Exam GH-500 Review - Quiz 2026 First-grade GH-500: Valid GitHub Advanced Security Test Voucher

2026 Latest Pass4guide GH-500 PDF Dumps and GH-500 Exam Engine Free Share: https://drive.google.com/open?id=1dyH7tNTUrWnigQ30_pWWSFBa6J2ptZjf

Elementary GH-500 practice materials as representatives in the line are enjoying high reputation in the market rather than some useless practice materials which cash in on your worries. We can relieve you of uptight mood and serve as a considerate and responsible company which never shirks responsibility. It is easy to get advancement by our GH-500 practice materials. On the cutting edge of this line for over ten years, we are trustworthy company you can really count on.

Microsoft GH-500 Exam Syllabus Topics:

Topic	Details
Topic 1	• 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	• 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 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 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 5	• 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.

Valid GH-500 Test Voucher, GH-500 Exam Pass4sure

The GitHub Advanced Security (GH-500) certification is a requirement if you want to succeed in the Microsoft industry quickly. But after deciding to take the GH-500 exam, the next challenge you face is the inability to find genuine GH-500 Questions for quick preparation. People who don't study with GH-500 real dumps fail the test and lose their precious resources.

Microsoft GitHub Advanced Security Sample Questions (Q123-Q128):

NEW QUESTION # 123
What is the first step you should take to fix an alert in secret scanning?

- A. Archive the repository.
- B. Revoke the alert if the secret is still valid.
- C. Remove the secret in a commit to the main branch.
- D. Update your dependencies.

Answer: B

Explanation:
Resolving alerts from secret scanning
After reviewing the details of a secret scanning alert, you should fix and then close the alert.
Fixing alerts
Once a secret has been committed to a repository, you should consider the secret compromised.
GitHub recommends the following actions for compromised secrets:
Verify that the secret committed to GitHub is valid.
Review and update any services that use the old token. For GitHub personal access tokens, delete the compromised token and create a new token.
Depending on the secret provider, check your security logs for any unauthorized activity.

NEW QUESTION # 124
Which CodeQL query suite provides queries of lower severity than the default query suite?

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

- C. github/codeql-go/ql/src@main

Answer: B

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 # 125
When using CodeQL, how does extraction for compiled languages work?

- A. By resolving dependencies to give an accurate representation of the codebase
- B. By generating one language at a time
- C. By monitoring the normal build process
- D. By running directly on the source code

Answer: C

Explanation:
For compiled languages, CodeQL performs extraction by monitoring the normal build process. This means it watches your usual build commands (like make, javac, or dotnet build) and extracts the relevant data from the actual build steps being executed.
CodeQL uses this information to construct a semantic database of the application.
This approach ensures that CodeQL captures a precise, real-world representation of the code and its behavior as it is compiled, including platform-specific configurations or conditional logic used during build.

NEW QUESTION # 126
Which of the following pre-defined roles is required to manage code scanning alerts in a repository?

- A. Triage
- B. Maintain
- C. Read
- D. View

Answer: C

Explanation:
Access requirements for security features
In this section, you can find the access required for security features, such as GitHub Advanced Security features.
Note: Repository roles for organizations
You can give organization members, outside collaborators, and teams of people different levels of access to repositories owned by an organization by assigning them to roles. Choose the role that best fits each person or team's function in your project without giving people more access to the project than they need.
From least access to most access, the roles for an organization repository are:
Read: Recommended for non-code contributors who want to view or discuss your project Triage: Recommended for contributors who need to proactively manage issues, discussions, and pull requests without write access Write: Recommended for contributors who actively push to your project Maintain: Recommended for project managers who need to manage the repository without access to sensitive or destructive actions Admin: Recommended for people who need full access to the project, including sensitive and destructive actions like managing security or deleting a repository

NEW QUESTION # 127
Which of the following is the best way to prevent developers from adding secrets to the repository?

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

Answer: D

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 # 128
.....

With a GH-500 certification, you can not only get a good position in many companies, but also make your financial free come true. Besides, you can have more opportunities and challenge that will make your life endless possibility. We promise you that GH-500 Actual Exam must be worth purchasing, and they can be your helper on your way to get success in gaining the GH-500 certificate. Come and you will be a winner!