GIAC.GWAPT.v2026-07-04.q62

Exam Code:	GWAPT
Exam Name:	GIAC Web Application Penetration Tester GWAPT
Certification Provider:	GIAC
Free Question Number:	62
Version:	v2026-07-04
# of views:	102
# of Questions views:	653
https://www.freecram.net/torrent/GIAC.GWAPT.v2026-07-04.q62.html	

NEW QUESTION: 1
What actions help secure session management? (Choose two)
A. Disabling user authentication
B. Regenerating session IDs after login
C. Enabling the HttpOnly attribute for cookies
D. Using weak session identifiers
Answer: (SHOW ANSWER)

NEW QUESTION: 2
Which feature of Burp Suite allows modification of HTTP/HTTPS requests before sending them to the server?
A. Spider
B. Intruder
C. Repeater
D. Scanner
Answer: (SHOW ANSWER)

NEW QUESTION: 3
Which of the following are indicators of sensitive information leakage during reconnaissance? (Choose two)
A. Secure cookie settings
B. Debug messages in HTTP responses
C. Correct user credentials
D. Hardcoded credentials in source code
Answer: (SHOW ANSWER)

NEW QUESTION: 4

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

A. Ignore the findings if there are no error messages

B. Decrypt the application's HTTPS traffic

C. Manually validate each XSS finding

D. Enable caching to enhance performance

Answer: (SHOW ANSWER)

NEW QUESTION: 5

While testing a web application with Burp Suite, you identify that a specific parameter might be vulnerable to SQL injection. What should you do next?

A. Modify unrelated parameters in the same request

B. Block the server's IP to prevent exploitation

C. Use SQLmap to automate the exploitation of the parameter

D. Report the issue without further testing

Answer: (SHOW ANSWER)

NEW QUESTION: 6

What are common uses of cookies in web applications? (Choose two)

A. To maintain user sessions

B. To enforce strict password policies

C. To encrypt all HTTP traffic

D. To store user preferences

Answer: (SHOW ANSWER)

NEW QUESTION: 7

What actions can mitigate the risk of authentication bypass vulnerabilities? (Choose two)

A. Avoiding the use of CAPTCHA

B. Disabling all user accounts

C. Requiring strong password policies

D. Implementing two-factor authentication

Answer: (SHOW ANSWER)

NEW QUESTION: 8

Which of the following are examples of web application misconfigurations? (Choose two)

A. Implementation of multi-factor authentication

B. Strong password policies

C. Exposed default files and directories

D. Enabled verbose error messages

Answer: (SHOW ANSWER)

NEW QUESTION: 9
Which technique is commonly used to identify active services running on a web server?
A. Creating phishing emails
B. Port scanning
C. Exploiting stored XSS vulnerabilities
D. Brute-forcing login credentials
Answer: (SHOW ANSWER)

NEW QUESTION: 10
Which of the following is a common indicator of a SQL injection vulnerability?
A. Error messages displaying database information
B. A missing Content-Security-Policy header
C. Directory listing enabled
D. Slow application response times
Answer: (SHOW ANSWER)

NEW QUESTION: 11
Which of the following measures help mitigate SQL injection risks? (Choose two)
A. Validating user inputs against a whitelist
B. Using prepared statements with placeholders
C. Displaying verbose error messages
D. Hardcoding user credentials in queries
Answer: (SHOW ANSWER)

NEW QUESTION: 12
What information can be gathered using the WHOIS lookup service?
A. Encrypted session tokens
B. Passwords of the web server administrator
C. Details of the application database schema
D. DNS records and email addresses of domain administrators
Answer: (SHOW ANSWER)

NEW QUESTION: 13
Which techniques help mitigate XSS vulnerabilities? (Choose two)
A. Output encoding
B. Enabling FTP
C. Avoiding use of HTML
D. Input validation
Answer: (SHOW ANSWER)

NEW QUESTION: 14

Which HTTP header is MOST effective at mitigating clickjacking attacks?
A. X-Frame-Options
B. Strict-Transport-Security
C. Content-Type
D. Set-Cookie
Answer: A (LEAVE A REPLY)

NEW QUESTION: 15
Which header is commonly used to prevent Cross-Site Request Forgery attacks?
A. Content-Type
B. Accept-Encoding
C. X-CSRF-Token
D. User-Agent
Answer: (SHOW ANSWER)

