2026 GitHub-Advanced-Security Reliable Dumps Sheet - GitHub Advanced Security GHAS Exam Realistic Real Exam Answers Free PDF

DOWNLOAD the newest PassLeaderVCE GitHub-Advanced-Security PDF dumps from Cloud Storage for free: https://drive.google.com/open?id=1bCi4pz7xuwOYKc-uS1u5qMF2U8yuEpfR

To increase your chances of passing GitHub's certification, we offer multiple formats for braindumps for all GitHub-Advanced-Security exam at PassLeaderVCE. However, since not all takers have the same learning styles, we devise a customizable module to suite your needs. More importantly, our commitment to help you become GitHub-Advanced-Security Certified does not stop in buying our products. We offer customer support services that offer help whenever you'll be need one.

GitHub GitHub-Advanced-Security Exam Syllabus Topics:

Topic	Details
Topic 1	• Describe GitHub Advanced Security best practices: This section of the exam measures skills of a GitHub Administrator and covers outlining recommended strategies for adopting GitHub Advanced Security at scale. Test?takers will explain how to apply security policies, enforce branch protections, shift left security checks, and use metrics from GHAS tools to continuously improve an organization's security posture.
Topic 2	• Configure and use dependency management: This section of the exam measures skills of a DevSecOps Engineer and covers configuring dependency management workflows to identify and remediate vulnerable or outdated packages. Candidates will show how to enable Dependabot for version updates, review dependency alerts, and integrate these tools into automated CI • CD pipelines to maintain secure software supply chains.
Topic 3	• Describe the GHAS security features and functionality: This section of the exam measures skills of a GitHub Administrator and covers identifying and explaining the built?in security capabilities that GitHub Advanced Security provides. Candidates should be able to articulate how features such as code scanning, secret scanning, and dependency management integrate into GitHub repositories and workflows to enhance overall code safety.

Topic 4	• Use code scanning with CodeQL: This section of the exam measures skills of a DevSecOps Engineer and covers working with CodeQL to write or customize queries for deeper semantic analysis. Candidates should demonstrate how to configure CodeQL workflows, understand query suites, and interpret CodeQL alerts to uncover complex code issues beyond standard static analysis.

GitHub-Advanced-Security Real Exam Answers - GitHub-Advanced-Security Certification Training

Our GitHub-Advanced-Security practice questions enjoy great popularity in this line. We provide our GitHub-Advanced-Security exam braindumps on the superior quality and being confident that they will help you expand your horizon of knowledge of the exam. They are time-tested GitHub-Advanced-Security Learning Materials, so they are classic. As well as our after-sales services. And we can always give you the most professional services on our GitHub-Advanced-Security training guide.

GitHub Advanced Security GHAS Exam Sample Questions (Q25-Q30):

NEW QUESTION # 25
What YAML syntax do you use to exclude certain files from secret scanning?

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

Answer: A

Explanation:
To exclude specific files or directories from being scanned by secret scanning in GitHub Actions, you can use thepaths-ignore:key within your YAML workflow file.
This tells GitHub toignore specified pathswhen scanning for secrets, which can be useful for excluding test data or non-sensitive mock content.
Other options listed are invalid:
* branches-ignore: excludes branches, not files.
* decrypt_secret.sh is not a YAML key.
* secret scanning.yml is not a recognized filename for configuration.

NEW QUESTION # 26
Which of the following formats are used to describe a Dependabot alert? (Each answer presents a complete solution. Choose two.)

- A. Common Weakness Enumeration (CWE)
- B. Exploit Prediction Scoring System (EPSS)
- C. Common Vulnerabilities and Exposures (CVE)
- D. Vulnerability Exploitability exchange (VEX)

Answer: A,C

Explanation:
Dependabot alerts utilize standardized identifiers to describe vulnerabilities:
* CVE (Common Vulnerabilities and Exposures):A widely recognized identifier for publicly known cybersecurity vulnerabilities.
* CWE (Common Weakness Enumeration):A category system for software weaknesses and vulnerabilities.
These identifiers help developers understand the nature of the vulnerabilities and facilitate the search for more information or remediation strategies.

NEW QUESTION # 27

Which of the following options are code scanning application programming interface (API) endpoints? (Each answer presents part of the solution. Choose two.)

- A. Delete all open code scanning alerts
- B. Get a single code scanning alert
- C. List all open code scanning alerts for the default branch
- D. Modify the severity of an open code scanning alert

Answer: B,C

Explanation:
The GitHub Code Scanning API includes endpoints that allow you to:
* List alertsfor a repository (filtered by branch, state, or tool) - useful for monitoring security over time.
* Get a single alertby its ID to inspect its metadata, status, and locations in the code.
However, GitHub doesnotsupport modifying the severity of alerts via API - severity is defined by the scanning tool (e.g., CodeQL).
Likewise, alertscannot be deletedvia the API; they are resolved by fixing the code or dismissing them manually.

NEW QUESTION # 28
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 consults with a security service and conducts a thorough vulnerability review.
- C. It generates Dependabot alerts by default for all private repositories.
- D. It notifies the repository administrators about the new alert.

Answer: A,D

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 Docs
These actions ensure that responsible parties are informed promptly to address the vulnerability.

NEW QUESTION # 29
When using CodeQL, what extension stores query suite definitions?

- A. .qls
- B. .ql
- C. .yml
- D. .qll

Answer: A

Explanation:
Query suite definitions in CodeQL are stored using the .qls file extension. A query suite defines a collection of queries to be run during an analysis and allows for grouping them based on categories like language, security relevance, or custom filters.
In contrast:
* .ql files are individual queries.
* .qll files are libraries used by .ql queries.
* .yml is used for workflows, not query suites.

NEW QUESTION # 30
.....

Most people are nervous and anxious to take part in the GitHub-Advanced-Security exam for the first time. Then it is easy for them to make mistakes. So it is important to get familiar with the real test environment. Also, the real test environment of the GitHub-Advanced-Security Study Materials can help you control time. After all, you must submit your practice in limited time in GitHub-Advanced-Security practice materials. Trust in our GitHub-Advanced-Security training guide, and you will get success for sure.

GitHub-Advanced-Security Real Exam Answers: https://www.passleadervce.com/GitHub-Certification/reliable-GitHub-Advanced-Security-exam-learning-guide.html

DOWNLOAD the newest PassLeaderVCE GitHub-Advanced-Security PDF dumps from Cloud Storage for free: https://drive.google.com/open?id=1bCi4pz7xuwOYKc-uS1u5qMF2U8yuEpfR