Free Microsoft GH-500 Practice Questions

Shared by Lawson on 13-08-2026

For More Free Questions and Preparation Resources

Check the Links on Last Page

Question 1

Question Type: MultipleChoice

-- [Use Code Scanning with CodeQL]

When using the advanced CodeQL code scanning setup, what is the name of the workflow file?

Options:

A- codeql-config.yml
B- codeql-scan.yml
C- codeql-workflow.yml
D- codeql-analysis.yml

Answer:

D

Explanation:

Comprehensive and Detailed Explanation:

In the advanced setup for CodeQL code scanning, GitHub generates a workflow file named codeql-analysis.yml. This file is located in the .github/workflows directory of your repository. It defines the configuration for the CodeQL analysis, including the languages to analyze, the events that trigger the analysis, and the steps to perform during the workflow.

Question 2

Question Type: MultipleChoice

-- [Configure and Use Secret Scanning]

What filter or sort settings can be used to prioritize the secret scanning alerts that present the most risk?

Options:

A- Sort to display the oldest first

B- Sort to display the newest first
C- Filter to display active secrets
D- Select only the custom patterns

Answer:

C

Explanation:

The best way to prioritize secret scanning alerts is to filter by active secrets --- these are secrets GitHub has confirmed are still valid and could be exploited. This allows security teams to focus on high-risk exposures that require immediate attention.

Sorting by time or filtering by custom patterns won't help with risk prioritization directly.

Question 3

Question Type: MultipleChoice

-- [Configure GitHub Actions Workflows]

As a repository owner, you do not want to run a GitHub Actions workflow when changes are made to any .txt or markdown files. How would you adjust the event trigger for a pull request that targets the main branch? (Each answer presents part of the solution. Choose three.)

on:

pull_request:

branches: [main]

Options:

A- - '/*.md'
B- - '/*.txt'
C- paths:
D- paths-ignore:
E- - 'docs/*.md'

Answer:

A, B, D

Explanation:

To exclude .txt and .md files from triggering workflows on pull requests to the main branch:

on: defines the event (e.g., pull_request)

pull_request: is the trigger

paths-ignore: is the key used to ignore file patterns

Example YAML:

yaml

CopyEdit

on:

pull_request:

branches:

- main

paths-ignore:

- '*.md'

- '*.txt'

Using paths: would include only specific files instead --- not exclude. paths-ignore: is correct here.

Question 4

Question Type: MultipleChoice

-- [Describe GitHub Advanced Security Best Practices]

What kind of repository permissions do you need to request a Common Vulnerabilities and Exposures (CVE) identification number for a security advisory?

Options:

A- Maintain

B- Admin
C- Triage
D- Write

Answer:

B

Explanation:

Requesting a CVE ID for a security advisory in a GitHub repository requires Admin permissions. This level of access is necessary because it involves managing sensitive security information and coordinating with external entities to assign a CVE, which is a formal process that can impact the public perception and security posture of the project.

Question 5

Question Type: MultipleChoice

-- [Configure and Use Secret Scanning]

What YAML syntax do you use to exclude certain files from secret scanning?

Options:

A- decrypt_secret.sh
B- paths-ignore:
C- branches-ignore:
D- secret scanning.yml

Answer:

B

Explanation:

To exclude specific files or directories from being scanned by secret scanning in GitHub Actions, you can use the paths-ignore: key within your YAML workflow file.

This tells GitHub to ignore specified paths when scanning for secrets, which can be useful for excluding test data or non-sensitive mock content.

Other options listed are invalid:

branches-ignore: excludes branches, not files.

decrypt_secret.sh is not a YAML key.

secret scanning.yml is not a recognized filename for configuration.

Question 6

Question Type: MultipleChoice

-- [Configure and Use Secret Scanning]

What is the first step you should take to fix an alert in secret scanning?

Options:

A- Archive the repository.
B- Update your dependencies.
C- Revoke the alert if the secret is still valid.
D- Remove the secret in a commit to the main branch.

Answer:

C

Explanation:

The first step when you receive a secret scanning alert is to revoke the secret if it is still valid. This ensures the secret can no longer be used maliciously. Only after revoking it should you proceed to remove it from the code history and apply other mitigation steps.

Simply deleting the secret from the code does not remove the risk if it hasn't been revoked --- especially since it may already be exposed in commit history.

Question 7

Question Type: MultipleChoice

-- [Configure GitHub Advanced Security Tools in GitHub Enterprise]

As a developer, you need to configure a code scanning workflow for a repository where GitHub Advanced Security is enabled. What minimum repository permission do you need?

Options:

A- Write
B- None
C- Admin
D- Read

Answer:

A

Explanation:

To create or modify a code scanning workflow file (typically under .github/workflows/codeql-analysis.yml), you must have Write access to the repository.

Write permission allows you to commit the workflow file, which is required to run or configure code scanning using GitHub Actions.