Sure! Here’s a set of 100 advanced multiple-choice questions (MCQs) on web application penetration testing, including OWASP Top 10 vulnerabilities and other relevant topics. I've bolded the correct options for you.

Web Application Penetration Testing MCQs

1. What does OWASP stand for?
- A) Open Web Application Security Project
- B) Online Web Application Security Protocol
- C) Open Web Application Security Program
- D) Online Web Application Security Project
- **A) Open Web Application Security Project**

2. Which of the following is the most critical vulnerability according to OWASP Top 10?
- A) Cross-Site Scripting (XSS)
- B) SQL Injection
- C) Insecure Deserialization
- D) Broken Authentication
- **B) SQL Injection**

3. What type of attack can allow an attacker to execute arbitrary scripts in a user's browser?
- A) SQL Injection
- B) Cross-Site Scripting (XSS)
- C) CSRF
- D) Directory Traversal
- **B) Cross-Site Scripting (XSS)**

4. Which OWASP Top 10 category deals with insecure data storage?
- A) Security Misconfiguration

- B) Sensitive Data Exposure
- C) Insufficient Logging & Monitoring
- D) Broken Access Control
- **B) Sensitive Data Exposure**

5. What is the primary purpose of a Web Application Firewall (WAF)?
- A) To encrypt data
- B) To filter and monitor HTTP traffic
- C) To perform load balancing
- D) To authenticate users
- **B) To filter and monitor HTTP traffic**

6. What vulnerability allows an attacker to execute commands on a server through a web application?
- A) Command Injection
- B) XML Injection
- C) CSRF
- D) Cross-Site Scripting (XSS)
- **A) Command Injection**

7. Which of the following is a common method for preventing SQL Injection attacks?
- A) Using dynamic SQL
- B) Validating user input
- C) Using stored procedures
- D) Both B and C
- **D) Both B and C**

8. In the context of web applications, what does CSRF stand for?
- A) Cross-Site Resource Forgery
- B) Cross-Site Request Forgery

- C) Client-Side Resource Forgery
- D) Client-Side Request Forgery
- **B) Cross-Site Request Forgery**

9. What kind of attack is SQL Injection?
- A) A network attack
- B) A web-based attack
- C) A social engineering attack
- D) A denial-of-service attack
- **B) A web-based attack**

10. Which HTTP header can help prevent XSS attacks by specifying trusted sources for scripts?
- A) Content-Security-Policy
- B) X-Frame-Options
- C) X-Content-Type-Options
- D) Strict-Transport-Security
- **A) Content-Security-Policy**

11. What is the purpose of using HTTPS in web applications?
- A) To improve speed
- B) To enhance usability
- C) To secure data in transit
- D) To allow caching
- **C) To secure data in transit**

12. Which of the following describes a "Broken Authentication" vulnerability?
- A) Insecurely storing passwords
- B) Exposing sensitive data
- C) Weak session management

- D) All of the above
- **D) All of the above**

13. Which attack involves sending unauthorized commands to an application to manipulate its behavior?
- A) XSS
- B) CSRF
- C) Command Injection
- D) Path Traversal
- **C) Command Injection**

14. The OWASP Top 10 is updated every:
- A) Year
- B) 18 months
- C) 3 years
- D) 5 years
- **B) 18 months**

15. What type of vulnerability does "Insecure Direct Object Reference" (IDOR) represent?
- A) Authentication vulnerability
- B) Access control vulnerability
- C) Injection vulnerability
- D) Configuration vulnerability
- **B) Access control vulnerability**

16. Which of the following is NOT a type of Cross-Site Scripting (XSS)?
- A) Reflected XSS
- B) Stored XSS
- C) DOM-based XSS
- D) Executed XSS

- **D) Executed XSS**

17. What is the main goal of a penetration test?
  - A) To destroy data
  - B) To assess the security of an application
  - C) To test user interface
  - D) To enhance performance
  - **B) To assess the security of an application**

