Free Questions for S90.19 by ebraindumps

Shared by Hodge on 29-01-2024

For More Free Questions and Preparation Resources

Check the Links on Last Page

Question 1

Question Type: MultipleChoice

An ESB is introduced into an IT enterprise, primarily to enable communication between a set of disparate Web services. As a first step, the ESB needs to be configured to carry out data model transformation in order to overcome differences in the XML schemas used by the Web services. However, the messages exchanged by the Web services need to be encrypted. What needs to be done in order for the ESB to enable communication between the Web services without compromising message confidentiality?

Options:

A- The messages need to be digitally signed instead of encrypted.

B- The ESB needs to be configured so that it can decrypt and encrypt messages.

C- The Web services need to be designed to support transport-layer security instead of message-layer security.

D- In this scenario, the ESB cannot enable communication between the Web services without compromising message confidentiality.

Answer:

B

Question 2

Question Type: MultipleChoice

Service A, residing outside the private network of an organization, provides logic that sanitizes message error information on behalf of other services that reside inside the private network, behind a firewall. Where is the vulnerability in this architecture?

Options:

A- There is no central management of error messages. Instead, policy enforcement points should be used so that all services are required to comply with a policy that states that any error message generated needs to be free of sensitive data.

B- The sanitization logic resides outside the private network. Therefore, if communication between Service A and the services within the private network is compromised, an attacker can get access to sensitive data from non-sanitized messages generated by services inside the private network.

C- There is no single sign-on mechanism in place, which puts all services (within and outside the private network) at risk.

D- None of the above.

Answer:

B

Question 3

Question Type: MultipleChoice

Which of the following statements is true?

Options:

A- When the maxOccurs attribute in an XML schema element is not specified it creates a security risk because attackers can specify this element multiple times.

B- When numeric ranges within an XML schema are not specified it creates a security risk because attackers can introduce very large numeric values within the message data.

C- When the xsd:any element is used within an XML schema it can introduce a security risk because it allows attackers to extend the schema.

D- All of above.

Answer:

D

Question 4

Question Type: **MultipleChoice**

The Message Screening pattern can be applied to a service acting as a trusted subsystem for an underlying database. That way, the database would be protected from SOL injection attacks.

Options:

A- True

B- False

Answer:

A

Question 5

Question Type: **MultipleChoice**

Service A accesses a legacy system. There is a requirement to secure Service A so that it can only be accessed by authorized service consumers. The current service architecture doesn't allow the delegation of service consumer credentials to the legacy system. Which pattern needs to be applied in order to fulfill this security requirement?

Options:

A- Brokered Authentication

B- Direct Authentication

C- Data Origin Authentication

D- None of the above.

Answer:

D

Question 6

Question Type: **MultipleChoice**

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

Options:

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 7

Question Type: MultipleChoice

Service A is part of a large service composition. Following an attack, Service A becomes non-responsive. Which of the following attacks could be responsible for Service A's non-responsiveness?

Options:

A- Buffer overrun attack

B- Exception generation attack

C- XML parser attack

D- None of the above.

Answer:

A, C