

Target reconcile-expense-ledger

No malicious behavior observed

We ran it 4 times, with a normal setup, LC_MESSAGES set and docs:plan BASE.json CURRENT.json. It contacted pypi.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 2 info

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

Scope

Package	reconcile-expense-ledger
Source	clawhub 1.0.0
SHA-256	be3cd9d6b30f309d47f3d4d47103ed50bd97bfae83a9980455f6f7a2a10f498a
Files	7
Scanned	26 Oct 2026, 19:09 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, guided:LC_MESSAGES, docs:plan BASE.json CURRENT.json.
Note	batch:clawhub:2026-10-26

Findings summary

ID	Severity	Confidence	Finding
F01	Low	Info	Network destinations contacted
F02	Low	Info	Loaded the project's .env file

Observed behavior

Install step	none
Runs as	python3 <skill>/scripts/ledger_tools.py; python3 <skill>/scripts/ledger_tools.py plan BASE.json CURRENT.json; ls -la; ls -la skill; find . -maxdepth 3 -not -path; head -100
Network	pypi.org (4 conn, 1448 B sent; while running)



Credentials	./.env (read)
Files written	./.git/index.lock (written) ./.venv/pyvenv.cfg (written)

Finding details

F01 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

```
pypi.org
```

Remediation

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

F02 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 cat)
```

Remediation

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

Run log

scripts:baseline ok 1.5s

no new behavior

scripts:guided:LC_MESSAGES ok 2.2s

no new behavior



scripts:docs:plan BASE.json CURRENT.json ok 1.0s

no new behavior

llm:baseline ok 81.9s

new behavior: dns:pypi.org, exec:curl, ownread:./env, write:./.git/index, write:./.git/index.lock | 8 model steps, 11 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.