GH-500 Test Simulates: GitHub Advanced Security & GH-500 Study Guide

BTW, DOWNLOAD part of Dumpcollection GH-500 dumps from Cloud Storage: https://drive.google.com/open?id=1QPEiCLkHBgaqPvFfwDcpxA3vDuWGPZLc

Dumpcollection has become the front-runner of this career and help exam candidates around the world win in valuable time. With years of experience dealing with GH-500 exam, they have thorough grasp of knowledge which appears clearly in our GH-500 exam questions. All GH-500 study materials you should know are written in them with three versions to choose from. In case there are any changes happened to the GH-500 Exam, the experts keep close eyes on trends of it and compile new updates constantly. It means we will provide the new updates freely for you later.

We put ourselves in your shoes and look at things from your point of view. About your problems with our GH-500 exam simulation, our considerate staff usually make prompt reply to your mails especially for those who dislike waiting for days. The sooner we can reply, the better for you to solve your doubts about GH-500 Training Materials. And we will give you the most professional suggestions on the GH-500 study guide.

>> Study GH-500 Materials <<

Renowned GH-500 Learning Quiz display the most useful Exam Brain Dumps - Dumpcollection

The Microsoft GH-500 certification exam always gives a tough time to their candidates. So you have to plan well and prepare yourself as per the recommended Microsoft GH-500 exam study material. For the quick and complete GH-500 exam preparation the Dumpcollection Microsoft GH-500 Practice Test questions are the ideal selection. With the Dumpcollection Microsoft GH-500 PDF Questions and practice test software, you will get everything that you need to learn, prepare and pass the difficult GH-500 exam with good scores.

Microsoft GH-500 Exam Syllabus Topics:

Topic	Details

Topic 1	• 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 2	• 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 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	• 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 5	• 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.

Microsoft GitHub Advanced Security Sample Questions (Q70-Q75):

NEW QUESTION # 70

When using CodeQL, what extension stores query suite definitions?

- A. .qls
- B. .yml
- C. .qll
- D. .ql

Answer: A

Explanation:
Query suite definitions in CodeQL are stored using the .qls file extension. A query suite defines a collection of queries to be run during an analysis and allows for grouping them based on categories like language, security relevance, or custom filters.
In contrast:
.ql files are individual queries.
.qll files are libraries used by .ql queries.
.yml is used for workflows, not query suites.

NEW QUESTION # 71
How would you build your code within the CodeQL analysis workflow? Each answer presents a complete solution. (Choose two.)

- A. Upload compiled binaries.
- B. Use CodeQL's autobuild action.
- C. Implement custom build steps.
- D. Use jobs.analyze.runs-on.
- E. Use CodeQL's init action.
- F. Ignore paths.

Answer: B,E

Explanation:
[B] Build Modes
The CodeQL Action supports different build modes for analyzing the source code. The available build modes are:
none: The database will be created without building the source code. Available for all interpreted languages and some compiled languages.
*-> autobuild: The database will be created by attempting to automatically build the source code.
Available for all compiled languages.
manual: The database will be created by building the source code using a manually specified build command. To use this build mode, specify manual build steps in your workflow between the init and analyze steps. Available for all compiled languages.
[D] Actions
This repository contains several actions that enable you to analyze code in your repository using CodeQL and upload the analysis to GitHub Code Scanning. Actions in this repository also allow you to upload to GitHub analyses generated by any SARIF-producing SAST tool.
Actions for CodeQL analyses:
*-> init: Sets up CodeQL for analysis.
analyze: Finalizes the CodeQL database, runs the analysis, and uploads the results to Code Scanning.

NEW QUESTION # 72
Which of the following formats are used to describe a code scanning alert from CodeQL?

- A. GitHub Security Advisory (GHSA)
- B. Vulnerability Exploitability eXchange (VEX)
- C. Common Vulnerabilities and Exposures (CVE)
- D. Common Weakness Enumeration (CWE)

Answer: D

Explanation:
Common Weakness Enumeration (CWE) is used by CodeQL to describe the vulnerabilities it detects in code scanning alerts. CodeQL's queries are designed to identify a wide range of weaknesses, and each security query is associated with one or more

specific CWEs, providing developers with standardized identifiers for the types of vulnerabilities found.
By associating alerts with CWEs, CodeQL provides a structured and informative approach to vulnerability management, making it easier for development teams to understand, address, and prevent security issues.
Note: The Common Weakness Enumeration (CWE) system is an industry-standard way of cataloging insecure software development patterns. CodeQL runs hundreds of queries out of the box that are able to detect an even greater number of CWEs. We went back through our existing queries, and aligned dozens of them with updated CWE IDs to give users better insight into the potential impact of a security issue when an alert is flagged up by code scanning.
Incorrect:
[Not B]
Vulnerability Exploitability eXchange (VEX) is not used by CodeQL; rather, CodeQL and VEX are complementary tools in software security: CodeQL identifies code vulnerabilities, while VEX communicates the exploitability of a vulnerability within a specific product context, helping users focus on relevant threats.
[Not C]
GitHub Advisories (GHSA) is a database of CVEs and GitHub-originated security advisories affecting the open source world. Advisories may or may not be documented in the National Vulnerability Database. Dependency-Track integrates with GHSA by mirroring advisories via GitHub's public GraphQL API.
[Not D]
CodeQL finds the vulnerability, and CVE provides the universally recognized identifier and description for that specific vulnerability, allowing for better communication and faster response within the cybersecurity community.
Common Vulnerabilities and Exposures (CVE) is a standardized dictionary that provides unique identifiers for publicly known cybersecurity weaknesses in software and hardware. Maintained by the MITRE Corporation and funded by the U.S. Department of Homeland Security, CVE ensures a common language for cybersecurity professionals to track, discuss, and address vulnerabilities effectively across the industry. Each CVE entry includes an identifier, a description, and references to publicly available information about the vulnerability.

