# GH-500 Exam Resources & GH-500 Actual Questions & GH-500 Exam Guide

2026 Latest RealValidExam GH-500 PDF Dumps and GH-500 Exam Engine Free Share: https://drive.google.com/open?id=1fXUeTs-s2MhFb5uy8N3056rVHhZUgLs3

It is worth mentioning that, the simulation test is available in our software version. With the simulation test, all of our customers will get accustomed to the GH-500 exam easily, and get rid of bad habits, which may influence your performance in the real GH-500 exam. In addition, the mode of GH-500 learning guide questions and answers is the most effective for you to remember the key points. During your practice process, the GH-500 Test Questions would be absorbed, which is time-saving and high-efficient. Considerate 24/7 service shows our attitudes, we always consider our candidates' benefits and we guarantee that our GH-500 test questions are the most excellent path for you to pass the exam.

## Microsoft GH-500 Exam Syllabus Topics:

| Topic | Details |
|---|---|
| Topic 1 | • Configure and use Dependabot and Dependency Review: Focused on Software Engineers and Vulnerability Management Specialists, this section describes tools for managing vulnerabilities in dependencies. Candidates learn about the dependency graph and how it is generated, the concept and format of the Software Bill of Materials (SBOM), definitions of dependency vulnerabilities, Dependabot alerts and security updates, and Dependency Review functionality. It covers how alerts are generated based on the dependency graph and GitHub Advisory Database, differences between Dependabot and Dependency Review, enabling and configuring these tools in private repositories and organizations, default alert settings, required permissions, creating Dependabot configuration files and rules to auto-dismiss alerts, setting up Dependency Review workflows including license checks and severity thresholds, configuring notifications, identifying vulnerabilities from alerts and pull requests, enabling security updates, and taking remediation actions including testing and merging pull requests. |
| Topic 2 | • Configure and use Code Scanning with CodeQL: This domain measures skills of Application Security Analysts and DevSecOps Engineers in code scanning using both CodeQL and third-party tools. It covers enabling code scanning, the role of code scanning in the development lifecycle, differences between enabling CodeQL versus third-party analysis, implementing CodeQL in GitHub Actions workflows versus other CI tools, uploading SARIF results, configuring workflow frequency and triggering events, editing workflow templates for active repositories, viewing CodeQL scan results, troubleshooting workflow failures and customizing configurations, analyzing data flows through code, interpreting code scanning alerts with linked documentation, deciding when to dismiss alerts, understanding CodeQL limitations related to compilation and language support, and defining SARIF categories. |

| | |
|---|---|
| Topic 3 | • Describe the GHAS security features and functionality: This section of the exam measures skills of Security Engineers and Software Developers and covers understanding the role of GitHub Advanced Security (GHAS) features within the overall security ecosystem. Candidates learn to differentiate security features available automatically for open source projects versus those unlocked when GHAS is paired with GitHub Enterprise Cloud (GHEC) or GitHub Enterprise Server (GHES). The domain includes knowledge of Security Overview dashboards, the distinctions between secret scanning and code scanning, and how secret scanning, code scanning, and Dependabot work together to secure the software development lifecycle. It also covers scenarios contrasting isolated security reviews with integrated security throughout the development lifecycle, how vulnerable dependencies are detected using manifests and vulnerability databases, appropriate responses to alerts, the risks of ignoring alerts, developer responsibilities for alerts, access management for viewing alerts, and the placement of Dependabot alerts in the development process. |
| Topic 4 | • Describe GitHub Advanced Security best practices, results, and how to take corrective measures: This section evaluates skills of Security Managers and Development Team Leads in effectively handling GHAS results and applying best practices. It includes using Common Vulnerabilities and Exposures (CVE) and Common Weakness Enumeration (CWE) identifiers to describe alerts and suggest remediation, decision-making processes for closing or dismissing alerts including documentation and data-based decisions, understanding default CodeQL query suites, how CodeQL analyzes compiled versus interpreted languages, the roles and responsibilities of development and security teams in workflows, adjusting severity thresholds for code scanning pull request status checks, prioritizing secret scanning remediation with filters, enforcing CodeQL and Dependency Review workflows via repository rulesets, and configuring code scanning, secret scanning, and dependency analysis to detect and remediate vulnerabilities earlier in the development lifecycle, such as during pull requests or by enabling push protection. |
| Topic 5 | • Configure and use secret scanning: This domain targets DevOps Engineers and Security Analysts with the skills to configure and manage secret scanning. It includes understanding what secret scanning is and its push protection capability to prevent secret leaks. Candidates differentiate secret scanning availability in public versus private repositories, enable scanning in private repos, and learn how to respond appropriately to alerts. The domain covers alert generation criteria for secrets, user role-based alert visibility and notification, customizing default scanning behavior, assigning alert recipients beyond admins, excluding files from scans, and enabling custom secret scanning within repositories. |

