

Target ai-crawler-readiness

No malicious behavior observed

We ran it 4 times, with a normal setup, docs:/datasets/llms/facets facet=state and docs:/datasets/llms/search state=present sort=rank_asc. 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 1 info

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

Scope

Package	ai-crawler-readiness
Source	clawhub 1.0.1
SHA-256	bc53621def87d843562ab1bf5783e010ff2ed9a010194b32edc1a4a266d14f9a
Files	5
Scanned	26 Oct 2026, 17:55 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, docs:/datasets/llms/facets facet=state, docs:/datasets/llms/search state=present sort=rank_asc.
Note	batch:clawhub:2026-10-26

Findings summary

ID	Severity	Confidence	Finding
F01	Low	Info	Loaded the project's .env file

Observed behavior

Install step	none
Runs as	bash <skill>/scripts/crawlora.sh; bash <skill>/scripts/crawlora.sh /datasets/llms/facets facet=state; bash <skill>/scripts/crawlora.sh /datasets/llms/search state=present sort=rank_asc; ls -la; ls -la skill; cat skill/SKILL.md
Network	no connections

Credentials	./.env (read)
Files written	nothing outside its own folder

Finding details

F01 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.

Run log

scripts:baseline ok 0.4s

no new behavior

scripts:docs:/datasets/llms/facets facet=state ok 0.4s

no new behavior

scripts:docs:/datasets/llms/search state=present sort=rank_asc ok 0.4s

no new behavior

llm:baseline ok 18.4s

new behavior: ownread:./.env | 8 model steps, 10 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.