GH-500 Practice Exams (Web-Based and Desktop) Software
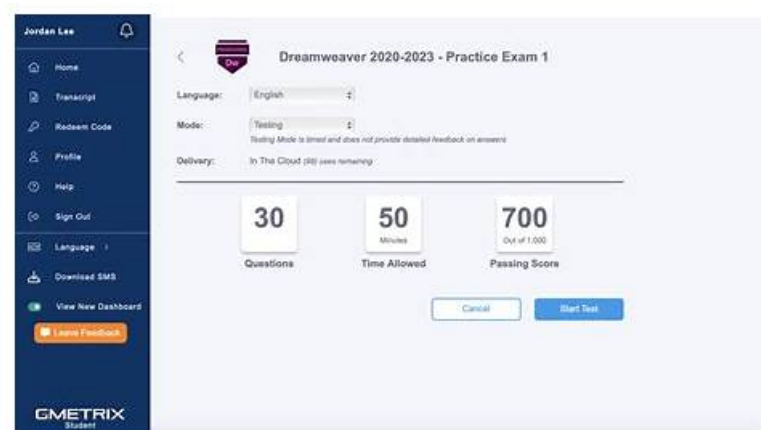

BONUS!!! Download part of Prep4sureExam GH-500 dumps for free: https://drive.google.com/open?id=1oSZgFnLXxaUJSm2l5VOjfWIZ8B3TFBnp

Nowadays passing the GH-500 test certification is extremely significant for you and can bring a lot of benefits to you. Passing the GH-500 test certification does not only prove that you are competent in some area but also can help you enter in the big company and double your wage. And our GH-500 Exam Questions are in good quality. As long as you study with our GH-500 learning guide, you will find that the content is easily to understand and the displays are enjoyable.

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	• 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 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.

Trustworthy Microsoft Test GH-500 Questions Answers With Interarctive Test Engine & Newest Exam GH-500 Success

No one lose interest during using our GH-500 actual exam and become regular customers eventually. With free demos to take reference, as well as bountiful knowledge to practice, even every page is carefully arranged by our experts, our GH-500 Exam Materials are successful with high efficiency and high quality to navigate you throughout the process. If you pay attention to using our GH-500 practice engine, thing will be solved easily.

Microsoft GitHub Advanced Security Sample Questions (Q72-Q77):

NEW QUESTION # 72
What is the purpose of the SECURITY.md file in a GitHub repository?

- A. readme.md
- B. contributing.md
- C. security.md
- D. support.md

Answer: C

Explanation:

The correct place to look is the SECURITY.md file. This file provides contributors and security researchers with instructions on how to responsibly report vulnerabilities. It may include contact methods, preferred communication channels (e.g., security team email), and disclosure guidelines.

This file is considered a GitHub best practice and, when present, activates a "Report a vulnerability" button in the repository's Security tab.

NEW QUESTION # 73

Which of the following workflow events would trigger a dependency review? (Each answer presents a complete solution. Choose two.)

- A. commit
- B. pull_request
- C. trigger
- D. workflow_dispatch

Answer: B,D

Explanation:
Comprehensive and Detailed Explanation:
Dependency review is triggered by specific events in GitHub workflows:
pull_request: When a pull request is opened, synchronized, or reopened, GitHub can analyze the changes in dependencies and provide a dependency review.
workflow_dispatch: This manual trigger allows users to initiate workflows, including those that perform dependency reviews.
The trigger and commit options are not recognized GitHub Actions events and would not initiate a dependency review.

NEW QUESTION # 74

What are Dependabot security updates?

- A. Automated pull requests that help you update dependencies that have known vulnerabilities
- B. Automated pull requests to update the manifest to the latest version of the dependency
- C. Compatibility scores to let you know whether updating a dependency could cause breaking changes to your project
- D. Automated pull requests that keep your dependencies updated, even when they don't have any vulnerabilities

Answer: A

Explanation:
Dependabot security updates are automated pull requests triggered when GitHub detects a vulnerability in a dependency listed in your manifest or lockfile. These PRs upgrade the dependency to the minimum safe version that fixes the vulnerability.
This is separate from regular updates (which keep versions current even if not vulnerable).

NEW QUESTION # 75

In a private repository, what minimum requirements does GitHub need to generate a dependency graph? (Each answer presents part of the solution. Choose two.)

- A. Write access to the dependency manifest and lock files for an enterprise
- B. Read-only access to the dependency manifest and lock files for a repository
- C. Dependency graph enabled at the organization level for all new private repositories
- D. Read-only access to all the repository's files

Answer: B,C

Explanation:
Comprehensive and Detailed Explanation:
To generate a dependency graph for a private repository, GitHub requires:
Dependency graph enabled: The repository must have the dependency graph feature enabled. This can be configured at the organization level to apply to all new private repositories.
Access to manifest and lock files: GitHub needs read-only access to the repository's dependency manifest and lock files (e.g., package.json, requirements.txt) to identify and map dependencies.

NEW QUESTION # 76

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

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

Answer: B,D

Explanation:
Comprehensive and Detailed Explanation:
When setting up CodeQL analysis for compiled languages, there are two primary methods to build your code:
GitHub Docs
Autobuild: CodeQL attempts to automatically build your codebase using the most likely build method. This is suitable for standard build processes.
GitHub Docs
Custom Build Steps: For complex or non-standard build processes, you can implement custom build steps by specifying explicit build commands in your workflow. This provides greater control over the build process.
GitHub Docs
The init action initializes the CodeQL analysis but does not build the code. The jobs.analyze.runs-on specifies the operating system for the runner but is not directly related to building the code. Uploading compiled binaries is not a method supported by CodeQL for analysis.

NEW QUESTION # 77

......

Maybe you have desired the GH-500 certification for a long time but don't have time or good methods to study. Maybe you always thought study was too boring for you. Our GH-500 study materials will change your mind. With our products, you will soon feel the happiness of study. Thanks to our diligent experts, wonderful study tools are invented for you to pass the GH-500 Exam. You can try the demos first and find that you just can't stop studying. Using our GH-500 study materials, you will just want to challenge yourself and get to know more.

- www.stes.tyc.edu.tw, www.stes.tyc.edu.tw, www.stes.tyc.edu.tw, myportal.utt.edu.tt, www.stes.tyc.edu.tw, lms.ait.edu.za, www.stes.tyc.edu.tw, www.wcs.edu.eu, careerxpand.com, Disposable vapes

2025 Latest Prep4sureExam GH-500 PDF Dumps and GH-500 Exam Engine Free Share: https://drive.google.com/open?id=1oSZgFnLXxaUJSm2l5VOjfWIZ8B3TFBnp