About integration with code scanning

In this article

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.

> 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 ⚭

As an alternative to running code scanning within GitHub, you can perform analysis elsewhere, using the CodeQL CLI or another static analysis tool, and then upload the results. For more information, see "[Using code scanning with your existing CI system](#)."

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](#)."

Integrations with webhooks ⚭

You can use code scanning webhooks to build or configure integrations, such as [GitHub Apps](#) or [OAuth apps](#), that subscribe to code scanning events in your repository. For example, you could build an integration that creates an issue on GitHub Enterprise Cloud or sends you a Slack notification when a new code scanning alert is added in your repository. For more information, see "[Webhooks documentation](#)" and "[Webhook events and payloads](#)."

Further reading ⚭

- "[About code scanning](#)"
- "[Using code scanning with your existing CI system](#)"
- "[SARIF support for code scanning](#)"