DUMPSARENA

FCPFortiWeb 7.4 Administrator

Fortinet FCP_FWB_AD-7.4

Version Demo

Total Demo Questions: 2

Total Premium Questions: 23

Buy Premium PDF

https://dumpsarena.co

sales@dumpsarena.co

sales@dumpsarena.co
dumpsarena.co

Topic Break Down

Topic	No. of Questions
Topic 1, Deployment and configuration	5
Topic 2, Encryption and authentication	3
Topic 3, Web application security	13
Topic 4, API protection	1
Topic 5, System administration	1
Total	23

QUESTION NO: 1

An application uses hidden form fields to store the price and product identifier during a checkout workflow. The application does not adequately validate those values when the form is submitted.

Which FortiWeb feature is best suited to detect a client modifying the hidden form values?

A. Enable Hidden Fields protection in the HTTP protection profile.

B. Enable Cookie Security in the HTTP protection profile.

C. Create a URL access rule for the checkout URL.

D. Create a DoS prevention policy for the checkout URL.

ANSWER: A

Explanation:

Hidden Fields protection is designed to detect tampering with hidden form values between the response containing the form and the subsequent client submission. It is appropriate when the integrity of application workflow values must be maintained.

Cookie security protects cookies rather than HTML hidden fields. URL access controls determine whether a client can access a URL, but do not compare form values. DoS prevention addresses request volume and does not validate transaction parameters.

QUESTION NO: 2

An organization must grant its audit team access to FortiWeb logs and configuration information. The audit team must not be able to create, modify, or delete FortiWeb objects.

What is the most appropriate configuration?

A. Create a read-only administrator profile and assign it to the audit administrators.

B. Create a web authentication user group for the audit team.

C. Add the audit team addresses to a trusted IP list.

D. Create a server policy that permits access from the audit network.

ANSWER: A

Explanation:

Create an administrator profile that grants read-only permissions for the required FortiWeb functions, and assign that profile to the audit administrators. Administrator profiles control access to FortiWeb configuration and monitoring functions. A web authentication user group applies to users accessing protected web applications, not to FortiWeb administrative access. Restricting the audit team by trusted IP address or using a server policy does not provide the required permission separation.