[2025-September-NewBraindump2go GH-500 Dumps PDF Free[Q1-Q31

2025/September Latest Braindump2go GH-500 Exam Dumps with PDF and VCE Free Updated Today! Following are some new Braindum2go GH-500 Exam Questions!Question: 1 ? [Configure and Use Code Scanning]After investigating a code scanning alert related to injection, you determine that the input is properly sanitized using custom logic. What should be your next step?A. Draft a pull request to update the open-source query.B. Ignore the alert.C. Open an issue in the CodeQL repository.D. Dismiss the alert with the reason "false positive."Answer: D Explanation:When you identify that a code scanning alert is a false positive?such as when your code uses a custom sanitization method not recognized by the analysis?you should dismiss the alert with the reason "false positive." This action helps improve the accuracy of future analyses and maintains the relevance of your security alerts. As per GitHub's documentation:"If you dismiss a CodeQL alert as a false positive result, for example because the code uses a sanitization library that isn't supported, consider contributing to the CodeQL repository and improving the analysis."By dismissing the alert appropriately, you ensure that your codebase's security alerts remain actionable and relevant.Question: 2 ? [Configure and Use Dependency Management]When does Dependabot alert you of a vulnerability in your software development process?A. When a pull request adding a vulnerable dependency is openedB. As soon as a vulnerable dependency is detectedC. As soon as a pull request is opened by a contributorD. When Dependabot opens a pull request to update a vulnerable dependencyAnswer: B Explanation:Dependabot alerts are generated as soon as GitHub detects a known vulnerability in one of your dependencies. GitHub does this by analyzing your repository's dependency graph and matching it against vulnerabilities listed in the GitHub Advisory Database. Once a match is found, the system raises an alert automatically without waiting for a PR or manual action.This allows organizations to proactively mitigate vulnerabilities as early as possible, based on real- time detection.Reference: GitHub Docs ? About Dependabot alerts; Managing alerts in GitHub DependabotQuestion: 3 ? [Configure and Use Dependency Management] Which of the following is the most complete method for Dependabot to find vulnerabilities in third- party dependencies?A. Dependabot reviews manifest files in the repositoryB. CodeQL analyzes the code and raises vulnerabilities in third-party dependenciesC. A dependency graph is created, and Dependabot compares the graph to the GitHub Advisory databaseD. The build tool finds the vulnerable dependencies and calls the Dependabot APIAnswer: C Explanation:Dependabot builds a dependency graph by analyzing package manifests and lockfiles in your repository. This graph includes both direct and transitive dependencies. It then compares this graph against the GitHub Advisory Database, which includes curated, security-reviewed advisories.This method provides a comprehensive and automated way to discover all known vulnerabilities across your dependency tree.Reference: GitHub Docs ? About the dependency graph; About Dependabot alertsQuestion: 4 ? [Describe the GHAS Security Features and Functionality] What is a security policy? A. An automatic detection of security vulnerabilities and coding errors in new or modified codeB. A security alert issued to a community in response to a vulnerabilityC. A file in a GitHub repository that provides instructions to users about how to report a security vulnerabilityD. An alert about dependencies that are known to contain security vulnerabilitiesAnswer: C Explanation:A security policy is defined by a SECURITY.md file in the root of your repository or .github/ directory. This file informs contributors and security researchers about how to responsibly report vulnerabilities. It improves your project's transparency and ensures timely communication and mitigation of any reported issues.Adding this file also enables a ?Report a vulnerability? button in the repository's Security tab. Reference: GitHub Docs ? Adding a security policy to your repositoryQuestion: 5 ? [Configure GitHub Advanced Security Tools in GitHub Enterprise]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. IgnoreB. Participating and @mentionsC. All ActivityD. Custom Answer: DExplanation: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.Reference: GitHub Docs ? Configuring notifications; Managing security alertsQuestion: 6 ? [Configure GitHub Advanced Security Tools in GitHub Enterprise]Which of the following Watch settings could you use to get Dependabot alert notifications? (Each answer presents part of the solution. Choose two.)A. The Custom settingB. The Participating and @mentions settingC. The All Activity settingD. The Ignore setting Answer: A, CExplanation:Comprehensive and Detailed Explanation:To receive Dependabot alert notifications for a repository, you can utilize the following Watch settings:Custom setting: Allows you to tailor your notifications, enabling you to subscribe specifically to security alerts, including those from Dependabot. All Activity setting: Subscribes you to all notifications for the repository, encompassing issues, pull requests, and security alerts like those from Dependabot.The Participating and @mentions setting limits notifications to conversations you're directly involved in or mentioned, which may not include security alerts. The Ignore setting unsubscribes you from all notifications, including critical

