100% Pass 2026 Microsoft GH-500: GitHub Advanced Security–High Pass-Rate Reliable Braindumps

P.S. Free & New GH-500 dumps are available on Google Drive shared by Exams-boost: https://drive.google.com/open?id=19sB-cklFLVQ7jKfMRIK1WJo9q9cQZH69

It is not hard to know that GH-500 torrent prep is compiled by hundreds of industry experts based on the syllabus and development trends of industries that contain all the key points that may be involved in the examination. Therefore, with GH-500 exam questions, you no longer need to purchase any other review materials, and you also don't need to spend a lot of money on tutoring classes. At the same time, GH-500 Test Guide will provide you with very flexible learning time in order to help you pass the exam.

To make sure your situation of passing the certificate efficiently, our GH-500 practice materials are compiled by first-rank experts. So the proficiency of our team is unquestionable. They help you review and stay on track without wasting your precious time on useless things. They handpicked what the GH-500 Study Guide usually tested in exam recent years and devoted their knowledge accumulated into these GH-500 actual tests.

>> GH-500 Reliable Braindumps <<

Quiz GH-500 - Useful GitHub Advanced Security Reliable Braindumps

Our users of the GH-500 learning guide are all over the world. Therefore, we have seen too many people who rely on our GH-500 exam materials to achieve counterattacks. Everyone's success is not easily obtained if without our GH-500 study questions. Of course, they have worked hard, but having a competent assistant is also one of the important factors. And our GH-500 Practice Engine is the right key to help you get the certification and lead a better life!

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 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	• 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 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.

Microsoft GitHub Advanced Security Sample Questions (Q36-Q41):

NEW QUESTION # 36
Which of the following tasks can be performed by a security team as a proactive measure to help address secret scanning alerts? Each answer presents a complete solution. (Choose two.)

- A. Document alternatives to storing secrets in the source code.
- B. Dismiss alerts that are older than 90 days.
- C. Enable system for cross-domain identity management (SCIM) provisioning for the enterprise.
- D. Configure a webhook to monitor for secret scanning alert events.

Answer: A,D

Explanation:

[D] Integrate Secret Scanning into the Development Lifecycle:
*-> Pre-commit hooks:
Implement pre-commit hooks in version control systems to scan code for secrets before they are even committed.
[B] Implement a Comprehensive Secret Scanning Policy:
Define Secrets: Clearly define what constitutes a secret within your organization.
Scanning Scope: Specify which environments and repositories need to be scanned and how often.
Roles and Responsibilities: Define roles and responsibilities for managing secret scanning and remediation.
Incorrect:
[A] You can manage the lifecycle of your enterprise's user accounts from your identity provider (IdP) using System for Cross-domain Identity Management (SCIM).

NEW QUESTION # 37
What should you do after receiving an alert about a dependency added in a pull request?

- A. Update the vulnerable dependencies before the branch is merged
- B. Fork the branch and deploy the new fork
- C. Deploy the code to your default branch
- D. Disable Dependabot alerts for all repositories owned by your organization

Answer: A

Explanation:
If an alert is raised on a pull request dependency, best practice is to update the dependency to a secure version before merging the PR. This prevents the vulnerable version from entering the main codebase.
Merging or deploying the PR without fixing the issue exposes your production environment to known risks.

NEW QUESTION # 38
Which CodeQL query suite provides queries of lower severity than the default query suite?

- A. security-extended
- B. github/codeql/cpp/ql/src@main
- C. github/codeql-go/ql/src@main

Answer: A

Explanation:
The security-extended query suite includes additional CodeQL queries that detect lower severity issues than those in the default security-and-quality suite.
It's often used when projects want broader visibility into code hygiene and potential weak spots beyond critical vulnerabilities.
The other options listed are paths to language packs, not query suites themselves.

NEW QUESTION # 39
You have enabled Dependabot alerts on your repository. If Dependabot detects a vulnerable dependency, it sends an alert when:

- A. a contributor adds the vulnerable dependency to a manifest in the repository.
- B. the vulnerability is removed from the GitHub Advisory Database.
- C. manifests and lock files are out of date and a version needs to be updated.
- D. a contributor makes a change to a function in the code.

Answer: A

Explanation:
Detection of insecure dependencies
Dependabot performs a scan of the default branch of your repository to detect insecure dependencies, and sends Dependabot alerts when:
* A new advisory is added to the GitHub Advisory Database.
* The dependency graph for a repository changes. For example, when a contributor pushes a commit to change the packages or versions it depends on, or when the code of one of the dependencies changes.

Additionally, GitHub can review any dependencies added, updated, or removed in a pull request made against the default branch of a repository, and flag any changes that would reduce the security of your project. This allows you to spot and deal with vulnerable dependencies before, rather than after, they reach your codebase.
Note: When you push a commit to GitHub that changes or adds a supported manifest or lock file to the default branch, the dependency graph is automatically updated. In addition, the graph is updated when anyone pushes a change to the repository of one of your dependencies.

NEW QUESTION # 40
By default, who will receive an e-mail when a secret has been detected in a repository? Each answer presents a complete solution. (Choose two.)

- A. security analyst
- B. users with the Admin repository role
- C. users with the Write repository role
- D. users with the Maintain repository role
- E. user who committed the secret

Answer: B,E

Explanation:
When a new secret is detected, GitHub notifies all users with access to security alerts for the repository according to their notification preferences.
These users include:
Repository administrators. [D]
Security managers.
Users with custom roles with read/write access
Organization owners and enterprise owners, if they are administrators of repositories where secrets were leaked Note Commit authors who've accidentally committed secrets will be notified, regardless of their notification preferences. [B]

NEW QUESTION # 41
.....

and obtain a free download on 【 www.pdfvce.com 】 Certificate GH-500 Exam

- 100% Pass Quiz Microsoft - Newest GH-500 Reliable Braindumps Go to website { www.validtorrent.com } open and search for [GH-500] to download for free GH-500 High Quality
- thebookmarknight.com, hyperbookmarks.com, gretafeyu278459.wikibyby.com, 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, saulimkc675018.blognody.com, qasimxuch606715.blogacep.com, harleyrudq711794.blog-mall.com, marcnazy377280.blgwiki.com, guideyoursocial.com, georgiaihkx398159.newsbloger.com, Disposable vapes

BTW, DOWNLOAD part of Exams-boost GH-500 dumps from Cloud Storage: https://drive.google.com/open?id=19sB-cklFLVQ7jKfMRIK1WJo9q9cQZH69