Module 10.2\_Assigment

**Assignment: Shared Code Repository - Git Exercise**

Rajesh Ayyappanpillai

GitHub username : bellevuerajesh or bellevue.rajesh@gmail.com

[**Using the GITHUB\_TOKEN in a workflow**](https://docs.github.com/en/actions/security-for-github-actions/security-guides/automatic-token-authentication#using-the-github_token-in-a-workflow)

You can use the GITHUB\_TOKEN by using the standard syntax for referencing secrets: ${{ secrets.GITHUB\_TOKEN }}. Examples of using the GITHUB\_TOKEN include passing the token as an input to an action, or using it to make an authenticated GitHub API request.

Important

An action can access the GITHUB\_TOKEN through the github.token context even if the workflow does not explicitly pass the GITHUB\_TOKEN to the action. As a good security practice, you should always make sure that actions only have the minimum access they require by limiting the permissions granted to the GITHUB\_TOKEN. For more information, see [Permissions for the GITHUB\_TOKEN](https://docs.github.com/en/actions/security-for-github-actions/security-guides/automatic-token-authentication#permissions-for-the-github_token).

When you use the repository's GITHUB\_TOKEN to perform tasks, events triggered by the GITHUB\_TOKEN, with the exception of workflow\_dispatch and repository\_dispatch, will not create a new workflow run. This prevents you from accidentally creating recursive workflow runs. For example, if a workflow run pushes code using the repository's GITHUB\_TOKEN, a new workflow will not run even when the repository contains a workflow configured to run when push events occur.

Commits pushed by a GitHub Actions workflow that uses the GITHUB\_TOKEN do not trigger a GitHub Pages build.

[**Example 1: passing the GITHUB\_TOKEN as an input**](https://docs.github.com/en/actions/security-for-github-actions/security-guides/automatic-token-authentication#example-1-passing-the-github_token-as-an-input)

This example workflow uses the [GitHub CLI](https://docs.github.com/en/actions/using-workflows/using-github-cli-in-workflows), which requires the GITHUB\_TOKEN as the value for the GH\_TOKEN input parameter:

YAML

name: Open new issue

on: workflow\_dispatch

jobs:

open-issue:

runs-on: ubuntu-latest

permissions:

contents: read

issues: write

steps:

- run: |

gh issue --repo ${{ github.repository }} \

create --title "Issue title" --body "Issue body"

env:

GH\_TOKEN: ${{ secrets.GITHUB\_TOKEN }}

[**Example 2: calling the REST API**](https://docs.github.com/en/actions/security-for-github-actions/security-guides/automatic-token-authentication#example-2-calling-the-rest-api)

You can use the GITHUB\_TOKEN to make authenticated API calls. This example workflow creates an issue using the GitHub REST API:

name: Create issue on commit

on: [ push ]

jobs:

create\_issue:

runs-on: ubuntu-latest

permissions:

issues: write

steps:

- name: Create issue using REST API

run: |

curl --request POST \

--url https://api.github.com/repos/${{ github.repository }}/issues \

--header 'authorization: Bearer ${{ secrets.GITHUB\_TOKEN }}' \

--header 'content-type: application/json' \

--data '{

"title": "Automated issue for commit: ${{ github.sha }}",

"body": "This issue was automatically created by the GitHub Action workflow \*\*${{ github.workflow }}\*\*. \n\n The commit hash was: \_${{ github.sha }}\_."

}' \

--fail

[**Permissions for the GITHUB\_TOKEN**](https://docs.github.com/en/actions/security-for-github-actions/security-guides/automatic-token-authentication#permissions-for-the-github_token)

For information about the API endpoints GitHub Apps can access with each permission, see [Permissions required for GitHub Apps](https://docs.github.com/en/rest/overview/permissions-required-for-github-apps).

The following table shows the permissions granted to the GITHUB\_TOKEN by default. People with admin permissions to an enterprise, organization, or repository, can set the default permissions to be either permissive or restricted. For information on how to set the default permissions for the GITHUB\_TOKEN for your enterprise, organization, or repository, see [Enforcing policies for GitHub Actions in your enterprise](https://docs.github.com/en/enterprise-cloud@latest/admin/policies/enforcing-policies-for-your-enterprise/enforcing-policies-for-github-actions-in-your-enterprise#enforcing-a-policy-for-workflow-permissions-in-your-enterprise), [Disabling or limiting GitHub Actions for your organization](https://docs.github.com/en/organizations/managing-organization-settings/disabling-or-limiting-github-actions-for-your-organization#setting-the-permissions-of-the-github_token-for-your-organization), or [Managing GitHub Actions settings for a repository](https://docs.github.com/en/repositories/managing-your-repositorys-settings-and-features/enabling-features-for-your-repository/managing-github-actions-settings-for-a-repository#setting-the-permissions-of-the-github_token-for-your-repository).