Pass Guaranteed Quiz 2026 GH-500: GitHub Advanced Security Perfect Test Practice

P.S. Free & New GH-500 dumps are available on Google Drive shared by PassSureExam: https://drive.google.com/open?id=1R1sDAc-WX3n1D__QWx92AEUZ__1M6iyB

It is apparent that a majority of people who are preparing for the GH-500 exam would unavoidably feel nervous as the exam approaching, since you have clicked into this website, you can just take it easy now--our GH-500 learning materials. Our company has spent more than 10 years on compiling study materials for the exam, and now we are delighted to be here to share our GH-500 Study Materials with all of the candidates for the exam in this field. There are so many striking points of our GH-500 preparation exam.

Microsoft GH-500 Exam Syllabus Topics:

Topic	Details
Topic 1	- 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 2	- 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 3	• 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 4	• 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 5	• 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.

Pass Guaranteed 2026 Microsoft Latest GH-500: Test GitHub Advanced Security Practice

It is quite convenient to study with our GH-500 study materials. If you are used to study with paper-based materials you can choose the PDF version which is convenient for you to print. If you would like to get the mock test before the real GH-500 exam you can choose the software version, and if you want to study in anywhere at any time then our online APP version is your best choice since you can download it in any electronic devices. And the price of our GH-500 learning guide is favorable.

Microsoft GitHub Advanced Security Sample Questions (Q22-Q27):

NEW QUESTION # 22
Which of the following steps should you follow to integrate CodeQL into a third-party continuous integration system? (Each answer presents part of the solution. Choose three.)

- A. Upload scan results
- B. Process alerts
- C. Install the CLI
- D. Analyze code
- E. Write queries

Answer: A,C,D

Explanation:
When integrating CodeQL outside of GitHub Actions (e.g., in Jenkins, CircleCI):
Install the CLI: Needed to run CodeQL commands.
Analyze code: Perform the CodeQL analysis on your project with the CLI.
Upload scan results: Export the results in SARIF format and use GitHub's API to upload them to your repo's security tab.
You don't need to write custom queries unless extending functionality. "Processing alerts" happens after GitHub receives the results.

NEW QUESTION # 23
After investigating a code scanning alert related to injection, you determine that the input is properly sanitized using custom logic. What should be your next step?

- A. Open an issue in the CodeQL repository.
- B. Ignore the alert.
- C. Dismiss the alert with the reason "false positive."
- D. Draft a pull request to update the open-source query.

Answer: C

Explanation:
When you identify that a code scanning alert is a false positive-such as when your code uses a custom sanitization method not recognized by the analysis-you should dismiss the alert with the reason "false positive." This action helps improve the accuracy of future analyses and maintains the relevance of your security alerts.
As per GitHub's documentation:
"If you dismiss a CodeQL alert as a false positive result, for example because the code uses a sanitization library that isn't supported, consider contributing to the CodeQL repository and improving the analysis." By dismissing the alert appropriately, you ensure that your codebase's security alerts remain actionable and relevant.

NEW QUESTION # 24
Which of the following options are code scanning application programming interface (API) endpoints? (Each answer presents part of the solution. Choose two.)

- A. Get a single code scanning alert
- B. Modify the severity of an open code scanning alert
- C. List all open code scanning alerts for the default branch
- D. Delete all open code scanning alerts

Answer: A,C

Explanation:
The GitHub Code Scanning API includes endpoints that allow you to:
List alerts for a repository (filtered by branch, state, or tool) - useful for monitoring security over time.
Get a single alert by its ID to inspect its metadata, status, and locations in the code.
However, GitHub does not support modifying the severity of alerts via API - severity is defined by the scanning tool (e.g., CodeQL). Likewise, alerts cannot be deleted via the API; they are resolved by fixing the code or dismissing them manually.

NEW QUESTION # 25
Which of the following formats are used to describe a Dependabot alert? (Each answer presents a complete solution. Choose two.)

- A. Common Vulnerabilities and Exposures (CVE)
- B. Exploit Prediction Scoring System (EPSS)
- C. Vulnerability Exploitability exchange (VEX)
- D. Common Weakness Enumeration (CWE)

Answer: A,D

Explanation:
Dependabot alerts utilize standardized identifiers to describe vulnerabilities:
CVE (Common Vulnerabilities and Exposures): A widely recognized identifier for publicly known cybersecurity vulnerabilities.

CWE (Common Weakness Enumeration): A category system for software weaknesses and vulnerabilities.
These identifiers help developers understand the nature of the vulnerabilities and facilitate the search for more information or remediation strategies.

NEW QUESTION # 26
Which details do you have to provide to create a custom pattern for secret scanning? (Each answer presents part of the solution. Choose two.)

- A. The secret format
- B. A list of repositories to scan
- C. The name of the pattern
- D. Additional match requirements for the secret format

Answer: A,C

Explanation:
When defining a custom pattern for secret scanning, two key fields are required:
Name of the pattern: A unique label to identify the pattern
Secret format: A regular expression that defines what the secret looks like (e.g., token format) You can optionally specify additional match requirements (like required context keywords), but they're not mandatory. Listing repositories is also not part of the required fields during pattern creation.

NEW QUESTION # 27
......

We have always been made rapid progress on our GH-500 training materials because of the merits of high-efficiency and perfect after-sales services online for 24 hours. Studying with our GH-500 actual exam, you can get the most professional information and achieve your dreaming scores by your first go. We can claim that as long as you study with our GH-500 Exam Guide for 20 to 30 hours, you will pass your GH-500 exam confidently.

Exam GH-500 Answers: https://www.passsureexam.com/GH-500-pass4sure-exam-dumps.html www.stes.tyc.edu.tw, 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, Disposable vapes

What's more, part of that PassSureExam GH-500 dumps now are free: https://drive.google.com/open?id=1R1sDAc-WX3n1D__QWx92AEUZ__1M6iyB