NEW QUESTION: 16
A web application does not log users out after a period of inactivity. What is the best way to address this issue?
A. Allow unlimited session durations for trusted users
B. Implement automatic session timeout policies
C. Require re-authentication every minute
D. Disable user sessions altogether
Answer: (SHOW ANSWER)

NEW QUESTION: 17
What is the primary role of a web server in web applications?
A. To encrypt data transmitted over the network
B. To store and deliver content such as HTML, CSS, and JavaScript files
C. To provide backend logic for user requests
D. To manage client-side user sessions
Answer: (SHOW ANSWER)

NEW QUESTION: 18
During a penetration test, you find a login form vulnerable to CSRF. What is your next step?
A. Inject SQL commands into the login form
B. Test if session cookies are protected with the SameSite attribute
C. Create a phishing attack against the login page
D. Flood the login endpoint with requests
Answer: (SHOW ANSWER)

NEW QUESTION: 19
What is credential stuffing?
A. Injecting SQL commands into login fields
B. Forcing a server reboot through unauthorized commands
C. Exploiting buffer overflow vulnerabilities
D. Using stolen credentials from one breach to log into another system
Answer: (SHOW ANSWER)

NEW QUESTION: 20
Which tools are effective for discovering XSS vulnerabilities? (Choose two)
A. OWASP ZAP
B. Nikto
C. Wireshark
D. Burp Suite
Answer: (SHOW ANSWER)

NEW QUESTION: 21
Which of the following are common session management vulnerabilities? (Choose two)
A. Random session ID generation
B. Use of encrypted session cookies
C. Session IDs stored in URLs
D. Lack of session timeout policies
Answer: (SHOW ANSWER)

NEW QUESTION: 22
What are key defenses against credential stuffing attacks? (Choose two)
A. Encrypting all HTTP requests
B. Implementing multi-factor authentication (MFA)
C. Avoiding logging user actions
D. Enforcing unique passwords across accounts
Answer: (SHOW ANSWER)

NEW QUESTION: 23

During reconnaissance, you discover that the web application's /admin directory is exposed. What would you do next?

A. Attempt to log in using default credentials

B. Run a port scan on the server

C. Flood the /admin directory with HTTP requests

D. Monitor application uptime

Answer: (SHOW ANSWER)

NEW QUESTION: 24

What are key objectives of mapping a web application? (Choose two)

A. Identifying all available pages and endpoints

B. Encrypting user credentials

C. Discovering potential input fields

D. Reducing server downtime

Answer: (SHOW ANSWER)

NEW QUESTION: 25

What is the primary purpose of web application testing tools?

A. To create user-friendly web application interfaces

B. To detect physical vulnerabilities in network cables

C. To enhance application load times

D. To identify and exploit vulnerabilities in web applications

Answer: (SHOW ANSWER)

NEW QUESTION: 26

Which vulnerability occurs when user input is returned in an HTTP response without proper encoding?

A. CSRF

B. Reflected XSS

C. SQL Injection

D. Command Injection

Answer: (SHOW ANSWER)

NEW QUESTION: 27

Which methods help prevent session fixation attacks? (Choose two)

A. Enabling directory listing

B. Allowing password reuse

C. Regenerating session IDs after login

D. Setting cookies with the Secure flag

Answer: (SHOW ANSWER)

NEW QUESTION: 28
Which of the following is a common misconfiguration in web applications?
A. Disabling directory browsing
B. Implementing input validation
C. Default or weak administrator credentials
D. Use of HTTPS
Answer: (SHOW ANSWER)

NEW QUESTION: 29
What does HTTPS provide that HTTP does not?
A. Support for dynamic web pages
B. Faster data transmission
C. Encryption and secure communication
D. Automatic session management
Answer: (SHOW ANSWER)

NEW QUESTION: 30
What are common indicators of a CSRF attack? (Choose two)
A. Unusual administrative actions performed without user consent
B. Unauthorized password changes
C. Frequent timeout errors in the web application
D. Disconnected user sessions
Answer: A,B (LEAVE A REPLY)

NEW QUESTION: 31
What are typical signs of a successful brute-force attack? (Choose two)
A. Increased CPU utilization
B. Repeated login failures in the logs
C. Unauthorized access to restricted resources
D. Outdated SSL certificates
Answer: (SHOW ANSWER)

