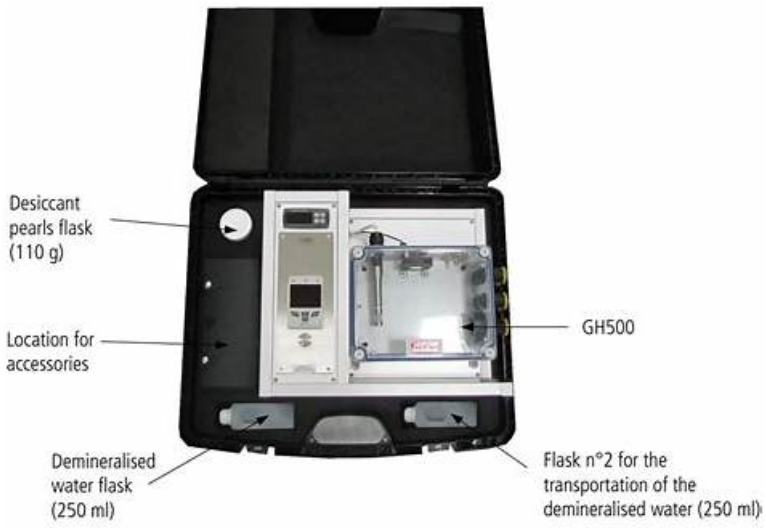
GH-500 Lernressourcen, GH-500 Zertifizierungsprüfung



Die Microsoft GH-500 Zertifizierungsunterlagen von DeutschPrüfung sind unbedingt die Unterlagen für Microsoft GH-500 Zertifizierungsprüfung, an der Sie glauben können. Falls Sie nicht glauben, probieren Sie bitte persönlich, dann können Sie diese Tatsachen wissen. Klicken Sie bitte die Demo von DeutschPrüfung Website. PDF-Versionen und Software-Versionen sind beide vorhanden. Probieren Sie bitte zuerst. Sie können persönlich die Qualität der Microsoft GH-500 Dumps überprüfen.

Warum versprechen wir, dass wir Ihnen Geld zurückgeben, wenn Sie die Microsoft GH-500 Prüfung nicht bestehen? Denn zahlose Kunden, die unsere Prüfungssofteware benutzt haben, bestehen die Microsoft GH-500 Zertifizierungsprüfung, was uns die Konfidenz bringt. Microsoft GH-500 Prüfung ist eine sehr wichtige Beweis der IT-Fähigkeit für die Angestellte im IT-Gewerbe. Aber die Prüfung ist auch schwierig. Die Arbeiter von DeutschPrüfung haben die Microsoft GH-500 Prüfungsunterlagen mit große Einsätze geforscht. Die Software ist das Geistesprodukt vieler IT-Spezialist.

>> GH-500 Lernressourcen <<

GH-500 GitHub Advanced Security neueste Studie Torrent & GH-500 tatsächliche prep Prüfung

Haben Sie DeutschPrüfung, haben Sie den Schlüssel zum Erfolg, denn Sie können damit die Microsoft GH-500 Zertifizierungsprüfung zügig bestehen. Unsere Berufsgruppe aus gut ausgebildeten und erfahrenen IT-Eliten haben die Entwicklungen der ständig veränderten IT-Branche untersucht und erforscht, dann erstellen Sie die Schulungsunterlagen zur Microsoft GH-500 Zertifizierungsprüfung für DeutschPrüfung. Ihre Autorität ist zweifellos. Bevor Sie unsere Prüfungsmaterialien kaufen, können Sie die Demo durch unsere Webseite DeutschPrüfung herunterladen.

Microsoft GH-500 Prüfungsplan:

Thema	Einzelheiten
Thema 1	• Describe the GHAS security features and functionality: This section of the exam measures skills of Security Engineers and Software Developers and covers understanding the role of GitHub Advanced Security (GHAS) features within the overall security ecosystem. Candidates learn to differentiate security features available automatically for open source projects versus those unlocked when GHAS is paired with GitHub Enterprise Cloud (GHEC) or GitHub Enterprise Server (GHES). The domain includes knowledge of Security Overview dashboards, the distinctions between secret scanning and code scanning, and how secret scanning, code scanning, and Dependabot work together to secure the software development lifecycle. It also covers scenarios contrasting isolated security reviews with integrated security throughout the development lifecycle, how vulnerable dependencies are detected using manifests and vulnerability databases, appropriate responses to alerts, the risks of ignoring alerts, developer responsibilities for alerts, access management for viewing alerts, and the placement of Dependabot alerts in the development process.

