



Target aimegeo-query-map

No malicious behavior observed

We ran it 8 times, with a normal setup, LC_MESSAGES set, docs:examples/success/input.json --output-dir result and a GitHub Actions environment. 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 0 info

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

Scope

Package	aimegeo-query-map
Source	clawhub 1.0.1
SHA-256	9f07d920d81cc544ab9abfcf163f4c1578519a995f738fd9fa8dd775434d6734
Files	22
Scanned	27 Oct 2026, 11:24 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. 8 runs: baseline, guided:LC_MESSAGES, docs:examples/success/input.json --output-dir result, ci-github.
Note	batch:clawhub:2026-10-27

Observed behavior

Install step	none
Runs as	python3 <skill>/scripts/map_queries.py; python3 <skill>/scripts/map_queries.py examples/success/input.json --output-dir result; python3 <skill>/scripts/self_test.py; /usr/bin/python3 <skill>/scripts/map_queries.py <skill>/examples/failure/cross-audience.js; /usr/bin/python3 <skill>/scripts/map_queries.py /tmp/query-map-test-r3qpa7uh/input.json --; /usr/bin/python3 <skill>/scripts/map_queries.py /tmp/query-map-test-r3qpa7uh/missing.json
Network	no connections
Credentials	no planted credential touched
Files written	nothing outside its own folder



Run log

scripts:baseline ok 1.3s

no new behavior

scripts:guided:LC_MESSAGES ok 1.2s

no new behavior

scripts:docs:examples/success/input.json --output-dir result ok 1.0s

no new behavior

scripts:baseline ok 6.6s

new behavior: write:./input.json, write:./map-audit.json, write:./out, write:./é®é¢âä, »é¢âââ®¹â½¢â¼æ å°èj".csv

scripts:guided:LC_MESSAGES ok 7.2s

no new behavior

scripts:ci-github ok 6.6s

no new behavior

obedient:baseline ok 8.2s

new behavior: write:./result/map-audit.json, write:./result/é®é¢âä, »é¢âââ®¹â½¢â¼æ å°èj".csv,

write:<skill>/result/.query-map-8r649k1x/map-audit.json,

write:<skill>/result/.query-map-8r649k1x/é®é¢âä, »é¢âââ®¹â½¢â¼æ å°èj".csv

obedient:guided:LC_MESSAGES ok 8.6s

new behavior: write:<skill>/result/.query-map-hs_osp3u/map-audit.json,

write:<skill>/result/.query-map-hs_osp3u/é®é¢âä, »é¢âââ®¹â½¢â¼æ å°èj".csv

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.