



Target `xinjianxue-bazi`

No malicious behavior observed

We ran it 1 time, with a normal setup. It contacted `api.xinjianxue.com` and `registry.npmjs.org`. 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 4 info

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

Scope

Package	<code>xinjianxue-bazi</code>
Source	<code>clawhub 1.0.0</code>
SHA-256	<code>e10cf9ec185c72ff509462661bdfe851dd516fd33cdea7e3e5bf39b1cc90fd87</code>
Files	6
Scanned	26 Oct 2026, 18:52 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

Findings summary

ID	Severity	Confidence	Finding
F01	Low	Info	Used the planted login with its own service (<code>registry.npmjs.org</code>)
F02	Low	Info	Network destinations contacted
F03	Low	Info	Loaded the project's <code>.env</code> file
F04	Low	Info	A tool read its own credentials (e.g. <code>gh</code> , <code>aws</code> , <code>ssh</code>)

Observed behavior

Install step	none
Runs as	<code>ls -la ./skill; find ./skill -type f; head -50; cat references/api.md; cat references/payment.md; cat references/reading.md</code>
Network	<code>api.xinjianxue.com</code> (4 conn, 610 B sent; while running) <code>registry.npmjs.org</code> (1 conn, 431 B sent; while running)



Credentials	<code>./.env</code> (read) <code>~/.npmrc</code> (own tool, normal)
Files written	nothing outside its own folder

Finding details

F01 Used the planted login with its own service (registry.npmjs.org)

Severity: Low Confidence: Info Observed in: llm:baseline

A planted login went to the service it belongs to, as normal authentication (npm sending its token to registry.npmjs.org while installing).

Description

A planted login was sent to the service it belongs to, only as the Authorization header of ordinary requests: for example npm sending the `~/.npmrc` token to registry.npmjs.org while installing dependencies.

Impact

None in itself: this is how the package manager authenticates. Publishing, unpublishing or creating tokens with it would be reported as exfiltration.

Evidence

```
~/.npmrc (npm) sent only as the login header of ordinary requests (no publish)
```

Remediation

No action needed.

F02 Network destinations contacted

Severity: Low Confidence: Info Observed in: llm:baseline

The package connected to these hosts.

Description

Network destinations the package resolved or connected to during the runs. All traffic was captured by the sandbox; nothing reached the internet.

Impact

Context only. Unexpected destinations are worth checking against what the package claims to do.

Evidence

```
api.xinjianxue.com
```

```
registry.npmjs.org
```

Remediation

Confirm each host is expected (the package's API, its registry). Allowlist expected egress in production.



F03 Loaded the project's .env file

Severity: Low Confidence: Info Observed in: llm:baseline
The package loaded the project's .env file.

Description

The process loaded the project's .env file. Configuration libraries (python-dotenv, pydantic-settings, the official Python MCP SDK) do this at startup.

Impact

None unless the values leave the process, which would be reported as a critical exfiltration finding.

Evidence

```
./.env (by sed)
```

Remediation

No action needed. Keep long-lived secrets out of project .env files where possible.

F04 A tool read its own credentials (e.g. gh, aws, ssh)

Severity: Low Confidence: Info Observed in: llm:baseline
A tool opened its own login or config file, such as npm reading ~/.npmrc.

Description

A tool opened its own configuration or login file, such as npm reading ~/.npmrc or gh reading its hosts file.

Impact

None in itself: this is how those tools work. Listed so the report shows every credential access.

Evidence

```
~/.npmrc (by npm)
```

Remediation

No action needed.

Run log

llm:baseline ok 30.7s

new behavior: dns:api.xinjianxue.com, dns:registry.npmjs.org, exec:curl, ownread:./.env, ownread:~/.npmrc | 8 model steps, 8 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.