security alerts.GitHub Docs+1GitHub Docs+1Reference: GitHub Docs ? Configuring notifications; Managing security alertsQuestion: 7? [Configure and Use Dependency Management]Which Dependabot configuration fields are required? (Each answer presents part of the solution. Choose three.)A. directoryB. package-ecosystemC. milestoneD. schedule.intervalE. allowAnswer: A, B, D Explanation:Comprehensive and Detailed Explanation:When configuring Dependabot via the dependabot.yml file, the following fields are mandatory for each update configuration:directory: Specifies the location of the package manifest within the repository. This tells Dependabot where to look for dependency files.package-ecosystem: Indicates the type of package manager (e.g., npm, pip, maven) used in the specified directory.schedule.interval: Defines how frequently Dependabot checks for updates (e.g., daily, weekly). This ensures regular scanning for outdated or vulnerable dependencies.The milestone field is optional and used for associating pull requests with milestones. The allow field is also optional and used to specify which dependencies to update.GitLabReference: GitHub Docs ? Configuration options for dependency updatesQuestion: 8 ? [Configure and Use Code Scanning]What is required to trigger code scanning on a specified branch?A. The repository must be private.B. Secret scanning must be enabled on the repository.C. Developers must actively maintain the repository.D. The workflow file must exist in that branch. Answer: DExplanation:Comprehensive and Detailed Explanation:For code scanning to be triggered on a specific branch, the branch must contain the appropriate workflow file, typically located in the .github/workflows directory. This YAML file defines the code scanning configuration and specifies the events that trigger the scan (e.g., push, pull_request).Without the workflow file in the branch, GitHub Actions will not execute the code scanning process for that branch. The repository's visibility (private or public), the status of secret scanning, or the activity level of developers do not directly influence the triggering of code scanning.Reference: GitHub Docs ? About workflows; About code scanning alertsQuestion: 9 ? [Describe GitHub Advanced Security Best Practices]As a contributor, you discovered a vulnerability in a repository. Where should you look for the instructions on how to report the vulnerability?A. support.mdB. readme.mdC. contributing.mdD. security.mdAnswer: DExplanation: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.Reference: GitHub Docs ? Adding a security policy to your repositoryQuestion: 10 ? [Configure and Use Dependency Management]Assuming there is no custom Dependabot behavior configured, where possible, what does Dependabot do after sending an alert about a vulnerable dependency in a repository?A. Creates a pull request to upgrade the vulnerable dependency to the minimum possible secure versionB. Scans repositories for vulnerable dependencies on a schedule and adds those files to a manifestC. Constructs a graph of all the repository's dependencies and public dependents for the default branchD. Scans any push to all branches and generates an alert for each vulnerable repositoryAnswer: A Explanation:After generating an alert for a vulnerable dependency, Dependabot automatically attempts to create a pull request to upgrade that dependency to the minimum required secure version?if a fix is available and compatible with your project.This automated PR helps teams fix vulnerabilities quickly with minimal manual intervention. You can also configure update behaviors using dependabot.yml, but in the default state, PR creation is automatic.Reference: GitHub Docs ? About Dependabot alerts; About Dependabot security updatesQuestion: 11 ? [Configure and Use Secret Scanning]What is the first step you should take to fix an alert in secret scanning?A. Archive the repository.B. Update your dependencies.C. Revoke the alert if the secret is still valid.D. Remove the secret in a commit to the main branch.Answer: C Explanation:The first step when you receive a secret scanning alert is to revoke the secret if it is still valid. This ensures the secret can no longer be used maliciously. Only after revoking it should you proceed to remove it from the code history and apply other mitigation steps.Simply deleting the secret from the code does not remove the risk if it hasn't been revoked ? especially since it may already be exposed in commit history.Reference: GitHub Docs ? About secret scanning alerts; Remediating a secret scanning alertQuestion: 12 ? [Configure and Use Dependency Management]A dependency has a known vulnerability. What does the warning message include?A. The security impact of these changesB. An easily understandable visualization of dependency changeC. How many projects use these componentsD. A brief description of the vulnerabilityAnswer: D 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.Reference: GitHub Docs ? About Dependabot alerts; Reviewing and managing alertsQuestion: 13 ? [Configure and Use Dependency Management]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 generates a Dependabot alert and displays it on the Security tab for the repository.B. It notifies the repository administrators about

