Microsoft GH-500 Exam Dumps - Pass Exam in One Go

BTW, DOWNLOAD part of Actual4Exams GH-500 dumps from Cloud Storage: https://drive.google.com/open?id=10gYSirKx_WyrEa9IQ4IwILuzY3QrX3xF

The GH-500 latest exam torrents have different classifications for different qualification examinations, which can enable students to choose their own learning mode for themselves according to the actual needs of users. The GH-500 exam questions offer a variety of learning modes for users to choose from, which can be used for multiple clients of computers and mobile phones to study online, as well as to print and print data for offline consolidation. Our reasonable price and GH-500 Latest Exam torrents supporting practice perfectly, as well as in the update to facilitate instant upgrade for the users in the first place, compared with other education platform on the market, the GH-500 test torrent can be said to have high quality performance, let users spend the least money to meet their maximum needs.

Microsoft GH-500 Exam Syllabus Topics:

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

100% Pass 2026 Microsoft GH-500 Fantastic New Test Labs

They are committed to assisting you in Microsoft GH-500 exam preparation and boosting the GH-500 exam candidate's confidence to pass it. The GitHub Advanced Security (GH-500) exam questions are designed and verified by Microsoft exam trainers. They check and ensure each GH-500 Practice Questions are real, updated, and accurate. So rest assured that with the GitHub Advanced Security (GH-500) practice exams you can get success in challenging the GH-500 exam easily.

Microsoft GitHub Advanced Security Sample Questions (Q80-Q85):

NEW QUESTION # 80
You have enabled security updates for a repository. When does GitHub mark a Dependabot alert as resolved for that repository?

- A. When you dismiss the Dependabot alert
- B. When you merge a pull request that contains a security update
- C. When the pull request checks are successful
- D. When Dependabot creates a pull request to update dependencies

Answer: B

Explanation:
A Dependabot alert is marked as resolved only after the related pull request is merged into the repository. This indicates that the vulnerable dependency has been officially replaced with a secure version in the active codebase.
Simply generating a PR or passing checks does not change the alert status; merging is the key step.

NEW QUESTION # 81
Which of the following is the most proactive and practical way to prevent new secret scanning alerts?

- A. Scan for non-provider patterns
- B. Configure a secret scanning Actions workflow.
- C. Use feature branches
- D. Enable push protection.

Answer: D

Explanation:
To prevent new secret scanning alerts, enable push protection to block secrets from being committed in the first place, and manage push protection patterns to disable blocking for specific, low-risk secret types or false positives.
Enable Push Protection
Prevent new commits: Push protection proactively scans code for secrets before they are pushed to a repository. If a secret is detected, the push is blocked, providing immediate feedback to developers and preventing secrets from entering the codebase.
Configure patterns: You can configure which secret patterns are blocked at the organization or enterprise level. By disabling patterns that frequently generate false positives, you can reduce the number of new alerts.

NEW QUESTION # 82
Assuming that notification settings and Dependabot alert recipients have not been customized, which user account setting should you use to get an alert when a vulnerability is detected in one of your repositories?

- A. enable all for Dependency graph
- B. enable all in existing repositories
- C. enable all for Dependabot alerts
- D. enable by default for new public repositories

Answer: C

Explanation:
To ensure you're notified whenever a vulnerability is detected via Dependabot, you mustenablealerts for Dependabotin your personal notification settings. This applies to both new and existing repositories. It ensures you get timely alerts about security vulnerabilities.
[Not C] The dependency graph must be enabled for scanning, but does not send alerts itself.

NEW QUESTION # 83
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. Draft a pull request to update the open-source query.
- B. Open an issue in the CodeQL repository.
- C. Dismiss the alert with the reason "false positive."
- D. Ignore the alert.

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 # 84
Which of the following workflow events would trigger a dependency review? (Each answer presents a complete solution. Choose two.)

- A. workflow_dispatch
- B. pull_request
- C. commit
- D. trigger

Answer: B,C

Explanation:
About the dependency review action
The "dependency review action" refers to the specific action that can report on differences in a pull request within the GitHub Actions context. You can use the dependency review action in your repository to enforce dependency reviews on your pull requests.
[D] The action uses the dependency review REST API to get the diff of dependency changes between the base commit and head commit. You can use the dependency review API to get the diff of dependency changes, including vulnerability data, between any two commits on a repository. [A]
[D] dependency-review-action
The dependency review action scans your pull requests for dependency changes, and will raise an error if any vulnerabilities or invalid licenses are being introduced. The action is supported by an API endpoint that diffs the dependencies between any two revisions on your default branch.
Incorrect:
[Not B] The workflow_dispatch event adds a layer of flexibility and control to your GitHub workflows, enabling manual triggers with custom inputs. Whether integrating with external systems or managing deployments directly from GitHub, workflow_dispatch provides the tools necessary for robust workflow management.

NEW QUESTION # 85
.....

GitHub Advanced Security GH-500 study guide are high quality, since we have a professional team to collect the information for the exam, and we can ensure you that GH-500 study guide you receive are the latest information we have. In order to strengthen your confidence for Microsoft GH-500 Exam Dumps, we are pass guarantee and money back guarantee.

500 Ppt

- New New GH-500 Test Labs | Reliable Microsoft GH-500: GitHub Advanced Security 100% Pass □ The page for free download of ▷ GH-500 ◁ on ☀ www.pdfvce.com □☀□ will open immediately □GH-500 Valid Exam Labs
- New New GH-500 Test Labs | Reliable Microsoft GH-500: GitHub Advanced Security 100% Pass □ The page for free download of ☀ GH-500 □☀□ on 【 www.pdfdumps.com 】 will open immediately □GH-500 Latest Braindumps Files
- GH-500 Exam □ GH-500 Exam □ GH-500 100% Accuracy □ Easily obtain （ GH-500 ） for free download through ➡ www.pdfvce.com □□□ □GH-500 Exam Collection Pdf
- Updated New GH-500 Test Labs - Passing GH-500 Exam is No More a Challenging Task □ Download 【 GH-500 】 for free by simply searching on ▶ www.prep4sures.top ◀ □GH-500 Latest Braindumps Files
- bookmarkja.com, heathltcb996912.blog-kids.com, susanzgah323152.digitollblog.com, thekiwisocial.com, aronuucy484369.blogthisbiz.com, mysocialfeeder.com, 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, barbaragjxp536174.blog4youth.com, www.stes.tyc.edu.tw, Disposable vapes

DOWNLOAD the newest Actual4Exams GH-500 PDF dumps from Cloud Storage for free: https://drive.google.com/open?id=10gYSirKx_WyrEa9IQ4IwILuzY3QrX3xF