100% Pass 2026 GH-500: GitHub Advanced Security– Trustable Free Download

What's more, part of that PrepAwayExam GH-500 dumps now are free: https://drive.google.com/open?id=1IKYIeqGl1HKoC_3nBEgTswGKD1E5JfXy

Our valid GH-500 exam dumps will provide you with free dumps demo with accurate answers that based on the real exam. These GH-500 real questions and answers contain the latest knowledge points and the requirement of the certification exam. High quality and accurate of GH-500 Pass Guide will be 100% guarantee to clear your test and get the certification with less time and effort.

Microsoft GH-500 Exam Syllabus Topics:

Topic	Details
Topic 1	• 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 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	• 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 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.

Reliable GH-500 Dumps Questions & Pdf GH-500 Dumps

Working in IT field, you definitely want to prove your ability by passing IT certification test. Moreover, the colleagues and the friends with IT certificate have been growing. In this case, if you have none, you will not be able to catch up with the others. For example like Microsoft GH-500 Certification Exam, it is a very valuable examination, which must help you realize your wishes.

Microsoft GitHub Advanced Security Sample Questions (Q10-Q15):

NEW QUESTION # 10
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 # 11

As a repository owner, you want to receive specific notifications, including security alerts, for an individual repository. Which repository notification setting should you use?

- A. Ignore
- B. Custom
- C. All Activity
- D. Participating and @mentions

Answer: B

Explanation:
Using the Custom setting allows you to subscribe to specific event types, such as Dependabot alerts or vulnerability notifications, without being overwhelmed by all repository activity. This is essential for repository maintainers who need fine-grained control over what kinds of events trigger notifications.
This setting is configurable per repository and allows users to stay aware of critical issues while minimizing notification noise.

NEW QUESTION # 12

Assuming that notification and alert recipients are not customized, what does GitHub do when it identifies a vulnerable dependency in a repository where Dependabot alerts are enabled? (Each answer presents part of the solution. Choose two.)

- A. It generates a Dependabot alert and displays it on the Security tab for the repository.
- B. It notifies the repository administrators about the new alert.
- C. It generates Dependabot alerts by default for all private repositories.
- D. It consults with a security service and conducts a thorough vulnerability review.

Answer: A,B

Explanation:
Comprehensive and Detailed Explanation:
When GitHub identifies a vulnerable dependency in a repository with Dependabot alerts enabled, it performs the following actions:
Generates a Dependabot alert: The alert is displayed on the repository's Security tab, providing details about the vulnerability and affected dependency.
Notifies repository maintainers: By default, GitHub notifies users with write, maintain, or admin permissions about new Dependabot alerts.
GitHub Docs
These actions ensure that responsible parties are informed promptly to address the vulnerability.

NEW QUESTION # 13

Who can fix a code scanning alert on a private repository?

- A. Users who have Write access to the repository
- B. Users who have Read permissions within the repository
- C. Users who have the Triage role within the repository
- D. Users who have the security manager role within the repository

Answer: A

Explanation:
Comprehensive and Detailed Explanation:
In private repositories, users with write access can fix code scanning alerts. They can do this by committing changes that address the issues identified by the code scanning tools. This level of access ensures that only trusted contributors can modify the code to resolve potential security vulnerabilities.
GitHub Docs
Users with read or triage roles do not have the necessary permissions to make code changes, and the security manager role is primarily focused on managing security settings rather than directly modifying code.
Reference:
GitHub Docs

NEW QUESTION # 14
When does Dependabot alert you of a vulnerability in your software development process?

- A. As soon as a pull request is opened by a contributor
- B. When Dependabot opens a pull request to update a vulnerable dependency
- C. As soon as a vulnerable dependency is detected
- D. When a pull request adding a vulnerable dependency is opened

Answer: C

Explanation:
Dependabot alerts are generated as soon as GitHub detects a known vulnerability in one of your dependencies. GitHub does this by analyzing your repository's dependency graph and matching it against vulnerabilities listed in the GitHub Advisory Database. Once a match is found, the system raises an alert automatically without waiting for a PR or manual action.
This allows organizations to proactively mitigate vulnerabilities as early as possible, based on real-time detection.

NEW QUESTION # 15
......

There is no denying the fact that everyone in the world wants to find a better job to improve the quality of life. Generally speaking, these jobs are offered only by some well-known companies. In order to enter these famous companies, we must try our best to get some certificates as proof of our ability such as the GH-500 Certification. And our GH-500 exam questions are the exactly tool to help you get the GH-500 certification. Just buy our GH-500 study materials, then you will win it.