the new alert.C. It generates Dependabot alerts by default for all private repositories.D. It consults with a security service and conducts a thorough vulnerability review.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 DocsThese actions ensure that responsible parties are informed promptly to address the vulnerability. Reference: GitHub Docs ? About Dependabot alerts; Configuring notifications for Dependabot alerts Question: 14 ? [Configure and Use Secret Scanning]What do you need to do before you can define a custom pattern for a repository?A. Provide a regular expression for the format of your secret pattern.B. Add a secret scanning custom pattern.C. Enable secret scanning on the repository.D. Provide match requirements for the secret format. Stack OverflowAnswer: C Explanation:Comprehensive and Detailed Explanation:Before defining a custom pattern for secret scanning in a repository, you must enable secret scanning for that repository. Secret scanning must be active to utilize custom patterns, which allow you to define specific formats (using regular expressions) for secrets unique to your organization.Once secret scanning is enabled, you can add custom patterns to detect and prevent the exposure of sensitive information tailored to your needs.Reference: GitHub Docs ? Managing alerts from secret scanningQuestion: 15 ? [Configure and Use Dependency Management]Assuming that no custom Dependabot behavior is configured, who has the ability to merge a pull request created via Dependabot security updates?A. An enterprise administratorB. A user who has write access to the repositoryC. A user who has read access to the repositoryD. A repository member of an enterprise organizationAnswer: B Explanation:Comprehensive and Detailed Explanation:By default, users with write access to a repository have the ability to merge pull requests, including those created by Dependabot for security updates. This access level allows contributors to manage and integrate changes, ensuring that vulnerabilities are addressed promptly.Users with only read access cannot merge pull requests, and enterprise administrators do not automatically have merge rights unless they have write or higher permissions on the specific repository.Reference: GitHub Docs ? About Dependabot security updates; Configuring Dependabot security updatesQuestion: 16 ? [Configure and Use Code Scanning]Who can fix a code scanning alert on a private repository?A. Users who have the Triage role within the repositoryB. Users who have Read permissions within the repositoryC. Users who have Write access to the repositoryD. Users who have the security manager role within the repositoryAnswer: C 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 DocsUsers 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 ? Resolving code scanning alerts GitHub DocsQuestion: 17 ? [Describe the GHAS Security Features and Functionality]Which of the following information can be found in a repository's Security tab?A. Number of alerts per GHAS featureB. Two-factor authentication (2FA) optionsC. Access managementD. GHAS settingsAnswer: AExplanation:The Security tab in a GitHub repository provides a central location for viewing security-related information, especially when GitHub Advanced Security is enabled. The following can be accessed: Number of alerts related to: Code scanningSecret scanningDependency (Dependabot) alertsSummary and visibility into open, closed, and dismissed security issues.It does not show 2FA options, access control settings, or configuration panels for GHAS itself. Those belong to account or organization-level settings.Reference: GitHub Docs ? Managing security and analysis settings for your repositoryQuestion: 18 ? [Configure and Use Secret Scanning]How many alerts are created when two instances of the same secret value are in the same repository?A. 1B. 2C. 3D. 4Answer: A Explanation:When multiple instances of the same secret value appear in a repository, only one alert is generated. Secret scanning works by identifying exposed credentials and token patterns, and it groups identical matches into a single alert to reduce noise and avoid duplication.This makes triaging easier and helps teams focus on remediating the actual exposed credential rather than reviewing multiple redundant alerts.Reference: GitHub Docs ? About secret scanning alertsQuestion: 19 ? [Configure and Use Secret Scanning]What happens when you enable secret scanning on a private repository?A. Repository administrators can view Dependabot alerts.B. Your team is subscribed to security alerts.C. GitHub performs a read-only analysis on the repository.D. Dependency review, secret scanning, and code scanning are enabled.Answer: C Explanation:When secret scanning is enabled on a private repository, GitHub performs a read-only analysis of the repository's contents. This includes the entire Git history and files to identify strings that match known secret patterns or custom-defined patterns.GitHub does not alter the repository, and enabling secret scanning does not automatically enable code scanning or dependency review ? each must be configured separately.Reference: GitHub Docs ? Managing secret scanning for repositoriesQuestion: 20 ? [Configure and Use Dependency Management]You have enabled security updates for a repository.

