PrepAwayPDF

ONLINE TEST ENGINE

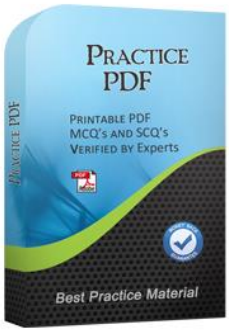
- Online Tool, Convenient, easy to study.
- Practice Online Anytime
- Instant Online Access
- Test History and Performance Review
- Supports All Web Browsers
- Supports Windows / Mac / Android / iOS, etc.

Online Test Engine

DESKTOP TEST ENGINE

- Installable Software Application
- Supports MS Operating System
- Simulates Real Exam Environment
- Two Modes For Practice
- Builds Exam Confidence
- Practice Offline Anytime

Desktop Test Engine



PDF PRACTICE Q&A'S

- Printable PDF Format
- Study Anywhere, Anytime
- Prepared by IT Experts
- 365 Days Free Updates
- Instant Access to Download
- Free PDF Demo Available

PDF Practice Q&A's

60920	59520	59062	59146
Demo Downloads	Successfull Cases	Satisfied Clients	The number of consulting

http://www.prepawaypdf.com/

Best Professional Test Guide Help You Pass and Provide Safe Shopping

Exam : **GWAPT**

Title : GIAC Web Application Penetration Tester GWAPT

Vendor : GIAC

Version : DEMO

NO.1 Which HTTP response codes indicate successful requests? (Choose two)
A. 200
B. 301
C. 403
D. 201
Answer: AD

NO.2 What techniques can attackers use in SQL injection attacks? (Choose two)
A. Bypassing login forms
B. Injecting malicious SQL into query strings
C. Exploiting DNS caching mechanisms
D. Using buffer overflow vulnerabilities
Answer: AB

NO.3 Which testing methods are supported by fuzzing tools? (Choose two)
A. Identifying buffer overflow vulnerabilities
B. Brute force attacks
C. Validating secure encryption algorithms
D. Input randomization
Answer: A,D

NO.4 What common configuration errors can expose sensitive data? (Choose two)
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C. Using outdated SSL/TLS protocols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: AC

NO.5 What are key features of HTTPS? (Choose two)
A. It encrypts communication between a client and a server
B. It uses the HTTP/3 protocol for faster connections
C. It authenticates the identity of the web server
D. It allows users to bypass firewalls
Answer: AC

NO.6 Which of the following is a common indicator of a credential stuffing attack?
A. Sudden server crashes
B. Repeated login attempts from various IP addresses
C. Large volumes of outgoing email
D. Unauthorized access to application logs
Answer: B

NO.7 Which tool is effective for analyzing JavaScript vulnerabilities in modern web applications?

A. Nmap
B. SonarQube
C. OWASP ZAP
D. OpenVAS
Answer: C

NO.8 What is the primary goal of a Cross-Site Request Forgery (CSRF) attack?
A. Execute JavaScript in a victim's browser
B. Steal session cookies
C. Force a victim to perform an unwanted action
D. Gain shell access to the server
Answer: C

NO.9 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

NO.10 Which of the following is a common indicator of a SQL injection vulnerability?
A. Error messages displaying database information
B. Slow application response times
C. A missing Content-Security-Policy header
D. Directory listing enabled
Answer: A

NO.11 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

NO.12 Which methods are commonly used to detect XSS vulnerabilities? (Choose two)
A. Manual code review
B. Sending crafted payloads in user input fields
C. Hashing sensitive data
D. Encrypting cookies
Answer: AB

NO.13 What practices help secure web application authentication mechanisms? (Choose two)
A. Using salted password hashes

B. Enabling directory listing
C. Limiting session timeout durations
D. Using CAPTCHA for login forms
Answer: AD

NO.14 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