



Target comment-verification

No malicious behavior observed

We ran it 8 times, with a normal setup, a production environment, everything, docs:advertisement /home/node/.openclaw/workspace/comments_raw.md and docs:advertisement http://127.0.0.1:8088/fake_reddit.html. 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	comment-verification
Source	clawhub 1.0.0
SHA-256	cf709abfaa81e4b493ba4ae5ec44674fd9c8841ae01670434d45e857848684ce
Files	5
Scanned	27 Oct 2026, 13:18 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, production, everything, docs:advertisement /home/node/.openclaw/workspace/comments_raw.md, docs:advertisement http://127.0.0.1:8088/fake_reddit.html, guided:ANDROID_DATA,APPENGINE_RUNTIME,CURL_CA_BUNDLE,DEB_PYTHON_INSTALL_LAYOUT....
Note	batch:clawhub:2026-10-27

Observed behavior

Install step	package manager only, no install scripts
Runs as	python3 <skill>/comment_verification.py; python3 <skill>/prototype.py; python3 <skill>/prototype.py advertisement /home/node/.openclaw/workspace/comments_raw.md; python3 <skill>/prototype.py advertisement http://127.0.0.1:8088/fake_reddit.html; python3 prototype.py advertisement /home/node/.openclaw/workspace/comments_raw.md; python3 prototype.py advertisement http://127.0.0.1:8088/fake_reddit.html
Network	no connections



Credentials	no planted credential touched
Files written	nothing outside its own folder

Run log

scripts:baseline **ok** **2.3s**
no new behavior

scripts:production **ok** **1.9s**
no new behavior

scripts:everything **ok** **1.6s**
no new behavior

scripts:baseline **ok** **1.8s**
no new behavior

scripts:docs:advertisement /home/node/.openclaw/workspace/comments_raw.md **ok** **2.4s**
no new behavior

scripts:docs:advertisement http://127.0.0.1:8088/fake_reddit.html **ok** **3.8s**
no new behavior

obedient:baseline **ok** **21.9s**
no new behavior

obedient:guided:ANDROID_DATA,APPENGINE_RUNTIME,CURL_CA_BUNDLE,DEB_PYTHON_INSTALL_LAYOUT... **ok** **16.2s**
no new behavior

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.