GitHub.GitHub-Advanced-Security.v2026-03-16.q25

Exam Code:	GitHub-Advanced-Security
Exam Name:	GitHub Advanced Security GHAS Exam
Certification Provider:	GitHub
Free Question Number:	25
Version:	v2026-03-16
# of views:	113
# of Questions views:	250
https://www.dumpsdb.com/dumps/GitHub/GitHub-Advanced-Security/GitHub.GitHub-Advanced-Security.v2026-03-16.q25	

NEW QUESTION: 1
Secret scanning will scan:
A. A continuous integration system.
B. Any Git repository.
C. The GitHub repository.
D. External services.
Answer: C (LEAVE A REPLY)
Secret scanning is a feature provided by GitHub that scans the contents of your GitHub repositories for known types of secrets, such as API keys and tokens. It operates within the GitHub environment and does not scan external systems, services, or repositories outside of GitHub. Its primary function is to prevent the accidental exposure of sensitive information within your GitHub-hosted code.

NEW QUESTION: 2
What filter or sort settings can be used to prioritize the secret scanning alerts that present the most risk?
A. Sort to display the oldest first
B. Sort to display the newest first
C. Filter to display active secrets
D. Select only the custom patterns
Answer: C (LEAVE A REPLY)

The best way toprioritizesecret scanning alerts is tofilter by active secrets- these are secrets GitHub has confirmed are still valid and could be exploited. This allows security teams to focus on high-risk exposures that require immediate attention.
Sorting by time or filtering by custom patterns won't help with risk prioritization directly.

NEW QUESTION: 3
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: (SHOW ANSWER)
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.

NEW QUESTION: 4
Which CodeQL query suite provides queries of lower severity than the default query suite?
A. github/codeql-go/ql/src@main
B. github/codeql/cpp/ql/src@main
C. security-extended
Answer: C (LEAVE A REPLY)
Thesecurity-extendedquery suite includes additional CodeQL queries that detectlower severity issuesthan those in the default security-and-quality suite.
It's often used when projects want broader visibility into code hygiene and potential weak spots beyond critical vulnerabilities.
The other options listed arepaths to language packs, not query suites themselves.

NEW QUESTION: 5
Which of the following workflow events would trigger a dependency review? (Each answer presents a complete solution. Choose two.)
A. pull_request
B. workflow_dispatch
C. trigger
D. commit
Answer: (SHOW ANSWER)
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: 6
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: (SHOW ANSWER)
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.

NEW QUESTION: 7
Which of the following information can be found in a repository's Security tab?
A. Number of alerts per GHAS feature
B. Two-factor authentication (2FA) options
C. Access management
D. GHAS settings
Answer: (SHOW ANSWER)
TheSecurity tabin 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 ofalertsrelated to:
* Code scanning
* Secret scanning
* Dependency (Dependabot) alerts
* Summary and visibility into open, closed, and dismissed security issues.

It doesnotshow 2FA options, access control settings, or configuration panels for GHAS itself. Those belong to account or organization-level settings.

NEW QUESTION: 8
Which Dependabot configuration fields are required? (Each answer presents part of the solution. Choose three.)
A. directory
B. package-ecosystem
C. milestone
D. schedule.interval
E. allow
Answer: (SHOW ANSWER)
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 tellsDependabot 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.
GitLab

NEW QUESTION: 9
A repository's dependency graph includes:
A. Dependencies parsed from a repository's manifest and lock files.
B. Annotated code scanning alerts from your repository's dependencies.
C. A summary of the dependencies used in your organization's repositories.
D. Dependencies from all your repositories.
Answer: (SHOW ANSWER)
Thedependency graphin a repository is built byparsing manifest and lock files(like package.json, pom.xml, requirements.txt). It helps GitHub detect dependencies and cross-reference them with known vulnerability databases for alerting.
It is specific to each repository and does not show org-wide or cross-repo summaries.