18. Which vulnerability allows attackers to bypass security measures by exploiting a weak authentication mechanism?
  - A) Security Misconfiguration
  - B) Broken Authentication
  - C) Sensitive Data Exposure
  - D) Insufficient Logging
  - **B) Broken Authentication**

19. What does "Sensitive Data Exposure" primarily address?
  - A) Improper logging
  - B) Insufficient encryption
  - C) Cross-Site Scripting
  - D) User access control
  - **B) Insufficient encryption**

20. Which of the following methods can be used to prevent CSRF attacks?
  - A) Use of CAPTCHA
  - B) Implementing Anti-CSRF tokens
  - C) Enforcing HTTPS
  - D) Both B and C
  - **D) Both B and C**

21. What is the purpose of a session hijacking attack?
  - A) To alter session timeouts
  - B) To steal user credentials
  - C) To take over a user's session
  - D) To corrupt session cookies
  - **C) To take over a user's session**

22. Which of the following is an example of a logic flaw?
  - A) SQL Injection
  - B) Cross-Site Scripting
  - C) Privilege escalation
  - D) Directory Traversal
  - **C) Privilege escalation**

23. What is the role of input validation in web security?
  - A) To reduce response time
  - B) To authenticate users
  - C) To ensure that only valid data is processed
  - D) To encrypt sensitive data
  - **C) To ensure that only valid data is processed**

24. Which of the following headers helps prevent Clickjacking?
  - A) Content-Security-Policy
  - B) X-Frame-Options
  - C) X-Content-Type-Options
  - D) Referrer-Policy
  - **B) X-Frame-Options**

25. The use of default credentials in a web application is a common example of:
  - A) Security Misconfiguration
  - B) Sensitive Data Exposure
  - C) Injection flaw
  - D) Insufficient Logging
  - **A) Security Misconfiguration**

26. What kind of attack is typically mitigated by validating all user input?
  - A) DoS attacks
  - B) SQL Injection
  - C) Phishing attacks
  - D) Man-in-the-Middle attacks
  - **B) SQL Injection**

27. Which of the following can be considered a part of a web application security framework?
  - A) Regular security audits
  - B) Secure coding practices
  - C) Threat modeling
  - D) All of the above
  - **D) All of the above**

28. What type of attack does a Directory Traversal vulnerability allow?
  - A) Data injection
  - B) Unauthorized file access
  - C) Denial of Service
  - D) Session fixation
  - **B) Unauthorized file access**

29. In web application security, what does the term "black-box testing" refer to?

- A) Testing with source code access
- B) Testing without any prior knowledge of the application
- C) Testing from a user's perspective only
- D) Testing only the database
- **B) Testing without any prior knowledge of the application**

30. Which of the following is a common method to secure sensitive data at rest?
  - A) Using firewalls
  - B) Data encryption
  - C) User authentication
  - D) Regular updates
  - **B) Data encryption**

31. What is a common consequence of an XSS attack?
  - A) Data loss
  - B) Theft of cookies
  - C) Network downtime
  - D) All of the above
  - **B) Theft of cookies**

32. Which vulnerability occurs when a web application exposes data it should not?
  - A) Cross-Site Scripting
  - B) Sensitive Data Exposure
  - C) SQL Injection
  - D) Cross-Site Request Forgery
  - **B) Sensitive Data Exposure**

33. Which of the following is NOT a part of the OWASP Top 10?
  - A) Insufficient Logging

- B) XML External Entities (XXE)
- C) Unvalidated Redirects and Forwards
- **D) Network Misconfiguration

Certainly! Here’s the continuation of the advanced MCQs on web application penetration testing:

34. Which of the following is NOT a part of the OWASP Top 10?
- A) Insufficient Logging
- B) XML External Entities (XXE)
- C) Unvalidated Redirects and Forwards
- D) Network Misconfiguration
- **D) Network Misconfiguration**

