GH-500 Practice Mock, Valid GH-500 Learning Materials

BTW, DOWNLOAD part of It-Tests GH-500 dumps from Cloud Storage: https://drive.google.com/open?id=1aV-rWLzTsrYEHQDPX06BP-j1CW5fCRZg

The Microsoft GH-500 practice questions come with three easy-to-use and install formats. The certification for the Microsoft GH-500 exam is a valuable, well-recognized professional credential. You can develop your skills and become a recognized specialist with the GitHub Advanced Security GH-500 Certification in addition to learning about new technology requirements.

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 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 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 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.

GH-500 Exam Practice Mock– Fantastic Valid GH-500 Learning Materials Pass Success

We are popular not only because our outstanding GH-500 practice dumps, but also for our well-praised after-sales service. After purchasing our GH-500 practice materials, the free updates will be sent to your mailbox for one year long if our experts make any of our GH-500 Guide materials. They are also easily understood by exam candidates.Our GH-500 actual exam can secedes you from tremendous materials with least time and quickest pace based on your own drive and practice to win.

Microsoft GitHub Advanced Security Sample Questions (Q37-Q42):

NEW QUESTION # 37
Which of the following is the most complete method for Dependabot to find vulnerabilities in third- party dependencies?

- A. The build tool finds the vulnerable dependencies and calls the Dependabot API.
- B. Dependabot reviews manifest files in the repository.
- C. CodeQL analyzes the code and raises vulnerabilities in third-party dependencies.
- D. A dependency graph is created, and Dependabot compares the graph to the GitHub Advisory database.

Answer: D

Explanation:
Security Alerts
Dependabot security alerts is a native GitHub service designed for the efficient management of vulnerable dependencies. It continuously scans the project's dependency graph, comparing it to the GitHub security advisory database. Upon detecting a vulnerable dependency version, it prompts developers with a security alert. Dependabot leverages the dependency graph to execute vulnerability scans. To generate this graph, it parses both manifest and lock files residing in the repository's default branch and constructs a comprehensive representation of the complete dependency tree.
Note: GitHub Advisory Database is one of the data sources that GitHub uses to identify vulnerable dependencies and malware. It's a free, curated database of security advisories for common package ecosystems on GitHub. It includes both data reported directly to GitHub from GitHub Security Advisories, as well as official feeds and community sources. This data is reviewed and curated by GitHub to ensure that false or unactionable information is not shared with the development community.

NEW QUESTION # 38
When code scanning is enabled, what is one default event that triggers a scan?

- A. Pushing a change.
- B. Deleting a branch.
- C. Creating a new branch.
- D. Merging a branch.

Answer: A

NEW QUESTION # 39
A secret scanning alert should be closed as "used in tests" when a secret is:

- A. In the readme.md file.
- B. Not a secret in the production environment.
- C. Solely used for tests.
- D. In a test file.

Answer: C

Explanation:
If a secret is intentionally used in a test environment and poses no real-world security risk, you may close the alert with the reason "used in tests". This helps reduce noise and clarify that the alert was reviewed and accepted as non-critical.
Just being in a test file isn't enough unless its purpose is purely for testing.

NEW QUESTION # 40
Which of the following formats are used to describe a Dependabot alert? Each answer presents a complete solution. (Choose two.)

- A. Vulnerability Exploitability eXchange (VEX)
- B. Common Weakness Enumeration (CWE)
- C. Common Vulnerabilities and Exposures (CVE)
- D. Exploit Prediction Scoring System (EPSS)

Answer: A,B

Explanation:
Dependabot alerts utilize standardized identifiers to describe vulnerabilities:
CVE (Common Vulnerabilities and Exposures):A widely recognized identifier for publicly known cybersecurity vulnerabilities.
CWE (Common Weakness Enumeration):A category system for software weaknesses and vulnerabilities.
These identifiers help developers understand the nature of the vulnerabilities and facilitate the search for more information or remediation strategies.
Note:
Dependabot alerts utilize standardized identifiers like Common Vulnerabilities and Exposures (CVE) identifiers and GitHub Advisory IDs to describe vulnerabilities within your project's dependencies. These identifiers help link the specific vulnerability to a standardized database entry, providing more context and details about the issue.
Publicly disclosed CWEs used by the Dismiss low impact issues for development-scoped dependencies rule Along with the ecosystem:npm and scope:development alert metadata, we use the following GitHub-curated Common Weakness Enumerations (CWEs) to filter out low impact alerts for the Dismiss low impact issues for development-scoped dependencies rule. We regularly improve this list and vulnerability patterns covered by built-in rules.
Resource Management Issues
CWE-400 Uncontrolled Resource Consumption
CWE-770 Allocation of Resources Without Limits or Throttling
Etc.
Incorrect:
[Not A] Dependabot alerts, combined with Vulnerability Exploitability eXchange (VEX), help users understand and manage vulnerabilities in their dependencies. Dependabot provides alerts when vulnerable dependencies are found, and VEX adds context about whether those vulnerabilities are actually exploitable in a specific environment.
VEX (Vulnerability Exploitability eXchange):
Purpose:

