# GH-500 Original Questions: GitHub Advanced Security & GH-500 Answers Real Questions & GH-500 Exam Cram


What's more, part of that BraindumpsPrep GH-500 dumps now are free: https://drive.google.com/open?id=12idYW6cOjqqwUxN8NVnZhsnRDBx0zHWO

The smartest way of getting high passing score in GH-500 valid test is choosing latest and accurate certification learning materials. The up-to-date GH-500 exam answers will save you from wasting much time and energy in the exam preparation. The content of our GH-500 Dumps Torrent covers the key points of exam, which will improve your ability to solve the difficulties of GH-500 real questions. Just add our exam dumps to your cart to get certification.

BraindumpsPrep provides you with a free demo of Microsoft GH-500 Questions so you do not have any doubts about the quality of our exam prep material. Similarly, We also provide free updates up to 365 days after purchasing GitHub Advanced Security dumps questions, so that you always get the latest Microsoft dumps.

**>> GH-500 Valid Test Topics <<**

## Valid GH-500 Exam Duration | GH-500 Valid Exam Prep

Certification GH-500 exam on the first attempt. The demand of the GitHub Advanced Security exam is growing at a rapid pace day by day and almost everyone is planning to pass it so that they can improve themselves for better futures in the BraindumpsPrep sector. GH-500 has tried its best to make this learning material the most user-friendly so the applicants don't face excessive issues.

## Microsoft GH-500 Exam Syllabus Topics:

| Topic | Details |
|---|---|
| | |

| | |
|---|---|
| Topic 1 | • 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. |
| 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 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. |

## Microsoft GitHub Advanced Security Sample Questions (Q63-Q68):

**NEW QUESTION # 63**

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

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

**NEW QUESTION # 64**
What does a CodeQL database of your repository contain?

- A. A build for Go projects to set up the project
- B. A representation of all of the source code
- C. A build of the code and extracted data
- D. Build commands for C/C++, C#, and Java

**Answer: C**

Explanation:
GitHub
Agentic AI for AppSec Teams
Explanation:
Comprehensive and Detailed Explanation:
A CodeQL database contains a representation of your codebase, including the build of the code and extracted data. This database is used to run CodeQL queries to analyze your code for potential vulnerabilities and errors.
GitHub Docs

**NEW QUESTION # 65**
When using CodeQL, how does extraction for compiled languages work?

- A. By monitoring the normal build process
- B. By running directly on the source code
- C. By generating one language at a time
- D. By resolving dependencies to give an accurate representation of the codebase

**Answer: A**

Explanation:
For compiled languages, CodeQL performs extraction by monitoring the normal build process. This means it watches your usual build commands (like make, javac, or dotnet build) and extracts the relevant data from the actual build steps being executed. CodeQL uses this information to construct a semantic database of the application.
This approach ensures that CodeQL captures a precise, real-world representation of the code and its behavior as it is compiled, including platform-specific configurations or conditional logic used during build.

**NEW QUESTION # 66**
How would you build your code within the CodeQL analysis workflow? (Each answer presents a complete solution. Choose two.)

- A. Use jobs.analyze.runs-on.
- B. Upload compiled binaries.
- C. Implement custom build steps.
- D. Use CodeQL's init action.

- E. Use CodeQL's autobuild action.
- F. Ignore paths.

**Answer: C,E**

Explanation:
Comprehensive and Detailed Explanation:
When setting up CodeQL analysis for compiled languages, there are two primary methods to build your code:
GitHub Docs
Autobuild: CodeQL attempts to automatically build your codebase using the most likely build method. This is suitable for standard build processes.
GitHub Docs
Custom Build Steps: For complex or non-standard build processes, you can implement custom build steps by specifying explicit build commands in your workflow. This provides greater control over the build process.
GitHub Docs
The init action initializes the CodeQL analysis but does not build the code. The jobs.analyze.runs-on specifies the operating system for the runner but is not directly related to building the code. Uploading compiled binaries is not a method supported by CodeQL for analysis.

**NEW QUESTION # 67**
Where can you view code scanning results from CodeQL analysis?

- A. At Security advisories
- B. The repository's code scanning alerts
- C. A CodeQL database
- D. A CodeQL query pack

**Answer: B**

Explanation:
All results from CodeQL analysis appear under the repository's code scanning alerts tab. This section is part of the Security tab and provides a list of all current, fixed, and dismissed alerts found by CodeQL.
A CodeQL database is used internally during scanning but does not display results. Query packs contain rules, not results. Security advisories are for published vulnerabilities, not per-repo findings.

**NEW QUESTION # 68**
.....

- Valid GH-500 Test Pattern □ GH-500 Exam Training □ Valid GH-500 Test Pattern ▸ Search for ☀ GH-500 □☀□ and download exam materials for free through 「 www.prep4away.com 」 □GH-500 Online Version
- GH-500 Latest Learning Material □ Vce GH-500 File □ GH-500 Reliable Mock Test □ Open ▸ www.pdfvce.com ◂ enter □ GH-500 □ and obtain a free download □Valid Test GH-500 Experience
- Up to one year of Free Microsoft GH-500 Exam Questions Updates 👆 Search for ⇛ GH-500 ⇚ on [ www.pdfdumps.com ] immediately to obtain a free download □GH-500 Exam Training
- Excellent GH-500 Valid Test Topics | Latest Updated Valid GH-500 Exam Duration and Trustworthy GitHub Advanced Security Valid Exam Prep □ Go to website ➡ www.pdfvce.com □□□ open and search for ➡ GH-500 □□□ to download for free □GH-500 Reliable Braindumps
- Vce GH-500 File □ GH-500 Latest Learning Material □ GH-500 Reliable Braindumps □ Search for ▸ GH-500 ◂ and easily obtain a free download on ▹ www.dumpsquestion.com ◃ □Valid GH-500 Study Guide
- myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, www.stes.tyc.edu.tw, www.stes.tyc.edu.tw, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, www.stes.tyc.edu.tw, www.stes.tyc.edu.tw, www.stes.tyc.edu.tw, matrixbreach.com, www.stes.tyc.edu.tw, www.stes.tyc.edu.tw, Disposable vapes

DOWNLOAD the newest BraindumpsPrep GH-500 PDF dumps from Cloud Storage for free: https://drive.google.com/open?id=12idYW6cOjqqwUxN8NVnZhsnRDBx0zHWO