Thema 2	• Configure and use secret scanning: This domain targets DevOps Engineers and Security Analysts with the skills to configure and manage secret scanning. It includes understanding what secret scanning is and its push protection capability to prevent secret leaks. Candidates differentiate secret scanning availability in public versus private repositories, enable scanning in private repos, and learn how to respond appropriately to alerts. The domain covers alert generation criteria for secrets, user role-based alert visibility and notification, customizing default scanning behavior, assigning alert recipients beyond admins, excluding files from scans, and enabling custom secret scanning within repositories.
Thema 3	• Configure and use Dependabot and Dependency Review: Focused on Software Engineers and Vulnerability Management Specialists, this section describes tools for managing vulnerabilities in dependencies. Candidates learn about the dependency graph and how it is generated, the concept and format of the Software Bill of Materials (SBOM), definitions of dependency vulnerabilities, Dependabot alerts and security updates, and Dependency Review functionality. It covers how alerts are generated based on the dependency graph and GitHub Advisory Database, differences between Dependabot and Dependency Review, enabling and configuring these tools in private repositories and organizations, default alert settings, required permissions, creating Dependabot configuration files and rules to auto-dismiss alerts, setting up Dependency Review workflows including license checks and severity thresholds, configuring notifications, identifying vulnerabilities from alerts and pull requests, enabling security updates, and taking remediation actions including testing and merging pull requests.
Thema 4	• Configure and use Code Scanning with CodeQL: This domain measures skills of Application Security Analysts and DevSecOps Engineers in code scanning using both CodeQL and third-party tools. It covers enabling code scanning, the role of code scanning in the development lifecycle, differences between enabling CodeQL versus third-party analysis, implementing CodeQL in GitHub Actions workflows versus other CI tools, uploading SARIF results, configuring workflow frequency and triggering events, editing workflow templates for active repositories, viewing CodeQL scan results, troubleshooting workflow failures and customizing configurations, analyzing data flows through code, interpreting code scanning alerts with linked documentation, deciding when to dismiss alerts, understanding CodeQL limitations related to compilation and language support, and defining SARIF categories.
Thema 5	• Describe GitHub Advanced Security best practices, results, and how to take corrective measures: This section evaluates skills of Security Managers and Development Team Leads in effectively handling GHAS results and applying best practices. It includes using Common Vulnerabilities and Exposures (CVE) and Common Weakness Enumeration (CWE) identifiers to describe alerts and suggest remediation, decision-making processes for closing or dismissing alerts including documentation and data-based decisions, understanding default CodeQL query suites, how CodeQL analyzes compiled versus interpreted languages, the roles and responsibilities of development and security teams in workflows, adjusting severity thresholds for code scanning pull request status checks, prioritizing secret scanning remediation with filters, enforcing CodeQL and Dependency Review workflows via repository rulesets, and configuring code scanning, secret scanning, and dependency analysis to detect and remediate vulnerabilities earlier in the development lifecycle, such as during pull requests or by enabling push protection.

Microsoft GitHub Advanced Security GH-500 Prüfungsfragen mit Lösungen (Q49-Q54):

49. Frage
Which of the following options would close a Dependabot alert?

- A. Viewing the dependency graph
- B. Creating a pull request to resolve the vulnerability that will be approved and merged
- C. Viewing the Dependabot alert on the Dependabot alerts tab of your repository
- D. Leaving the repository in its current state

Antwort: B

Begründung:
A Dependabot alert is only marked as resolved when the related vulnerability is no longer present in your code - specifically after you merge a pull request that updates the vulnerable dependency.

Simply viewing alerts or graphs does not affect their status. Ignoring the alert by leaving the repo unchanged keeps the vulnerability active and unresolved.

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

Antwort: B

Begründung:
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.

51. Frage
Which of the following is the best way to prevent developers from adding secrets to the repository?

- A. Configure a security manager
- B. Enable push protection
- C. Create a CODEOWNERS file
- D. Make the repository public

Antwort: B

Begründung:
The best proactive control is push protection. It scans for secrets during a git push and blocks the commit before it enters the repository.
Other options (like CODEOWNERS or security managers) help with oversight but do not prevent secret leaks.
Making a repo public would increase the risk, not reduce it.

52. Frage
After investigating a code scanning alert related to injection, you determine that the input is properly sanitized using custom logic. What should be your next step?

- A. Dismiss the alert with the reason "false positive."
- B. Draft a pull request to update the open-source query.
- C. Open an issue in the CodeQL repository.
- D. Ignore the alert.

Antwort: A

Begründung:
When you identify that a code scanning alert is a false positive-such as when your code uses a custom sanitization method not recognized by the analysis-you should dismiss the alert with the reason "false positive." This action helps improve the accuracy of future analyses and maintains the relevance of your security alerts.
As per GitHub's documentation:
"If you dismiss a CodeQL alert as a false positive result, for example because the code uses a sanitization library that isn't supported, consider contributing to the CodeQL repository and improving the analysis." By dismissing the alert appropriately, you ensure that your codebase's security alerts remain actionable and relevant.

