**This version of GitHub Enterprise was discontinued on 2023-03-15.** No patch releases will be made, even for critical security issues. For better performance, improved security, and new features, upgrade to the latest version of GitHub Enterprise. For help with the upgrade, contact GitHub Enterprise support.

# About code scanning with CodeQL

**In this article**

You can use CodeQL to identify vulnerabilities and errors in your code. The results are shown as code scanning alerts in GitHub.

Code scanning is available for organization-owned repositories in GitHub Enterprise Server. This feature requires a license for GitHub Advanced Security. For more information, see "About GitHub Advanced Security."

**Note:** Your site administrator must enable code scanning for your GitHub Enterprise Server instance before you can use this feature. For more information, see "Configuring code scanning for your appliance."

## About code scanning with CodeQL

CodeQL is the code analysis engine developed by GitHub to automate security checks. You can analyze your code using CodeQL and display the results as code scanning alerts.

There are two main ways to use CodeQL analysis for code scanning:

- Add the CodeQL workflow to your repository. This uses the github/codeql-action to run the CodeQL CLI. For more information, see "Configuring code scanning for a repository."
- Run the CodeQL CLI directly in an external CI system and upload the results to GitHub. For more information, see "About CodeQL code scanning in your CI system."

On GitHub Enterprise Server 3.4, the CodeQL action uses CodeQL CLI version 2.7.6 by default. We recommend that you use the same version of the CodeQL CLI if you run analysis in an external CI system.

For information about code scanning alerts, see "About code scanning alerts."

## About CodeQL

CodeQL treats code like data, allowing you to find potential vulnerabilities in your code with greater confidence than traditional static analyzers.

1. You generate a CodeQL database to represent your codebase.

2. Then you run CodeQL queries on that database to identify problems in the codebase.

3. The query results are shown as code scanning alerts in GitHub Enterprise Server when you use CodeQL with code scanning.

CodeQL supports both compiled and interpreted languages, and can find vulnerabilities and errors in code that's written in the supported languages.

- C/C++
- C#
- Go
- Java
- JavaScript/TypeScript
- Python
- Ruby

**Notes**:

- CodeQL analysis for Ruby is currently in beta. During the beta, analysis of Ruby will be less comprehensive than CodeQL analysis of other languages.
- Use `javascript` to analyze code written in JavaScript, TypeScript or both.

For more information, see the documentation on the CodeQL website: "Supported languages and frameworks."

## About CodeQL queries

GitHub experts, security researchers, and community contributors write and maintain the default CodeQL queries used for code scanning. The queries are regularly updated to improve analysis and reduce any false positive results. The queries are open source, so you can view and contribute to the queries in the `github/codeql` repository. For more information, see CodeQL on the CodeQL website. You can also write your own queries. For more information, see "About CodeQL queries" in the CodeQL documentation.

If you are scanning your code with the advanced setup or an external CI system, you can run additional queries as part of your analysis. The queries you want to run must belong to a QL pack in a repository. Queries must only depend on the standard libraries (that is, the libraries referenced by an `import LANGUAGE` statement in your query), or libraries in the same QL pack as the query.