Tracking code scanning alerts in issues using task lists

In this article

You can add code scanning alerts to issues using task lists. This makes it easy to create a plan for development work that includes fixing alerts.

> **Who can use this feature**
> If you have write permission to a repository you can track code scanning alerts in issues using task lists.

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."

Note: The tracking of code scanning alerts in issues is in beta and subject to change.

This feature supports running analysis natively using GitHub Actions or externally using existing CI/CD infrastructure, as well as third-party code scanning tools, but *not* third-party tracking tools.

About tracking code scanning alerts in issues

Code scanning alerts integrate with task lists in GitHub Issues to make it easy for you to prioritize and track alerts with all your development work. To track a code scanning alert in an issue, add the URL for the alert as a task list item in the issue. For more information about task lists, see "About task lists."

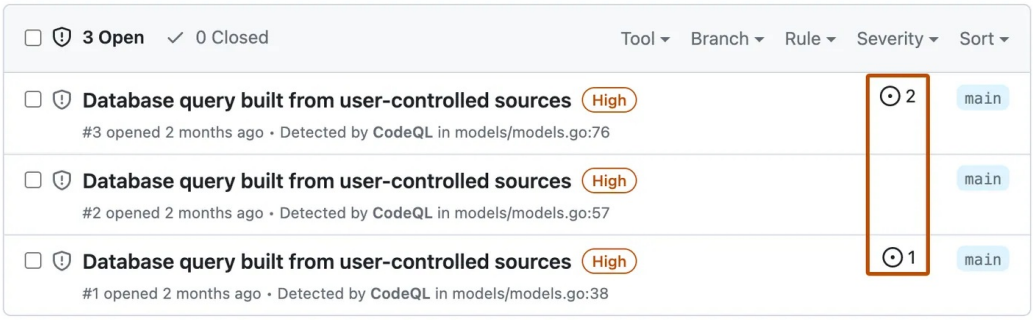
You can also quickly create a new issue to track an alert:

- From a code scanning alert. For more information, see "Creating a tracking issue from a code scanning alert."
- From the API. For more information, see "Creating a tracking issue from the API."

You can use more than one issue to track the same code scanning alert, and issues can belong to different repositories from the repository where the code scanning alert was found.

GitHub Enterprise Cloud provides visual cues in different locations of the user interface to indicate when you are tracking code scanning alerts in issues.

- The code scanning alerts list page will show which alerts are tracked in issues so that you can view at a glance which alerts still require processing and how many issues they are tracked in.

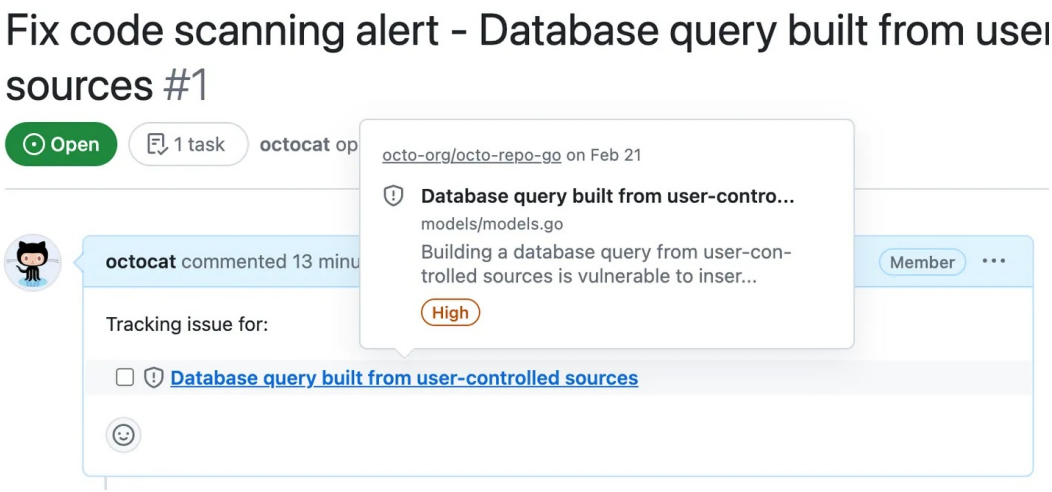


- A "tracked in" section will also show in the corresponding alert page.

- On the tracking issue, GitHub displays a security badge icon in the task list and on the hovercard.

> Only users with write permissions to the repository will see the unfurled URL to the alert in the issue, as well as the hovercard. For users with read permissions to the repository, or no permissions at all, the alert will appear as a plain URL.

The color of the icon is grey because an alert has a status of "open" or "closed" on every branch. The issue tracks an alert, so the alert cannot have a single open/closed state in the issue. If the alert is closed on one branch, the icon color will not change.



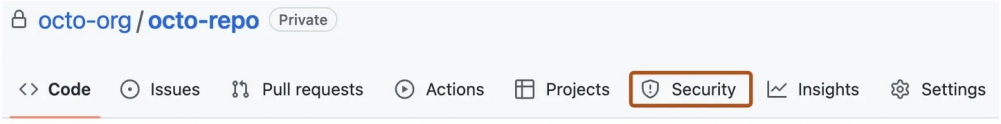
The status of the tracked alert won't change if you change the checkbox state of the corresponding task list item (checked/unchecked) in the issue.

Creating a tracking issue

Instead of tracking a code scanning alert in an existing issue, you can create a new issue to track an alert directly. You can create tracking issues for code scanning alerts from the alert itself, or from the API.

Creating a tracking issue from a code scanning alert

1. On GitHub.com, navigate to the main page of the repository.
2. Under the repository name, click **Security**. If you cannot see the "Security" tab, select the ··· dropdown menu, and then click **Security**.



3. In the left sidebar, click **Code scanning alerts**.
4. Under "Code scanning," click the alert you'd like to explore to display the detailed alert page.
5. Optionally, to find the alert to track, you can use the free-text search or the drop-down menus to filter and locate the alert. For more information, see "Managing code scanning alerts for your repository."
6. Towards the top of the page, on the right side, click **Create issue**.

   GitHub automatically creates an issue to track the alert and adds the alert as a task list item. GitHub prepopulates the issue:

   - The title contains the name of the code scanning alert.
   - The body contains the task list item with the full URL to the code scanning alert.

7. Optionally, edit the title and the body of the issue.

   > **Warning:** You may want to edit the title of the issue as it may expose security information. You can also edit the body of the issue. Make sure that you keep the task list item with a link to the alert otherwise the issue will no longer track the alert.

8. Click **Submit new issue**.

Creating a tracking issue from the API

1. Begin creating an issue through the API. For more information, see "Create an issue."
2. Provide the code scanning link within the body of the issue. You must use the following task list syntax to create the tracked relationship: `- [ ] FULL-URL-TO-THE-CODE-SCANNING-ALERT`.

   For example, if you add `- [ ] https://github.com/octocat-org/octocat-repo/security/code-scanning/17` to an issue, the issue will track the code scanning

alert that has an ID number of 17 in the **Security** tab of the `octocat-repo` repository in the `octocat-org` organization.