Sure! Here are 100 additional advanced MCQs on web application penetration testing, ensuring no repeats from the previous set:

1. What does the term "SQL Injection" refer to?
- A) Inserting SQL queries into user input fields
- B) Encrypting SQL queries
- C) Using SQL for data storage
- D) None of the above
- **A) Inserting SQL queries into user input fields**

2. What is the main goal of "penetration testing"?
- A) To improve user experience
- B) To identify vulnerabilities
- C) To develop applications
- D) To increase application speed
- **B) To identify vulnerabilities**

3. Which HTTP status code indicates a successful request?
- A) 200
- B) 404
- C) 500
- D) 403
- **A) 200**

4. What does "Cross-Site Scripting" (XSS) allow an attacker to do?
- A) Access the database
- B) Inject malicious scripts into web pages
- C) Redirect users to different sites
- D) All of the above
- **B) Inject malicious scripts into web pages**

5. What is the function of a Web Application Firewall (WAF)?
 - A) To manage user sessions
 - B) To filter and monitor HTTP traffic
 - C) To encrypt sensitive data
 - D) To store user passwords
 - **B) To filter and monitor HTTP traffic**

6. Which type of attack can be mitigated using prepared statements?
 - A) Cross-Site Scripting
 - B) SQL Injection
 - C) Denial of Service
 - D) Credential Stuffing
 - **B) SQL Injection**

7. What is the purpose of "input validation"?
 - A) To increase application speed
 - B) To ensure user inputs are safe and expected
 - C) To enhance user experience
 - D) To manage database connections
 - **B) To ensure user inputs are safe and expected**

8. What is a common sign of a successful XSS attack?
 - A) Unexplained account lockouts
 - B) Unexpected pop-ups or alerts
 - C) Slow application performance
 - D) Unauthorized file access
 - **B) Unexpected pop-ups or alerts**

9. Which of the following is a secure method of storing passwords?
- A) Hashing with salt
- B) Storing in plain text
- C) Encrypting without salt
- D) Using predictable patterns
- **A) Hashing with salt**

10. What does "brute force attack" involve?
- A) Exploiting vulnerabilities in software
- B) Trying multiple combinations to guess credentials
- C) Phishing for user credentials
- D) None of the above
- **B) Trying multiple combinations to guess credentials**

11. Which of the following can help mitigate CSRF attacks?
- A) Use of secure cookies
- B) Implementing anti-CSRF tokens
- C) User input validation
- D) Encrypting all requests
- **B) Implementing anti-CSRF tokens**

12. What is a "session hijacking" attack?
- A) Gaining unauthorized access by stealing session tokens
- B) Exploiting vulnerabilities in the application
- C) Injecting malicious code into sessions
- D) None of the above
- **A) Gaining unauthorized access by stealing session tokens**

13. Which of the following vulnerabilities can lead to data exposure?

- A) Insufficient Logging
- B) Security Misconfiguration
- C) Unvalidated Redirects
- D) All of the above
- **D) All of the above**

14. What is the purpose of "Content Security Policy" (CSP)?
- A) To prevent SQL Injection
- B) To restrict resources the browser is allowed to load
- C) To encrypt data
- D) To log user activity
- **B) To restrict resources the browser is allowed to load**

15. What does "Cross-Origin Resource Sharing" (CORS) allow?
- A) Requests from different origins
- B) Unauthorized access to resources
- C) Cookie sharing across domains
- D) None of the above
- **A) Requests from different origins**

16. What is "directory traversal"?
- A) Accessing files and directories stored outside the intended directory
- B) Injecting SQL queries into URLs
- C) Modifying web application settings
- D) None of the above
- **A) Accessing files and directories stored outside the intended directory**

17. What does the term "phishing" refer to?
- A) Exploiting software vulnerabilities

- B) Tricking individuals into revealing sensitive information
- C) Injecting code into web applications
- D) None of the above
- **B) Tricking individuals into revealing sensitive information**

18. What is "open redirection"?
- A) Redirecting users to a secure page
- B) Allowing attackers to redirect users to malicious sites
- C) Automatically logging users out
- D) None of the above
- **B) Allowing attackers to redirect users to malicious sites**

