

# Updated GitHub-Advanced-Security Download Free Dumps & Trustable Dump GitHub-Advanced-Security Collection & Hot GitHub GitHub Advanced Security GHAS Exam



What's more, part of that PDFDumps GitHub-Advanced-Security dumps now are free: [https://drive.google.com/open?id=1f0Xgk43ObCCtU4iI46tRxVLvs\\_0TCjCC](https://drive.google.com/open?id=1f0Xgk43ObCCtU4iI46tRxVLvs_0TCjCC)

There are totally three versions of GitHub-Advanced-Security practice materials which are the most suitable versions for you: PDF, software and app versions. We promise ourselves and exam candidates to make these GitHub-Advanced-Security preparation prep top notch. So if you are in a dark space, our GitHub-Advanced-Security Study Guide can inspire you make great improvements. With the high pass rate of our GitHub-Advanced-Security learning engine as 98% to 100%, you can be confident and ready to pass the exam easily.

## GitHub GitHub-Advanced-Security Exam Syllabus Topics:

Topic	Details
Topic 1	<ul style="list-style-type: none"><li>• 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.</li></ul>
Topic 2	<ul style="list-style-type: none"><li>• Configure and use code scanning: This section of the exam measures skills of a DevSecOps Engineer and covers enabling and customizing GitHub code scanning with built-in or marketplace rulesets. Examinees must know how to interpret scan results, triage findings, and configure exclusion or override settings to reduce noise and focus on high-priority vulnerabilities.</li></ul>
Topic 3	<ul style="list-style-type: none"><li>• 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of a DevSecOps Engineer and covers configuring dependency management workflows to identify and remediate vulnerable or outdated packages.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</li><li>• CD pipelines to maintain secure software supply chains.</li></ul>
Topic 4	<ul style="list-style-type: none"><li>• 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.</li></ul>

Topic 5	<ul style="list-style-type: none"> <li>• 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.</li> </ul>
Topic 6	<ul style="list-style-type: none"> <li>• 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.</li> </ul>

>> **GitHub-Advanced-Security Download Free Dumps** <<

## **Dump GitHub-Advanced-Security Collection, GitHub-Advanced-Security Latest Test Vce**

You will not only get familiar with the GitHub Advanced Security GHAS Exam (GitHub-Advanced-Security) exam environment but also enhance your time management skills which will be quite helpful in the final GitHub-Advanced-Security certification exam. The GitHub-Advanced-Security desktop practice test software will install on your Windows-based computer and laptop. Very easy to install and provide a user-friendly interface to GitHub-Advanced-Security Exam candidates. Whereas the GitHub-Advanced-Security web-based practice test software is concerned, it is a browser-based application that works with all the latest browsers.

### **GitHub Advanced Security GHAS Exam Sample Questions (Q15-Q20):**

#### **NEW QUESTION # 15**

What is required to trigger code scanning on a specified branch?

- A. The repository must be private.
- **B. The workflow file must exist in that branch.**
- C. Secret scanning must be enabled on the repository.
- D. Developers must actively maintain the repository.

**Answer: B**

Explanation:

Comprehensive and Detailed Explanation:

For code scanning to be triggered on a specific branch, the branch must contain the appropriate workflow file, typically located in the .github/workflows directory. This YAML file defines the code scanning configuration and specifies the events that trigger the scan (e.g., push, pull\_request).

Without the workflow file in the branch, GitHub Actions will not execute the code scanning process for that branch. The repository's visibility (private or public), the status of secret scanning, or the activity level of developers do not directly influence the triggering of code scanning.

#### **NEW QUESTION # 16**

When does Dependabot alert you of a vulnerability in your software development process?

- A. When Dependabot opens a pull request to update a vulnerable dependency
- **B. As soon as a vulnerable dependency is detected**
- C. As soon as a pull request is opened by a contributor
- D. When a pull request adding a vulnerable dependency is opened

**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.

#### NEW QUESTION # 17

As a developer, you need to configure a code scanning workflow for a repository where GitHub Advanced Security is enabled. What minimum repository permission do you need?

- A. Admin
- **B. Write**
- C. Read
- D. None

**Answer: B**

Explanation:

To create or modify a code scanning workflow file (typically under `.github/workflows/codeql-analysis.yml`), you must have Write access to the repository.

Write permission allows you to commit the workflow file, which is required to run or configure code scanning using GitHub Actions.

#### NEW QUESTION # 18

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

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

**Answer: D**

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 # 19

Where in the repository can you give additional users access to secret scanning alerts?

- A. Security
- **B. Settings**
- C. Secrets
- D. Insights

**Answer: B**

Explanation:

To grant specific users access to view and manage secret scanning alerts, you do this via the `Settings` tab of the repository. From there, under the "Code security and analysis" section, you can add individuals or teams with roles such as security manager.

The Security tab only displays alerts; access control is handled in Settings.

#### NEW QUESTION # 20

.....

Many people worry about buying electronic products on Internet, like our GitHub-Advanced-Security preparation quiz, because they think it is a kind of dangerous behavior which may bring some virus for their electronic product, especially for their computer

which stores a great amount of privacy information. We must emphasize that our GitHub-Advanced-Security simulating materials are absolutely safe without viruses, if there is any doubt about this after the pre-sale, we provide remote online guidance installation of our GitHub-Advanced-Security exam practice.

- [illegible]