

Free PDF 2026 GitHub Useful GitHub-Advanced-Security Latest Exam Pdf



DOWNLOAD the newest ActualVCE GitHub-Advanced-Security PDF dumps from Cloud Storage for free:
<https://drive.google.com/open?id=1fo61LP9z2yxikhf-LIBPZ5S0TmbSSGHL>

They work closely and check all GitHub GitHub-Advanced-Security PDF questions one by one and they ensure the best possible answers to GitHub GitHub-Advanced-Security exam dumps. So you can trust the GitHub-Advanced-Security practice test and start this journey with complete peace of mind and satisfaction. The GitHub Advanced Security GHAS Exam (GitHub-Advanced-Security) exam PDF questions will not assist you in GitHub Advanced Security GHAS Exam (GitHub-Advanced-Security) exam preparation but also provide you with in-depth knowledge about the GitHub Advanced Security GHAS Exam (GitHub-Advanced-Security) exam topics. This knowledge will be helpful to you in your professional life. So GitHub Advanced Security GHAS Exam (GitHub-Advanced-Security) exam questions are the ideal study material for quick GitHub GitHub-Advanced-Security exam preparation.

GitHub GitHub-Advanced-Security Exam Syllabus Topics:

Topic	Details
Topic 1	<ul style="list-style-type: none">• 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.
Topic 2	<ul style="list-style-type: none">• Configure GitHub Advanced Security tools in GitHub Enterprise: This section of the exam measures skills of a GitHub Administrator and covers integrating GHAS features into GitHub Enterprise Server or Cloud environments. Examinees must know how to enable advanced security at the enterprise level, manage licensing, and ensure that scanning and alerting services operate correctly across multiple repositories and organizational units.

Topic 3	<ul style="list-style-type: none"> • 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of a DevSecOps Engineer and covers configuring dependency management workflows to identify and remediate vulnerable or outdated packages.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 4	<ul style="list-style-type: none"> • 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 5	<ul style="list-style-type: none"> • 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.

>> **GitHub-Advanced-Security Latest Exam Pdf** <<

GitHub-Advanced-Security Practice Mock | GitHub-Advanced-Security New Dumps Book

All questions on our GitHub-Advanced-Security exam questions are strictly in accordance with the knowledge points on newest test syllabus. Also, our experts are capable of predicating the difficult knowledge parts of the GitHub-Advanced-Security exam according to the test syllabus. We have tried our best to simply the difficult questions of our GitHub-Advanced-Security Practice Engine to be understood by the customers all over the world. No matter the students, office staffs, even someone who know nothing about this subject can totally study it without difficulty.

GitHub Advanced Security GHAS Exam Sample Questions (Q17-Q22):

NEW QUESTION # 17

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

- **A. Dependency review**
- B. Dependency graph
- C. Dependabot alert
- D. The repository's Security tab

Answer: A

Explanation:

Dependency review runs as part of a pull request and shows which dependencies are being added, removed, or changed and highlights vulnerabilities associated with any added packages.

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

The dependency graph is an overview, Dependabot alerts notify post-merge, and the Security tab shows the aggregated alert list.

NEW QUESTION # 18

What kind of repository permissions do you need to request a Common Vulnerabilities and Exposures (CVE) identification number for a security advisory?

- A. Maintain
- B. Triage
- C. Write
- **D. Admin**

Answer: D

Explanation:

Requesting a CVE ID for a security advisory in a GitHub repository requires Admin permissions. This level of access is necessary because it involves managing sensitive security information and coordinating with external entities to assign a CVE, which is a formal process that can impact the public perception and security posture of the project.

NEW QUESTION # 19

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. Users need to reply to a 2FA challenge before any push events.
- C. Buttons for sensitive actions in the GitHub UI are disabled.
- D. Secret scanning alerts must be closed before a branch can be merged into the repository.

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 Docs

NEW QUESTION # 20

What do you need to do before you can define a custom pattern for a repository?

- A. Add a secret scanning custom pattern.
- B. Provide a regular expression for the format of your secret pattern.
- **C. Enable secret scanning on the repository.**
- D. Provide match requirements for the secret format. Stack Overflow

Answer: 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.

NEW QUESTION # 21

As a developer with write access, you navigate to a code scanning alert in your repository. When will GitHub close this alert?

- **A. After you fix the code by committing within the pull request**
- B. After you find the code and click the alert within the pull request
- C. When you use data-flow analysis to find potential security issues in code
- D. After you triage the pull request containing the alert

Answer: A

Explanation:

GitHub automatically closes a code scanning alert when the vulnerable code is fixed in the same branch where the alert was generated, usually via a commit inside a pull request. Simply clicking or triaging an alert does not resolve it. The alert is re-evaluated after each push to the branch, and if the issue no longer exists, it is marked as resolved.

NEW QUESTION # 22

There is no doubt that advanced technologies are playing an important role in boosting the growth of GitHub companies. This is the reason why the employees have now started upgrading their skillset with the GitHub Advanced Security GHAS Exam (GitHub-Advanced-Security) certification exam because they want to work with those latest applications and save their jobs. They attempt the GitHub Advanced Security GHAS Exam (GitHub-Advanced-Security) exam to validate their skills and try to get their dream job.

[illegible]

P.S. Free 2025 GitHub GitHub-Advanced-Security dumps are available on Google Drive shared by ActualVCE: <https://drive.google.com/open?id=1fo61LP9z2yxikhfLBPZ5S0TmbSSGHL>