



CERTSWARRIOR

GIAC GWAPT

GIAC Web Application Penetration Tester (GWAPT)

Questions&AnswersPDF

ForMoreInformation:

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

Features:

- 90DaysFreeUpdates
- 30DaysMoneyBackGuarantee
- InstantDownloadOncePurchased
- 24/7OnlineChat Support
- ItsLatestVersion

Latest Version: 6.1

Question: 1

Which tool is effective for analyzing JavaScript vulnerabilities in modern web applications?

Response:

- A. Nmap
- B. SonarQube
- C. OWASP ZAP
- D. OpenVAS

Answer: C

Question: 2

What type of SQL injection attack modifies a database without revealing the results to the attacker?

Response:

- A. Blind SQL injection
- B. Error-based SQL injection
- C. Union-based SQL injection
- D. Second-order SQL injection

Answer: A

Question: 3

What is the purpose of the "Content-Security-Policy" HTTP header?

Response:

- A. To enable directory browsing
- B. To enforce client-side encryption
- C. To restrict the sources of content that can be loaded by the browser
- D. To allow cross-origin resource sharing

Answer: C

Question: 4

A penetration test reveals that session cookies do not have the HttpOnly attribute set. What is the recommended mitigation?

Response:

- A. Add the HttpOnly attribute to all session cookies
- B. Add the HttpOnly attribute to all session cookies
- C. Store session data in local storage instead
- D. Set long expiration times for session cookies

Answer: A

Question: 5

Which of the following measures help mitigate SQL injection risks?
(Choose two)

Response:

- A. Using prepared statements with placeholders
- B. Hardcoding user credentials in queries
- C. Validating user inputs against a whitelist
- D. Displaying verbose error messages

Answer: A,C

Question: 6

A web application is suspected to have hidden directories and files. Which tool would you use to confirm their existence?

Response:

- A. Nikto
- B. SQLmap
- C. Burp Suite
- D. Dirb

Answer: D

Question: 7

What common configuration errors can expose sensitive data?
(Choose two)

Response:

- A. Storing sensitive data in plaintext
- B. Enabling the SameSite attribute for cookies
- C. Using outdated SSL/TLS protocols
- D. Implementing secure authentication mechanisms

Answer: A,C

Question: 8

During a security assessment, you find that verbose error messages are enabled. What is the immediate action you should recommend?

Response:

- A. Disabling verbose error messages and replacing them with generic ones
- B. Running additional port scans to identify vulnerabilities
- C. Disabling all authentication mechanisms
- D. Flooding the server with HTTP requests

Answer: A

Question: 9

Which features improve session security in web applications?

(Choose two)

Response:

- A. Use of short session expiration times
- B. Encryption of session data
- C. Allowing session reuse across multiple devices
- D. Hardcoding session tokens

Answer: A,B

Question: 10

Which tool is commonly used as a web application proxy for penetration testing?

Response:

- A. Burp Suite
- B. Nmap

- C. Wireshark
- D. Metasploit

Answer: A



CERTSWARRIOR

FULL PRODUCT INCLUDES:

Money Back Guarantee



Instant Download after Purchase



90 Days Free Updates



PDF Format Digital Download



24/7 Live Chat Support



Latest Syllabus Updates



For More Information – Visit link below:

<https://www.certswarrior.com>

16 USD Discount Coupon Code: U89DY2AQ