Jeopardy

APPLICATION SECURITY
BY
CHRISTOPHER ROBINSON
MELANIE MCKEAN

Acknowledgements

Created by Educational Technology Network. www.edtechnetwork.com 2009

All In One CSSLP Exam Guide by WM. Arthur Conklin and Daniel Shoemaker

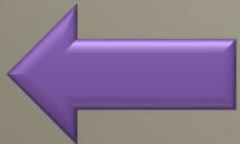| Secure Software Requirements	Secure Software Design	Secure Software Implementation	Secure Software Testing	Secure Installation and Deployment
100	100	100	100	100
200	200	200	200	200
300	300	300	300	300
400	400	400	400	400
500	500	500	500	500

Secure Software Requirements – 100 Points

QUESTION:

- These type of requirements will address issues such as access by unauthorized users and denial of service attacks.

ANSWER:

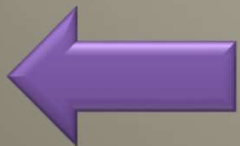- What are availability requirements?

Secure Software Requirements – 200 Points

QUESTION:

- In this type of access control mechanism, users are assigned to a set of roles and the roles are assigned the access permissions.

ANSWER:
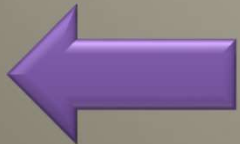
- What is Role-Based Access Control (RBAC)?

QUESTION:

- This is a technique used to present a known attack methodology to the development team.
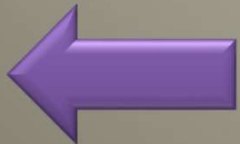
ANSWER:

- What is a Misuse case?

Secure Software Requirements – 400 Points

QUESTION:

- This process involves the mapping of high-level policy statements into lower-level policies until the policies are implementable.

ANSWER:
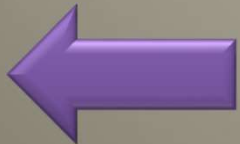
- What is policy decomposition?

Secure Software Requirements – 500 Points

QUESTION:

- This sequence and timing issue in software is resolved through atomic actions under mutual exclusion conditions.
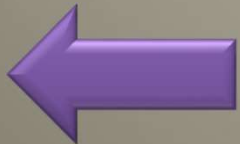
ANSWER:

- What is a race condition?

Secure Software Design – 100 Points

QUESTION:

- The code within the system that can be accessed by unauthorized parties.
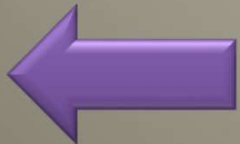
ANSWER:

- What is the attack surface of software?

Secure Software Design – 200 Points

QUESTION:

- This secure design principle is also know as KISS… (Keep it Simple Stupid).
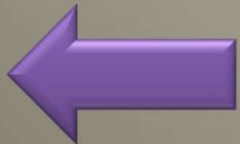
ANSWER:

- What is Economy of Mechanism?

Secure Software Design – 300 Points

QUESTION:

- A process used to identify and document all of the threats to a system.

ANSWER:
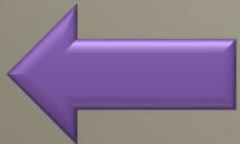
- What is threat modeling?

Secure Software Design – 400 Points

QUESTION:

- A form of architecture that uses the Web as a transfer mechanism and the client as a processing device, typically for display formatting control functions.

ANSWER:

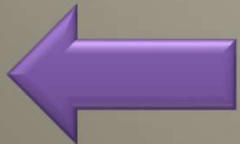- What are Rich Internet Applications (RIAs)?

Secure Software Design – 500 Points

QUESTION:

- This type of code can have a performance advantage over other types of code.
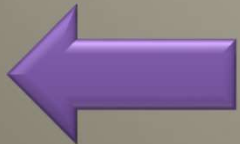
ANSWER:

- What is unmanaged code?

QUESTION:

- An attack performed by an attacker inputting a specific string to manipulate the SQL statement to do something other than that intended by the programmer or designer.
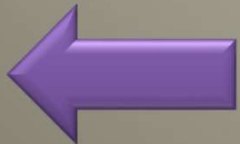
ANSWER:

- What is a SQL injection attack?

