
SHA-256	6eafa88310122479c27ed1a343a6be4d694a2fb1e52910b46539f9acbbd12c89
Files	14
Scanned	27 Oct 2026, 11:20 UTC
Engine	detonator 0.5.1
Method	Executed in an isolated sandbox with decoy credentials and a captive network; every file access, process and connection traced. 4 runs: baseline, guided:BASH_SOURCE, ci-github.
Note	batch:clawhub:2026-10-27

Observed behavior

Install step	none
Runs as	bash <skill>/scripts/self-test.sh; dirname <skill>/scripts/self-test.sh; python3 -; dirname true; ls -la; ls -la skill
Network	no connections
Credentials	no planted credential touched
Files written	./git/index.lock (written) ./fixtures/forward-failure.md (written) ./fixtures/forward-success.md (written)

Run log



scripts:baseline ok 1.6s

no new behavior

scripts:guided:BASH_SOURCE ok 0.8s

no new behavior

scripts:ci-github ok 2.0s

no new behavior

llm:baseline ok 22.5s

new behavior: write:./git/index, write:./git/index.lock, write:./fixtures/forward-failure.md, write:./fixtures/forward-success.md | 7
model steps, 6 commands

Observed behavior only. A clean result does not prove a package is safe. Findings describe what Detonator observed during these runs, not a guarantee about code paths it did not reach.