NEW QUESTION: 10
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 (LEAVE A REPLY)
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.

NEW QUESTION: 11
Which of the following secret scanning features can verify whether a secret is still active?
A. Push protection
B. Validity checks
C. Branch protection
D. Custom patterns
Answer: B (LEAVE A REPLY)
Validity checks, also calledsecret validation, allow GitHub to check if a detected secret isstill active. If verified as live, the alert is marked as"valid", allowing security teams to prioritize the most critical leaks.
Push protectionblockssecrets but does not check their validity. Custom patterns are user-defined and do not include live checks.

NEW QUESTION: 12
Why should you dismiss a code scanning alert?
A. If you fix the code that triggered the alert
B. To prevent developers from introducing new problems
C. If it includes an error in code that is used only for testing
D. If there is a production error in your code
Answer: C (LEAVE A REPLY)
You shoulddismissa code scanning alert if the flagged code isnot a true security concern, such as:
* Code in test files
* Code paths that are unreachable or safe by design
* False positives from the scanner
Fixing the code would automaticallyresolvethe alert - not dismiss it. Dismissing is for valid exceptions or noise reduction.

NEW QUESTION: 13

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 Database

B. In the dependency graph

C. In security advisories reported on GitHub

D. In manifest and lock files

Answer: (SHOW ANSWER)

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 Docs

Security 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.

NEW QUESTION: 14

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: (SHOW ANSWER)

Using theCustomsetting 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.

NEW QUESTION: 15

Which of the following benefits do code scanning, secret scanning, and dependency review provide?

A. Confidentially report security vulnerabilities and privately discuss and fix security vulnerabilities in your repository's code

B. Search for potential security vulnerabilities, detect secrets, and show the full impact of changes to dependencies
C. Automatically raise pull requests, which reduces your exposure to older versions of dependencies
D. View alerts about dependencies that are known to contain security vulnerabilities
Answer: B (LEAVE A REPLY)
These three features provide a complete layer of defense:
* Code scanningidentifies security flaws in your source code
* Secret scanningdetects exposed credentials
* Dependency reviewshows the impact of package changes during a pull request
Together, they give developers actionable insight into risk and coverage throughout the SDLC.

NEW QUESTION: 16
As a repository owner, you do not want to run a GitHub Actions workflow when changes are made to any .txt or markdown files. How would you adjust the event trigger for a pull request that targets the main branch?
(Each answer presents part of the solution. Choose three.)
* on:
* pull_request:
* branches: [main]
A. - '/*.md'
B. - '/*.txt'
C. paths:
D. paths-ignore:
E. - 'docs/*.md'
Answer: (SHOW ANSWER)
Toexclude.txt and .md files from triggering workflows on pull requests to the main branch:
* on: defines the event (e.g., pull_request)
* pull_request: is the trigger
* paths-ignore: is the key used to ignore file patterns
Example YAML:
yaml
CopyEdit
on:
pull_request:
branches:
- main
paths-ignore:
- '*.md'
- '*.txt'

Using paths: would include only specific files instead - not exclude. paths-ignore: is correct here.

NEW QUESTION: 17
Where can you use CodeQL analysis for code scanning? (Each answer presents part of the solution. Choose two.)
A. In a third-party Git repository
B. In a workflow
C. In an external continuous integration (CI) system
D. In the Files changed tab of the pull request
Answer: (SHOW ANSWER)
* In a workflow: GitHub Actions workflows are the most common place for CodeQL code scanning.
The codeql-analysis.yml defines how the analysis runs and when it triggers.
* In an external CI system: GitHub allows you to run CodeQL analysis outside of GitHub Actions.
Once complete, the results can be uploaded using the upload-sarif action to make alerts visible in the repository.
You cannot run or trigger analysis from third-party repositories directly, and theFiles changed tabin pull requests only shows diff - not analysis results.

NEW QUESTION: 18
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 (LEAVE A REPLY)
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 Docs
These actions ensure that responsible parties are informed promptly to address the vulnerability.

