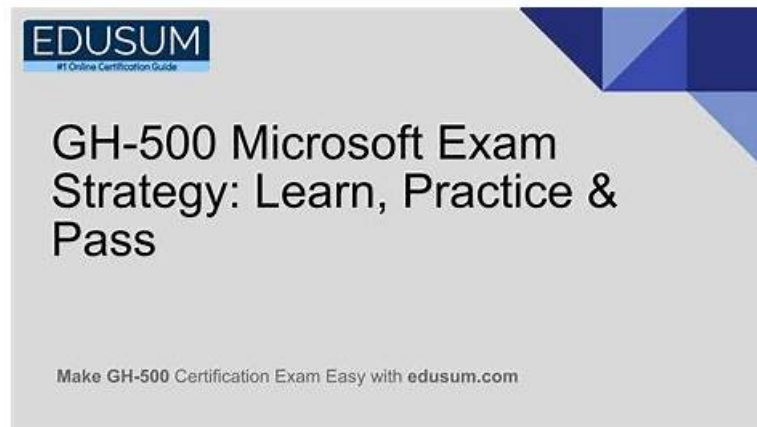


Valid New GH-500 Exam Guide & Correct GH-500 Review Guide & GH-500 Free Dumps



DOWNLOAD the newest DumpsKing GH-500 PDF dumps from Cloud Storage for free: <https://drive.google.com/open?id=1n8w9IWYuXbmCIqw9Ve6FkqdcwREjkVj8>

Our GH-500 exam torrent boosts 3 versions and they include PDF version, PC version, and APP online version. The 3 versions boost their each strength and using method. For example, the PC version of GH-500 exam torrent boosts installation software application, simulates the Real GH-500 Exam, supports MS operating system and boosts 2 modes for practice and you can practice offline at any time. You can learn the APP online version of GH-500 guide torrent in the computers, cellphones and laptops and you can choose the most convenient method to learn.

The DumpsKing supports Microsoft GH-500 exam candidates by listening to their worries, resolving their problems, and offering them actual exam questions. The exam candidate has several concerns before choosing any platform. They want a platform that satisfies them and promises to help them prepare for the GH-500 test successfully on the first time.

>> **New GH-500 Exam Guide** <<

2026 100% Free GH-500 –Efficient 100% Free New Exam Guide | GitHub Advanced Security Review Guide

With GH-500 study materials, you will have more flexible learning time. With GH-500 study materials, you can flexibly arrange your study time according to your own life. You don't need to be in a hurry to go to classes after work as the students who take part in a face-to-face class, and you also never have to disrupt your schedule for learning. GH-500 Study Materials help you not only to avoid all the troubles of learning but also to provide you with higher learning quality than other students'.

Microsoft GH-500 Exam Syllabus Topics:

Topic	Details
Topic 1	<ul style="list-style-type: none">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 2	<ul style="list-style-type: none"> • 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	<ul style="list-style-type: none"> • 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 4	<ul style="list-style-type: none"> • 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	<ul style="list-style-type: none"> • 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.

Microsoft GitHub Advanced Security Sample Questions (Q97-Q102):

NEW QUESTION # 97

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

Answer: D

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 # 98

If default code security settings have not been changed at the repository, organization, or enterprise level, which repositories receive Dependabot alerts?

- A. repositories owned by an enterprise account
- **B. none**
- C. private repositories
- D. repositories owned by an organization

Answer: B

Explanation:

When Dependabot detects vulnerable dependencies in your repositories, we generate a Dependabot alert and display it on the Security tab for the repository. GitHub notifies the maintainers of affected repositories about the new alert according to their notification preferences.

Dependabot is enabled by default on all public repositories, and needs to be enabled on private repositories.

Note:

By default, no repositories receive Dependabot alerts unless configuration is explicitly enabled.

GitHub does not enable Dependabot alerts automatically for any repositories unless:

The feature is turned on manually

It's configured at the organization or enterprise level via security policies This includes public, private, and enterprise-owned repositories -manual activation is required.

NEW QUESTION # 99

Which of the following is the best way to prevent developers from adding secrets to the repository?

- A. Create a CODEOWNERS file
- **B. Enable push protection**
- C. Make the repository public
- D. Configure a security manager

Answer: B

Explanation:

The best proactive control is push protection. It scans for secrets during a git push and blocks the commit before it enters the repository.

Other options (like CODEOWNERS or security managers) help with oversight but do not prevent secret leaks.

Making a repo public would increase the risk, not reduce it.

