



Vendor: GIAC

Exam Code: GWAPT

Exam Name: GIAC Web Application Penetration Tester

Version: DEMO

QUESTION 1

What tools are commonly used to test for Cross-Site Scripting vulnerabilities? (Choose two)

- A. Burp Suite
- B. Wireshark
- C. OWASP ZAP
- D. Metasploit

Answer: AC

QUESTION 2

What are key steps to prevent SQL injection attacks? (Choose two)

- A. Implementing input validation
- B. Disabling parameterized queries
- C. Restricting database user privileges
- D. Allowing unrestricted SQL queries

Answer: AC

QUESTION 3

What is the primary purpose of session management in web applications?

- A. To encrypt all transmitted data
- B. To maintain user state and track interactions with the application
- C. To ensure that only administrators can access the application
- D. To optimize application performance

Answer: B

QUESTION 4

You discover that a web application reflects user input in the URL. How can you confirm a Reflected XSS vulnerability?

- A. Inject `<script>alert('XSS')</script>` in the URL and observe browser behavior
- B. Perform SQL injection tests
- C. Reboot the web server
- D. Test all API endpoints

Answer: A

QUESTION 5

A web application uses AJAX for dynamic content updates but has no fallback for older browsers. What is the best course of action?

- A. Provide fallback mechanisms for non-AJAX-supported browsers
- B. Disable AJAX functionality entirely
- C. Use plain text responses instead of JSON
- D. Redirect users with older browsers to a different site

Answer: A

QUESTION 6

Which method is most effective in preventing SQL injection attacks?

- A. Using parameterized queries or prepared statements
- B. Hiding database error messages
- C. Encrypting the database
- D. Disabling SQL logging

Answer: A

QUESTION 7

Which of the following HTTP headers is often used to prevent CSRF attacks?

- A. X-CSRF-Token
- B. Content-Type
- C. User-Agent
- D. Authorization

Answer: A

QUESTION 8

During an automated scan with OWASP ZAP, you identify several potential XSS vulnerabilities. What is the best follow-up action?

- A. Manually validate each XSS finding
- B. Ignore the findings if there are no error messages
- C. Enable caching to enhance performance
- D. Decrypt the application's HTTPS traffic

Answer: A

QUESTION 9

Which of the following are common methods to mitigate Cross-Site Scripting (XSS) vulnerabilities? (Choose two)

- A. Input validation
- B. Disabling cookies
- C. Encoding special characters
- D. Encrypting data in transit

Answer: AC

QUESTION 10

Which of the following describes AJAX?

- A. A programming language used for web development
- B. A technique for updating parts of a webpage without refreshing the entire page
- C. A protocol used for encrypting web communications
- D. A tool for managing databases

Answer: B

QUESTION 11

During a web application test, you find that the application echoes back input provided in the "Search" field without sanitizing it. How would you test for a potential reflected XSS vulnerability?

- A. Inject `<script>alert('XSS')</script>` into the search field and observe the output
- B. Perform a SQL injection using `' OR 1=1 --`
- C. Attempt to brute-force the admin login page
- D. Flood the application with excessive HTTP requests

Answer: A

QUESTION 12

What are key defenses against credential stuffing attacks? (Choose two)

- A. Enforcing unique passwords across accounts
- B. Implementing multi-factor authentication (MFA)
- C. Encrypting all HTTP requests
- D. Avoiding logging user actions

Answer: AB

QUESTION 13

What are the key functionalities of OWASP ZAP? (Choose two)

- A. Automated vulnerability scanning
- B. Real-time HTTP request/response analysis
- C. Traffic encryption
- D. Firewall configuration

Answer: AB

QUESTION 14

What are key signs that an application might be vulnerable to SQL injection? (Choose two)

- A. Detailed error messages from the database
- B. Use of parameterized queries
- C. Allowing input directly into SQL statements
- D. Encryption of sensitive data

Answer: AC

Thank You for Trying Our Product

Lead2pass Certification Exam Features:

- ★ More than **99,900** Satisfied Customers Worldwide.
- ★ Average **99.9%** Success Rate.
- ★ **Free Update** to match latest and real exam scenarios.
- ★ **Instant Download** Access! No Setup required.
- ★ Questions & Answers are downloadable in **PDF** format and **VCE** test engine format.
- ★ Multi-Platform capabilities - **Windows, Laptop, Mac, Android, iPhone, iPod, iPad**.
- ★ **100%** Guaranteed Success or **100%** Money Back Guarantee.
- ★ **Fast**, helpful support **24x7**.



View list of all certification exams: <http://www.lead2pass.com/all-products.html>



Microsoft



ORACLE



CITRIX



JUNIPER
NETWORKS



EMC²
where information lives

10% Discount Coupon Code: ASTR14