

# High-quality Latest GH-500 Dumps Pdf and Practical New GH-500 Exam Pass4sure & Effective GitHub Advanced Security Valid Exam Materials



What's more, part of that TestValid GH-500 dumps now are free: <https://drive.google.com/open?id=1rYoXUIHGYwXVLLhKwuIW4rvkEIAc4qTa>

Our GH-500 test guide is suitable for you whichever level you are in right now. Whether you are in entry-level position or experienced exam candidates who have tried the exam before, this is the perfect chance to give a shot. A growing number of exam candidates are choosing our GH-500 Exam Questions, why are you still hesitating? As long as you have make up your mind, our GitHub Advanced Security study question is available in five minutes, so just begin your review now! This could be a pinnacle in your life.

## Microsoft GH-500 Exam Syllabus Topics:

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

Topic 2	<ul style="list-style-type: none"> <li>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.</li> </ul>
Topic 3	<ul style="list-style-type: none"> <li>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.</li> </ul>
Topic 4	<ul style="list-style-type: none"> <li>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.</li> </ul>
Topic 5	<ul style="list-style-type: none"> <li>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.</li> </ul>

>> Latest GH-500 Dumps Pdf <<

## New GH-500 Exam Pass4sure - GH-500 Valid Exam Materials

TestValid has assembled a brief yet concise study material that will aid you in acing the GitHub Advanced Security (GH-500) exam on the first attempt. This prep material has been compiled under the expert guidance of 90,000 experienced Microsoft professionals from around the globe. TestValid offers the complete package that includes all exam questions conforming to the syllabus for passing the GitHub Advanced Security (GH-500) exam certificate in the first try.

## Microsoft GitHub Advanced Security Sample Questions (Q19-Q24):

### NEW QUESTION # 19

As a developer, you need to configure a code scanning workflow for a repository where GitHub Advanced Security is enabled. What minimum repository permission do you need?

- A. Write
- B. Admin
- C. None
- D. Read

**Answer: A**

Explanation:

To create or modify a code scanning workflow file (typically under `.github/workflows/codeql-analysis.yml`), you must have Write access to the repository.

Write permission allows you to commit the workflow file, which is required to run or configure code scanning using GitHub Actions.

### NEW QUESTION # 20

Why should you dismiss a code scanning alert?

- A. To prevent developers from introducing new problems
- B. If you fix the code that triggered the alert
- C. If there is a production error in your code
- D. If it includes an error in code that is used only for testing

**Answer: D**

Explanation:

You should dismiss a code scanning alert if the flagged code is not a true security concern, such as:

Code in test files

Code paths that are unreachable or safe by design

False positives from the scanner

Fixing the code would automatically resolve the alert - not dismiss it. Dismissing is for valid exceptions or noise reduction.

### NEW QUESTION # 21

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

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

**Answer: B**

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 # 22

In the pull request, how can developers avoid adding new dependencies with known vulnerabilities?

- A. Enable Dependabot alerts.
- B. Add a workflow with the dependency review action.
- C. Enable Dependabot security updates.
- D. Add Dependabot rules.

**Answer: B**

To detect and block vulnerable dependencies before merge, developers should use the [Dependency Review GitHub Action](#) in their pull request workflows. It scans all proposed dependency changes and flags any packages with known vulnerabilities. This is a preventative measure during development, unlike Dependabot, which reacts after the fact.

### What were the long-term impacts of the Cultural Revolution on Chinese society?

- Answer: C**

Requesting a CVE ID for a security advisory in a GitHub repository requires Admin permissions. This level of access is necessary because it involves managing sensitive security information and coordinating with external entities to assign a CVE, which is a formal process that can impact the public perception and security posture of the project.

• • • • •

**New GH-500 Exam Pass4sure:** <https://www.testvalid.com/GH-500-exam-collection.html>

- [illegible]

marcialfredo.blogofoto.com, www.stes.tyc.edu.tw, lms.ait.edu.za, 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, 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,  
Disposable vapes

BONUS!!! Download part of TestValid GH-500 dumps for free: <https://drive.google.com/open?id=1rYoXUIHGYwXVLLhKwuIW4rvkElAc4qTa>