35. Which technique is often used to exploit the "Cross-Site Request Forgery" (CSRF) vulnerability?
- A) Cookie theft
- B) Malicious JavaScript
- C) Malicious form submissions
- D) Session hijacking
- **C) Malicious form submissions**

36. What is the main purpose of threat modeling in web application security?
- A) To identify potential vulnerabilities
- B) To fix existing bugs
- C) To encrypt sensitive data
- D) To enhance user experience
- **A) To identify potential vulnerabilities**

37. What is the impact of "Insecure Deserialization"?
  - A) Denial of service
  - B) Data leakage
  - C) Remote code execution
  - D) User impersonation
  - **C) Remote code execution**

38. Which of the following is a common tool used for web application penetration testing?
  - A) Wireshark
  - B) Burp Suite
  - C) Nmap
  - D) Metasploit
  - **B) Burp Suite**

39. Which vulnerability is characterized by a lack of proper access controls allowing unauthorized users to access restricted resources?
  - A) SQL Injection
  - B) Broken Access Control
  - C) Security Misconfiguration
  - D) Cross-Site Scripting
  - **B) Broken Access Control**

40. What type of malware can be used in an SQL Injection attack to extract sensitive data?
  - A) Trojans
  - B) Worms
  - C) Bots
  - D) Ransomware
  - **A) Trojans**

41. In terms of web security, what does the acronym "SSL" stand for?

- A) Secure Socket Layer
- B) Secure Security Layer
- C) Secure Software Layer
- D) Secure Service Layer
- **A) Secure Socket Layer**

42. Which of the following can be used to enforce strong authentication mechanisms in web applications?
  - A) Multi-Factor Authentication (MFA)
  - B) Basic Authentication
  - C) Plain-text passwords
  - D) Session cookies
  - **A) Multi-Factor Authentication (MFA)**

43. What is a common result of a successful session fixation attack?
  - A) User data encryption
  - B) User account takeover
  - C) Data loss
  - D) Unauthorized access to APIs
  - **B) User account takeover**

44. What is the primary method for preventing SQL Injection in modern web applications?
  - A) Using ORM (Object-Relational Mapping) frameworks
  - B) Using database-level permissions
  - C) Relying on input sanitization
  - D) Implementing strong passwords
  - **A) Using ORM (Object-Relational Mapping) frameworks**

45. Which of the following best describes a "Man-in-the-Middle" (MitM) attack?
  - A) Direct access to the database

  - B) Intercepting and altering communication
  - C) Attacking client-side applications
  - D) Social engineering attacks
  - **B) Intercepting and altering communication**

46. What technique can be used to mitigate XSS attacks?
  - A) Content Security Policy (CSP)
  - B) HSTS
  - C) Tokenization
  - D) Input sanitation
  - **A) Content Security Policy (CSP)**

47. Which of the following attacks involves an attacker tricking a user into submitting a request that they did not intend to?
  - A) SQL Injection
  - B) Cross-Site Request Forgery (CSRF)
  - C) Session Fixation
  - D) Path Traversal
  - **B) Cross-Site Request Forgery (CSRF)**

48. What kind of attack can be prevented by using the "SameSite" cookie attribute?
  - A) SQL Injection
  - B) Cross-Site Scripting
  - C) Cross-Site Request Forgery
  - D) Directory Traversal
  - **C) Cross-Site Request Forgery**

49. What is the primary purpose of logging in web applications?
  - A) To enhance user experience
  - B) To improve application performance

  - C) To monitor for suspicious activity
  - D) To enable data caching
  - **C) To monitor for suspicious activity**

50. Which of the following is a common practice to enhance password security?
  - A) Storing passwords in plain text
  - B) Using hashing algorithms
  - C) Allowing short passwords
  - D) Using predictable patterns
  - **B) Using hashing algorithms**

