

# Evaluating the security settings of a repository

## In this article

About evaluating a repository's security settings

Suggesting a security policy for a repository

Reporting a vulnerability in a repository

---

Security researchers can assess the security settings of a public repository, suggest a security policy and report a vulnerability.

### Who can use this feature

Anyone can view a public repository's security settings, and contact the repository maintainers regarding security issues.

## About evaluating a repository's security settings [↗](#)

---

Evaluating a public repository's security settings can help security researchers understand the repository's security posture. This information can help you decide whether to engage with the repository maintainers, for example, by reporting a vulnerability in the repository.

If a repository is public, high level information about the repository's security settings is available to anyone. For example, you can see whether the repository has a security policy, and whether private vulnerability reporting is enabled. You can also view published and closed security advisories for the repository. If no security policy is associated with a repository, you can suggest one. If the repository has private vulnerability reporting enabled, you can privately report security vulnerabilities directly to repository maintainers.

If you have admin permissions to the repository, and the repository is owned by an organization, you can see more detailed information about the repository's security settings through the security overview. For more information on the security overview, see "[About security overview](#)" in the GitHub Enterprise Cloud documentation.

If a repository is private, you can only see the security settings if you have admin permissions to the repository or have been granted special security permissions covering the repository, for example, as an organization-wide security manager.

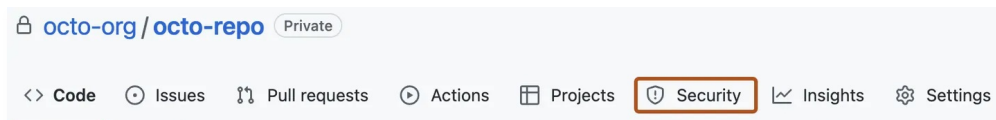
## Suggesting a security policy for a repository [↗](#)

---

If you do not have admin or security permissions for a public repository, you can still suggest a security policy to the repository maintainers if one doesn't already exist. The repository maintainers can then choose to accept or reject your suggestion. If the repository maintainers accept your suggestion, the security policy will be associated with the repository.

<sup>1</sup> 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**.



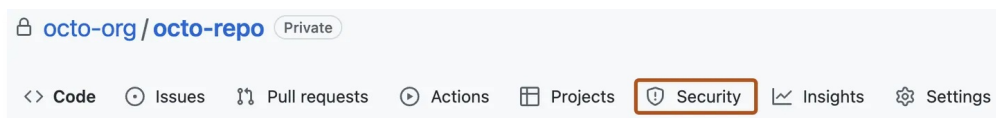
- 3 If the repository has a security policy, it will be displayed. If no security policy is associated with the repository, click **Suggest a policy**.
- 4 A SECURITY.md file will be created in the repository's default branch. The file will contain a template for a security policy. You can edit the file to add your suggested security policy.
- 5 When you are done, click **Commit changes**.
- 6 Fill out the **Commit changes** dialog.
  - Under "Commit message", enter a commit message.
  - Optionally, under "Extended description", describe the changes being made.
  - Select "Create a new branch for this commit and start a pull request"
  - Click **Commit changes**.
- 7 Click **Create pull request**.
- 8 Optionally, leave a comment.
- 9 Click **Create pull request**.

## Reporting a vulnerability in a repository [🔗](#)

If you do not have admin or security permissions for a public repository, you can still privately report a security vulnerability to repository maintainers if private vulnerability reporting is enabled. The repository maintainers can then choose to accept or reject your report. If the repository maintainers accept your report, a security advisory will be created for the repository.

**Note:** If the repository doesn't have private vulnerability reporting enabled, you need to initiate the reporting process by following the instructions in the security policy for the repository, or create an issue asking the maintainers for a preferred security contact. For more information, see "[About coordinated disclosure of security vulnerabilities](#)."

- 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 Click **Report a vulnerability** to open the advisory form.
- 4 Fill in the advisory details form.



**Tip:** In this form, only the title and description are mandatory. (In the general draft security advisory form, which the repository maintainer initiates, specifying the ecosystem is also required.) However, we recommend security researchers provide as much information as possible on the form so that the maintainers can make an informed decision about the submitted report. You can adopt the template used by our security researchers from the GitHub Security Lab, which is available on the [github/securitylab repository](#)."

For more information about the fields available and guidance on filling in the form, see "[Creating a repository security advisory](#)" and "[Best practices for writing repository security advisories](#)."


- 5 At the bottom of the form, click **Submit report**. GitHub will display a message letting you know that maintainers have been notified and that you have a pending credit for this security advisory.

**Tip:** When the report is submitted, GitHub automatically adds the reporter of the vulnerability as a collaborator and as a credited user on the proposed advisory.


- 6 Optionally, click **Start a temporary private fork** if you want to start to fix the issue. Note that only the repository maintainer can merge changes from that private fork into the parent repository.

  security-researcher-1 added as a collaborator 1 minute ago

---

**Collaborate on a patch in private**  
Use a temporary private fork of **octo-org/octo-repo** to collaborate on a fix.

Start a temporary private fork

**Thank you for reporting a vulnerability.**  
Your report is being reviewed by **octo-org-octo-repo** owners. You will be notified if the report is published as an advisory.

## Legal

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