

Target quarterly-tax-ranger

No malicious behavior observed

We ran it 7 times, with a normal setup, LC_MESSAGES set, docs:--demo and the clock moved a year ahead. 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	quarterly-tax-ranger
Source	clawhub 1.0.0
SHA-256	911177ea51bc890ce0babece06989cfabfa891d920ec30d6c8160bb0eb167dff
Files	7
Scanned	26 Oct 2026, 17:20 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. 7 runs: baseline, guided:LC_MESSAGES, docs:--demo, time-travel.
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	python3 <skill>/scripts/quarterly_tax.py; python3 <skill>/scripts/quarterly_tax.py --demo; python3 scripts/quarterly_tax.py --demo; python3 scripts/quarterly_tax.py --prior-tax 8200 --profit 65000; python3 scripts/quarterly_tax.py --prior-tax 8200 --filing single; head -50
Network	no connections



Credentials	./.env (read)
Files written	./scripts/quarterly_tax.py (written)

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 cat)
```

Remediation

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

Run log

scripts:baseline ok 1.9s

no new behavior

scripts:guided:LC_MESSAGES ok 2.2s

no new behavior

scripts:docs:--demo ok 1.4s

no new behavior

obedient:baseline ok 5.6s

no new behavior

obedient:guided:LC_MESSAGES ok 4.8s

no new behavior

obedient:time-travel ok 5.0s

no new behavior

llm:baseline ok 24.5s

new behavior: ownread:./.env, write:./scripts/quarterly_tax.py | 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.