

PRACTICE QUESTIONS

Microsoft

GH-500

GitHub Advanced Security

SHARED BY [u/humbleturtle1991](#) on aiexamcerts

EDITION Free Set 2

QUESTIONS 10

SHARED October 15, 2026

EXAM Microsoft GH-500, GitHub Advanced Security

Shared by [u/humbleturtle1991](#) 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. Which CodeQL artifact contains the data extracted from source code that queries run against?
- A A SARIF file produced by the analyze step
 - B A workflow artifact uploaded to the run summary
 - C The dependency graph of the repository
 - D A CodeQL database

Answer: D

A CodeQL database holds the extracted representation of the code, and queries run against it to find issues. A SARIF file is the output format for results, which makes it a tempting distractor. Workflow artifacts and the dependency graph are unrelated to the extracted code model.

2. Dependabot alerts require a GitHub Advanced Security license on private repositories.
- A True
 - B False

Answer: B (False)

False. Dependabot alerts are available on private repositories without a GHAS license, because they rely on the dependency graph and the Advisory Database. A GHAS license adds code scanning, secret scanning and dependency review.

3. Which of these is one of the reasons a developer can choose to bypass push protection for a detected secret?
- A Reviewed and approved by the security team
 - B It's used in tests
 - C The credential was already rotated and deleted
 - D Skip scanning for this branch only

Answer: B

The bypass reasons offered are it's a false positive, I'll fix it later and it's used in tests. Approval-style wording is not one of the fixed choices, even though an organization can require review of bypass requests. Skipping a branch is not a bypass reason at all.

4. Each Dependabot update entry requires a _____ key that sets how often the check runs.

Answer: schedule

Every update entry in `dependabot.yml` needs a `schedule` with an interval such as `daily`, `weekly` or `monthly`. Without it the entry is not valid for version updates. Security updates are triggered by alerts and are not set by this key.

5. Which two items does a CodeQL advanced setup workflow need? (Choose two.)

- A A `dependabot.yml` file in the `.github` directory
- B An init step that sets up the CodeQL tooling and database
- C A `CODEOWNERS` file that names the security team
- D An analyze step that runs the queries against the database
- E A custom secret scanning pattern for the repository

Answer: B, D

The init step prepares CodeQL and creates the database, and the analyze step runs the queries and produces results. A `dependabot.yml` file and a `CODEOWNERS` file are useful but are not required by the CodeQL workflow itself. A custom secret pattern belongs to secret scanning, not to code scanning.

6. Which REST API endpoint returns the secret scanning alerts for a repository?

- A `/repos/{owner}/{repo}/actions/secrets`
- B `/repos/{owner}/{repo}/dependabot/secrets/public-key`
- C `/repos/{owner}/{repo}/secret-scanning/alerts`
- D `/repos/{owner}/{repo}/code-scanning/alerts`

Answer: C

The `secret-scanning/alerts` endpoint returns secret scanning alerts for the repository. The Actions secrets and Dependabot secrets endpoints manage encrypted secret values for workflows and Dependabot runs, not alerts. The `code-scanning/alerts` endpoint returns code scanning results, which is a different feature.

7. Which Dependabot version update setting combines several related package updates into a single pull request?

- A `ignore`, which excludes selected dependencies or versions from updates
- B `groups`, which collects matching dependencies into one pull request
- C `registries`, which declares private package sources
- D `open-pull-requests-limit`, which caps how many pull requests stay open

Answer: B

The `groups` key lets related dependencies, selected by name or pattern, arrive in one pull request so reviewers handle them together. The `ignore` key is the tempting choice because it also shapes which updates appear, but it excludes updates rather than combining them. Registries and the open pull requests limit control sources and volume, not grouping.

8. The organization security overview can show which repositories have secret scanning enabled.
- A True
 - B False

Answer: A (True)

True. The security overview lists enablement status for security features across repositories and summarizes open alerts. Teams use it to find repositories that are not covered before they audit them.

9. A maintainer decides that a code scanning alert will not be fixed in this release. Which state does the alert show after that decision?
- A fixed
 - B dismissed
 - C open
 - D archived in the repository history

Answer: B

A dismissed alert records a reason such as won't fix, false positive or used in tests, and it stays in the history. Fixed means the code no longer triggers the query, which is the tempting but wrong state. Open means no decision has been made, and archived is not a code scanning alert state.

10. Which organization view summarizes enabled security features and open alerts across its repositories?
- A Security overview
 - B Branch rulesets
 - C Audit log export
 - D Dependency graph page of one repository

Answer: A

The security overview is the organization-level view that summarizes enablement and alerts across repositories. Branch rulesets control merges and pushes, and the audit log records administrative events rather than findings. The dependency graph page shows one repository, which makes it a tempting but narrower choice.