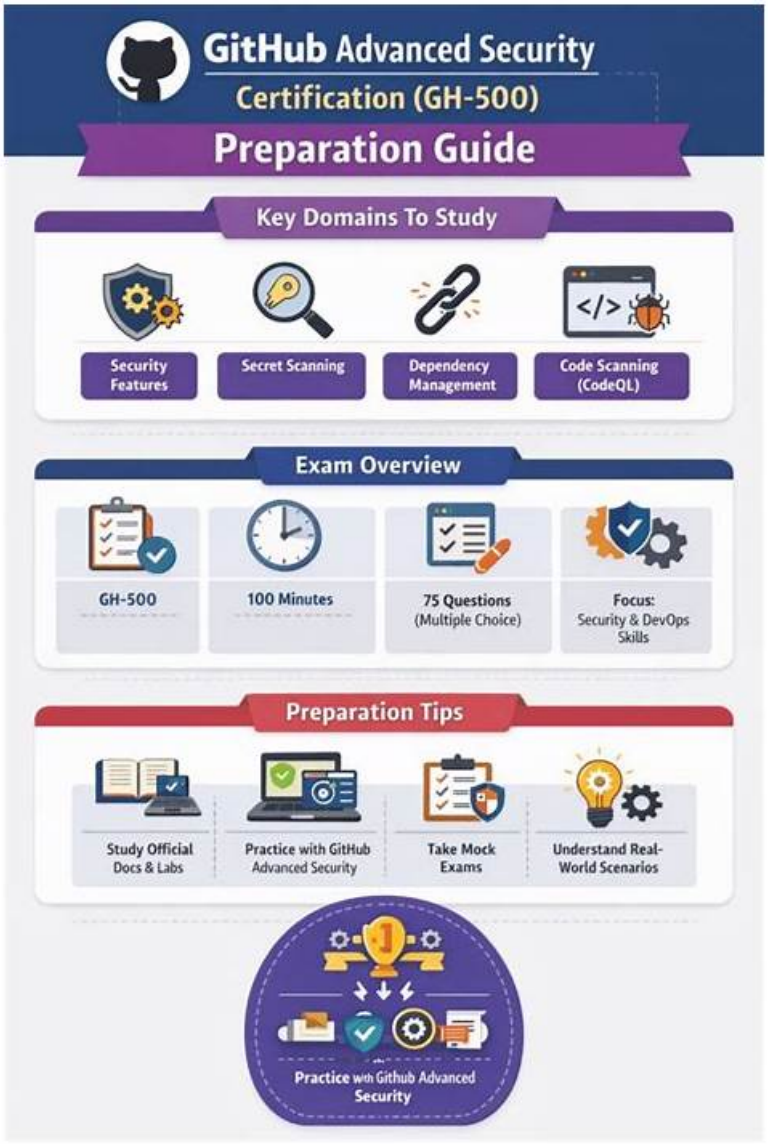
GH-500 Exam Prep | Reliable GH-500 Exam Sample



2026 Latest PassLeader GH-500 PDF Dumps and GH-500 Exam Engine Free Share: https://drive.google.com/open?id=1TATTkrqR4FNxxNYLlknCIpgzQX9pCCvt

Taking the GitHub Advanced Security GH-500 test and beginning GitHub Advanced Security GH-500 exam preparation with the suggested GH-500 exam preparation materials is the best and quickest course of action. You can rely on Microsoft GH-500 Exam Questio GitHub Advanced Security GH-500 for thorough GH-500 exam preparation.

As is known to us, people who want to take the GH-500 exam include different ages, different fields and so on. It is very important for company to design the GH-500 exam prep suitable for all people. However, our company has achieved the goal. We can promise that the GH-500 test questions from our company will be suitable all people. There are many functions about our study materials beyond your imagination. You can purchase our GH-500 reference guide according to your own tastes. We believe that the understanding of our GH-500 study materials will be very easy for you.

>> GH-500 Exam Prep <<

Quiz 2026 Microsoft - GH-500 - GitHub Advanced Security Exam Prep

The greatest product or service in the world comes from the talents in the organization. Talents have given life to work and have driven companies to move forward. Paying attention to talent development has become the core strategy for today's corporate

development. Perhaps you will need our GH-500 Learning Materials. No matter what your ability to improve, our GH-500 practice questions can meet your needs. And with our GH-500 exam questions, you will know you can be better.

