

Latest GH-500 Study Question Give You 100% Valid Exam Reference Guide



These latest GitHub Advanced Security (GH-500) Questions were made by 2Pass4sure professionals after working day and night so that users can prepare for the Microsoft GH-500 exam successfully. 2Pass4sure even guarantees you that you can pass the Microsoft GH-500 Certification test on the first try with your untiring efforts.

Microsoft GH-500 Exam Syllabus Topics:

Topic	Details
Topic 1	<ul style="list-style-type: none">• 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	<ul style="list-style-type: none"> 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 3	<ul style="list-style-type: none"> 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	<ul style="list-style-type: none"> 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 5	<ul style="list-style-type: none"> 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.

>> New GH-500 Braindumps Free <<

Exam GH-500 Bootcamp | Reliable GH-500 Exam Pdf

A lot of applicants have studied from Microsoft GH-500 practice material. They have rated it positively because they have cracked Microsoft GH-500 Certification on their first try. 2Pass4sure guarantees its customers that they can pass the GH-500 test on the first attempt.

Microsoft GitHub Advanced Security Sample Questions (Q58-Q63):

NEW QUESTION # 58

A repository's dependency graph includes:

- A. A summary of the dependencies used in your organization's repositories.
- **B. Dependencies parsed from a repository's manifest and lock files.**
- C. Annotated code scanning alerts from your repository's dependencies.
- D. Dependencies from all your repositories.

Answer: B

Explanation:

The dependency graph in a repository is built by parsing manifest and lock files (like package.json, pom.xml, requirements.txt). It helps GitHub detect dependencies and cross-reference them with known vulnerability databases for alerting. It is specific to each repository and does not show org-wide or cross-repo summaries.

NEW QUESTION # 59

Where can you find a deleted line of code that contained a secret value?

- A. Dependency graph
- B. Insights
- **C. Commits**
- D. Issues

Answer: C

Explanation:

Secrets committed and then deleted are still accessible in the repository's Git history. To locate them, navigate to the Commits tab. GitHub's secret scanning can detect secrets in both current and historical commits, which is why remediation should also include revoking the secret, not just removing it from the latest code.

NEW QUESTION # 60

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

- A. Use CodeQL's init action.
- B. Upload compiled binaries.
- **C. Use CodeQL's autobuild action.**
- D. Ignore paths.
- E. Use jobs.analyze.runs-on.
- **F. Implement custom build steps.**

Answer: C,F

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 # 61

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

Dependabot alerts?

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

Answer: A

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.

NEW QUESTION # 62

Which patterns are secret scanning validity checks available to?

- A. Push protection patterns
- B. Custom patterns
- C. High entropy strings
- **D. Partner patterns**

Answer: D

Explanation:

Validity checks - where GitHub verifies if a secret is still active - are available for partner patterns only. These are secrets issued by GitHub's trusted partners (like AWS, Slack, etc.) and have APIs for GitHub to validate token activity status.

Custom patterns and high entropy patterns do not support automated validity checks.

NEW QUESTION # 63

.....

To avail of all these benefits you need to pass the Microsoft GH-500 exam which is a difficult exam that demands firm commitment and complete GitHub Advanced Security (GH-500) exam questions preparation. For the well and quick GH-500 Exam Dumps preparation, you can get help from 2Pass4sure GH-500 Questions which will provide you with everything that you need to learn, prepare and pass the GitHub Advanced Security (GH-500) certification exam.

Exam GH-500 Bootcamp: <https://www.2pass4sure.com/GitHub-Administrator/GH-500-actual-exam-braindumps.html>

- GH-500 Reliable Dumps Book ☐ Updated GH-500 Test Cram ☐ Valid Test GH-500 Format ☐ Open website ✓
www.pass4test.com ☐ ✓ ☐ and search for ➡ GH-500 ☐ for free download ☐ GH-500 Reliable Dumps Sheet
- GH-500 Reliable Torrent ☐ GH-500 Reliable Dumps Sheet ☐ GH-500 Guaranteed Success ☐ Go to website ➡
www.pdfvce.com ☐ open and search for ➡ GH-500 ☐ to download for free ☐ GH-500 Reliable Dumps Book
- Free PDF Quiz 2025 Professional Microsoft New GH-500 Braindumps Free ☐ Simply search for ➡ GH-500 ☐ ☐ for free download on > www.passtestking.com < ☐ Reliable GH-500 Dumps
- Download GH-500 Fee ☐ Latest GH-500 Dumps Book ☐ GH-500 Guaranteed Success ☐ Open website ☀
www.pdfvce.com ☐ ☀ ☐ and search for [GH-500] for free download ☐ Latest GH-500 Dumps Book
- GH-500 Reliable Torrent ☐ Relevant GH-500 Questions ☐ GH-500 Book Pdf ☐ Search on ▶ www.pdfidumps.com ◀
for ➡ GH-500 ☐ to obtain exam materials for free download ☐ GH-500 Book Pdf
- Pass Guaranteed Quiz Microsoft - GH-500 - GitHub Advanced Security Useful New Braindumps Free ☐ Search for ☐
GH-500 ☐ and download exam materials for free through ▶ www.pdfvce.com ◀ ☐ Exam GH-500 Price
- Realistic New GH-500 Braindumps Free - Pass GH-500 Exam ☐ Search for > GH-500 ☐ on ▶ www.examdisscuss.com
◀ immediately to obtain a free download ☐ GH-500 Study Test
- Microsoft New GH-500 Braindumps Free: GitHub Advanced Security - Pdfvce Pass-leading Provider ☐ The page for free
download of ✓ GH-500 ☐ ✓ ☐ on { www.pdfvce.com } will open immediately ☐ GH-500 Reliable Dumps Book
- Microsoft New GH-500 Braindumps Free: GitHub Advanced Security - www.pass4leader.com Pass-leading Provider ☐
Enter (www.pass4leader.com) and search for [GH-500] to download for free ☐ Updated GH-500 Test Cram

- [illegible]