



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: 6.0

Question: 1

In a Reflected Cross-Site Scripting attack, where is the malicious payload executed?

Response:

- A. On the server-side database
- B. Within the victim's browser via an HTTP response
- C. As part of the network traffic analysis
- D. In the server's application logs

Answer: B

Question: 2

Which of the following tools can be used to perform reconnaissance on a web application?

(Choose two)

Response:

- A. Nmap
- B. Nikto
- C. MS Word
- D. Apache Log Viewer

Answer: A,B

Question: 3

You have identified that a web server discloses its software version in HTTP headers. What is the next logical step?

Response:

- A. Conduct a DoS attack against the server
- B. Search for vulnerabilities associated with the disclosed software version
- C. Perform brute-force attacks on user accounts
- D. Ignore the information

Answer: B

Question: 4

How can a web application developer prevent Reflected XSS vulnerabilities?

Response:

- A. By using client-side validation only
- B. By encrypting session cookies
- C. By encoding user input before displaying it
- D. By disabling JavaScript

Answer: C

Question: 5

During a penetration test, you find a login form vulnerable to CSRF. What is your next step?

Response:

- A. Test if session cookies are protected with the SameSite attribute
- B. Flood the login endpoint with requests
- C. Create a phishing attack against the login page
- D. Inject SQL commands into the login form

Answer: A

Question: 6

What are the outputs of performing a web application mapping process?

(Choose two)

Response:

- A. A flowchart of application functionality
- B. A report of missing patches
- C. A list of accessible URLs and endpoints
- D. A database schema

Answer: A,C

Question: 7

What are typical signs of a successful brute-force attack?

(Choose two)

Response:

- A. Increased CPU utilization
- B. Unauthorized access to restricted resources
- C. Repeated login failures in the logs
- D. Outdated SSL certificates

Answer: B,C

Question: 8

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

Response:

- 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: 9

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: 10

What practices help secure web application authentication mechanisms?

(Choose two)

Response:

- A. Using salted password hashes
- B. Enabling directory listing
- C. Limiting session timeout durations
- D. Using CAPTCHA for login forms

Answer: A,D



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