CodeSec by Contrast
Cheat sheet

Use the 'contrast' command for fast and accurate security analysis of your applications, APIs, serverless functions, and libraries.

Code: Java, .NET, JavaScript
Serverless: AWS Lambda - Java, Python
Libraries: Java, .NET, Javascript, Ruby, Python, Go, PHP

Install

Homebrew brew tap contrastsecurity/tap
brew install contrast

npm npm install --location=global @contrast/contrast

Binaries available from Artifactory

Need some help?

contrast help Displays general usage guide OR
--help After main command for specific help.

Get started at: .contrastsecurity.com/
developer/codesec

Check out: support.contrastsecurity.com

Learn more at : developer.contrastsecurity.com

Join the discussion: dev.to/codesec

Contrast
SECURITY

Get started

Usage   contrast [command] [options]

Commands top level

auth Authenticate
scan Search folder and scan
lambda SAST scan on an AWS lambda function
audit Search folder and audit dependency issues
version Displays version of Contrast CLI
config Displays stored credentials
help Displays general usage guide

contrast config options

Removes stored credentials
contrast config --clear, -c

Run a SAST scan / autodetect your project
contrast scan options

Provide or specify a project name
contrast scan --name, -n

Specify language
contrast scan --language, -l

Path of file to scan
contrast scan --file, -f

Wait for scan
contrast scan --timeout <number>

Displays usage guide
contrast scan --help

Scan a lambda function
contrast lambda options

AWS lambda function to scan ®
contrast lambda --function-name, -f

Lists available lambda functions ®
contrast lambda --list-functions, -l

AWS Endpoint override
contrast lambda --endpoint-url -e

Region override, default to AWS
contrast lambda --region -r

Works like in AWS CLI
DEFAULT_REGION env var

AWS configuration profile override
--profile, -p

Return response in JSON
--json-output, -j

Run a dependency check / autodetect your files
contrast audit options

Perform an SCA audit on this file
contrast audit --file, -f

Excludes developer dependencies
contrast audit --ignore-dev

Generate and save an SBOM (Software Bill of Materials) CycloneDX
contrast audit --save, -s (spdx option available)

Wait for audit
contrast audit --timeout <number>

Fail builds by specifying severity thresholds
contrast audit --fail <severity>

Displays usage guide
contrast audit --help

® Required