Vendor:WGU

Exam Code:SECURE-SOFTWARE-DESIGN

Exam Name:WGUSecure Software Design (KEO1) Exam

Version: Demo

QUESTION 1

Credit card numbers are encrypted when stored in the database but are automatically decrypted when data is fetched. The testing tool intercepted the GET response, and testers were able to view credit card numbers as clear text. How should the organization remediate this vulnerability?

A. Never cache sensitive data

B. Ensure there is an audit trail for all sensitive transactions

C. Ensure all data in transit is encrypted

D. Enforce role-based authorization controls in all application layers

Correct Answer: C

Reference: https://owasp.org/www-project-proactive-controls/v3/en/c8-protect-data-everywhere

---

QUESTION 2

The security team has a library of recorded presentations that are required viewing for all new developers in the organization. The video series details organizational security policies and demonstrates how to define, test for, and code for possible throats.

Which category of secure software best practices does this represent?

A. Attack models

B. Training

C. Architecture analysis

D. Code review

Correct Answer: B

Reference: https://changemanagementinsight.com/change-management-in-cyber-security/

QUESTION 3

Using a web-based common vulnerability scoring system (CVSS) calculator, a security response team member performed an assessment on a reported vulnerability in the company\\'s claims intake component. The base score of the vulnerability was 3.5 and changed to 5.9 after adjusting temporal and environmental metrics.

Which rating would CVSS assign this vulnerability?

A. Critical severity

B. High severity

C. Low severity

D. Medium severity

Correct Answer: D

Reference: https://nvd.nist.gov/vuln-metrics/cvss

QUESTION 4

Which type of security analysis is limited by the fact that a significant time investment of a highly skilled team member is required?

A. Fuzz testing

B. Dynamic code analysis

C. Manual code review

D. Static code analysis

Correct Answer: C

Reference: https://www.pwc.com/gx/en/issues/cybersecurity/digital-trust-insights-2021/cyber-talent-workforce.html

---

QUESTION 5

In which step of the PASTA threat modeling methodology is vulnerability and exploit analysis performed?

A. Define technical scope

B. Attack modeling

C. Define objectives

D. Application decomposition

Correct Answer: B

Reference: https://versprite.com/blog/what-is-pasta-threat-modeling/

QUESTION 6

Which category classifies identified threats that do not have defenses in place and expose the application to exploits?

A. Fully mitigated threat

B. Threat profile

C. Unmitigated threats

D. Partially mitigated threat

Correct Answer: C

Reference: https://cyberinsight.co/what-are-the-4-security-classification/

QUESTION 7

Which threat modeling step collects exploitable weaknesses within the product?

A. Analyze the target

B. Rate threats

C. Identify and document threats

D. Set the scope

Correct Answer: C

Reference: https://owasp.org/www-community/Threat_Modeling_Process

---

QUESTION 8

Senior IT staff has determined that a new product will be hosted in the cloud and will support web and mobile users. Developers will need to deliver secure REST services, Android and IOS mobile apps, and a web application. Developers are currently determining how to deliver each part of the overall product.

Which phase of the software development lifecycle (SDLC) is being described?

A. Maintenance

B. End of life

C. Deployment

D. Design

Correct Answer: D

Reference: https://theproductmanager.com/topics/software-development-life-cycle/

QUESTION 9

Which threat modeling approach concentrates on things the organization wants to protect?

A. Asset-centric

B. Server-centric

C. Attacker-centric

D. Application-centric

Correct Answer: A

QUESTION 10

Using a web-based common vulnerability scoring system (CVSS) calculator, a security response team member performed an assessment on a reported vulnerability in the company\\'s customer portal. The base score of the vulnerability was

9.9 and changed to 8.0 after adjusting temporal and environmental metrics. Which rating would CVSS assign this vulnerability?

A. Medium severity

B. Critical severity

C. Low severity

D. High severity

Correct Answer: D

Reference: https://nvd.nist.gov/vuln-metrics/cvss

QUESTION 11

Which type of threat exists when an attacker can intercept and manipulate form data after the user clicks the save button but before the request is posted to the API?

A. Elevation of privilege

B. Spoofing

C. Tampering

D. Information disclosure

Correct Answer: C

Reference: https://www.sentinelone.com/cybersecurity-101/what-is-a-man-in-the-middle-mitm-attack/

QUESTION 12

The organization has contracted with an outside firm to simulate an attack on the new software product and report findings and remediation recommendations. Which activity of the Ship SDL phase is being performed?

A. Penetration testing

B. Policy compliance analysis

C. Open-source licensing review

D. Final security review

Correct Answer: A

Reference: https://www.oreilly.com/library/view/core-software-security/9781466560963/xhtml/chapter7.xhtml