GIAC

GWEB
GIAC Certified Web Application Defender

Questions And Answers PDF Format:

For More Information – Visit link below:
https://www.certsgrade.com/

Version = Product

Latest Version: 6.0

Question: 1

Which practice is essential for maintaining security in web applications that handle serialization and deserialization?
Response:

A. Using the most efficient serialization library
B. Restricting serialized data to authenticated users
C. Monitoring the size of serialized data
D. Logging all serialization and deserialization operations

Answer: B

Question: 2

In a typical three-tier web application architecture, the _____ tier is responsible for processing business logic, performing computations, and making decisions.
Response:

A. Client
B. Presentation
C. Business Logic
D. Data

Answer: C

Question: 3

When configuring CORS policies, what considerations should be made to ensure security? (Choose Two)
Response:

A. Always set the Access-Control-Allow-Origin header to "*"
B. Validate the origin before sending back any CORS headers
C. Use withCredentials for sensitive cross-origin requests
D. Restrict the HTTP methods that can be used cross-origin

Answer: B,D

Question: 4

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: 5

Which of the following is an essential security practice for protecting a web service using SOAP?
Response:

A. Utilizing SOAP attachments for all confidential data exchanges
B. Employing WS-Security standards for message integrity and confidentiality
C. Restricting SOAP messages to less than 2KB to prevent buffer overflow attacks
D. Using only HTTP GET requests to simplify SOAP message handling

Answer: B

Question: 6

How does the use of third-party security services like Cloudflare or Akamai benefit web application security?
Response:

A. They provide outsourced content management systems
B. They offer distributed denial of service (DDoS) protection
C. They replace the need for web application firewalls
D. They offer free hosting services

Answer: B

Question: 7

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: 8

AJAX calls can be vulnerable to interception and manipulation. Which of the following is an effective countermeasure to secure AJAX calls?
Response:

A. Using simple HTTP authentication for AJAX requests
B. Implementing strong session management with secure tokens
C. Allowing cross-origin requests without restrictions
D. Employing GET requests for transferring sensitive information

Answer: B

Question: 9

What are effective proactive defense measures for a web application?
(Choose Two)
Response:

A. Deploying a web application firewall (WAF)
B. Implementing network-level DDoS protection
C. Conducting regular security awareness training
D. Using intrusion detection systems at the application layer

Answer: A,D

Question: 10

In the context of file uploads, what are two critical security checks to implement?
(Choose Two)
Response:

A. Verifying the file extension only

B. Checking the file MIME type against a whitelist

C. Ensuring the uploaded file is not executable on the server

D. Allowing all file types but scanning for size

Answer: B,C