NEW QUESTION # 73
A repository's dependency graph includes:

- A. a summary of the dependencies used in your organization's repositories.
- B. annotated code scanning alerts from your repository's dependencies.
- C. dependencies parsed from a repository's manifest and lock files.
- D. dependencies from all your repositories.

Answer: C

Explanation:
The dependency graph includes all the dependencies of a repository that are detailed in the manifest and lock files, or their equivalent, for supported ecosystems, as well as any dependencies that are submitted using the dependency submission API. This includes:
Direct dependencies, that are explicitly defined in a manifest or lock file or have been submitted using the dependency submission API.
Indirect dependencies of these direct dependencies, also known as transitive dependencies or sub-dependencies.

NEW QUESTION # 74
Which of the following secret scanning features can verify whether a secret is still active?

- A. custom patterns
- B. push protection
- C. validity checks
- D. branch protection

Answer: C

Explanation:
Performing validity checks
Validity checks help you prioritize alerts by telling you which secrets are active or inactive.

NEW QUESTION # 75
.....

We also update frequently to guarantee that the client can get more learning GH-500 exam resources and follow the trend of the times. So if you use our GH-500 study materials you will pass the test with high success probability. And our GH-500 learning guide is high-effective. If you study with our GH-500 practice engine for 20 to 30 hours, then you can pass the exam with confidence and achieve the certification as well.

GH-500 Authentic Exam Hub: https://www.dumpcollection.com/GH-500_braindumps.html

- GH-500 Quiz Torrent: GitHub Advanced Security - GH-500 Exam Guide - GH-500 Test Bootcamp □ ➡ www.pdfdumps.com □□□ is best website to obtain " GH-500 " for free download □GH-500 Valid Exam Forum
- Exam GH-500 Topics □ GH-500 Reliable Test Notes □ GH-500 Reliable Test Notes □ Go to website 《 www.pdfvce.com 》 open and search for □ GH-500 □ to download for free □Reliable GH-500 Exam Test
- GH-500 Reliable Test Guide □ GH-500 Authorized Certification □ GH-500 Reliable Test Guide □ Open [www.prep4away.com] and search for 【 GH-500 】 to download exam materials for free □GH-500 Authorized Certification
- Microsoft GH-500 Exam | Study GH-500 Materials - Offer you Valid GH-500 Authentic Exam Hub □ Easily obtain free download of " GH-500 " by searching on ▹ www.pdfvce.com ◃ □GH-500 Latest Exam Cost
- Microsoft GH-500 Exam | Study GH-500 Materials - Offer you Valid GH-500 Authentic Exam Hub □ { www.prep4sures.top } is best website to obtain □ GH-500 □ for free download □GH-500 Reliable Test Notes
- Exam GH-500 Format □ GH-500 Authorized Certification □ GH-500 Latest Test Question ↴ Search for { GH-500 } and download it for free on （ www.pdfvce.com ） website □Actual GH-500 Test Answers
- Microsoft GH-500 Exam | Study GH-500 Materials - Offer you Valid GH-500 Authentic Exam Hub □ Download [GH-500] for free by simply entering ➥ www.troytecdumps.com □ website □Valid GH-500 Test Camp
- 2026 Perfect 100% Free GH-500 – 100% Free Study Materials | GH-500 Authentic Exam Hub □ Go to website ⇛ www.pdfvce.com ⇚ open and search for 「 GH-500 」 to download for free □Exam GH-500 Topics
- High Pass-Rate Study GH-500 Materials offer you accurate Authentic Exam Hub | GitHub Advanced Security □ Open 「 www.examcollectionpass.com 」 and search for ✔ GH-500 □✔□ to download exam materials for free □GH-500 Latest Exam Cost
- Valid GH-500 Exam Sims □ GH-500 Latest Test Practice □ GH-500 Book Pdf □ Go to website { www.pdfvce.com } open and search for 「 GH-500 」 to download for free □GH-500 Reliable Test Guide
- GH-500 Study Demo □ Reliable GH-500 Exam Test □ GH-500 Study Demo □ Search for ➡ GH-500 □□□ and easily obtain a free download on 《 www.examcollectionpass.com 》 □Exam GH-500 Study Solutions
- total-bookmark.com, mysocialport.com, majayaee015329.nico-wiki.com, www.stes.tyc.edu.tw, hamzahqaar881152.plpwiki.com, honeygngh078684.blogars.com, matteopdvr972864.blogcudinti.com, lilyqred594078.blogdemls.com, wibki.com, elijahimsa932352.tdlwiki.com, Disposable vapes

What's more, part of that Dumpcollection GH-500 dumps now are free: https://drive.google.com/open?id=1QPEiCLkHBgaqPvFfwDcpxA3vDuWGPZLc