

Target business-location-screening

No malicious behavior observed

We ran it 4 times, with a normal setup, docs:/datasets/google-map-businesses/facets facet=category q=coffee and docs:/datasets/google-map-businesses/nearby lat=37.7768 lon=-122.3980. 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	business-location-screening
Source	clawhub 1.0.0
SHA-256	89e668b7038f3359a87986a9db0ff3b97888565be97b1f8e3820824ce5278fad
Files	5
Scanned	26 Oct 2026, 17:54 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/google-map-businesses/facets facet=category q=coffee, docs:/datasets/google-map-businesses/nearby lat=37.7768 lon=-122.3980.
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/google-map-businesses/facets facet=category q=c; bash <skill>/scripts/crawlora.sh /datasets/google-map-businesses/nearby lat=37.7768 lon=-1; ls -la; ls -la skill; cat skill/scripts/crawlora.sh



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 cat)
```

Remediation

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

Run log

scripts:baseline ok 0.5s

no new behavior

scripts:docs:/datasets/google-map-businesses/facets facet=category q=coffee ok 0.5s

no new behavior

scripts:docs:/datasets/google-map-businesses/nearby lat=37.7768 lon=-122.3980 ok 0.7s

no new behavior

llm:baseline ok 13.1s

new behavior: ownread:./.env | 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.