VEX provides a standardized way to communicate whether a vulnerability is actually exploitable in a specific context, like a particular product or environment.
Functionality:
VEX can be used to convey that a vulnerability doesn't pose a risk in a specific scenario, potentially due to specific configurations or mitigations.
Example:
If a product uses a vulnerable component, but that component is not reachable or has a mitigation in place, VEX can be used to communicate that the vulnerability is not exploitable.
[Not D]
Dependabot helps users focus on the most important alerts by including EPSS scores that indicate likelihood of exploitation, now generally available [February 2025] Dependabot alerts now feature the Exploit Prediction Scoring System (EPSS) from the global Forum of Incident Response and Security Teams (FIRST), helping you better assess vulnerability risks.
EPSS scores predict the likelihood of a vulnerability being exploited, with scores ranging from 0 to
1 (0 to 100%). Higher scores mean higher risk. We also show the EPSS score percentile, indicating how a vulnerability compares to others.
For example, a 90.534% EPSS score at the 95th percentile means:
90.534% chance of exploitation in the next 30 days
95% of other vulnerabilities are less likely to be exploited
You can use EPSS scores to help prioritize dependency vulnerabilities based on exploit likelihood.

NEW QUESTION # 41
Which of the following is the best way to dispose of a compromised secret?

- A. Remove the secret from the code base.
- B. Update any services that use the secret.
- C. Create a new secret.
- D. Revoke the secret.

Answer: D

Explanation:
Remediating a leaked secret in your repository
Revoke the secret
It is not sufficient to simply remove the secret from your codebase. The most important remediation step is revoking the secret with the secret's provider. By revoking the secret, you drastically reduce the potential for the secret to be exploited.
Note:
You should consider any leaked secret to be immediately compromised and it is essential that you undertake proper remediation steps, such as revoking the secret. Simply removing the secret from the codebase, pushing a new commit, or deleting and recreating the repository do not prevent the secret from being exploited.

NEW QUESTION # 42
.....

500 □ and obtain a free download on □ www.prepawayete.com □ □GH-500 Exam Cram Pdf

- Test GH-500 Registration □ Reliable GH-500 Exam Camp □ Exam GH-500 Actual Tests □ Go to website ➥ www.pdfvce.com □ open and search for □ GH-500 □ to download for free □Exam GH-500 Actual Tests
- Practice Microsoft GH-500 Exam Questions in Your Preferred Format with www.dumpsquestion.com □ Search on □ www.dumpsquestion.com □ for ➡ GH-500 □□□ to obtain exam materials for free download □Test GH-500 Centres
- Fast Download GH-500 Practice Mock - Leader in Qualification Exams - Reliable Valid GH-500 Learning Materials □ Search for □ GH-500 □ and download it for free on □ www.pdfvce.com □ website □Test GH-500 Centres
- Test GH-500 Centres □ Reliable GH-500 Practice Materials □ Test GH-500 Registration □ Enter （ www.pdfdumps.com ） and search for " GH-500 " to download for free □Test GH-500 Registration
- GH-500 Test Question □ GH-500 Braindumps Downloads □ Practice Test GH-500 Pdf □ Open ☀ www.pdfvce.com □☀□ enter { GH-500 } and obtain a free download □Exam GH-500 Actual Tests
- Test GH-500 Centres □ Hottest GH-500 Certification □ Reliable GH-500 Test Simulator □ Open ➠ www.vceengine.com □ and search for 「 GH-500 」 to download exam materials for free □Test GH-500 Centres
- www.stes.tyc.edu.tw, myportal.utt.edu.tt, ignouclasses.in, kel.zprcw.top, www.stes.tyc.edu.tw, www.stes.tyc.edu.tw, myportal.utt.edu.tt, Disposable vapes

BTW, DOWNLOAD part of It-Tests GH-500 dumps from Cloud Storage: https://drive.google.com/open?id=1aV-rWLzTsrYEHQDPX06BP-j1CW5fCRZg