TruffleHog

Secret scanner

CONCEPTS

Every finding is verified by calling the provider's API. A verified hit is a live credential: rotate it first, clean history second.

Source git, files, S3...
↓ chunks
Detectors regex + keywords
↓ candidates
Verify call provider API
↓ status
Result verified / unknown / unverified

Unknown means verification failed (network or API error), not that the secret is safe. Unverified means detected but not confirmed live.

Exit code is 0 even with findings unless you pass --fail (then 183). Exit 1 means the scan itself had errors.

SCAN SOURCES

`trufflehog git <uri>`
Scan a git repo by URL or file:// path

`trufflehog git file://.`
Scan the local repo's history

SCAN SOURCES (cont.)

`trufflehog filesystem <path>...`
Scan files and directories

`trufflehog github --org=<org>`
Scan every repo of an org

`trufflehog github --repo=<url>`
Scan one GitHub repo

`trufflehog gitlab --token=<token>`
Scan GitLab repos

`trufflehog docker --image <image>`
Scan a container image

`trufflehog s3 --bucket=<name>`
Scan an S3 bucket

`<cmd> | trufflehog stdin`
Scan piped data

GIT AND GITHUB OPTIONS

`--since-commit <ref>`
Scan only commits after this ref

`--branch <name>`
Scan one branch

`--issue-comments`
Also scan GitHub issue comments

GIT AND GITHUB OPTIONS (cont.)

`--pr-comments`
Also scan pull request comments

`--token <token>`
GitHub token to avoid rate limits

RESULTS AND OUTPUT

`--results=verified`
Show only confirmed live secrets

`--results=verified,unknown`
Also keep unknown (verification failed)

`--results=unverified`
Show detected but unconfirmed only

`--json / -j`
Output one JSON object per finding

`--sarif`
Output SARIF for code scanning

`--no-verification`
Skip API checks; report all matches

`--fail`
Exit 183 when results are found

RESULTS AND OUTPUT (cont.)

`--no-update`
Do not check for a newer version

`--log-level <n>`
Verbosity from 0 to 5; -1 disables

DETECTORS AND FILTERS

`--include-detectors <names>`
Run only these detectors (names or IDs)

`--exclude-detectors <names>`
Skip these detectors; wins over include

`--filter-entropy <n>`
Drop low-entropy matches, try 3.0

`--config <file>`
Load custom detectors from a YAML file

`trufflehog:ignore`
Comment on a line to skip its finding

ANALYZE AND INSTALL

`trufflehog analyze`
Show permissions of a found credential

ANALYZE AND INSTALL (cont.)

`trufflehog help <command>`
Flags for one subcommand

`trufflehog --version`
Print the installed version

`brew install trufflehog`
Install on macOS or Linuxbrew

`docker run --rm -it -v "$PWD:/pwd" trufflesecurity/trufflehog:latest github --repo <url>`
Run in Docker

`curl -sSfL <install.sh URL> | sh -s -- -b /usr/local/bin`
Install script from the repo's scripts/

CI

`uses: trufflesecurity/trufflehog@main`
GitHub Action step; checkout with fetch-depth: 0

`extra_args: --results=verified,unknown`
Pass flags to the Action

`trufflehog git file://. --since-commit main --branch <b> --fail`
PR-style scan of new commits