ISTQB
CT-STE
Certified Tester Security Test Engineer (CT-STE)

For More Information – Visit link below:
https://www.examsempire.com/

Product Version

1. **Up to Date products, reliable and verified.**
2. **Questions and Answers in PDF Format.**

Latest Version: 6.0

Question: 1

How can security testing improve measurability within an ISMS?
Response:

A. Security tests can be used as objective analysis within the Check step of the PDCA cycle to measure effectiveness of a PDCA cycle.
B. All Security testing generates quantifiable insights into the security of a system that can be used to measure ISMS effectiveness.
C. The more security tests pass a test for a system under test, the better and more effective the ISMS is.
D. The effectiveness of an ISMS is better the more security testing techniques are used.

Answer: A

Question: 2

When using open-source software, which of the following is NOT a critical factor to consider when addressing security concerns?
Response:

A. Alignment with OWASP and active security audits by the contributors.
B. Frequency and availability of security patches and updates.
C. Your team's ability to manage and customize the tool for your environment.
D. Licensing requirements and compliance with open-source security guidelines.

Answer: C

Question: 3

You are responsible for the system's security. Somebody in your team is interested in security testing and does a penetration test on your system, which includes OWASP Top-10 vulnerabilities. The corresponding test report consists only of succeeded and failed testcases covering these vulnerabilities. Which reasoning on accepting or rejecting the test report is correct?
Response:

A. Accepting, as the penetration test was done by an internal colleague who knows the specific security style guides.

B. Rejecting, as your acceptance criteria for security were not communicated and are not considered in the test report. So it's unclear if the corresponding test techniques were used and if the test results are relevant for your yearly security style guide conformance check.
C. Accepting, as OWASP is Best Practice and defines a general list of acceptance criteria.
D. Rejecting, because a security code style guide should be tested by white-box testing approaches, not by black-box dynamic pentests.
E. Accepting, as OWASP reflects your security code style guide.

Answer: B,D

Question: 4

During component testing, which compiler warning would trigger the security tester most?
Response:

A. Those indicating security problems that must be fixed
B. Those indicating potential issues that should be investigated
C. Those indicating coding issues that will cause functional suitability defects
D. Those indicating poor programming practices that will increase maintainability

Answer: B

Question: 5

When you use test oracles for an application from standards and best practices, what do you have to consider?
Response:

A. Such test oracles are valid independent from any application parameters
B. Such test oracles can only be used as fuzzy hints for security testing
C. Such test oracles can not be used for security testing
D. The less specific an application and its context is, the more efficient is reusing such test

Answer: D

Question: 6

A new start-up enterprise in the banking industry has developed a new core system. The development team has focused on good usability and excellent performance so far. Before going live, the executive board wants to get an independent view about the level of security. They are asking you as security tester to do a black-box-pentest. The task is to test for the most critical vulnerabilities that could be exploitable for the new banking app.

If you want to fulfill this job, how can you leverage standards for your task?
Response:

A. You select relevant weaknesses within CWEs standard and execute listed test cases
B. You select relevant weaknesses within CWE, choose available exploits for selected CWEs and apply them
C. You select relevant weaknesses within CWE, you prioritize selected CWEs based on CWSS standard, and you select relevant CVEs covering prioritized CWE
D. You select relevant weaknesses within CWE, you prioritize selected CWEs based on CVSS standard and derivate individual test cases related the CVSS
E. For each selected CVE you derive test cases for the banking app and execute them

Answer: C,E

Question: 7

In a CI/CD environment a new pipeline is being put together for the next project you are working on. Which one of the following would you recommend being the first triggered step as part of the pipeline?
Response:

A. SCA
B. SAST
C. DAST
D. IAST

Answer: A

Question: 8

Security Test reports should be handled with a high level of confidentiality. What type of data being part of most security test reports motivates this classification?
Response:

A. Name of the security tester, timeframe for test execution, test results (passed and failed test cases)
B. Used test environment, pre-set preconditions of the executed tests, used test data, procedure of test execution, detected behavior
C. List of tested CVE vulnerabilities, list of named developers, identified software development method, identified software development tools
D. Used security coding conventions, identified functional test coverage, applied vulnerability scans

Answer: B

Question: 9

Each attack is different. However, certain steps are common for almost every attack. These steps can be defined as:
Response:

A. Information gathering step, followed by exploitation/gaining access and at the end persisting/maintaining access.
B. Social engineering, followed by brute-force attack and at the end persisting/maintaining access
C. Exploitation/gaining access followed by social engineering to understand the results and at the end clearing tracks
D. Information gathering, followed by clearing tracks and at the end social engineering to have a better baselining

Answer: A

Question: 10

Which one of the following options describes Zero Trust?
Response:

A. Any user requires continuous verification of identity regardless of the user's location.
B. Any device and user with access to the system is trusted by default.
C. Only devices within the trusted network get access to systems.
D. All users are granted the level of access they need.

Answer: A

Thank You for Trying Our Product

Special 16 USD Discount Coupon: NSZUBG3X

Email: support@examsempire.com

Check our Customer Testimonials and ratings available on every product page.

Visit our website.

https://examsempire.com/