53. Frage
Which CodeQL query suite provides queries of lower severity than the default query suite?

- A. github/codeql-go/ql/src@main
- B. security-extended
- C. github/codeql/cpp/ql/src@main

Antwort: B

Begründung:
The security-extended query suite includes additional CodeQL queries that detect lower severity issues than those in the default security-and-quality suite.
It's often used when projects want broader visibility into code hygiene and potential weak spots beyond critical vulnerabilities.
The other options listed are paths to language packs, not query suites themselves.

54. Frage
.....

Die Kandidaten können die Schulungsunterlagen zur Microsoft GH-500 Zertifizierungsprüfung von DeutschPrüfung in einer Simulationsumgebung lernen. Sie können die Prüfungssorte und die Testzeit kontrollieren. In DeutschPrüfung können Sie sich ohne Druck und Stress gut auf die Microsoft GH-500 Prüfung vorbereiten. Zugleich können Sie auch einige häufige Fehler vermeiden. So werden Sie mehr Selbstbewusstsein in der Microsoft GH-500 Prüfung haben. In der realen Prüfung können Sie Ihre Erfahrungen wiederholen, um Erfolg in der Prüfung zu erzielen.

GH-500 Zertifizierungsprüfung: https://www.deutschpruefung.com/GH-500-deutsch-pruefungsfragen.html

- GH-500 Studienmaterialien: GitHub Advanced Security - GH-500 Zertifizierungstraining □ Sie müssen nur zu □ de.fast2test.com □ gehen um nach kostenloser Download von ➽ GH-500 □ zu suchen □GH-500 Zertifizierungsantworten
- GH-500 Probesfragen □ GH-500 Examsfragen □ GH-500 Testengine □ Suchen Sie jetzt auf [www.itzert.com] nach 「 GH-500 」 und laden Sie es kostenlos herunter □GH-500 Prüfungs-Guide
- GH-500 Musterprüfungsfragen □ GH-500 Testfagen □ GH-500 Probesfragen □ Öffnen Sie □ www.zertsoft.com □ geben Sie ▸ GH-500 ◂ ein und erhalten Sie den kostenlosen Download □GH-500 Lerntipps
- Microsoft GH-500 VCE Dumps - Testking IT echter Test von GH-500 □ Suchen Sie auf der Webseite ➥ www.itzert.com □ nach ▹ GH-500 ◃ und laden Sie es kostenlos herunter ↗ GH-500 Zertifizierungsfragen
- GH-500 Deutsche Prüfungsfragen □ GH-500 Deutsche Prüfungsfragen □ GH-500 Testengine □ Suchen Sie auf ▹ www.zertpruefung.ch ◃ nach kostenlosem Download von ▸ GH-500 ◂ □GH-500 Probesfragen
- GH-500 Prüfungsguide: GitHub Advanced Security - GH-500 echter Test - GH-500 sicherlich-zu-bestehen □ Öffnen Sie die Website “ www.itzert.com ” Suchen Sie ➥ GH-500 □ Kostenloser Download □GH-500 Prüfungsfrage
- GH-500 Schulungsunterlagen □ GH-500 Schulungsunterlagen □ GH-500 Online Prüfungen □ Sie müssen nur zu ➤ www.pruefungfrage.de □ gehen um nach kostenloser Download von □ GH-500 □ zu suchen □GH-500 Examsfragen
- Die anspruchsvolle GH-500 echte Prüfungsfragen von uns garantiert Ihre bessere Berufsaussichten! □ Öffnen Sie die Webseite ➡ www.itzert.com □□□ und suchen Sie nach kostenloser Download von ✔ GH-500 □✔□ □GH-500 Prüfungsfrage
- GH-500 Antworten □ GH-500 Probesfragen ✔□ GH-500 Musterprüfungsfragen □ Sie müssen nur zu □ www.zertfragen.com □ gehen um nach kostenloser Download von 《 GH-500 》 zu suchen □GH-500 Examsfragen
- GH-500 Zertifizierungsantworten □ GH-500 Zertifizierungsfragen □ GH-500 Antworten □ Suchen Sie auf ⇛ www.itzert.com ⇚ nach kostenlosem Download von ➽ GH-500 □ □GH-500 Lerntipps
- GH-500 Prüfungsfragen Prüfungsvorbereitungen 2025: GitHub Advanced Security - Zertifizierungsprüfung Microsoft GH-500 in Deutsch Englisch pdf downloaden □ Öffnen Sie ▸ www.zertsoft.com ◂ geben Sie ✔ GH-500 □✔□ ein und erhalten Sie den kostenlosen Download □GH-500 Testengine
- billsha472.pages10.com, www.stes.tyc.edu.tw, www.stes.tyc.edu.tw, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, bbs.74ax.com, 202.53.128.110, study.stcs.edu.np, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, www.stes.tyc.edu.tw, wordcollective.org, Disposable vapes