51. What vulnerability type is associated with allowing user input in file paths?
  - A) Cross-Site Scripting
  - B) Path Traversal
  - C) SQL Injection
  - D) XML Injection
  - **B) Path Traversal**

52. What does the acronym "XSS" stand for in web security?
  - A) Cross-Site Scripting
  - B) Cross-Site Security
  - C) Cross-Site Session
  - D) Cross-Origin Security
  - **A) Cross-Site Scripting**

53. Which of the following is an example of an insecure configuration?
  - A) Secure SSL certificates
  - B) Default settings unchanged
  - C) Proper user permissions

- D) Encrypted databases
- **B) Default settings unchanged**

54. Which technique can be used to exploit an XXE (XML External Entity) vulnerability?
  - A) Data injection
  - B) File inclusion
  - C) Remote file access
  - D) All of the above
  - **D) All of the above**

55. Which of the following is a consequence of weak session management?
  - A) Improved security
  - B) User data loss
  - C) Account takeover
  - D) Enhanced performance
  - **C) Account takeover**

56. What is the primary risk of using third-party libraries in web applications?
  - A) Increased application speed
  - B) Potential vulnerabilities in the libraries
  - C) Better functionality
  - D) Enhanced user experience
  - **B) Potential vulnerabilities in the libraries**

57. In web security, what does "salt" refer to?
  - A) A security protocol
  - B) Random data added to passwords before hashing
  - C) A type of encryption
  - D) A security framework

- **B) Random data added to passwords before hashing**

58. What is the function of "input sanitization"?
  - A) To store user data securely
  - B) To remove harmful characters from user input
  - C) To enhance user interface
  - D) To speed up application performance
  - **B) To remove harmful characters from user input**

59. What does the term "session timeout" refer to?
  - A) Time taken to establish a session
  - B) Duration before a session becomes inactive
  - C) Time taken to log a user out
  - D) Maximum duration for user authentication
  - **B) Duration before a session becomes inactive**

60. Which of the following is a way to protect against SQL Injection attacks?
  - A) Disabling error messages
  - B) Input validation and parameterized queries
  - C) Using GET requests
  - D) Allowing users to execute raw SQL
  - **B) Input validation and parameterized queries**

61. What is the purpose of the "HTTPOnly" flag in cookies?
  - A) To restrict cookies to secure connections
  - B) To prevent client-side scripts from accessing cookies
  - C) To limit cookie size
  - D) To enable cross-domain access
  - **B) To prevent client-side scripts from accessing cookies**

62. Which vulnerability can allow an attacker to redirect users to malicious sites?
  - A) SQL Injection
  - B) Open Redirect
  - C) Cross-Site Scripting
  - D) Cross-Site Request Forgery
  - **B) Open Redirect**

63. What is the primary risk associated with "Insufficient Logging and Monitoring"?
  - A) Data encryption failure
  - B) Inability to detect security incidents
  - C) Slower application performance
  - D) User access issues
  - **B) Inability to detect security incidents**

64. Which type of attack allows an attacker to read arbitrary files on the server?
  - A) SQL Injection
  - B) Directory Traversal
  - C) Cross-Site Scripting
  - D) XML External Entity (XXE) Attack
  - **B) Directory Traversal**

65. What kind of user input should always be validated?
  - A) Numeric inputs
  - B) Text inputs
  - C) All user inputs
  - D) Only sensitive inputs
  - **C) All user inputs**

66. What is the main purpose of the Content Security Policy (CSP) header?
  - A) To secure HTTP connections

- B) To restrict resources the user agent is allowed to load
  - C) To manage user sessions
  - D) To log user activity
  - **B) To restrict resources the user agent is allowed to load**

67. What type of web application vulnerability can lead to unauthorized access to API endpoints?
  - A) SQL Injection
  - B) Broken Access Control
  - C) Cross-Site Scripting
  - D) XML External Entities
  - **B) Broken Access Control**

