GH-500

GH-500 Exam

GitHub Advanced Security Exam

Version: 4.0

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

E xpl anati on:

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 opened

B. As soon as a vulnerable dependency is detected

C. As soon as a pull request is opened by a contributor

D. When Dependabot opens a pull request to update a vulnerable dependency

Answer: 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 Dependabot

Question: 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 repository

B. CodeQL analyzes the code and raises vulnerabilities in third-party dependencies

C. A dependency graph is created, and Dependabot compares the graph to the GitHub Advisory database

D. The build tool finds the vulnerable dependencies and calls the Dependabot API

Answer: 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 alerts

Question: 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 code

B. A security alert issued to a community in response to a vulnerability

C. A file in a GitHub repository that provides instructions to users about how to report a security vulnerability

D. An alert about dependencies that are known to contain security vulnerabilities

Answer: 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 repository

Question: 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. Ignore

B. Participating and @mentions

C. All Activity

D. Custom

Answer: D

Explanation:

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 alerts