NEW QUESTION # 100

Which of the following features helps to prioritize secret scanning alerts that present an immediate risk?

- **A. Secret validation**
- B. Push protection
- C. Non-provider patterns
- D. Custom pattern dry runs

Answer: A

Explanation:

Secret validation checks whether a secret found in your repository is still valid and active with the issuing provider (e.g., AWS, GitHub, Stripe). If a secret is confirmed to be active, the alert is marked as verified, which means it's considered a high-priority issue because it presents an immediate security risk.

This helps teams respond faster to valid, exploitable secrets rather than wasting time on expired or fake tokens.

NEW QUESTION # 101

What is the purpose of the SECURITY.md file in a GitHub repository?

- A. readme.md
- B. support.md
- C. contributing.md
- D. security.md

Answer: D

Explanation:

The correct place to look is the SECURITY.md file. This file provides contributors and security researchers with instructions on how to responsibly report vulnerabilities. It may include contact methods, preferred communication channels (e.g., security team email), and disclosure guidelines.

This file is considered a GitHub best practice and, when present, activates a "Report a vulnerability" button in the repository's Security tab.

NEW QUESTION # 102

.....

As we all know that the higher position always ask for the more capable man. So your strength and efficiency will really bring you more job opportunities. You must complete your goals in the shortest possible time. How to make it? Our GH-500 exam materials can give you a lot of help. Our GH-500 Study Guide is famous for its high-effective and high-efficiency advantages. If you study with our GH-500 practice engine, you can get the latest and specialized information in the subject and you will be rewarded with the certification.

GH-500 Review Guide: <https://www.dumpsking.com/GH-500-testking-dumps.html>

- GH-500 Exam Actual Tests New GH-500 Braindumps Questions GH-500 Exam Actual Tests Download GH-500 for free by simply searching on " www.examcollectionpass.com" Free GH-500 Sample
- New GH-500 Braindumps Questions Practice GH-500 Mock Free GH-500 Sample Download GH-500 for free by simply entering www.pdfvce.com website GH-500 Examcollection Questions Answers
- Pass-Sure Microsoft New GH-500 Exam Guide Are Leading Materials - 100% Pass-Rate GH-500: GitHub Advanced Security Search for GH-500 and download it for free on www.torrentvce.com website Practice GH-500 Engine
- Exam GH-500 Preparation Latest GH-500 Test Simulator Practice GH-500 Engine Download GH-500 for free by simply searching on www.pdfvce.com Practice GH-500 Mock
- GH-500 Minimum Pass Score GH-500 Authorized Pdf Exam GH-500 Preparation Go to website www.pdfdumps.com open and search for GH-500 to download for free New GH-500 Test Simulator
- Pass Guaranteed Efficient GH-500 - New GitHub Advanced Security Exam Guide Immediately open www.pdfvce.com and search for GH-500 to obtain a free download GH-500 Valid Test Test
- New GH-500 Exam Guide Exam Latest Release | Updated GH-500 Review Guide Search on www.prepawayexam.com for GH-500 to obtain exam materials for free download GH-500 Examcollection Questions Answers
- Valid GH-500 Practice Materials GH-500 Minimum Pass Score GH-500 Test Simulator Free Search for GH-500 and download it for free on www.pdfvce.com website GH-500 Minimum Pass Score
- Marvelous New GH-500 Exam Guide | Easy To Study and Pass Exam at first attempt - Accurate Microsoft GitHub Advanced Security Search on www.testkingpass.com for GH-500 to obtain exam materials for free download GH-500 Hot Questions
- Latest GH-500 Test Simulator Real GH-500 Exam Dumps Valid GH-500 Practice Materials Easily obtain free download of GH-500 by searching on (www.pdfvce.com) Real GH-500 Exam Dumps
- Exam GH-500 Preparation New GH-500 Test Simulator GH-500 Test Simulator Free Search on www.troytecdumps.com for GH-500 to obtain exam materials for free download Exam GH-500 Preparation
- arranjqd271254.estate-blog.com, bookmarkshome.com, dillanecmw757107.vidublog.com, geilebookmarks.com, kingbookmark.com, philippvpu708998.bloggactivo.com, social-lyft.com, freedirectory4u.com, getsocialsource.com, jayvavk570296.buscawiki.com, Disposable vapes

2026 Latest DumpsKing GH-500 PDF Dumps and GH-500 Exam Engine Free Share: <https://drive.google.com/open?id=1n8w9IWYuXbmCIqw9Ve6FkqdcwREjkVj8>