

Target `xinjianxue-meihua`

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	<code>xinjianxue-meihua</code>
Source	<code>clawhub 1.0.0</code>
SHA-256	<code>ded9c09aed8c020c681f2dd2cd86ce3b536a33a78b0581b4a1c8938bd573f0ec</code>
Files	<code>6</code>
Scanned	<code>26 Oct 2026, 18:51 UTC</code>
Engine	<code>detonator 0.5.1</code>
Method	<code>Executed in an isolated sandbox with decoy credentials and a captive network; every file access, process and connection traced. 1 runs: baseline.</code>
Note	<code>batch:clawhub:2026-10-26</code>

Observed behavior

Install step	<code>none</code>
Runs as	<code>ls -R; cat references/api.md; cat references/payment.md; cat references/reading.md; cat _meta.json; cat skill-card.md</code>
Network	<code>no connections</code>
Credentials	<code>no planted credential touched</code>
Files written	<code>nothing outside its own folder</code>

Run log

11m:baseline ok 6.4s
no new behavior | 3 model steps, 2 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.