NEW QUESTION: 19
You have enabled security updates for a repository. When does GitHub mark a Dependabot alert as resolved for that repository?
A. When you merge a pull request that contains a security update
B. When you dismiss the Dependabot alert
C. When the pull request checks are successful
D. When Dependabot creates a pull request to update dependencies
Answer: (SHOW ANSWER)
A Dependabot alert is marked asresolvedonly after the relatedpull request is mergedinto 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.

NEW QUESTION: 20
A secret scanning alert should be closed as "used in tests" when a secret is:
A. In the readme.md file.
B. In a test file.
C. Solely used for tests.
D. Not a secret in the production environment.
Answer: (SHOW ANSWER)
If a secret isintentionally used in a test environmentandposes no real-world security risk, you may close the alert with the reason"used in tests". This helps reduce noise and clarify that the alert was reviewed and accepted as non-critical.
Just being in a test file isn't enough unless itspurpose is purely for testing.

NEW QUESTION: 21
Which patterns are secret scanning validity checks available to?
A. High entropy strings
B. Custom patterns
C. Partner patterns

D. Push protection patterns

Answer: C (LEAVE A REPLY)

Validity checks- where GitHub verifies if a secret is still active - are available forpartner patternsonly.

These are secrets issued by GitHub's trusted partners (like AWS, Slack, etc.) and have APIs for GitHub to validate token activity status.

Custom patterns and high entropy patterns donotsupport automated validity checks.

NEW QUESTION: 22

Which security feature shows a vulnerable dependency in a pull request?

A. Dependency graph

B. Dependency review

C. Dependabot alert

D. The repository's Security tab

Answer: B (LEAVE A REPLY)

Dependency reviewruns as part of a pull request and showswhich dependencies are being added, removed, or changed- andhighlights vulnerabilitiesassociated with any added packages.

It works in real-time and is specifically designed for use during pull request workflows.

Thedependency graphis an overview,Dependabot alertsnotify post-merge, and theSecurity tabshows the aggregated alert list.

NEW QUESTION: 23

What does code scanning do?

A. It contacts maintainers to ask them to create security advisories if a vulnerability is found

B. It prevents code pushes with vulnerabilities as a pre-receive hook

C. It analyzes a GitHub repository to find security vulnerabilities

D. It scans your entire Git history on branches present in your GitHub repository for any secrets

Answer: C (LEAVE A REPLY)

Code scanningis a static analysis feature that examines your source code to identifysecurityvulnerabilities andcoding errors. It runs either on every push, pull request, or a scheduled time depending on the workflow configuration.

It doesnotautomatically contact maintainers, scan full Git history, or block pushes unless explicitly configured to do so.

NEW QUESTION: 24

What role is required to change a repository's code scanning severity threshold that fails a pull request status check?

A. Maintain

B. Write
C. Triage
D. Admin
Answer: (SHOW ANSWER)
To change the threshold that defines whether a pull request fails due to code scanning alerts (such as blocking merges based on severity), the user must haveAdminaccess on the repository. This is because modifying these settings falls under repository configuration privileges.
Users with Write, Maintain, or Triage roles do not have the required access to modify rulesets or status check policies.

NEW QUESTION: 25
Which of the following steps should you follow to integrate CodeQL into a third-party continuous integration system? (Each answer presents part of the solution. Choose three.)
A. Process alerts
B. Analyze code
C. Upload scan results
D. Install the CLI
E. Write queries
Answer: (SHOW ANSWER)
When integrating CodeQL outside of GitHub Actions (e.g., in Jenkins, CircleCI):
* Install the CLI: Needed to run CodeQL commands.
* Analyze code: Perform the CodeQL analysis on your project with the CLI.
* Upload scan results: Export the results in SARIF format and use GitHub's API to upload them to your repo's security tab.
You don't need to write custom queries unless extending functionality. "Processing alerts" happens after GitHub receives the results.