

Code security documentation

Build security into your GitHub workflow with features to keep secrets and vulnerabilities out of your codebase, and to maintain your software supply chain.

[Overview](#)

Start here

Securing your repository

You can use a number of GitHub features to help keep your repository secure.

Securing your organization

You can use a number of GitHub features to help keep your organization secure.

Creating a repository security advisory

You can create a draft security advisory to privately discuss and fix a security vulnerability in your open source project.

Configuring default setup for code scanning

You can quickly secure code in your repository with default setup for code scanning.

Popular

About Dependabot alerts

GitHub Enterprise Cloud sends Dependabot alerts when we detect that your repository uses a vulnerable dependency or malware.

About coordinated disclosure of security vulnerabilities

Vulnerability disclosure is a coordinated effort between security reporters and repository maintainers.

Keeping your actions up to date with Dependabot

You can use Dependabot to keep the actions you use updated to the latest versions.

Configuration options for the dependabot.yml file

Detailed information for all the options you can use to customize how Dependabot maintains your repositories.

What's new [View all →](#)

GitHub Advanced Security is part of GitHub Enterprise Cloud trial

October 24

[Code scanning default setup automatically includes all CodeQL supported languages](#)

October 23

[Authress is now a GitHub secret scanning partner](#)

October 20

Guides

Configuring Dependabot security updates

You can use Dependabot security updates or manual pull requests to easily update vulnerable dependencies.

@GitHub

Configuring Dependabot version updates

You can configure your repository so that Dependabot automatically updates the packages you use.

@GitHub

Configuring default setup for code scanning

You can quickly secure code in your repository with default setup for code scanning.

@GitHub

Securing your end-to-end supply chain

Introducing best practice guides on complete end-to-end supply chain security including personal accounts, code, and build processes.

@GitHub

All Code security docs

Getting started with code security

[GitHub security features](#)

[Dependabot quickstart guide](#)

[Securing your repository](#)

[Securing your organization](#)

[Adding a security policy to your repository](#)

[Auditing security alerts](#)

[Best practices for preventing data leaks in your organization](#)

Adopting GitHub Advanced Security at scale

[Introduction to adopting GitHub Advanced Security at scale](#)

[Phase 1: Align on your rollout strategy and goals](#)

[Phase 2: Preparing to enable at scale](#)

[Phase 3: Pilot programs](#)

[Phase 4: Create internal documentation](#)

[Phase 5: Rollout and scale code scanning](#)

[Phase 6: Rollout and scale secret scanning](#)

Keeping secrets secure with secret scanning

[About secret scanning](#)

[Secret scanning partner program](#)

[Configuring secret scanning for your repositories](#)

[Defining custom patterns for secret scanning](#)

[Managing alerts from secret scanning](#)

[Secret scanning patterns](#)

[Push protection for repositories and organizations](#)

[Push protection for users](#)

[Pushing a branch blocked by push protection](#)

[Troubleshooting secret scanning](#)

Finding security vulnerabilities and errors in your code with code scanning

[Introduction to code scanning](#) • 2 articles

[Enabling code scanning](#) • 2 articles

[Creating an advanced setup for for code scanning](#) • 6 articles

[Managing code scanning alerts](#) • 4 articles

[Managing your code scanning configuration](#) • 4 articles

[Integrating with code scanning](#) • 4 articles

[Troubleshooting code scanning](#) • 20 articles

[Troubleshooting SARIF uploads](#) • 6 articles

Use the CodeQL CLI to secure your code

[Getting started with the CodeQL CLI](#) • 6 articles

[Using the advanced functionality of the CodeQL CLI](#) • 14 articles

[CodeQL CLI commands manual](#) • 73 articles

Working with security advisories

[Working with global security advisories from the GitHub Advisory Database](#) • 4 articles

[Working with repository security advisories](#) • 12 articles

[Guidance on reporting and writing information about vulnerabilities](#) • 4 articles

Securing your software supply chain

[Understanding your software supply chain](#) • 9 articles

[End-to-end supply chain](#) • 4 articles

Keeping your supply chain secure with Dependabot

[Identifying vulnerabilities in your project's dependencies with Dependabot alerts](#) • 4 articles

[Prioritizing Dependabot alerts with Dependabot alert rules](#) • 4 articles

[Automatically updating dependencies with known vulnerabilities with Dependabot security updates](#) • 2 articles

[Keeping your dependencies updated automatically with Dependabot version updates](#) • 5 articles

[Working with Dependabot](#) • 9 articles

Viewing security information for your organization or enterprise

[About security overview](#)

[Assessing adoption of code security features](#)

[Assessing your code security risk](#)

[Filtering alerts in security overview](#)

[Enabling security features for multiple repositories](#)

[Exporting data from the risk and coverage pages](#)

[Viewing metrics for secret scanning push protection in your organization](#)

Legal

© 2023 GitHub, Inc. [Terms](#) [Privacy](#) [Status](#) [Pricing](#) [Expert services](#) [Blog](#)