Integrating with code scanning

You can integrate third-party code analysis tools with GitHub code scanning by uploading data as SARIF files.

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 integration with code scanning

You can perform code scanning externally and then display the results in GitHub, or configure webhooks that listen to code scanning activity in your repository.

Using code scanning with your existing CI system

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.

Uploading a SARIF file to GitHub

You can upload SARIF files generated outside GitHub and see code scanning alerts from third-party tools in your repository.

SARIF support for code scanning

To display results from a third-party static analysis tool in your repository on GitHub, you'll need your results stored in a SARIF file that supports a specific subset of the SARIF 2.1.0 JSON schema for code scanning. If you use the default CodeQL static analysis engine, then your results will display in your repository on GitHub automatically.

Legal

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