Using code scanning with your existing CI system

In this article

About using code scanning with your existing CI system
Setting up your analysis tool
Analyzing code
Generating a token for authentication with GitHub Enterprise Cloud
Uploading your results to GitHub Enterprise Cloud

You can analyze your code with the CodeQL CLI or another tool in a third-party continuous integration system and upload the results to GitHub.com. The resulting code scanning alerts are shown alongside any alerts generated within GitHub Enterprise Cloud.

Code scanning is available for all public repositories on GitHub.com. To use code scanning in a private repository owned by an organization, you must have a license for GitHub Advanced Security. For more information, see "About GitHub Advanced Security."

About using code scanning with your existing CI system

As an alternative to running code scanning within GitHub using GitHub Actions, you can analyze code in an external continuous integration or continuous delivery/deployment (CI/CD) system, then upload the results to GitHub Enterprise Cloud.

You can add the CodeQL CLI to your third-party system, or use another third-party static analysis tool that can produce results as Static Analysis Results Interchange Format (SARIF) 2.1.0 data. For more information about the supported SARIF format, see "SARIF support for code scanning."

The CodeQL CLI is a standalone, command-line tool that you can use to analyze code. For more information, see "About the CodeQL CLI."

Alerts for code scanning that you generate externally are displayed in the same way as those for code scanning that you generate within GitHub. If you run code scanning using multiple configurations, the same alert will sometimes be generated by more than one configuration. If an alert comes from multiple configurations, you can view the status of the alert for each configuration on the alert page. For more information, see "About code scanning alerts."

Note: Uploading SARIF data to display as code scanning results in GitHub Enterprise Cloud is supported for organization-owned repositories with GitHub Advanced Security enabled, and public repositories on GitHub.com. For more information, see "Managing security and analysis settings for your repository."

Setting up your analysis tool

You will first need to download your analysis tool of choice and set it up with your CI system.

If you are using the CodeQL CLI, you need to make the full contents of the CodeQL CLI bundle available to every CI server that you want to run CodeQL code scanning analysis on. For more information, see "Setting up the CodeQL CLI."

Once you've made your analysis tool available to servers in your CI system, you're ready to generate data.

Analyzing code

To analyze code with the CodeQL CLI or another analysis tool, you will want to check out the code you want to analyze and set up the codebase environment, making sure that any dependencies are available. You may also want to find the build command for the codebase, typically available in your CI system's configuration file.

You can then complete the steps to analyze your codebase and produce results, which will differ based on the static analysis tool you are using.

If you are using the CodeQL CLI, you will first need to create a CodeQL database from your code, then analyze the database to produce SARIF results. For more information, see "Preparing your code for CodeQL analysis" and "Analyzing your code with CodeQL queries."

Generating a token for authentication with GitHub Enterprise Cloud

Each CI server needs a GitHub App or personal access token to use to upload results to GitHub Enterprise Cloud, whether you are using the CodeQL CLI, the REST API, or another method. You must use an access token or a GitHub App with the `security_events` write permission. If CI servers already use a token with this scope to checkout repositories from GitHub Enterprise Cloud, you could potentially use the same token. Otherwise, you should create a new token with the `security_events` write permission and add this to the CI system's secret store. For information, see "Creating GitHub Apps" and "Managing your personal access tokens."

For more information on the different methods for uploading results to GitHub Enterprise Cloud, see "Uploading a SARIF file to GitHub."

Uploading your results to GitHub Enterprise Cloud

Once you have analyzed your code, produced SARIF results, and ensured you can authenticate with GitHub Enterprise Cloud, you can upload the results to GitHub Enterprise Cloud. For more information on the different methods you can use to upload your results, see "Uploading a SARIF file to GitHub."

For specific details on uploading your results to GitHub Enterprise Cloud using the CodeQL CLI, see "Uploading CodeQL analysis results to GitHub."

By default, code scanning expects one SARIF results file per analysis for a repository. Consequently, when you upload a second SARIF results file for a commit, it is treated as a replacement for the original set of data. You may want to upload two different SARIF files for one analysis if, for example, your analysis tool generates a different SARIF file for each language it analyzes or each set of rules it uses. If you want to upload more than

one set of results for a commit in a repository, you must identify each set of results as a unique set. The way to specify a category for a SARIF upload varies according to the analysis method. For more information, see "SARIF support for code scanning."

Legal

© 2023 GitHub, Inc. Terms Privacy Status Pricing Expert services Blog