# Free Sample GH-500 Questions - GH-500 Reliable Braindumps Book

The Microsoft desktop practice test software and web-based Understanding GitHub Advanced Security GH-500 practice test both simulate the actual exam environment and identify your mistakes. With these two Microsoft GH-500 practice exams, you will get the actual GH-500 Exam environment. Whereas the RealValidExam PDF file is ideal for restriction-free test preparation. You can open this PDF file and revise GH-500 real exam questions at any time.

## Microsoft GitHub Advanced Security Sample Questions (Q11-Q16):

**NEW QUESTION # 11**
What step is required to run a SARIF-compatible (Static Analysis Results Interchange Format) tool on GitHub Actions?

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

**Answer: B**

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.

## NEW QUESTION # 12

In a private repository, what minimum requirements does GitHub need to generate a dependency graph? (Each answer presents part of the solution. Choose two.)

- A. Read-only access to all the repository's files
- B. Read-only access to the dependency manifest and lock files for a repository
- C. Dependency graph enabled at the organization level for all new private repositories
- D. Write access to the dependency manifest and lock files for an enterprise

**Answer: B,C**

Explanation:
Comprehensive and Detailed Explanation:
To generate a dependency graph for a private repository, GitHub requires:
Dependency graph enabled: The repository must have the dependency graph feature enabled. This can be configured at the organization level to apply to all new private repositories.
Access to manifest and lock files: GitHub needs read-only access to the repository's dependency manifest and lock files (e.g., package.json, requirements.txt) to identify and map dependencies.

## NEW QUESTION # 13

What is required to trigger code scanning on a specified branch?

- A. Developers must actively maintain the repository.
- B. The workflow file must exist in that branch.
- C. The repository must be private.
- D. Secret scanning must be enabled on the repository.

**Answer: B**

Explanation:
Comprehensive and Detailed Explanation:
For code scanning to be triggered on a specific branch, the branch must contain the appropriate workflow file, typically located in the .github/workflows directory. This YAML file defines the code scanning configuration and specifies the events that trigger the scan (e.g., push, pull_request).
Without the workflow file in the branch, GitHub Actions will not execute the code scanning process for that branch. The repository's visibility (private or public), the status of secret scanning, or the activity level of developers do not directly influence the triggering of code scanning.

## NEW QUESTION # 14

Secret scanning will scan:

- A. External services.
- B. A continuous integration system.
- C. Any Git repository.
- D. The GitHub repository.

**Answer: D**

Explanation:
Secret scanning is a feature provided by GitHub that scans the contents of your GitHub repositories for known types of secrets, such as API keys and tokens. It operates within the GitHub environment and does not scan external systems, services, or repositories outside of GitHub. Its primary function is to prevent the accidental exposure of sensitive information within your GitHub-hosted code.

## NEW QUESTION # 15

What role is required to change a repository's code scanning severity threshold that fails a pull request status check?

- A. Maintain
- B. Write
- C. Triage
- D. Admin

**Answer: D**

Explanation:
To change the threshold that defines whether a pull request fails due to code scanning alerts (such as blocking merges based on severity), the user must have Admin access on the repository. This is because modifying these settings falls under repository configuration privileges.
Users with Write, Maintain, or Triage roles do not have the required access to modify rulesets or status check policies.

## NEW QUESTION # 16

......

As far as our GH-500 practice test is concerned, the PDF version brings you much convenience with regard to the following two aspects. On the one hand, the PDF version contains demo where a part of questions selected from the entire version of our GH-500 test torrent is contained. In this way, you have a general understanding of our actual prep exam, which must be beneficial for your choice of your suitable exam files. On the other hand, our GH-500 Preparation materials can be printed so that you can study for the exams with papers and PDF version. With such benefits, why don't you have a try?

**Free Sample GH-500 Questions**: https://www.realvalidexam.com/GH-500-real-exam-dumps.html