68. Which attack involves an attacker sending unsolicited requests to a user without their consent?
  - A) Phishing
  - B) Clickjacking
  - C) CSRF
  - D) Brute Force
  - **C) CSRF**

69. What is the role of "encryption" in web security?
  - A) To improve application speed
  - B) To protect data confidentiality
  - C) To authenticate users
  - D) To enhance user experience
  - **B) To protect data confidentiality**

70. What does "patch management" refer to in web application security?
  - A) Regularly updating software to fix vulnerabilities
  - B) Monitoring user activity
  - C) Encrypting sensitive data
  - D) Managing user permissions
  - **A) Regularly updating software to fix vulnerabilities**

71. What is the potential impact of an "unvalidated redirect"?
  - A) Unauthorized data access
  - B) Redirection to malicious sites
  - C) Data corruption
  - D) Denial of service
  - **B) Redirection to malicious sites**

72. Which of the following techniques can be used to secure web applications?
  - A) Using outdated software
  - B) Employing security headers
  - C) Ignoring logs
  - D) Allowing user-generated content without checks
  - **B) Employing security headers**

73. What does the term "data breach" mean?
  - A) Loss of data integrity
  - B) Unauthorized access to sensitive information
  - C) Data backup failure
  - D) Network outage
  - **B) Unauthorized access to sensitive information**

74. Which type of attack can occur when a user is tricked into clicking on a malicious link?
  - A) Session Hijacking
  - B) Phishing
  - C) SQL Injection
  - D) All of the above
  - **B) Phishing**

75. What is the main consequence of improper error handling in web applications?
  - A) Application crashes
  - B) User confusion
  - C) Information leakage
  - D) Performance issues
  - **C) Information leakage**

76. In the context of web security, what is "threat intelligence"?
  - A) Understanding user behavior
  - B) Gathering and analyzing information on potential threats
  - C) Improving application performance
  - D) Encrypting sensitive data
  - **B) Gathering and analyzing information on potential threats**

77. What does "principle of least privilege" refer to in access control?
  - A) Granting all users administrative access
  - B) Limiting user access to only what is necessary for their role
  - C) Allowing unrestricted access to all resources
  - D) Granting privileges based on user requests
  - **B) Limiting user access to only what is necessary for their role**

78. Which of the following is a potential risk of using weak passwords?

  - A) Enhanced security
  - B) Increased user convenience
  - C) Account compromise
  - D) Faster login times
  - **C) Account compromise**

79. What does "DNS spoofing" involve?
  - A) Intercepting domain name system requests
  - B) Modifying website content
  - C) Manipulating SSL certificates
  - D) Injecting malware
  - **A) Intercepting domain name system requests**

80. What kind of information is typically targeted in a "data exfiltration" attack?
  - A) System performance data
  - B) Personal and financial data
  - C) Network configurations
  - D) User feedback
  - **B) Personal and financial data**

81. Which of the following describes "RAT" in cybersecurity?
  - A) Real-time analytics tool
  - B) Remote Access Trojan
  - C) Risk Assessment Tool
  - D) Rapid Application Testing
  - **B) Remote Access Trojan**

82. What type of attack exploits the trust between a user and a web application?
  - A) Phishing

- B) Cross-Site Request Forgery (CSRF)
- C) SQL Injection
- D) Code Injection
- **B) Cross-Site Request Forgery (CSRF)**

83. What is the potential impact of a "denial of service" (DoS) attack on a web application?
  - A) Data theft
  - B) Application downtime
  - C) Data loss
  - D) Unauthorized access
  - **B) Application downtime**

84. What does the term "credential stuffing" refer to?
  - A) Using unique credentials for each service
  - B) Attempting to access multiple accounts using stolen credentials
  - C) Repeatedly entering credentials until access is granted
  - D) Collecting user credentials for analysis
  - **B) Attempting to access multiple accounts using stolen credentials**

