

GIAC GWEB

GIAC Certified Web Application Defender

For More Information – Visit link below:

<https://www.examsempire.com/>

Product Version

- 1. Up to Date products, reliable and verified.**
- 2. Questions and Answers in PDF Format.**



<https://examsempire.com/>

Visit us at: <https://www.examsempire.com/gweb>

Latest Version: 6.0

Question: 1

What measures can be implemented to prevent CSRF attacks in web applications?

(Choose two)

Response:

- A. Using CAPTCHA for all form submissions
- B. Requiring re-authentication for sensitive transactions
- C. Allowing session tokens to be reused indefinitely
- D. Enforcing SameSite cookies for session management

Answer: B,D

Question: 2

Which of the following session management flaws can lead to session hijacking?

Response:

- A. Weak password policy
- B. Session tokens not being invalidated after logout
- C. The use of CAPTCHA
- D. Limiting login attempts

Answer: B

Question: 3

Which vulnerability allows an attacker to bypass the Same-Origin Policy and access restricted resources?

Response:

- A. SQL injection
- B. Cross-Origin Resource Sharing (CORS) misconfiguration
- C. Brute force attacks
- D. Directory traversal

Answer: B

Question: 4

What is the role of 'SameSite' cookie attribute in preventing CSRF attacks?

Response:

- A. It prevents cookies from being sent in cross-site requests
- B. It ensures cookies are only sent over HTTPS
- C. It isolates cookies to specific domain paths to prevent unauthorized access
- D. It encrypts cookies to prevent interception and tampering

Answer: A

Question: 5

Which technology is often used to enhance web performance but can also introduce security risks if not properly configured?

Response:

- A. WebSockets
- B. WebSockets
- C. HTTP/2
- D. WebRTC

Answer: A

Question: 6

Which technique is most effective in preventing SQL injection attacks?

Response:

- A. Client-side input validation
- B. Use of prepared statements and parameterized queries
- C. Encryption of all data entered by the user
- D. Limiting the length of input fields

Answer: B

Question: 7

Which protocol is commonly used to secure communications between web services?

Response:

- A. HTTPS
- B. SOAP
- C. XML-RPC
- D. REST

Answer: A

Question: 8

What are the key components of an HTTP request?
(Choose two)

Response:

- A. Request line
- B. URL scheme
- C. Response body
- D. Headers

Answer: A,D

Question: 9

When is it appropriate to use encryption over tokenization for protecting sensitive data?

Response:

- A. When the data needs to be processed or analyzed
- B. When there is no requirement for direct data retrieval
- C. When replacing data with a token suffices for processing
- D. When minimal changes to the existing system are preferred

Answer: A

Question: 10

Which of the following is an essential feature of a secure logging mechanism in a web application?

Response:

- A. Logging all user input verbatim
- B. Storing logs in a publicly accessible location for transparency
- C. Ensuring log integrity and confidentiality

D. Including sensitive user data for debugging purposes

Answer: C

Thank You for Trying Our Product

Special 16 USD Discount Coupon: NSZUBG3X

Email: support@examsempire.com

**Check our Customer Testimonials and ratings
available on every product page.**

Visit our website.

<https://examsempire.com/>