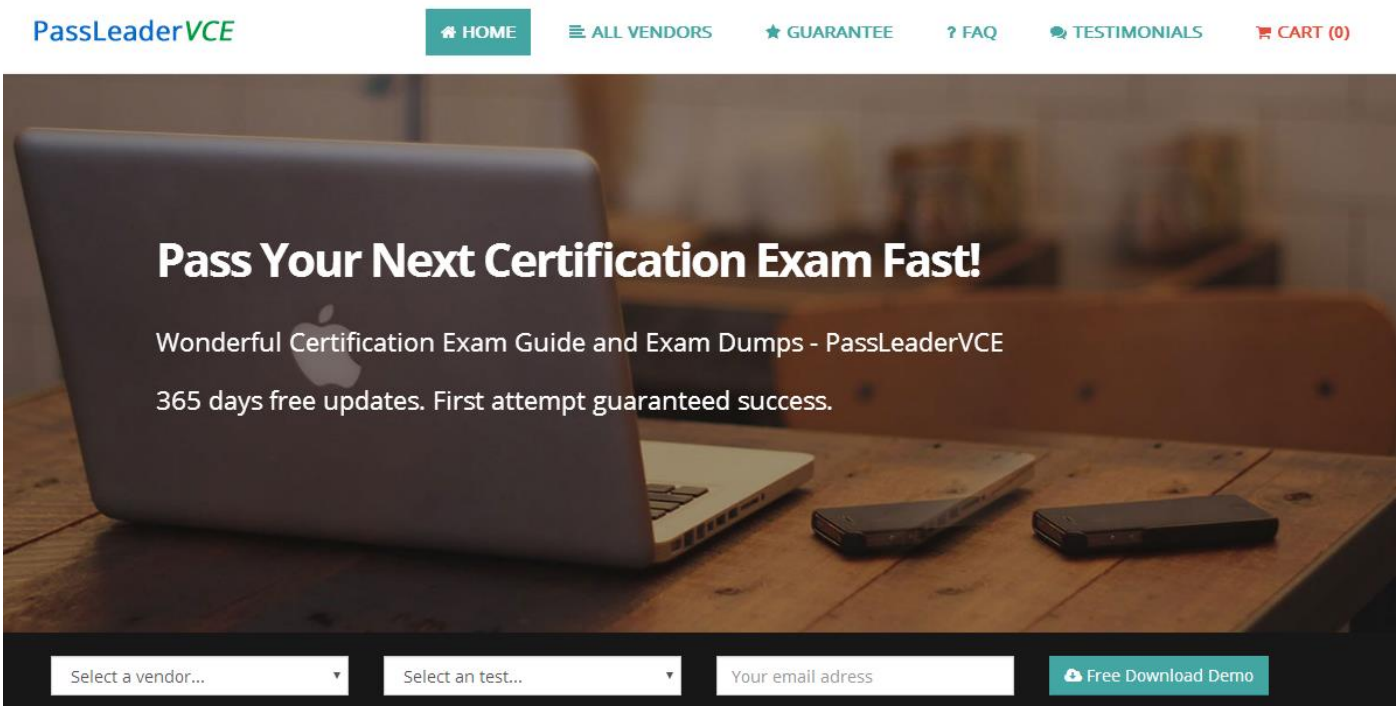
PassleaderVCE



http://www.passleadervce.com/

Wonderful Certification Exam Guide and Exam Dumps- PassLeaderVCE

Exam : **GitHub-Advanced-Security**

Title : GitHub Advanced Security GHAS Exam

Vendor : GitHub

Version : DEMO

NO.1 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: D

Explanation:

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.

NO.2 You are managing code scanning alerts for your repository. You receive an alert highlighting a problem with data flow. What do you click for additional context on the alert?

A. Show paths

B. Security

C. Code scanning alerts

Answer: A

Explanation:

When dealing with a data flow issue in a code scanning alert, clicking on "Show paths" provides a detailed view of the data's journey through the code. This includes the source of the data, the path it takes, and where it ends up (the sink). This information is crucial for understanding how untrusted data might reach sensitive parts of your application and helps in identifying where to implement proper validation or sanitization.

NO.3 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: A

Explanation:

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.

NO.4 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
Explanation:
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.

NO.5 In the pull request, how can developers avoid adding new dependencies with known vulnerabilities?
A. Enable Dependabot alerts.
B. Add Dependabot rules.
C. Add a workflow with the dependency review action.
D. Enable Dependabot security updates.
Answer: C
Explanation:
To detect and blockvulnerable dependencies before merge, developers should use theDependency Review GitHub Actionin their pull request workflows. It scans all proposed dependency changes and flags any packages with known vulnerabilities.
This is apreventative measureduring development, unlike Dependabot, which reactsafter the fact.

NO.6 When using CodeQL, how does extraction for compiled languages work?
A. By generating one language at a time
B. By resolving dependencies to give an accurate representation of the codebase
C. By monitoring the normal build process
D. By running directly on the source code
Answer: C
Explanation:
For compiled languages, CodeQL performs extraction bymonitoring 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.

NO.7 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: C

Explanation:

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.

NO.8 Which of the following Watch settings could you use to get Dependabot alert notifications? (Each answer presents part of the solution. Choose two.)

A. The Custom setting

B. The Participating and @mentions setting

C. The All Activity setting

D. The Ignore setting

Answer: A C

Explanation:

Comprehensive and Detailed Explanation:

To receive Dependabot alert notifications for a repository, you can utilize the following Watch settings:

Custom setting: Allows you to tailor your notifications, enabling you to subscribe specifically to security alerts, including those from Dependabot.

All Activity setting: Subscribes you to all notifications for the repository, encompassing issues, pull requests, and security alerts like those from Dependabot.

The Participating and @mentions setting limits notifications to conversations you're directly involved in or mentioned, which may not include security alerts. The Ignore setting unsubscribes you from all notifications, including critical security alerts.

GitHub Docs

+1

GitHub Docs

+1