

Target xiaohongshu-search-to-text

No malicious behavior observed

We ran it 8 times, with a normal setup, LC_MESSAGES and LINKDIGEST_API_KEY set and the environment variables it says it needs. 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	xiaohongshu-search-to-text
Source	clawhub 1.0.0
SHA-256	b1af1f4b4d35b527b14cfd6e6796a3467d215430f921391dc1314b65616161af
Files	5
Scanned	26 Oct 2026, 17:25 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. 8 runs: baseline, guided:LC_MESSAGES, LINKDIGEST_API_KEY, declared-env.
Note	batch:clawhub:2026-10-26

Observed behavior

Install step	none
Runs as	python3 <skill>/scripts/linkdigest.py; python3 <skill>/scripts/xhs_search.py; python3 {baseDir}/scripts/xhs_search.py æ½ åâ;å°; python3 {baseDir}/scripts/xhs_search.py æ½ åâ;å° --read 3; python3 {baseDir}/scripts/xhs_search.py skincare routine --format json
Network	no connections
Credentials	no planted credential touched
Files written	nothing outside its own folder

Run log



scripts:baseline ok 5.8s

no new behavior

scripts:guided:LC_MESSAGES, LINKDIGEST_API_KEY ok 4.2s

no new behavior

scripts:declared-env ok 5.3s

no new behavior

scripts:baseline ok 5.1s

no new behavior

scripts:guided:LC_MESSAGES, LINKDIGEST_API_KEY ok 5.3s

no new behavior

scripts:declared-env ok 5.4s

no new behavior

obedient:baseline ok 6.2s

no new behavior

obedient:declared-env ok 5.9s

no new behavior

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.