About code scanning

In this article

You can use code scanning to find security vulnerabilities and errors in the code for your project on 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."

You may not be able to enable or disable code scanning if an enterprise owner has set a GitHub Advanced Security (GHAS) policy at the enterprise level. For more information, see "Enforcing policies for code security and analysis for your enterprise."

About code scanning

Code scanning is a feature that you use to analyze the code in a GitHub repository to find security vulnerabilities and coding errors. Any problems identified by the analysis are shown in GitHub Enterprise Server.

You can use code scanning to find, triage, and prioritize fixes for existing problems in your code. Code scanning also prevents developers from introducing new problems. You can schedule scans for specific days and times, or trigger scans when a specific event occurs in the repository, such as a push.

If code scanning finds a potential vulnerability or error in your code, GitHub displays an alert in the repository. After you fix the code that triggered the alert, GitHub closes the alert. For more information, see "Managing code scanning alerts for your repository."

To monitor results from code scanning across your repositories or your organization, you can use webhooks and the code scanning API. For information about the webhooks for code scanning, see "Webhook events and payloads." For information about API endpoints, see "Code Scanning."

To get started with code scanning, see "Configuring default setup for code scanning."

About tools for code scanning

You can configure code scanning to use the CodeQL product maintained by GitHub or a third-party code scanning tool.

About CodeQL analysis

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. For more information about CodeQL, see "About code scanning with CodeQL."

About third-party code scanning tools

Code scanning is interoperable with third-party code scanning tools that output Static Analysis Results Interchange Format (SARIF) data. SARIF is an open standard. For more information, see "SARIF support for code scanning."

You can run third-party analysis tools within GitHub Enterprise Server using actions or within an external CI system. For more information, see "Configuring advanced setup for code scanning" or "Uploading a SARIF file to GitHub."

About the tool status page

The tool status page shows useful information about all of your code scanning tools. If code scanning is not working as you'd expect, the tool status page is a good starting point for debugging problems. For more information, see "About the tool status page for code scanning".