

# DUMPS ARENA

## Advanced SOA Security

SOA S90.19

Version Demo

Total Demo Questions: 10

Total Premium Questions: 83

Buy Premium PDF

<https://dumpsarena.co>

[sales@dumpsarena.co](mailto:sales@dumpsarena.co)

[sales@dumpsarena.co](mailto:sales@dumpsarena.co)  
[dumpsarena.co](https://dumpsarena.co)

**QUESTION NO: 1**

The same security policy has been redundantly implemented as part of the service contracts for Web services A, B and

C. In order to reduce the effort of maintaining multiple redundant service policies, it has been decided to centralize policy enforcement across these three services. Which of the following industry standards will need to be used for Web services A, B and C in order for their service contracts to share the same security policy document?

A. WS-PolicyAttachment

B. WS-SecureConversation

C. In order to reduce the effort of maintaining multiple redundant service policies, it has been decided to centralize policy enforcement across these three services. Which of the following industry standards will need to be used for Web services A, B and C in order for their service contracts to share the same security policy document?

WS-Trust

D. WS-Security

**ANSWER: A****QUESTION NO: 2**

A service is designed to respond to an error condition by issuing a message containing detailed error information. This message includes connection information for a database that is shared by numerous services within the service inventory. An attacker intentionally sends an invalid message to the service in order to trigger an error and receive the connection information. The attacker then proceeds to connect to the database and issues a series of malicious SQL queries that make the database non-responsive. As a result, a number of services within the service inventory are disabled. Which of the following types of attacks were successfully carried out?

A. SQL injection attack

B. Exception generation attack

C. Denial of service attack

D. Buffer overrun attack

**ANSWER: B C**

**QUESTION NO: 3**

When designing XML schemas to avoid data-centric threats, which of the following are valid considerations?

- A. The maxOccurs attribute needs to be specified using a restrictive value.
- B. The element needs to be avoided.
- C. The element can be used to create more restrictive user-defined simple types.
- D. All of the above.

**ANSWER: B D****QUESTION NO: 4**

The use of parameterized expressions can help avoid which type of attack?

- A. XML parser attack
- B. Buffer overrun attack
- C. XPath injection attack
- D. Exception generation attack

**ANSWER: C****QUESTION NO: 5**

Service A is only authorized to access one service capability of Service B. Service B acts as a trusted subsystem for several underlying resources which it accesses using its own set of credentials. Service B can therefore not become a victim of an insufficient authorization attack initiated by Service A.

- A. True
- B. False

**ANSWER: B****QUESTION NO: 6**

An XML bomb attack and an XML external entity attack are both considered types of XML parser attacks.

- A. True
- B. False

**ANSWER: A**

#### QUESTION NO: 7

Which of the following statements regarding the usage of security tokens for authentication and authorization are true?

- A. Security tokens can be validated without resorting to pre-shared secrets.
- B. Security tokens issued by a token issuer in the same security domain can be used with a different token issuer in a different security domain in order to get access to services in that domain.
- C. Security token issuance and cancellation are done by the relying party.
- D. Security tokens can only be issued by a legitimate token issuer.

**ANSWER: A B**

#### QUESTION NO: 8

The application of the Service Loose Coupling principle does not relate to the use of security policies as part of service contracts.

- A. True
- B. False

**ANSWER: B**

#### QUESTION NO: 9

Service A contains reporting logic that collects statistical data from different sources in order to produce a report document. One of the sources is a Web service that exists outside of the organizational boundary. Some of Service A's service consumers are encountering slow response times and periods of unavailability when invoking Service

- A. While investigating the cause, it has been discovered that some of the messages received from the external Web service contain excessive data and links to files (that are not XML schemas or policies). What can be done to address this issue?

define cardinality in message schemas

- B.** correlate request and response messages across different services
- C.** use precompiled XPath expressions
- D.** avoid downloading XML schemas at runtime

**ANSWER: A D**

**QUESTION NO: 10**

Security policies defined using WS-SecurityPolicy can be used to convey which of the following requirements to a service consumer?

- A.** Whether transport-layer or message-layer security needs to be used
- B.** The encryption type that needs to be used for transport-layer security
- C.** The algorithms that need to be used for cryptographic operations
- D.** The type of security token that must be used

**ANSWER: A C D**