QUESTION:

- A value concatenated to the password, or other value being hashed, effectively increasing its length beyond that of a rainbow table.
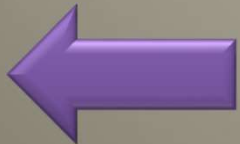
ANSWER:

- What is a salt value?

QUESTION:

- The processes to inspect code for weaknesses and vulnerabilities in which the execution of the code is a part of the testing.
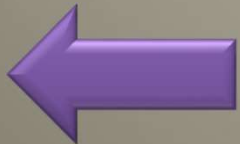
ANSWER:

- What is dynamic code analysis?

QUESTION:

- When programming specifies the what, but not the how, with respect to the tasks to be accomplished.
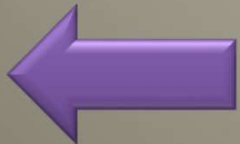
ANSWER:

- What is declarative programming?

Secure Software Implementation – 500 Points

QUESTION:

- This is defined as the extent to which a programming language prevents errors resulting from different data types in a program.

ANSWER:
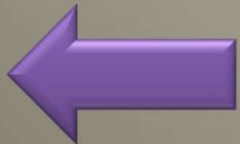
- What is type safety?

Secure Software Testing – 100 Points

QUESTION:

- A type of security testing where the attacker has no knowledge of the inner workings of the software under test.

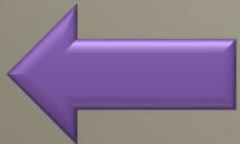**ANSWER:**

- What is Black-Box testing?

Secure Software Testing – 200 Points

QUESTION:

- This type of testing is conducted by developers as they develop code.
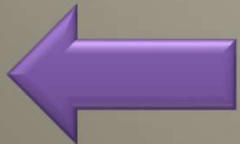
ANSWER:

- What is unit testing?

Secure Software Testing – 300 Points

QUESTION:

- An operational measure for what constitutes a minimum level of quality in the code.
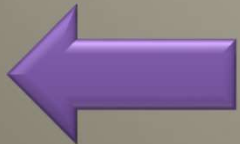
ANSWER:

- What is a bug bar?

Secure Software Testing – 400 Points

QUESTION:

- A brute-force method of addressing input validation issues and vulnerabilities.

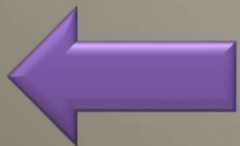**ANSWER:**

- What is fuzz testing?

Secure Software Testing – 500 Points

QUESTION:

- A peer-reviewed system describing security testing.

ANSWER:

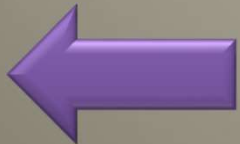- What is the Open Source Security Testing Methodology Manual (OSSTMM)?

QUESTION:

- The set of processes employed to create baseline configurations in an environment and managing configurations to comply with those baselines.

ANSWER:
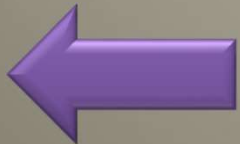
- What is configuration management?

Secure Installation, Deployment, Operations, Maintenance and Disposal – 200 Points

QUESTION:

- The business process associated with the packaging and release of software to production.

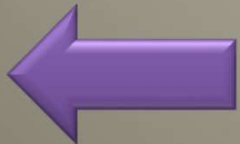**ANSWER:**

- What is release management?

QUESTION:

- A self-sustaining process that continues through its course with-out external stimuli.

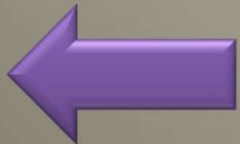**ANSWER:**

- What is bootstrapping?

Secure Installation, Deployment, Operations, Maintenance and Disposal – 400 Points

QUESTION:

- A replacement set of code designed to correct problems or vulnerabilities in existing software.

ANSWER:

- What is a patch?

Secure Installation, Deployment, Operations, Maintenance and Disposal – 500 Points

QUESTION:

- This is used to designate a configuration item's placement in the product hierarchy.

ANSWER:

- What is a PIN?