

Forgejo Actions | Security



- [Security Design](#)
 - [Runner selection](#)
 - [Pull requests from forks](#)
 - [Automatic token](#)
 - [Pull requests](#)
 - [pull_request_target](#)
 - [Runner](#)
 - [Docker, Podman and LXC runners](#)
 - [Host runners](#)
 - [Secrets](#)
 - [Security considerations](#)
 - [Runner](#)
 - [Secrets](#)
-

Forgejo Actions is a very flexible CI/CD system. It lets you write workflows that execute arbitrary code, with contents of potentially private repositories. This brings some security risks. This page details the security design of the Actions system, and any considerations you should be aware of.

Security Design

Forgejo Actions consists of two main parts: The Forgejo server, which contains the repository and hands out workflow runs; and the Forgejo Runner, which receives workflow runs and executes them. One server may have many different runner attached, which are registered to different users or organizations.

Runner selection

When a workflow is triggered, the Forgejo instance will try to find a runner to run the workflow. The runner will be selected from a pool of runners that consists of the following groups:

- Runners registered to the Forgejo instance by the instance administrators
- Runners registered to the user account or organization account that the repository belongs to
- Runners registered to the specific repository

Your workflow will never be executed by a runner that does not belong to one of these groups.

Pull requests from forks

When a repository is publicly available on a Forgejo instance with open registration, any user can open a pull request that includes code to be executed by Forgejo Actions. Checkout the [section dedicated to trust management](#) for more information.

Automatic token

When a workflow is started, a unique authentication token is automatically created. It can be used to read the repositories associated with the workflow, even when they are private. This token is automatically destroyed when the workflow finishes.

This token can only be used for interactions with the repository it was created for, and any attempt to use it on other repositories will return a 404 error.

Pull requests

Workflows triggered by the `pull_request` event are an exception. The token generated for these runs does *not* have write permissions for the repository, since a pull request is not verified and could contain an untested or malicious workflow.

`pull_request_target`

As an alternative to `pull_request` there is `pull_request_target`. Workflows with this event will run in the context of the `base` of the Pull Request, instead of the incoming commits. This means that the changes proposed in the PR are *not* available in the workflow. You cannot use this event to perform workflows that would check the incoming changes.

Because no untrusted code is available to the runner in this context, the restrictions on the token are lifted. That means you can use this event type to write to the repository, for example to change labels or place comments.

Runner

The Forgejo Runner attempts to isolate different workflow runs from each other as much as possible. How this is achieved depends on the kind of runner it is.

Docker, Podman and LXC runners

In the case of a runner which uses OCI (Docker, Podman) or LXC containers, a new container will be created for each workflows. The containers provide isolation from the host system and other containers.

However, if the container environment is misconfigured it may be possible for a workflow to escape its confinement and perform potentially malicious actions. This may compromise the runner, which means that any future workflows sent to this runner may also be compromised.

Host runners

Host runners have no real isolation. When a workflow finishes the appropriate folders are cleaned up, so any workflows that stay within the intended bounds shouldn't have any effect on each other.

It is *trivial* to 'escape' on a host runner, and all sorts of malicious things can be done.

Secrets

Secrets can be used to store passwords or tokens for use in a workflow. They are stored encrypted in the Forgejo database, and sent out to workflows when they are needed. [More information](#).

Forgejo Runner attempts to automatically redact secrets from the logs.

Security considerations

When using Actions, keep in mind the following considerations:

Runner

- Container runners are generally safe, but they may be compromised if misconfigured.
- Never trust a host runner if it is shared with other users.
- The safest option is to [host your own runner](#), and use it only for your trusted repositories.

Secrets

- Use the [secrets feature](#) to store API tokens and passwords for use in workflows.

- Do not print secrets to output, as these may be publicly visible.
-

#3

□ cocobook-sync ### 2025-07-07 00:24:05 UTC

□ cocobook-sync ### 2026-05-05 22:44:47 UTC