New Exam GH-500 Braindumps | GH-500 Latest Exam Vce

P.S. Free & New GH-500 dumps are available on Google Drive shared by Easy4Engine: https://drive.google.com/open?id=1aigdAbl33hfdhrwOlbwkGZVeuMcMC9nr

As job seekers looking for the turning point of their lives, it is widely known that the workers of recruitment is like choosing apples----viewing resumes is liking picking up apples, employers can decide whether candidates are qualified by the GH-500 appearances, or in other words, candidates' educational background and relating GH-500 professional skills. They develop the GH-500 exam guide targeted to real exam. The wide coverage of important knowledge points in our GH-500 latest braindumps would be greatly helpful for you to pass the exam.

It is known to us that getting the GH-500 certification is not easy for a lot of people, but we are glad to tell you good news. The GH-500 study materials from our company can help you get the certification in a short time. Now we are willing to introduce our GH-500 Practice Questions to you in detail, we hope that you can spare your valuable time to have a try on our products. Please believe that we will not let you down!

>> New Exam GH-500 Braindumps <<

Quiz Microsoft - GH-500 –Valid New Exam Braindumps

Do you know why you feel pressured to work? That is because your own ability and experience are temporarily unable to adapt to current job requirements. Our GH-500 exam questions can upgrade your skills and experience to the current requirements in order to have the opportunity to make the next breakthrough. Don't doubt about our GH-500 Study Guide! Just look at the warm feedbacks from our loyal customers, they all have became more successful in their career with the help of our GH-500 practice engine.

Microsoft GH-500 Exam Syllabus Topics:

Topic	Details
Topic 1	• 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 2	• 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 3	• 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 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	• 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.

Microsoft GitHub Advanced Security Sample Questions (Q69-Q74):

NEW QUESTION # 69
Who can fix a code scanning alert on a private repository?

- A. Users who have Read permissions within the repository
- B. Users who have Write access to the repository
- C. Users who have the security manager role within the repository
- D. Users who have the Triage role within the repository

Answer: B

Explanation:
Comprehensive and Detailed Explanation:
In private repositories, users with write access can fix code scanning alerts. They can do this by committing changes that address the

issues identified by the code scanning tools. This level of access ensures that only trusted contributors can modify the code to resolve potential security vulnerabilities.
GitHub Docs
Users with read or triage roles do not have the necessary permissions to make code changes, and the security manager role is primarily focused on managing security settings rather than directly modifying code.
Reference:
GitHub Docs

NEW QUESTION # 70
Which features require GitHub Advanced Security to be enabled for internal and private repositories in an organization? Each correct answer presents part of the solution. (Choose two.)

- A. secret scanning
- B. packages
- C. security policy
- D. dependency review

Answer: A,D

Explanation:
About GitHub Advanced Security products
GitHub has many features that help you improve and maintain the quality of your code. Some of these are included in all plans, such as dependency graph and Dependabot alerts.
Other security features require you to purchase one of GitHub's Advanced Security products:
GitHub Secret Protection, which includes features that help you detect and prevent secret leaks, such as secret scanning [B] and push protection.
GitHub Code Security, which includes features that help you find and fix vulnerabilities, like code scanning, premium Dependabot features, and dependency review [D].

NEW QUESTION # 71
You are configuring code scanning with CodeQL. What is one impact of using a language matrix in your workflow?

- A. CodeQL is configured to run analysis sequentially.
- B. You can use the languages parameter under the init action.
- C. CodeQL will only analyze the languages in the matrix.
- D. CodeQL excludes alerts for those dependencies specified in the language matrix.

Answer: C

Explanation:
If your workflow uses the language matrix, then CodeQL will only analyze the languages in the matrix.
Note:
The default CodeQL analysis workflow file created after configuring advanced setup for code scanning with CodeQL defines a matrix containing a property named language which lists the languages in your repository that will be analyzed. This matrix has been automatically pre- populated with supported languages detected in your repository. Using the language matrix allows CodeQL to run each language analysis in parallel and to customize analysis for each language. In an individual analysis, the name of the language from the matrix is provided to the init action as the argument for the languages input. We recommend that all workflows adopt this configuration.
Incorrect:
[Not A]
Using the language matrix allows CodeQL to run each language analysis in parallel.

NEW QUESTION # 72
Which of the following would raise secret scanning alerts?

- A. GitHub personal access token
- B. server-side request forgery

- C. cross site scripting (XSS)
- D. structured query language (SQL) injection

Answer: A

Explanation:
A secret scanning alert is raised when sensitive data, such as API keys, passwords, or access tokens, is detected in a code repository, often due to accidental inclusion by developers. The detection uses pattern-matching and entropy analysis to identify high-entropy strings that look like secrets, but can sometimes generate false positives from non-sensitive data like UUIDs. Alerts can also occur when a developer attempts to bypass the push protection feature that prevents secrets from being committed.

NEW QUESTION # 73
What YAML syntax do you use to exclude certain files from secret scanning?

- A. secret_scanning.yml
- B. decrypt_secret.sh
- C. branches-ignore:
- D. paths-ignore:

Answer: D

Explanation:
Excluding folders and files from secret scanning
You can customize secret scanning to automatically close alerts for secrets found in specific directories or files by configuring a secret_scanning.yml file in your repository.
Under Edit new file, type paths-ignore: followed by the paths you want to exclude from secret scanning. This tells secret scanning to automatically close alerts for everything in the docs directory.

NEW QUESTION # 74
.....

□ GH-500 □ and obtain a free download on [www.prepawaypdf.com] □Exam GH-500 Simulations

- albertdprq835681.bloggosite.com, thesocialroi.com, 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, hannakbbf802897.levitra-wiki.com, www.stes.tyc.edu.tw, larissajldd601367.wikiconverse.com, craigixhr883112.bleepblogs.com, dianepmhi522972.bimmwiki.com, 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, aronompw506217.ambien-blog.com, Disposable vapes

What's more, part of that Easy4Engine GH-500 dumps now are free: https://drive.google.com/open?id=1aigdAbl33hfdhrwOlbwkGZVeuMcMC9nr