Exam Name – Certified Advanced Software Security Tester (CASST)

Exam Code – CASST-001

Sample Exam

(Question): Which of the following test cases would best test a system's security procedure?

(A): Three unsuccessful login attempts will generate a lock-out message. Contact your manager or the System Administrator so they can give you a temporary password over the phone. You must then change the temporary password upon logging in. You log out then log back in using your newly created password.

(B): You receive a lock-out message after several attempts to log in. You call IT support to obtain a new password. You log in with the temporary password, log back out, then log in again and enter a new password.

(C): After several attempts you are locked out of the system. You use a password that worked previously. However, it no longer works. You attempt to create a new password but you are now locked out. A complete reboot of the machine is the next step to take you to the prompt to re-enter the password.

(D): After the first attempt to use an invalid password you immediately pull up a list of passwords on your notepad on your PC to ensure you are using the correct one. You try another password from the list and it works.

(Correct): A

(Question): At what point in the SDLC should there be checking to ensure that proper secure coding practices have been followed?

(A): Component testing
(B): Integration testing
(C): System testing
(D): Security acceptance testing

(Correct): A

(Question): You have been asked by the business analyst to help with defining the requirements for the security aspects of a system. This is a safety-critical system that stores medical information for patients and supplies this information to health professionals at hospitals, doctors' offices and ambulances. At what point in the lifecycle should the security requirements be documented and at what level of detail?

(A): They should not be documented formally because of the need to protect the security implementation within the code from outsiders

(B): They should be documented in a detailed and unambiguous way in the requirements documents during the requirements phase

(C): They should be documented during the design phase when the code approach is known rather than at the requirements phase when the approach is not known

(D): They should be restricted to the functional access and availability requirements from the user's perspective and should be documented during the requirements phase

(Correct): B

(Question): A deficiency has been discovered in production. If an unauthorized user copies a URL from a session of an authorized user, the unauthorized user can paste the URL into their session and continue to process with the authorized user's rights. In the case that was reported, the unauthorized user was able to use the authorized user's URL to change the system administration password. In order to close this gap, the developers will check the session ID and the user ID anytime a URL is used.

What is a realistic concern for this fix?

(A): It will not fix the problem and session hijacking will still be possible
(B): It will fix the problem, but the usability may be adversely affected
(C): It will fix the problem, but performance may be adversely affected
(D): It will not fix the problem and will expose a new vulnerability with session IDs

(Correct): C

(Question): During component level testing, why should the security tester review compiler warnings?

(A): Because these indicate security problems that must be fixed
(B): Because these indicate potential issues that should be investigated
(C): Because these indicate coding issues that will cause functional defects
(D): Because these indicate poor programming practices that will increase maintainability

(Correct): B

(Question): You have been testing a system that has 20 defined components. You have done extensive security testing on each of the components. The system is now ready to move into component integration security testing. How should you approach this testing?

(A): Since component integration testing is concerned with the summation of the vulnerabilities of the individual components, conducting the same tests on the integrated components is the best approach.

(B): The main risk is now in the integration of the components themselves, so testing should cover each interface and verify that there are no vulnerabilities in the interfaces and the components should also be retested.

(C): It is likely that new vulnerabilities are present with the integrated components as well as with the larger system and infrastructure that is now testable, so testing should expand to include these new areas.

(D): Since the components are now integrated, the security risks will be reduced because the possible interactions are now limited so only the integration points should be tested and no component re-testing is needed.

(Correct): C