When does GitHub mark a Dependabot alert as resolved for that repository?A. When Dependabot creates a pull request to update dependenciesB. When you dismiss the Dependabot alertC. When the pull request checks are successfulD. When you merge a pull request that contains a security updateAnswer: D Explanation:A Dependabot alert is marked as resolved only after the related pull request is merged into the repository. This indicates that the vulnerable dependency has been officially replaced with a secure version in the active codebase.Simply generating a PR or passing checks does not change the alert status; merging is the key step. Reference: GitHub Docs ? About Dependabot security updates; Managing Dependabot alertsQuestion: 21 ? [Use Code Scanning with CodeQL]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 init action.C. Ignore paths.D. Implement custom build steps.E. Use jobs.analyze.runs-on.F. Use CodeQL's autobuild action.Answer: D, FExplanation: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 DocsCustom 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.Reference: GitHub Docs ? CodeQL code scanning for compiled languagesQuestion: 22 ? [Configure and Use Dependency Management]Which of the following workflow events would trigger a dependency review? (Each answer presents a complete solution. Choose two.)A. pull_requestB. workflow_dispatchC. triggerD. commitAnswer: A, B 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.Reference: GitHub Docs ? Events that trigger workflowsQuestion: 23 ? [Configure and Use Dependency Management] You are a maintainer of a repository and Dependabot notifies you of a vulnerability. Where could the vulnerability have been disclosed? (Each answer presents part of the solution. Choose two.)A. In the National Vulnerability DatabaseB. In the dependency graphC. In security advisories reported on GitHubD. In manifest and lock filesAnswer: A, C Explanation: Comprehensive and Detailed Explanation:Dependabot alerts are generated based on data from various sources:National Vulnerability Database (NVD): A comprehensive repository of known vulnerabilities, which GitHub integrates into its advisory database.GitHub DocsSecurity Advisories Reported on GitHub: GitHub allows maintainers and security researchers to report and discuss vulnerabilities, which are then included in the advisory database.The dependency graph and manifest/lock files are tools used by GitHub to determine which dependencies are present in a repository but are not sources of vulnerability disclosures themselves.Reference: GitHub Docs ? About Dependabot alertsQuestion: 24 ? [Configure and Use Secret Scanning]Which of the following statements most accurately describes push protection for secret scanning custom patterns?A. Push protection must be enabled for all, or none, of a repository's custom patterns.B. Push protection is an opt-in experience for each custom pattern.C. Push protection is not available for custom patterns.D. Push protection is enabled by default for new custom patterns.Answer: B Explanation:Comprehensive and Detailed Explanation:Push protection for secret scanning custom patterns is an opt-in feature. This means that for each custom pattern defined in a repository, maintainers can choose to enable or disable push protectionindividually. This provides flexibility, allowing teams to enforce push protection on sensitive patterns while leaving it disabled for others. Reference: GitHub Docs ? Working with push protection from the command lineQuestion: 25 ? [Use Code Scanning with CodeQL]When using the advanced CodeQL code scanning setup, what is the name of the workflow file?A. codeql-config.ymlB. codeql-scan.ymlC. codeql-workflow.ymlD. codeql-analysis.ymlAnswer: D Explanation:Comprehensive and Detailed Explanation:In the advanced setup for CodeQL code scanning, GitHub generates a workflow file named codeql- analysis.yml. This file is located in the .github/workflows directory of your repository. It defines the configuration for the CodeQL analysis, including the languages to analyze, the events that trigger the analysis, and the steps to perform during the workflow.Reference: GitHub Docs ? Customizing your advanced setup for code scanningQuestion: 26 ? [Configure and Use Secret Scanning]Which of the following statements best describes secret scanning push protection?A. Commits that contain secrets are blocked before code is added to the repository.B. Secret scanning alerts must be closed before a branch can be merged into the repository.C. Buttons for sensitive actions in the GitHub UI are disabled.D. Users need to reply to a 2FA challenge before any push events.Answer: A Explanation: Comprehensive and Detailed Explanation:Secret scanning push protection is a proactive feature that scans for secrets in your code during the push process. If a secret is detected, the push is blocked, preventing the secret from being added to the repository. This

