GH-500 Exam Vce Free, GH-500 Latest Exam Test

DOWNLOAD the newest UpdateDumps GH-500 PDF dumps from Cloud Storage for free: https://drive.google.com/open?id=176TFc4Cd0XmgY7rlKTkmmZMeHZWzzfik

Various study forms are good for boosting learning interests. So our company has taken all customers' requirements into account. Some people are not good at operating computers. So you might worry about that the GH-500 certification materials are not suitable for you. Try to believe us. Our experts have taken your worries seriously. They have made it easy to operate for all people. Even if you know little about computers, you can easily begin to do exercises of the GH-500 Real Exam dumps.

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	• 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 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 GH-500 Latest Exam Test - Reliable GH-500 Braindumps Book

Our GH-500 study quiz boosts high quality and we provide the wonderful service to the client. We boost the top-ranking expert team which compiles our GH-500 guide prep elaborately and check whether there is the update every day and if there is the update the system will send the update automatically to the client. The content of our GH-500 Preparation questions is easy to be mastered and seizes the focus to use the least amount of answers and questions to convey the most important information.

Microsoft GitHub Advanced Security Sample Questions (Q13-Q18):

NEW QUESTION # 13
What role is required to change a repository's code scanning severity threshold that fails a pull request status check?

- A. Write
- B. Admin
- C. Triage
- D. Maintain

Answer: B

Explanation:
To change the threshold that defines whether a pull request fails due to code scanning alerts (such as blocking merges based on severity), the user must have Admin access on the repository. This is because modifying these settings falls under repository configuration privileges.
Users with Write, Maintain, or Triage roles do not have the required access to modify rulesets or status check policies.

NEW QUESTION # 14
What do you need to do before you can define a custom pattern for a repository?

- A. Add a secret scanning custom pattern.
- B. Provide a regular expression for the format of your secret pattern.
- C. Enable secret scanning on the repository.

- D. Provide match requirements for the secret format.

Answer: C

Explanation:
Stack Overflow
Explanation:
Comprehensive and Detailed Explanation:
Before defining a custom pattern for secret scanning in a repository, you must enable secret scanning for that repository. Secret scanning must be active to utilize custom patterns, which allow you to define specific formats (using regular expressions) for secrets unique to your organization.
Once secret scanning is enabled, you can add custom patterns to detect and prevent the exposure of sensitive information tailored to your needs.

NEW QUESTION # 15
Assuming that no custom Dependabot behavior is configured, who has the ability to merge a pull request created via Dependabot security updates?

- A. An enterprise administrator
- B. A user who has read access to the repository
- C. A repository member of an enterprise organization
- D. A user who has write access to the repository

Answer: D

Explanation:
Comprehensive and Detailed Explanation:
By default, users with write access to a repository have the ability to merge pull requests, including those created by Dependabot for security updates. This access level allows contributors to manage and integrate changes, ensuring that vulnerabilities are addressed promptly.
Users with only read access cannot merge pull requests, and enterprise administrators do not automatically have merge rights unless they have write or higher permissions on the specific repository.

NEW QUESTION # 16
Which of the following formats are used to describe a Dependabot alert? (Each answer presents a complete solution. Choose two.)

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

Answer: B,C

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 # 17
What is required to trigger code scanning on a specified branch?

- A. Developers must actively maintain the repository.
- B. Secret scanning must be enabled on the repository.
- C. The workflow file must exist in that branch.
- D. The repository must be private.

Answer: C

Explanation:
Comprehensive and Detailed Explanation:
For code scanning to be triggered on a specific branch, the branch must contain the appropriate workflow file, typically located in the .github/workflows directory. This YAML file defines the code scanning configuration and specifies the events that trigger the scan (e.g., push, pull_request).
Without the workflow file in the branch, GitHub Actions will not execute the code scanning process for that branch. The repository's visibility (private or public), the status of secret scanning, or the activity level of developers do not directly influence the triggering of code scanning.

NEW QUESTION # 18

......

For candidates who are going to buy GH-500 exam torrent online, you may pay much attention to the privacy protection. We respect the private information of you, if you choose us for your GH-500 exam materials, your personal information will be protected well. Once the order finishes, your personal information such as your name and email address will be concealed. In addition, we have a professional team to research the professional knowledge for GH-500 Exam Materials, and you can get the latest information timely. Free update for one year is available, and the update version for GH-500 training material will be sent to your email automatically.