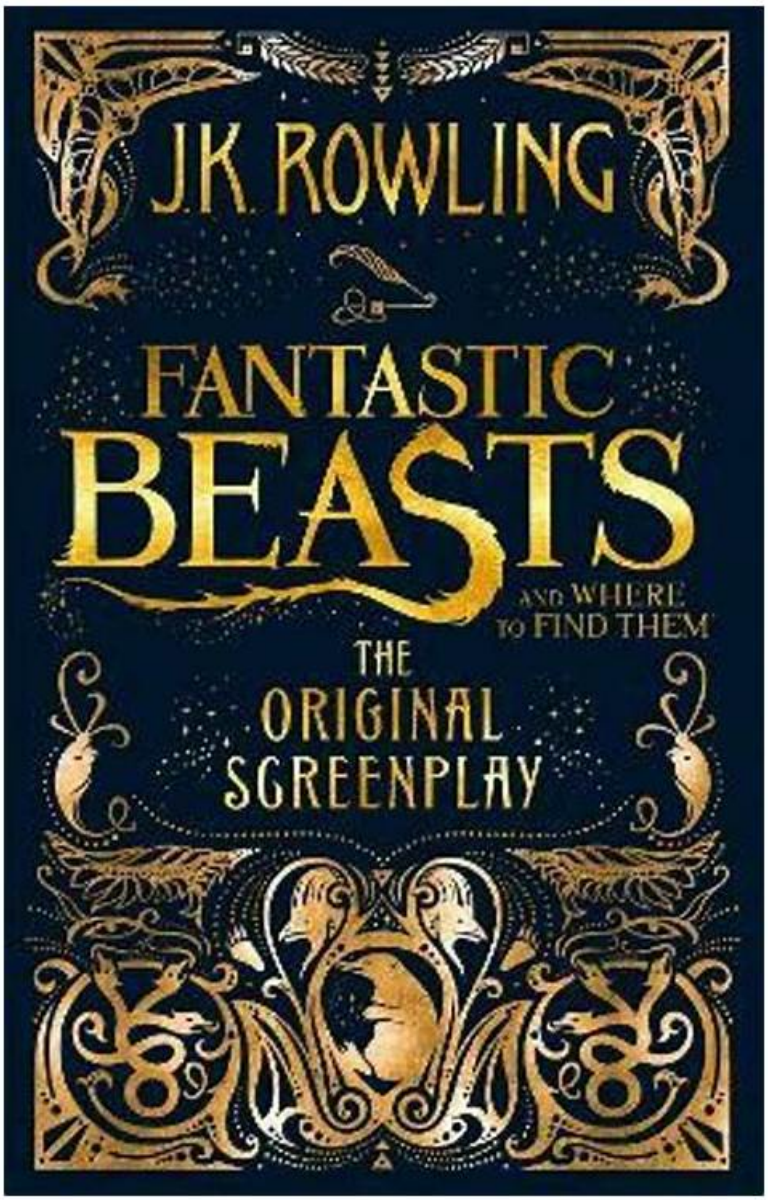
Fantastic Authorized GH-500 Pdf & Free PDF New GH-500 Test Papers & Top Microsoft GitHub Advanced Security



The software keeps track of the previous GitHub Advanced Security (GH-500) practice exam attempts and shows the changes of each attempt. You don't need to wait days or weeks to get your performance report. The software displays the result of the Microsoft GH-500 Practice Test immediately, which is an excellent way to understand which area needs more attention.

Microsoft GH-500 Exam Syllabus Topics:

Topic	Details

Topic 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.
Topic 2	• 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.
Topic 3	• 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.
Topic 4	• 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.
Topic 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.

Free PDF 2026 Microsoft GH-500: Valid Authorized GitHub Advanced Security Pdf

Our GitHub Advanced Security Web-Based Practice Exam is compatible with all major browsers, including Chrome, Internet Explorer, Firefox, Opera, and Safari. No specific plugins are required to take this GitHub Advanced Security practice test. It mimics a real GH-500 test atmosphere, giving you a true exam experience. This GitHub Advanced Security (GH-500) practice exam helps you become acquainted with the exam format and enhances your test-taking abilities.

Microsoft GitHub Advanced Security Sample Questions (Q64-Q69):

NEW QUESTION # 64
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. The name of the pattern
- B. Additional match requirements for the secret format
- C. The secret format
- D. A list of repositories to scan

Answer: A,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 # 65
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. All Activity
- C. Ignore
- 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 # 66
A secret scanning alert should be closed as "used in tests" when a secret is:

- A. Solely used for tests.
- B. In a test file.
- C. Not a secret in the production environment.
- D. In the readme.md file.

Answer: A

Explanation:
If a secret is intentionally used in a test environment and poses 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 its purpose is purely for testing.

NEW QUESTION # 67
Assuming that no custom Dependabot behavior is configured, who has the ability to merge a pull request created via Dependabot security updates?

- A. A repository member of an enterprise organization
- B. A user who has write access to the repository
- C. An enterprise administrator
- D. A user who has read access to the repository

Answer: B

Explanation:
Comprehensive and Detailed Explanation:
By default, users with write access to a repository have the ability to merge pull requests, including those created by Dependabot for security updates. This access level allows contributors to manage and integrate changes, ensuring that vulnerabilities are addressed promptly.
Users with only read access cannot merge pull requests, and enterprise administrators do not automatically have merge rights unless they have write or higher permissions on the specific repository.

NEW QUESTION # 68
What are Dependabot security updates?

- A. Automated pull requests to update the manifest to the latest version of the dependency
- B. Compatibility scores to let you know whether updating a dependency could cause breaking changes to your project
- C. Automated pull requests that help you update dependencies that have known vulnerabilities
- D. Automated pull requests that keep your dependencies updated, even when they don't have any vulnerabilities

Answer: C

Explanation:
Dependabot security updates are automated pull requests triggered when GitHub detects a vulnerability in a dependency listed in your manifest or lockfile. These PRs upgrade the dependency to the minimum safe version that fixes the vulnerability.
This is separate from regular updates (which keep versions current even if not vulnerable).

NEW QUESTION # 69
.....

- Quiz 2026 GH-500: GitHub Advanced Security Accurate Authorized Pdf □ Search for { GH-500 } and download it for free immediately on ➤ www.practicevce.com □ □GH-500 Test Duration
- 100% Pass Quiz 2026 Microsoft GH-500: Pass-Sure Authorized GitHub Advanced Security Pdf □ Search for ➡ GH-500 □□□ and download exam materials for free through ➡ www.pdfvce.com □□□ □GH-500 Pass Guaranteed
- Newest Authorized GH-500 Pdf Spend Your Little Time and Energy to Pass GH-500: GitHub Advanced Security exam ◴ Download ➤ GH-500 □ for free by simply searching on ➥ www.prepawayete.com □ □GH-500 Pass Guaranteed
- GH-500 Pass Guaranteed □ Vce GH-500 Torrent □ GH-500 Popular Exams □ Search for □ GH-500 □ and obtain a free download on [www.pdfvce.com] □GH-500 Reliable Test Sample
- GH-500 Valid Test Practice □ GH-500 Valid Test Practice ⧖ Vce GH-500 Torrent □ Search for " GH-500 " on " www.practicevce.com " immediately to obtain a free download □GH-500 Latest Exam Camp
- www.stes.tyc.edu.tw, myportal.utt.edu.tt, yy.hackp.com.cn, 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, myportal.utt.edu.tt, www.stes.tyc.edu.tw, 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, myportal.utt.edu.tt, Disposable vapes