

New GitHub-Advanced-Security Exam Cram - GitHub-Advanced-Security Test Topics Pdf



DOWNLOAD the newest Actual4Exams GitHub-Advanced-Security PDF dumps from Cloud Storage for free:
<https://drive.google.com/open?id=1lr6gLbMniiGnZEFoxFNywdxwaE0BmpFd>

With GitHub-Advanced-Security actual exam engine you will experience an evolution of products coupled with the experience and qualities of expertise. All the questions of GitHub-Advanced-Security free pdf are checked chosen by several times of refining and verification, and all the GitHub-Advanced-Security answers are correct and easy to understand. You can experience yourself a new dawn of technology with GitHub-Advanced-Security exam torrent. We guarantee you 100% pass. If you are still worried, you can read our refund policy. In case of failure, full refund.

GitHub Advanced Security GHAS Exam Practice exams of Actual4Exams i.e. desktop software and web-based are customizable and you can attempt them for multiple times. These practice exam save progress report of each attempt so you can assess it to find and overcome mistakes. As mentioned earlier, these GitHub Advanced Security GHAS Exam (GitHub-Advanced-Security) practice exams can be customized according to your requirements. You can change their time and numbers of GitHub Advanced Security GHAS Exam (GitHub-Advanced-Security) dumps questions as you want.

>> New GitHub-Advanced-Security Exam Cram <<

Well-Structured GitHub GitHub-Advanced-Security PDF Dumps

Are you still worried that you haven't found GitHub-Advanced-Security test dumps and review information? People around the world are likely to choose GitHub-Advanced-Security certification exam. Actual4Exams is the only learning website that can provide better GitHub-Advanced-Security Certification Training materials. If you are still worried, you can download GitHub-Advanced-Security free demo before purchasing our Actual4Exams GitHub-Advanced-Security certification training materials.

GitHub GitHub-Advanced-Security Exam Syllabus Topics:

Topic	Details
Topic 1	<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 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 secret scanning: This section of the exam measures skills of a DevSecOps Engineer and covers setting up and managing secret scanning in organizations and repositories. Test-takers must demonstrate how to enable secret scanning, interpret the alerts generated when sensitive data is exposed, and implement policies to prevent and remediate credential leaks.

GitHub Advanced Security GHAS Exam Sample Questions (Q53-Q58):

NEW QUESTION # 53

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

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

Answer: C,D

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 # 54

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. Participating and @mentions
- B. Ignore
- 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.

NEW QUESTION # 55

When using CodeQL, how does extraction for compiled languages work?

- A. By resolving dependencies to give an accurate representation of the codebase
- B. By running directly on the source code
- C. By monitoring the normal build process
- D. By generating one language at a time

Answer: 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.

NEW QUESTION # 56

Which details do you have to provide to create a custom pattern for secret scanning? (Each answer presents part of the solution. Choose two.)

- A. A list of repositories to scan
- B. The name of the pattern
- C. The secret format
- D. Additional match requirements for the secret format

Answer: B,C

Explanation:

When defining a custom pattern for secret scanning, two key fields are required:

* Name of the pattern: A unique label to identify the pattern

* Secret format: A regular expression that defines what the secret looks like (e.g., token format) You can optionally specify additional match requirements (like required context keywords), but they're not mandatory. Listing repositories is also not part of the required fields during pattern creation.

NEW QUESTION # 57

Which of the following is the most complete method for Dependabot to find vulnerabilities in third-party dependencies?

- A. CodeQL analyzes the code and raises vulnerabilities in third-party dependencies
- B. The build tool finds the vulnerable dependencies and calls the Dependabot API
- C. A dependency graph is created, and Dependabot compares the graph to the GitHub Advisory database
- D. Dependabot reviews manifest files in the repository

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.

NEW QUESTION # 58

.....

If you're still learning from the traditional old ways and silently waiting for the test to come, you should be awake and ready to take the exam in a different way. Study our GitHub-Advanced-Security study materials to write "test data" is the most suitable for your choice, after recent years show that the effect of our GitHub-Advanced-Security Study Materials has become a secret weapon of the examinee through qualification examination, a lot of the users of our GitHub-Advanced-Security study materials can get unexpected results in the examination.

GitHub-Advanced-Security Test Topics Pdf: <https://www.actual4exams.com/GitHub-Advanced-Security-valid-dump.html>

- GitHub-Advanced-Security Valid Guide Files □ GitHub-Advanced-Security Brain Dumps □ GitHub-Advanced-Security Latest Exam Cost □ Search for ▷ GitHub-Advanced-Security ↵ and easily obtain a free download on □ www.examcollectionpass.com □ □ GitHub-Advanced-Security Valid Test Preparation
- Free PDF GitHub - GitHub-Advanced-Security Useful New Exam Cram □ Open website ➔ www.pdfvce.com □ and search for { GitHub-Advanced-Security } for free download □ GitHub-Advanced-Security Brain Dumps
- GitHub-Advanced-Security Brain Dumps □ Exam GitHub-Advanced-Security Voucher □ Exam GitHub-Advanced-

Security Voucher Easily obtain free download of { GitHub-Advanced-Security } by searching on { www.dumpsmaterials.com } GitHub-Advanced-Security Latest Exam Cost

BTW, DOWNLOAD part of Actual4Exams GitHub-Advanced-Security dumps from Cloud Storage:

<https://drive.google.com/open?id=1lr6gLbMniiGnZEFoxFNywdxwaE0BmpFd>