Pass GH-500 Test - Exam GH-500 Revision Plan

BTW, DOWNLOAD part of CramPDF GH-500 dumps from Cloud Storage: https://drive.google.com/open?id=1r4sS1jN9aVcV145Bam2o6Hp7j90yfFQW

Even we have engaged in this area over ten years, professional experts never blunder in their handling of the GH-500 exam torrents. By compiling our GH-500 prepare torrents with meticulous attitude, the accuracy and proficiency of them is nearly perfect. As the leading elites in this area, our GH-500 prepare torrents are in concord with syllabus of the exam. They are professional backup to this fraught exam. So by using our GH-500 Exam torrents made by excellent experts, the learning process can be speeded up to one week. They have taken the different situation of customers into consideration and designed practical GH-500 test braindumps for helping customers save time. As elites in this area they are far more proficient than normal practice materials' editors, you can trust them totally.

As you can find that on our website, we have three versions of our GH-500 study materials for you: the PDF, Software and APP online. The PDF can be printale. While the Software and APP online can be used on computers. When you find it hard for you to learn on computers, you can learn the printed materials of the GH-500 Exam Questions. What is more, you absolutely can afford fort the three packages. The price is set reasonably. And the Value Pack of the GH-500 practice guide contains all of the three versions with a more favourable price.

>> Pass GH-500 Test <<

Free PDF 2026 GH-500: GitHub Advanced Security Unparalleled Pass Test

Continuous improvement is a good thing. If you keep making progress and transcending yourself, you will harvest happiness and growth. The goal of our GH-500 latest exam guide is prompting you to challenge your limitations. People always complain that they do nothing perfectly. The fact is that they never insist on one thing and give up quickly. Our GH-500 Study Dumps will assist you to overcome your shortcomings and become a persistent person. Once you have made up your minds to change, come to purchase our GH-500 training practice.

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	• 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	• 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 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	• 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.

Microsoft GitHub Advanced Security Sample Questions (Q65-Q70):

NEW QUESTION # 65

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

Answer: A,D

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 # 66
What filter or sort settings can be used to prioritize the secret scanning alerts that present the most risk?

- A. Sort to display the oldest first
- B. Select only the custom patterns
- C. Sort to display the newest first
- D. Filter to display active secrets

Answer: D

Explanation:
The best way to prioritize secret scanning alerts is to filter by active secrets - these are secrets GitHub has confirmed are still valid and could be exploited. This allows security teams to focus on high-risk exposures that require immediate attention.
Sorting by time or filtering by custom patterns won't help with risk prioritization directly.

NEW QUESTION # 67
A secret scanning alert should be closed as "used in tests" when a secret is:

- A. In the readme.md file.
- B. In a test file.
- C. Solely used for tests.
- D. Not a secret in the production environment.

Answer: C

Explanation:
If a secret is intentionally used in a test environment and poses no real-world security risk, you may close the alert with the reason "used in tests". This helps reduce noise and clarify that the alert was reviewed and accepted as non-critical.
Just being in a test file isn't enough unless its purpose is purely for testing.

NEW QUESTION # 68
What happens when you enable secret scanning on a private repository?

- A. Your team is subscribed to security alerts.
- B. Dependency review, secret scanning, and code scanning are enabled.
- C. GitHub performs a read-only analysis on the repository.
- D. Repository administrators can view Dependabot alerts.

Answer: C

Explanation:

When secret scanning is enabled on a private repository, GitHub performs a read-only analysis of the repository's contents. This includes the entire Git history and files to identify strings that match known secret patterns or custom-defined patterns.
GitHub does not alter the repository, and enabling secret scanning does not automatically enable code scanning or dependency review - each must be configured separately.

NEW QUESTION # 69
Which of the following statements most accurately describes push protection for secret scanning custom patterns?

- A. Push protection is not available for custom patterns.
- B. Push protection is enabled by default for new custom patterns.
- C. Push protection is an opt-in experience for each custom pattern.
- D. Push protection must be enabled for all, or none, of a repository's custom patterns.

Answer: C

Explanation:
Comprehensive and Detailed Explanation:
Push protection for secret scanning custom patterns is an opt-in feature. This means that for each custom pattern defined in a repository, maintainers can choose to enable or disable push protection individually. This provides flexibility, allowing teams to enforce push protection on sensitive patterns while leaving it disabled for others.

NEW QUESTION # 70
......

myportal.utt.edu.tt, myportal.utt.edu.tt, Disposable vapes

What's more, part of that CramPDF GH-500 dumps now are free: https://drive.google.com/open?id=1r4sS1jN9aVcV145Bam2o6Hp7j90yfFQW