85. Which of the following is a key practice for secure API development?
  - A) Exposing all endpoints publicly
  - B) Implementing proper authentication and authorization
  - C) Allowing cross-origin resource sharing without checks
  - D) Using predictable URL patterns
  - **B) Implementing proper authentication and authorization**

86. In web application security, what does "defense in depth" mean?
  - A) Relying on a single security measure
  - B) Implementing multiple layers of security controls

- C) Only using perimeter defenses
- D) Ignoring user security training
- **B) Implementing multiple layers of security controls**

87. What is the main function of "firewalls" in web application security?
- A) To manage user access
- B) To filter incoming and outgoing traffic
- C) To encrypt data
- D) To enhance application performance
- **B) To filter incoming and outgoing traffic**

88. Which attack vector is often used to exploit poor input validation?
- A) SQL Injection
- B) Data encryption
- C) Secure session management
- D) SSL/TLS configurations
- **A) SQL Injection**

89. What does the term "zero-day vulnerability" refer to?
- A) A vulnerability that has been publicly disclosed
- B) A vulnerability for which a patch is not yet available
- C) A vulnerability that has been patched
- D) A vulnerability that affects legacy systems
- **B) A vulnerability for which a patch is not yet available**

90. What is the role of "user education" in cybersecurity?
- A) To improve application performance
- B) To raise awareness about security threats
- C) To manage user permissions

- D) To encrypt sensitive data
- **B) To raise awareness about security threats**

91. What does "SQL injection" exploit in web applications?
  - A) User input validation
  - B) Poorly constructed database queries
  - C) Weak password policies
  - D) Insecure network protocols
  - **B) Poorly constructed database queries**

92. Which of the following can be used to protect against brute force attacks?
  - A) Limiting login attempts
  - B) Allowing unlimited login attempts
  - C) Using simple passwords
  - D) Ignoring failed login attempts
  - **A) Limiting login attempts**

93. What does "social engineering" involve?
  - A) Exploiting technical vulnerabilities
  - B) Manipulating individuals into divulging confidential information
  - C) Creating secure software
  - D) Conducting vulnerability assessments
  - **B) Manipulating individuals into divulging confidential information**

94. What is a "sandbox" in the context of web application security?
  - A) A secure environment for testing applications
  - B) A data storage solution
  - C) A type of firewall
  - D) A method for managing user permissions

  - **A) A secure environment for testing applications**

95. What does "data masking" refer to?
  - A) Encrypting sensitive data
  - B) Hiding data from unauthorized users
  - C) Changing data to obscure its meaning
  - D) Both B and C
  - **D) Both B and C**

96. Which of the following is a technique used to enhance password security?
  - A) Allowing short passwords
  - B) Encouraging password reuse
  - C) Implementing account lockout policies
  - D) Ignoring password complexity
  - **C) Implementing account lockout policies**

97. What is the impact of not implementing proper session management?
  - A) Enhanced user experience
  - B) Increased performance
  - C) Session hijacking and unauthorized access
  - D) Improved application security
  - **C) Session hijacking and unauthorized access**

98. Which of the following is a common method for preventing cross-origin attacks?
  - A) Allowing all origins
  - B) Implementing Cross-Origin Resource

Sharing (CORS)

- C) Disabling same-origin policies
- D) Ignoring cross-origin requests
- **B) Implementing Cross-Origin Resource Sharing (CORS)**

99. What is "API throttling"?
- A) Limiting the number of requests a user can make to an API
- B) Encrypting API requests
- C) Allowing unlimited API access
- D) Monitoring API performance
- **A) Limiting the number of requests a user can make to an API**

100. What does "Vulnerability Assessment" entail?
- A) Identifying and evaluating security weaknesses
- B) Exploiting identified vulnerabilities
- C) Encrypting sensitive information
- D) Creating user-friendly interfaces
- **A) Identifying and evaluating security weaknesses**

Feel free to reach out if you need any further assistance or clarification on specific topics! Good luck with your quiz competition!