helps prevent accidental exposure of sensitive information.GitHub DocsReference: GitHub Docs ? About push protectionQuestion: 27 ? [Configure and Use Dependency Management]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. Read-only access to all the repository's filesB. Dependency graph enabled at the organization level for all new private repositoriesC. Write access to the dependency manifest and lock files for an enterpriseD. Read-only access to the dependency manifest and lock files for a repositoryAnswer: B, D 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.Reference: GitHub Docs ? About the dependency graphQuestion: 28 ? [Use Code Scanning with CodeQL]What does a CodeQL database of your repository contain?A. A build for Go projects to set up the projectB. A build of the code and extracted dataC. Build commands for C/C++, C#, and JavaD. A representation of all of the source code GitHubAgentic AI for AppSec Teams Answer: BExplanation: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 DocsReference: GitHub Docs ? Preparing your code for CodeQL analysisQuestion: 29 ? [Use Code Scanning with CodeQL]When using CodeQL, how does extraction for compiled languages work?A. By generating one language at a timeB. By resolving dependencies to give an accurate representation of the codebaseC. By monitoring the normal build processD. By running directly on the source codeAnswer: C Explanation:For compiled languages, CodeQL performs extraction by monitoring the normal build process. This means it watches your usual build commands (like make, javac, or dotnet build) and extracts the relevant data from the actual build steps being executed. CodeQL uses this information to construct a semantic database of the application.This approach ensures that CodeQL captures a precise, real-world representation of the code and its behavior as it is compiled, including platform-specific configurations or conditional logic used during build.Reference: GitHub Docs ? CodeQL for compiled languagesQuestion: 30 ? [Configure and Use Secret Scanning]Which of the following features helps to prioritize secret scanning alerts that present an immediate risk?A. Non-provider patternsB. Push protectionC. Custom pattern dry runsD. Secret validationAnswer: D Explanation:Secret validation checks whether a secret found in your repository is still valid and active with the issuing provider (e.g., AWS, GitHub, Stripe). If a secret is confirmed to be active, the alert is marked as verified, which means it's considered a high-priority issue because it presents an immediate security risk.This helps teams respond faster to valid, exploitable secrets rather than wasting time on expired or fake tokens.Reference: GitHub Docs ? Secret validation in secret scanningQuestion: 31 ? [Configure and Use Secret Scanning]What is a prerequisite to define a custom pattern for a repository?A. Change the repository visibility to InternalB. Close other secret scanning alertsC. Specify additional match criteriaD. Enable secret scanningAnswer: DExplanation:You must enable secret scanning before defining custom patterns. Secret scanning provides the foundational capability for detecting exposed credentials, and custom patterns build upon that by allowing organizations to specify their own regex-based patterns for secrets unique to their environment.Without enabling secret scanning, GitHub will not process or apply custom patterns. Reference: GitHub Docs ? Custom patterns in secret scanningResources From:1.2025 Latest Braindump2go GH-500 Exam Dumps (PDF & VCE) Free Share: **https://www.braindump2go.com/gh-500.html**2.2025 Latest Braindump2go GH-500 PDF and GH-500 VCE Dumps Free Share: **https://drive.google.com/drive/folders/1AgRBYd2fpHdgXfX5Txrzujlm3uL_8jLS?usp=sharing3.2025 Free Braindump2go GH-500 Exam Questions Download:https://www.braindump2go.com/free-online-pdf/GH-500-VCE-Dumps(1-31).pdfFree Resources from Braindump2go,We Devoted to Helping You 100% Pass All Exams!**