Accelerate Your Certification with Microsoft GH-500 Practice Questions

Last chance to prepare smart! Get your hands on free Microsoft GitHub Advanced Security Exam PDF questions. Study real GH-500 dumps with verified answers and fast-track your certification success with PrepBolt GH-500 exam pdf questions and answers.

Thank you for Downloading GH-500 exam PDF Demo

https://prepbolt.com/GH-500.html

Question 1

Question Type: MultipleChoice

-- [Use Code Scanning with CodeQL]

Where can you use CodeQL analysis for code scanning? (Each answer presents part of the solution. Choose two.)

Options:

A- In a third-party Git repository
B- In a workflow
C- In an external continuous integration (CI) system
D- In the Files changed tab of the pull request

Answer:

B, C

Explanation:

In a workflow: GitHub Actions workflows are the most common place for CodeQL code scanning. The codeql-analysis.yml defines how the analysis runs and when it triggers.

In an external CI system: GitHub allows you to run CodeQL analysis outside of GitHub Actions. Once complete, the results can be uploaded using the upload-sarif action to make alerts visible in the repository.

You cannot run or trigger analysis from third-party repositories directly, and the Files changed tab in pull requests only shows diff --- not analysis results.

Question 2

Question Type: MultipleChoice

-- [Use Code Scanning with CodeQL]

What does code scanning do?

Options:

A- It contacts maintainers to ask them to create security advisories if a vulnerability is found
B- It prevents code pushes with vulnerabilities as a pre-receive hook
C- It analyzes a GitHub repository to find security vulnerabilities
D- It scans your entire Git history on branches present in your GitHub repository for any secrets

Answer:

C

Explanation:

Code scanning is a static analysis feature that examines your source code to identify security vulnerabilities and coding errors. It runs either on every push, pull request, or a scheduled time depending on the workflow configuration.

It does not automatically contact maintainers, scan full Git history, or block pushes unless explicitly configured to do so.

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

-- [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.

Question 5

Question Type: MultipleChoice

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

What step is required to run a SARIF-compatible (Static Analysis Results Interchange Format) tool on GitHub Actions?

Options:

A- Update the workflow to include a final step that uploads the results.
B- By default, the CodeQL runner automatically uploads results to GitHub on completion.
C- The CodeQL action uploads the SARIF file automatically when it completes analysis.
D- Use the CLI to upload results to GitHub.

Answer:

A

Explanation:

When using a SARIF-compatible tool within GitHub Actions, it's necessary to explicitly add a step in your workflow to upload the analysis results. This is typically done using the upload-sarif action, which takes the SARIF file generated by your tool and uploads it to GitHub for processing and display in the

Security tab. Without this step, the results won't be available in GitHub's code scanning interface.

Question 6

Question Type: MultipleChoice

-- [Describe GHAS Security Features and Functionality]

Which alerts do you see in the repository's Security tab? (Each answer presents part of the solution. Choose three.)

Options:

A- Repository permissions
B- Secret scanning alerts
C- Dependabot alerts
D- Security status alerts
E- Code scanning alerts

Answer:

B, C, E

Explanation:

In a repository's Security tab, you can view:

Secret scanning alerts: Exposed credentials or tokens

Dependabot alerts: Vulnerable dependencies from the advisory database

Code scanning alerts: Vulnerabilities in code detected via static analysis (e.g., CodeQL)

You won't see general 'security status alerts' (not a formal category) or permission-related alerts here.

Question 7

Question Type: MultipleChoice

-- [Configure and Use Dependency Management]

If default code security settings have not been changed at the repository, organization, or enterprise level, which repositories receive Dependabot alerts?

Options:

A- Repositories owned by an enterprise account
B- Private repositories
C- None
D- Repositories owned by an organization

Answer:

C

Explanation:

By default, no repositories receive Dependabot alerts unless configuration is explicitly enabled. GitHub does not enable Dependabot alerts automatically for any repositories unless:

The feature is turned on manually

It's configured at the organization or enterprise level via security policies

This includes public, private, and enterprise-owned repositories --- manual activation is required.

Thank You for trying GH-500 PDF Demo

To try our GH-500 practice exam software visit link below

https://prepbolt.com/GH-500.html

Start Your GH-500 Preparation

Use Coupon “SAVE50” for extra 50% discount on the purchase of Practice Test Software. Test your GH-500 preparation with actual exam questions.