

PRACTICE QUESTIONS

Microsoft

GH-500

GitHub Advanced Security

SHARED BY [u/gh500_hopeful](#) on aiexamcerts

EDITION Free Set 1

QUESTIONS 10

SHARED October 15, 2026

EXAM Microsoft GH-500, GitHub Advanced Security

Shared by [u/gh500_hopeful](#) on aiexamcerts

10 practice questions for the Microsoft GH-500 exam, GitHub Advanced Security, each followed by its answer and a short explanation. More free sets and the full practice exam: www.aiexamcerts.com/microsoft/gh-500. Spotted a mistake? Email support@aiexamcerts.com with the exam code GH-500 and the question number.

1. A team wants CodeQL to run the extra security queries beyond the default suite in its advanced setup workflow. Which setting does this?
- A on: workflow_dispatch, so the scan runs only when someone starts it by hand
 - B build-mode: none for every compiled language in the project
 - C category: /language:javascript-typescript, which names the results category
 - D queries: security-extended in the init step's configuration

Answer: D

The queries input set to security-extended tells CodeQL to run the broader set of security queries on top of the default suite. The category input only labels results and changes no query, which makes it a tempting but wrong choice. A manual trigger or a build mode affects when and how the scan runs, not which queries it uses.

2. Dependabot _____ updates keep dependencies current on a schedule, even when no vulnerability has been reported.

Answer: version

Version updates open pull requests on a schedule to keep dependencies current, whether or not a vulnerability is known. Security updates are the other type and are triggered by an alert. The two are configured in different places, so mixing them up is a common mistake.

3. What does a push protection bypass let a developer do?
- A Push a detected secret after choosing a recorded reason
 - B Turn off secret scanning for every repository in the whole organization
 - C Rotate the leaked token at the provider automatically
 - D Remove the secret from every fork of the repository

Answer: A

A bypass lets the developer continue a blocked push after picking one of the listed reasons, and the choice is recorded for review. Turning scanning off is an administrator decision and not a bypass. Automatic rotation and removal from forks are not things a bypass does, although a team may need to do both afterwards.

4. Push protection can block a commit that contains a supported secret before the commit reaches the remote branch.
- A True
 - B False

Answer: A (True)

True. Push protection checks the content of a push and rejects it when a supported secret is detected, so the secret is never stored on the remote branch. Secret scanning alerts for secrets already in history are a separate detection that works after the fact.

5. Which two statements about GitHub Advanced Security enablement are correct? (Choose two.)
- A Code scanning on a private repository needs a GHAS license
 - B Dependabot alerts on a private repository need a GHAS license
 - C Secret scanning must be enabled by a workflow file in each repository
 - D Secret scanning on a public repository needs no GHAS license
 - E Push protection needs a self-hosted runner to run

Answer: A, D

Private repositories need a GHAS license for code scanning, while public repositories receive secret scanning without one. Dependabot alerts are available on private repositories without a GHAS license, which makes option B a tempting error. Secret scanning is a repository setting rather than a workflow, and push protection runs on GitHub's side, not on a self-hosted runner.

6. Which action uploads SARIF results from a third-party scanner so that they appear as code scanning alerts?
- A actions/upload-artifact, which stores files as workflow artifacts
 - B actions/dependency-review-action, which checks pull request dependencies
 - C github/codeql-action/upload-sarif, which sends SARIF to the Security tab
 - D actions/attest-build-provenance, which signs build outputs

Answer: C

The codeql-action upload-sarif step sends a SARIF file to the repository so its findings appear as code scanning alerts. Upload-artifact keeps a file for download but does not create alerts, which makes it the tempting distractor. Dependency review and build provenance have different jobs and do not read SARIF.

7. What does enforcing push protection at the organization level accomplish?
- A It applies push protection to all repositories in the organization by default
 - B It removes existing secrets from the commit history of every repository
 - C It lets developers create custom patterns without an administrator's approval
 - D It disables secret scanning in every fork of the organization's repositories

Answer: A

Organization-level enforcement makes push protection apply across the organization's repositories, so teams do not have to turn it on one repository at a time. Removing secrets from history needs commit rewriting and is not a setting. Custom pattern creation is governed by permissions, and forks are not disabled by enforcement.

8. The dependency review action runs in a pull request workflow using the reference actions/_____.

Answer: dependency-review-action

The dependency-review-action checks the dependency changes in a pull request and fails when a newly added package has a vulnerability or license the policy blocks. It needs the dependency graph enabled on the repository. Dependabot version updates run on their own schedule and do not check pull requests in this way.

9. A code scanning alert appears on a pull request check. Which step lets the reviewer see the exact data flow path that CodeQL reports?
- A Open the workflow log for the analyze job and read its output lines
 - B Download the CodeQL database from the run summary
 - C Open the alert and view the code flow trace in its details
 - D Edit the SARIF file in a text editor

Answer: C

The alert details show the code flow, which is the path from source to sink that the query found, so reviewers can follow it step by step. The workflow log shows job progress rather than findings, which makes it a tempting place to look. Downloading the database or editing the SARIF file is possible, but it is far harder than reading the trace in the alert.

10. A developer wants a code scanning alert on a pull request to close without being dismissed. Which change to the pull request does this?
- A Fixing the code so the query no longer matches on the analyzed branch
 - B Adding an extra paragraph to the README file that explains the project
 - C Renaming the workflow file that runs the scan
 - D Increasing the timeout for the analyze job

Answer: A

When the flagged code changes so the query no longer matches on the analyzed branch, the next analysis no longer reports the alert and it is closed as fixed. Documentation edits, renaming the workflow and changing timeouts do not change what the query finds. Renaming the workflow is tempting because the alert appears to come from it.