Creating an advanced setup for for code scanning

For more granular control over your code scanning configuration, you can secure your code with advanced setup for code scanning.

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."

Configuring advanced setup for code scanning

You can configure advanced setup for a repository to find security vulnerabilities in your code using a highly customizable code scanning configuration.

Customizing your advanced setup for code scanning

You can customize how your advanced setup scans the code in your project for vulnerabilities and errors.

CodeQL code scanning for compiled languages

Understand the autobuild method CodeQL analysis uses to build code for compiled languages and learn how you can customize the build command if you need to.

Configuring advanced setup for code scanning with CodeQL at scale

You can use a script to configure advanced setup for code scanning for a specific group of repositories in your organization.

Recommended hardware resources for running CodeQL

Recommended specifications (RAM, CPU cores, and disk) for running CodeQL analysis on self-hosted machines, based on the size of your codebase.

Running CodeQL code scanning in a container

You can run code scanning in a container by ensuring that all processes run in the same container.