NEW QUESTION: 32
Which tool is commonly used for mapping the structure of a web application?
A. Metasploit
B. Burp Suite
C. Nessus
D. Wireshark
Answer: (SHOW ANSWER)

NEW QUESTION: 33
Which tool is commonly used as a web application proxy for penetration testing?
A. Wireshark
B. Metasploit
C. Burp Suite
D. Nmap
Answer: (SHOW ANSWER)

NEW QUESTION: 34
Which attribute of cookies helps prevent Cross-Site Scripting (XSS) attacks?
A. Path
B. Domain
C. SameSite
D. Secure
Answer: (SHOW ANSWER)

NEW QUESTION: 35
What tools are commonly used to test for Cross-Site Scripting vulnerabilities? (Choose two)
A. OWASP ZAP
B. Wireshark
C. Metasploit
D. Burp Suite
Answer: (SHOW ANSWER)

NEW QUESTION: 36
Which features are available in automated web application testing tools? (Choose two)
A. Automated exploitation of discovered flaws
B. Passive scanning for vulnerabilities
C. Secure credential storage
D. Logging of HTTP/HTTPS traffic
Answer: (SHOW ANSWER)

NEW QUESTION: 37

What is a potential consequence of improper session management?
A. Improved user experience
B. Reduced bandwidth usage
C. Unauthorized access to user accounts
D. Faster application load times
Answer: C (LEAVE A REPLY)

NEW QUESTION: 38
Which HTTP header helps prevent browsers from loading a page in a frame to mitigate clickjacking attacks?
A. Strict-Transport-Security
B. Content-Security-Policy
C. X-Frame-Options
D. X-XSS-Protection
Answer: (SHOW ANSWER)

NEW QUESTION: 39
A web application you are testing uses HTTP instead of HTTPS for login pages. What should you recommend?
A. Block all user login attempts until the issue is resolved
B. Implement HTTPS with SSL/TLS encryption
C. Implement IP restrictions for login access
D. Use CAPTCHA to secure the login form
Answer: B (LEAVE A REPLY)

NEW QUESTION: 40
What is the primary purpose of session management in web applications?
A. To optimize application performance
B. To ensure that only administrators can access the application
C. To maintain user state and track interactions with the application
D. To encrypt all transmitted data
Answer: (SHOW ANSWER)

NEW QUESTION: 41
Which HTTP response codes indicate successful requests? (Choose two)
A. 200
B. 403
C. 201
D. 301
Answer: A,C (LEAVE A REPLY)

NEW QUESTION: 42
A web application you are testing has directory listing enabled, exposing sensitive files. What should you recommend to mitigate this?
A. Enable verbose error logging
B. Restrict administrative access to internal users only
C. Increase the server timeout threshold
D. Disable directory listing in the web server configuration
Answer: D (LEAVE A REPLY)

NEW QUESTION: 43
Which actions help secure configuration settings in web applications? (Choose two)
A. Allowing all file uploads
B. Enabling verbose logging for all users
C. Disabling directory listing
D. Using secure default settings
Answer: (SHOW ANSWER)

NEW QUESTION: 44
You have identified that a web server discloses its software version in HTTP headers. What is the next logical step?
A. Perform brute-force attacks on user accounts
B. Conduct a DoS attack against the server
C. Ignore the information
D. Search for vulnerabilities associated with the disclosed software version
Answer: (SHOW ANSWER)

NEW QUESTION: 45
What is a SQL injection attack?
A. Exploiting buffer overflows in application code
B. Injecting malicious SQL code into a query to manipulate a database
C. Exploiting user sessions to hijack accounts
D. Using DNS spoofing to redirect users to malicious websites
Answer: (SHOW ANSWER)

NEW QUESTION: 46
What is the primary purpose of a Cross-Site Request Forgery (CSRF) attack?
A. To steal session cookies through a client-side script
B. To trick a victim into performing unwanted actions on a trusted website
C. To inject malicious SQL commands into a database
D. To exploit authentication bypass vulnerabilities
Answer: (SHOW ANSWER)

NEW QUESTION: 47
In a Reflected Cross-Site Scripting attack, where is the malicious payload executed?
A. In the server's application logs
B. As part of the network traffic analysis
C. On the server-side database
D. Within the victim's browser via an HTTP response
Answer: (SHOW ANSWER)

