

Target `ugc-ad-scripts`

# No malicious behavior observed

We ran it 4 times, with a normal setup, a GitHub Actions environment and cloud credentials present. It made no network connections. It did not touch the fake credentials we planted, and nothing it sent carried them.

| Recommendation          | Confidence | Findings                   |
|-------------------------|------------|----------------------------|
| <b>No action needed</b> | <b>n/a</b> | <b>0 high 0 med 1 info</b> |

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

## Scope

|         |                                                                                                                                                                                                                     |
|---------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Package | <code>ugc-ad-scripts</code>                                                                                                                                                                                         |
| Source  | <code>clawhub 1.0.0</code>                                                                                                                                                                                          |
| SHA-256 | <code>ff03e1f2fb27b5d1c99fcac676626fad1125ab652fded612737975ac02e504bc</code>                                                                                                                                       |
| Files   | 3                                                                                                                                                                                                                   |
| Scanned | 27 Oct 2026, 12:34 UTC                                                                                                                                                                                              |
| Engine  | <code>detonator 0.5.1</code>                                                                                                                                                                                        |
| Method  | Executed in an isolated sandbox with decoy credentials and a captive network; every file access, process and connection traced. 4 runs: <code>baseline</code> , <code>ci-github</code> , <code>cloud-creds</code> . |
| Note    | <code>batch:clawhub:2026-10-27</code>                                                                                                                                                                               |

## Findings summary

| ID  | Severity | Confidence | Finding                                     |
|-----|----------|------------|---------------------------------------------|
| F01 | Low      | Info       | Loaded the project's <code>.env</code> file |

## Observed behavior

|               |                                                                                                                                       |
|---------------|---------------------------------------------------------------------------------------------------------------------------------------|
| Install step  | <code>none</code>                                                                                                                     |
| Runs as       | <code>ls -la; find . -maxdepth 3 -not -path; head -100; sed s/=.*/=&lt;redacted&gt;/<br/>.env; cat README.md; cat package.json</code> |
| Network       | <code>no connections</code>                                                                                                           |
| Credentials   | <code>./.env (read)</code>                                                                                                            |
| Files written | <code>./ads/ugc-scripts/README.md (written)</code>                                                                                    |



## 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 sed)
```

#### Remediation

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

## Run log

**obedient:baseline** ok 0.6s

no new behavior

**obedient:ci-github** ok 0.5s

no new behavior

**obedient:cloud-creds** ok 0.4s

no new behavior

**llm:baseline** ok 37.4s

new behavior: ownread:./ .env, write:./ads/ugc-scripts/README.md | 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.