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.

Finding security vulnerabilities and errors in your code with code scanning

Keep your code secure by using code scanning to identify and fix potential security vulnerabilities and other errors in your code.

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."

- Automatically scanning your code for vulnerabilities and errors
  - About code scanning
  - About code scanning alerts
  - Triaging code scanning alerts in pull requests
  - Configuring code scanning for a repository
  - Managing code scanning alerts for your repository
  - Customizing code scanning
  - About code scanning with CodeQL
  - Recommended hardware resources for running CodeQL
  - Configuring the CodeQL workflow for compiled languages
  - Troubleshooting the CodeQL workflow
  - Running CodeQL code scanning in a container
  - Viewing code scanning logs
- Integrating with code scanning
  - About integration with code scanning
  - Uploading a SARIF file to GitHub
  - SARIF support for code scanning
- Using CodeQL code scanning with your existing CI system
  - About CodeQL code scanning in your CI system
  - Installing CodeQL CLI in your CI system
  - Configuring CodeQL CLI in your CI system
  - Migrating from the CodeQL runner to CodeQL CLI