19. Which of the following is a potential impact of "broken authentication"?
- A) Unauthorized access to accounts
- B) Application downtime
- C) Data loss
- D) None of the above
- **A) Unauthorized access to accounts**

20. What is the main goal of "social engineering" attacks?
- A) To exploit software vulnerabilities
- B) To manipulate individuals into disclosing information
- C) To inject code into applications
- D) None of the above
- **B) To manipulate individuals into disclosing information**

21. What does "tokenization" do in the context of web security?
- A) Converts sensitive data into non-sensitive tokens
- B) Encrypts data

- C) Bypasses security measures
- D) None of the above
- **A) Converts sensitive data into non-sensitive tokens**

22. What is "data exfiltration"?
- A) Loss of data integrity
- B) Unauthorized transfer of data
- C) Data encryption
- D) None of the above
- **B) Unauthorized transfer of data**

23. Which HTTP method is typically used for fetching resources?
- A) POST
- B) GET
- C) PUT
- D) DELETE
- **B) GET**

24. What does "SSL/TLS" protect against?
- A) Data interception during transmission
- B) SQL Injection
- C) Cross-Site Scripting
- D) None of the above
- **A) Data interception during transmission**

25. What is a common consequence of "insecure direct object references"?
- A) Denial of service
- B) Unauthorized access to sensitive data
- C) Application slowdown

  - D) None of the above
  - **B) Unauthorized access to sensitive data**

26. What does "malware" stand for?
  - A) Malicious software designed to harm or exploit systems
  - B) A type of antivirus software
  - C) Software designed to enhance security
  - D) None of the above
  - **A) Malicious software designed to harm or exploit systems**

27. Which of the following is a type of phishing attack?
  - A) Spear phishing
  - B) SQL Injection
  - C) CSRF
  - D) Denial of Service
  - **A) Spear phishing**

28. What does the term "vulnerability disclosure" refer to?
  - A) Publicly announcing vulnerabilities
  - B) Keeping vulnerabilities secret
  - C) Encrypting sensitive information
  - D) None of the above
  - **A) Publicly announcing vulnerabilities**

29. What does "buffer overflow" exploit?
  - A) Data storage limitations
  - B) Insufficient input validation
  - C) Session management issues
  - D) None of the above

  - **B) Insufficient input validation**

30. What is the purpose of a "honeypot" in cybersecurity?
  - A) To attract and deceive attackers
  - B) To store user data securely
  - C) To enhance application performance
  - D) None of the above
  - **A) To attract and deceive attackers**

31. Which of the following is a common vulnerability in web applications?
  - A) XML Injection
  - B) Network Misconfiguration
  - C) Security Misconfiguration
  - D) All of the above
  - **D) All of the above**

32. What does "API security" encompass?
  - A) Protecting the data transmitted via APIs
  - B) Ensuring proper authentication and authorization
  - C) All of the above
  - D) None of the above
  - **C) All of the above**

33. What is the potential risk of using outdated libraries in web applications?
  - A) Improved performance
  - B) Introduction of new features
  - C) Exploitation of known vulnerabilities
  - D) None of the

above
- **C) Exploitation of known vulnerabilities**

34. What is the purpose of "error handling" in web applications?
- A) To improve user experience
- B) To prevent information leakage
- C) To log user activity
- D) All of the above
- **B) To prevent information leakage**

35. What does "network segmentation" achieve?
- A) Reduces network performance
- B) Isolates network resources for better security
- C) Increases data redundancy
- D) None of the above
- **B) Isolates network resources for better security**

36. What is a "denial of service" (DoS) attack?
- A) Gaining unauthorized access to data
- B) Overloading a service to make it unavailable
- C) Injecting malware into an application
- D) None of the above
- **B) Overloading a service to make it unavailable**

37. What is the purpose of "session tokens"?
- A) To manage user preferences
- B) To track user sessions securely
- C) To encrypt user data

  - D) None of the above
  - **B) To track user sessions securely**

38. What does the term "remote code execution" (RCE) mean?
  - A) Executing code on a remote server
  - B) Running code on the user's machine
  - C) Attacking a local machine
  - D) None of the above
  - **A) Executing code on a remote server**

