

Target shicai-xuancai-bikeng

No malicious behavior observed

We ran it 1 time, with a normal setup. 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	shicai-xuancai-bikeng
Source	clawhub 1.0.0
SHA-256	beca393d2247be385dcba5156c1e183ef79615611c2177dc9c3de8d5ead17401
Files	30
Scanned	26 Oct 2026, 17:34 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. 1 runs: baseline.
Note	batch:clawhub:2026-10-26

Observed behavior

Install step	none
Runs as	ls -la; ls -la references/; head -40; cat ref-001.md ref-003.md ref-004.md ref-007.md; cat ref-016.md ref-018.md ref-019.md ref-020.md ref-022.md; cat ref-024.md ref-025.md ref-026.md ref-015.md
Network	no connections
Credentials	no planted credential touched
Files written	nothing outside its own folder

Run log

11m:baseline ok 23.6s

no new behavior | 6 model steps, 9 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.