NEW QUESTION: 48
Which configurations can help enhance web application security? (Choose two)
A. Disabling caching for all pages
B. Restricting IP addresses that can access admin portals
C. Enabling error message logging
D. Setting file permissions to restrict access
Answer: (SHOW ANSWER)

NEW QUESTION: 49
Which mechanisms can help prevent brute-force attacks on login pages? (Choose two)
A. Implementing CAPTCHAs
B. Enforcing account lockout policies
C. Storing passwords in plaintext
D. Disabling HTTPS
Answer: A,B (LEAVE A REPLY)

NEW QUESTION: 50
Which web technologies are considered part of a web application frontend? (Choose two)
A. CSS
B. PHP
C. HTML
D. Python
Answer: (SHOW ANSWER)

NEW QUESTION: 51
You discover that the web server is using an outdated version of Apache with known vulnerabilities. What should you recommend?
A. Update the Apache server to the latest version
B. Disable HTTPS on the server
C. Configure directory listing for better visibility
D. Ignore the issue if no active attacks are detected
Answer: (SHOW ANSWER)

NEW QUESTION: 52
What are key practices to prevent session fixation attacks? (Choose two)
A. Regenerating session IDs after user authentication
B. Implementing session expiration policies
C. Forcing users to use fixed session IDs
D. Allowing session reuse without revalidation
Answer: (SHOW ANSWER)

NEW QUESTION: 53
While reviewing a web application, you find a comment field vulnerable to stored XSS. How should this be remediated?
A. Use HTTPS for communication
B. Increase the session timeout
C. Block all user inputs
D. Sanitize all input and encode it before rendering in the browser
Answer: (SHOW ANSWER)

NEW QUESTION: 54
Which measures can prevent session hijacking? (Choose two)
A. Using HTTPS for secure communication
B. Implementing multi-factor authentication
C. Allowing cookies to be sent in plaintext
D. Allowing users to log in multiple times simultaneously
Answer: (SHOW ANSWER)

NEW QUESTION: 55
What is the primary purpose of HTTP in web applications?
A. To provide authentication for web applications
B. To facilitate communication between a web browser and a server
C. To store cookies securely
D. To encrypt data during transmission

Answer: (SHOW ANSWER)

NEW QUESTION: 56
Which encoding method should be used to safely display user input in HTML content?
A. Hex encoding
B. Base64 encoding
C. URL encoding
D. HTML entity encoding
Answer: (SHOW ANSWER)

NEW QUESTION: 57
What are key features of HTTPS? (Choose two)
A. It encrypts communication between a client and a server
B. It authenticates the identity of the web server
C. It uses the HTTP/3 protocol for faster connections
D. It allows users to bypass firewalls
Answer: (SHOW ANSWER)

NEW QUESTION: 58
What is the purpose of account lockout policies?
A. To encrypt user credentials
B. To log user activities
C. To prevent session hijacking
D. To protect against brute-force attacks by limiting login attempts
Answer: (SHOW ANSWER)

NEW QUESTION: 59
What is the primary goal of a SQL injection attack?
A. To manipulate URL parameters
B. To encrypt database records
C. To bypass authentication mechanisms and access sensitive data
D. To inject malicious scripts into a web page
Answer: (SHOW ANSWER)

NEW QUESTION: 60
During an assessment, you discover that a web application does not compress large files before sending them to the client. What is the best recommendation to improve performance?

A. Store the files in a database
B. Implement HTTPS encryption for all file transfers
C. Block large file requests
D. Enable Gzip compression on the web server

Answer: (SHOW ANSWER)

NEW QUESTION: 61
Which HTTP method is used to retrieve data from a server?
A. PUT
B. GET
C. DELETE
D. POST
Answer: (SHOW ANSWER)

NEW QUESTION: 62
Which type of Cross-Site Scripting (XSS) attack occurs when malicious input is stored on the target server?
A. Blind XSS
B. DOM-based XSS
C. Persistent XSS
D. Reflected XSS
Answer: C (LEAVE A REPLY)

Valid GWAPT Dumps shared by EduDump.com for Helping Passing GWAPT Exam! EduDump.com now offer the **newest GWAPT exam dumps**, the EduDump.com GWAPT exam **questions have been updated** and **answers have been corrected** get the **newest** EduDump.com GWAPT dumps with Test Engine here: https://www.edudump.com/exams/GIAC/GWAPT/premium/ (**143** Q&As Dumps, **35%OFF** **Special Discount Code: freecram**)