39. What is the impact of "data leakage"?
  - A) Unauthorized access to sensitive information
  - B) Improved application performance
  - C) Enhanced security measures
  - D) None of the above
  - **A) Unauthorized access to sensitive information**

40. What is the primary function of "encryption" in web applications?
  - A) To improve loading times
  - B) To protect data confidentiality
  - C) To manage user sessions
  - D) None of the above
  - **B) To protect data confidentiality**

41. What does "application security" focus on?
  - A) Network security measures
  - B) Protecting applications from threats
  - C) Physical security of servers
  - D) None of the above

- **B) Protecting applications from threats**

42. What is a "SQL map" tool used for?
  - A) Mapping website layouts
  - B) Detecting SQL Injection vulnerabilities
  - C) Managing database connections
  - D) None of the above
  - **B) Detecting SQL Injection vulnerabilities**

43. What does "credential management" entail?
  - A) Storing passwords in plain text
  - B) Implementing secure storage and retrieval of credentials
  - C) Ignoring password policies
  - D) None of the above
  - **B) Implementing secure storage and retrieval of credentials**

44. What does "DNS poisoning" involve?
  - A) Modifying domain name records to redirect traffic
  - B) Encrypting DNS requests
  - C) Protecting against DDoS attacks
  - D) None of the above
  - **A) Modifying domain name records to redirect traffic**

45. What is the main risk associated with "insufficient logging"?
  - A) Enhanced application performance
  - B) Difficulty in detecting security breaches
  - C) Increased user satisfaction
  - D) None of the above
  - **B) Difficulty in detecting security breaches**

46. Which of the following is a method to secure APIs?
  - A) Use of API keys
  - B) Allowing all origins for CORS
  - C) Ignoring authentication
  - D) None of the above
  - **A) Use of API keys**

47. What does "vulnerability scanning" do?
  - A) Exploits known vulnerabilities
  - B) Identifies security weaknesses
  - C) Encrypts sensitive data
  - D) None of the above
  - **B) Identifies security weaknesses**

48. What is a common cause of "server-side request forgery" (SSRF)?
  - A) Poorly configured firewalls
  - B) Allowing external resource requests
  - C) Unvalidated user input
  - D) None of the above
  - **B) Allowing external resource requests**

49. What is the primary purpose of "network firewalls"?
  - A) To encrypt traffic
  - B) To monitor and filter incoming and outgoing traffic
  - C) To manage user permissions
  - D) None of the above
  - **B) To monitor and filter incoming and outgoing traffic**

50. What does "web scraping" refer to?
 - A) Extracting data from websites
 - B) Attacking web applications
 - C) Managing web traffic
 - D) None of the above
 - **A) Extracting data from websites**

51. What is the main goal of "threat modeling"?
 - A) To enhance user experience
 - B) To identify and prioritize potential threats
 - C) To increase application speed
 - D) None of the above
 - **B) To identify and prioritize potential threats**

52. What does "integrity" in data security mean?
 - A) Data is available when needed
 - B) Data cannot be altered or tampered with
 - C) Data is encrypted
 - D) None of the above
 - **B) Data cannot be altered or tampered with**

53. What is the purpose of "security headers"?
 - A) To improve application performance
 - B) To enhance security by controlling how browsers handle content
 - C) To store user data
 - D) None of the above
 - **B) To enhance security by controlling how browsers handle content**

54. What is the potential risk of "improper error messages"?

  - A) Application downtime
  - B) Information leakage
  - C) Increased user satisfaction
  - D) None of the above
  - **B) Information leakage**

55. What does "sandboxing" achieve in web applications?
  - A) Running untrusted code in a secure environment
  - B) Encrypting sensitive data
  - C) Managing user sessions
  - D) None of the above
  - **A) Running untrusted code in a secure environment**

56. What is "whaling" in the context of phishing?
  - A) Targeting high-profile individuals
  - B) Attacking large organizations
  - C) Exploiting software vulnerabilities
  - D) None of the above
  - **A) Targeting high-profile individuals**

