Vendor:F5

Exam Code:F50-536

Exam Name:BIG-IP ASM v10.x

Version: Demo

QUESTION 1

Which of the following mitigation techniques is based on anomaly detection? (Choose 2)

A. Brute force attack prevention

B. Cross-site request forgery prevention

C. Web scraping attack prevention

D. Parameter tampering prevention

Correct Answer: AC

QUESTION 2

On a BIG-IP ASM 3600, in standalone mode, which of the following pool configurations is valid?

A. Pool named vs_pool with 1 pool member, no persistence, and no load balancing method

B. Pool named vs_pool with 1 pool member, cookie persistence, and ratio load balancing method

C. Pool named vs_pool with 2 pool members, cookie persistence, and ratio load balancing method

D. Pool named vs_pool with 3 pool members, source IP persistence, and least connections load balancing method

Correct Answer: A

QUESTION 3

A user is building a security policy using the Deployment Wizard and the Rapid Deployment application template. By default, which settings will be applied to the security policy? (Choose 3)

A. Data Guard will be enabled.

B. The enforcement mode will be set to transparent.

C. The encoding language will be set to auto detect.

D. Wildcard tightening will be enabled on file types and parameters.

E. The Attack signature set applied will be Generic Detection Signatures.

Correct Answer: ABE

QUESTION 4

Which level of parameter assumes the highest precedence in BIG-IP ASM System processing logic?

A. Flow

B. Object

C. Global

D. URL

Correct Answer: A

QUESTION 5

Which of the following methods of protection are used by the BIG-IP ASM System to mitigate buffer overflow attacks?

A. HTTP RFC compliancy checks

B. Length restrictions and attack signatures

C. Length restrictions and site cookie compliancy checks

D. Meta-character enforcement and HTTP RFC compliancy check

Correct Answer: B

QUESTION 6

Sensitive parameters is a feature used to hide sensitive information from being displayed in which of the following?

A. Client request

B. Server response

C. GUI and logs of BIG-IP ASM System

D. Configuration file of BIG-IP ASM System

Correct Answer: C

QUESTION 7

A security audit has determined that your web application is vulnerable to a cross-site scripting attack. Which of the following measures are appropriate when building a security policy? (Choose 2)

A. Cookie length must be restricted to 1024 bytes.

B. Attack signature sets must be applied to any user input parameters.

C. Parameter data entered for explicit objects must be checked for minimum and maximum values.

D. Parameter data entered for flow-level parameters must allow some meta-characters but not others.

Correct Answer: BD

QUESTION 8

Which of the following statements are correct regarding positive and negative security models? (Choose 2)

A. Positive security model allows all transactions by default.

B. Negative security model denies all transactions by default.

C. Negative security model allows all transactions by default and rejects only transactions that contain attacks.

D. Positive security model denies all transactions by default and uses rules that allow only those transactions that are considered safe and valid.

Correct Answer: CD

QUESTION 9

Tightening is a feature of which type of entity?

A. Explicit URLs

B. Attack signatures

C. Flow login URLs

D. Wildcard parameters

Correct Answer: D

QUESTION 10

A request is sent to the BIG-IP ASM System that generates a Length error violation. Which of the following length types provides a valid learning suggestion? (Choose 3)

A. URL

B. Cookie

C. Response

D. POST data

E. Query string

Correct Answer: ADE

QUESTION 11

Flow login allows for more granular protection of login and logout URLs within web applications. Which of the following are components of flow login? (Choose 3)

A. Schema

B. Login URLs

C. Login pages

D. Attack signatures

E. Access validation

Correct Answer: BCE

QUESTION 12

Which of the following statements are correct regarding Attack signatures? (Choose 2)

A. Attack signatures can apply to requests, responses, and parameters.

B. Attack signatures are the basis for positive security logic with the BIG-IP ASM System.

C. Any new Attack signature downloaded manually or automatically will be active and assigned directly to the security policy.

D. Individual Attack signatures can be assigned to the security policy. Only Attack signature sets can apply to the security policy.Individual Attack signatures can? be assigned to the security policy. Only Attack signature sets can apply to the security policy.

Correct Answer: AD