Valid GH-500 Test Online | GH-500 Valid Exam Questions

What's more, part of that Itbraindumps GH-500 dumps now are free: https://drive.google.com/open?id=1pmDPbRNWpeiLJG1fAZU6iNci9SjZQ7qF

Do you want to earn the Microsoft GH-500 certification to land a well-paying job or a promotion? Prepare with GH-500 real exam questions to crack the test on the first try. We offer our GitHub Advanced Security (GH-500) Dumps in the form of a real GH-500 Questions PDF file, a web-based Microsoft GH-500 Practice Questions, and GH-500 desktop practice test software. Now you can clear the GitHub Advanced Security test in a short time without wasting time and money with actual GH-500 questions of Itbraindumps.

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 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	• 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.

GH-500 Valid Exam Questions, Latest GH-500 Exam Forum

You may be busy in your jobs, learning or family lives and can't get around to preparing and takes the certificate exams but on the other side you urgently need some useful GH-500 certificates to improve your abilities in some areas. So is there a solution which can kill two birds with one stone to both make you get the certificate and spend little time and energy to prepare for the exam? Our GH-500study materials provide a variety of functions to help the clients improve their learning. For example, the function to stimulate the exam helps the clients test their learning results of the GH-500 study materials in an environment which is highly similar to the real exam.

Microsoft GitHub Advanced Security Sample Questions (Q34-Q39):

NEW QUESTION # 34
What does a CodeQL database of your repository contain?

- A. A representation of all of the source code
- B. Build commands for C/C++, C#, and Java
- C. A build for Go projects to set up the project
- D. A build of the code and extracted data

Answer: D

Explanation:
GitHub
Agentic AI for AppSec Teams
Explanation:

Comprehensive and Detailed Explanation:
A CodeQL database contains a representation of your codebase, including the build of the code and extracted data. This database is used to run CodeQL queries to analyze your code for potential vulnerabilities and errors.
GitHub Docs

NEW QUESTION # 35
Assuming that notification and alert recipients are not customized, what does GitHub do when it identifies a vulnerable dependency in a repository where Dependabot alerts are enabled? (Each answer presents part of the solution. Choose two.)

- A. It notifies the repository administrators about the new alert.
- B. It generates a Dependabot alert and displays it on the Security tab for the repository.
- C. It consults with a security service and conducts a thorough vulnerability review.
- D. It generates Dependabot alerts by default for all private repositories.

Answer: A,B

Explanation:
Comprehensive and Detailed Explanation:
When GitHub identifies a vulnerable dependency in a repository with Dependabot alerts enabled, it performs the following actions:
Generates a Dependabot alert: The alert is displayed on the repository's Security tab, providing details about the vulnerability and affected dependency.
Notifies repository maintainers: By default, GitHub notifies users with write, maintain, or admin permissions about new Dependabot alerts.
GitHub Docs
These actions ensure that responsible parties are informed promptly to address the vulnerability.

NEW QUESTION # 36
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. All Activity
- B. Ignore
- C. Participating and @mentions
- 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 # 37
Which CodeQL query suite provides queries of lower severity than the default query suite?

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

Answer: C

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 # 38
A dependency has a known vulnerability. What does the warning message include?

- A. An easily understandable visualization of dependency change
- B. A brief description of the vulnerability
- C. The security impact of these changes
- D. How many projects use these components

Answer: B

Explanation:
When a vulnerability is detected, GitHub shows a warning that includes a brief description of the vulnerability. This typically covers the name of the CVE (if available), a short summary of the issue, severity level, and potential impact. The message also links to additional advisory data from the GitHub Advisory Database.
This helps developers understand the context and urgency of the vulnerability before applying the fix.

NEW QUESTION # 39
.....

Closed cars will not improve, and when we are reviewing our qualifying examinations, we should also pay attention to the overall layout of various qualifying examinations. For the convenience of users, our GH-500 learning materials will be timely updated information associated with the qualification of the home page, so users can reduce the time they spend on the Internet, blindly to find information. Our GH-500 Learning Materials get to the exam questions can help users in the first place, and what they care about the test information, can put more time in learning a new hot spot content.