Microsoft GH-500 Exam Syllabus Topics:

Topic	Details
Topic 1	• 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 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	• 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 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	• 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 (Q68-Q73):

NEW QUESTION # 68
Which of the following is the best way to prevent developers from adding secrets to the repository?

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

Answer: C

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 # 69
The autobuild step in the CodeQL workflow has failed. What should you do?

- A. Remove specific build steps.
- B. Compile the source code.
- C. Remove the autobuild step from your code scanning workflow and add specific build steps.
- D. Use CodeQL, which implicitly detects the supported languages in your code base.

Answer: C

Explanation:
If autobuild fails (which attempts to automatically detect how to build your project), you should disable it in your workflow and replace it with explicit build commands, using steps like run: make or run: ./gradlew build.
This ensures CodeQL can still extract and analyze the code correctly.

NEW QUESTION # 70
What role is required to change a repository's code scanning severity threshold that fails a pull request status check?

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

Answer: D

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 # 71
What is a prerequisite to define a custom pattern for a repository?

- A. Enable secret scanning
- B. Close other secret scanning alerts
- C. Specify additional match criteria
- D. Change the repository visibility to Internal

Answer: A

Explanation:
You must enable secret scanning before defining custom patterns. Secret scanning provides the foundational capability for detecting exposed credentials, and custom patterns build upon that by allowing organizations to specify their own regex-based patterns for secrets unique to their environment.
Without enabling secret scanning, GitHub will not process or apply custom patterns.

NEW QUESTION # 72
Which of the following information can be found in a repository's Security tab?

- A. Two-factor authentication (2FA) options
- B. Number of alerts per GHAS feature
- C. GHAS settings
- D. Access management

Answer: B

Explanation:
The Security tab in a GitHub repository provides a central location for viewing security-related information, especially when GitHub Advanced Security is enabled. The following can be accessed:
Number of alerts related to:
Code scanning
Secret scanning
Dependency (Dependabot) alerts
Summary and visibility into open, closed, and dismissed security issues.
It does not show 2FA options, access control settings, or configuration panels for GHAS itself. Those belong to account or organization-level settings.

NEW QUESTION # 73
.....

materials for free through { www.pdfvce.com } □GH-500 Latest Questions

- Microsoft GH-500 Questions: Fosters Your Exam Passing Skills [2026] □ Simply search for 《 GH-500 》 for free download on ▹ www.validtorrent.com ◃ □Online GH-500 Bootcamps
- GH-500 Dumps Free Download □ Latest GH-500 Material □ GH-500 Mock Test ✳ Immediately open ➡ www.pdfvce.com □□□ and search for ▸ GH-500 ◂ to obtain a free download ☮GH-500 Certification
- 100% Pass 2026 Microsoft Perfect GH-500 Exam Prep □ Open website ✔ www.troytecdumps.com □✔□ and search for □ GH-500 □ for free download □GH-500 Valid Dumps Questions
- GH-500 Trustworthy Pdf □ Latest GH-500 Material □ GH-500 Valid Dumps Questions □ Search for 《 GH-500 》 and download it for free immediately on ➠ www.pdfvce.com □ □Exam GH-500 Overview
- GH-500 Dumps Free Download □ Exam GH-500 Overview □ GH-500 Dumps Free Download □ Open website [www.exam4labs.com] and search for ⇛ GH-500 ⇚ for free download □GH-500 Free Exam Dumps
- myportal.utt.edu.tt, www.stes.tyc.edu.tw, www.valentinacolonna.it, www.stes.tyc.edu.tw, 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, myportal.utt.edu.tt, www.stes.tyc.edu.tw, 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, myportal.utt.edu.tt, www.stes.tyc.edu.tw, 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, Disposable vapes

DOWNLOAD the newest PassLeader GH-500 PDF dumps from Cloud Storage for free: https://drive.google.com/open?id=1TATTkrqR4FNxxNYLlknCIpgzQX9pCCvt