57. What is a common sign of a "man-in-the-middle" (MITM) attack?
  - A) Slow network performance
  - B) Unexpected application errors
  - C) Unauthorized access to data
  - D) None of the above
  - **C) Unauthorized access to data**

58. What is "HTTP Strict Transport Security" (HSTS)?
  - A) A method to enforce secure connections

- B) A way to bypass security measures
- C) An encryption protocol
- D) None of the above
- **A) A method to enforce secure connections**

59. What does "multi-factor authentication" (MFA) provide?

- A) An additional layer of security for user accounts
- B) Faster login processes
- C) Simplified user management
- D) None of the above
- **A) An additional layer of security for user accounts**

60. What is the purpose of "security audits"?

- A) To enhance application performance
- B) To assess the effectiveness of security measures
- C) To log user activity
- D) None of the above
- **B) To assess the effectiveness of security measures**

61. What does "endpoint security" focus on?

- A) Protecting user devices from threats
- B) Securing network infrastructure
- C) Managing application performance
- D) None of the above
- **A) Protecting user devices from threats**

62. What is the potential impact of "insecure communications"?

- A) Data integrity
- B) Data interception

- C) Improved application speed
- D) None of the above
- **B) Data interception**

63. What does "input sanitization" aim to achieve?
- A) To improve data processing speed
- B) To clean user inputs to prevent injection attacks
- C) To enhance user experience
- D) None of the above
- **B) To clean user inputs to prevent injection attacks**

64. What is the role of "access control" in web security?
- A) To manage user permissions
- B) To enforce security policies
- C) Both A and B
- D) None of the above
- **C) Both A and B**

65. What does "security by obscurity" imply?
- A) Hiding security mechanisms to improve security
- B) Relying solely on complex systems for protection
- C) Ignoring security measures
- D) None of the above
- **A) Hiding security mechanisms to improve security**

66. What is

a "DDoS" attack?

  - A) A distributed denial-of-service attack
  - B) A method to improve server performance
  - C) A way to bypass security measures
  - D) None of the above
  - **A) A distributed denial-of-service attack**

67. What is the impact of "outdated software" on web security?
  - A) Improved performance
  - B) Introduction of new features
  - C) Increased vulnerability to attacks
  - D) None of the above
  - **C) Increased vulnerability to attacks**

68. What is the purpose of "privacy policies"?
  - A) To inform users about data collection and usage
  - B) To enhance user experience
  - C) To store user data securely
  - D) None of the above
  - **A) To inform users about data collection and usage**

69. What is "social engineering"?
  - A) Exploiting technical vulnerabilities
  - B) Manipulating individuals into divulging information
  - C) Encrypting sensitive data
  - D) None of the above
  - **B) Manipulating individuals into divulging information**

70. What does "digital forensics" focus on?
  - A) Recovering lost data

- B) Analyzing digital evidence from security incidents
- C) Managing network performance
- D) None of the above
- **B) Analyzing digital evidence from security incidents**

71. What is the impact of "insufficient encryption"?

- A) Data protection
- B) Data exposure
- C) Enhanced performance
- D) None of the above
- **B) Data exposure**

72. What does "information security" encompass?

- A) Protecting data from unauthorized access
- B) Managing user permissions
- C) Enhancing user experience
- D) None of the above
- **A) Protecting data from unauthorized access**

73. What is "packet sniffing"?

- A) Monitoring network traffic
- B) Injecting malicious packets
- C) Encrypting data packets
- D) None of the above
- **A) Monitoring network traffic**

74. What does "social engineering" focus on?

- A) Exploiting software vulnerabilities
- B) Manipulating individuals to gain access

- C) Encrypting sensitive information
- D) None of the above
- **B) Manipulating individuals to gain access**

75. What is the primary function of "network segmentation"?
  - A) Enhancing application performance
  - B) Isolating sensitive data for better security
  - C) Increasing user satisfaction
  - D) None of the above
  - **B) Isolating sensitive data for better security**

76. What does "data integrity" ensure?
  - A) Data is kept confidential
  - B) Data cannot be altered without detection
  - C) Data is always available
  - D) None of the above
  - **B) Data cannot be altered without detection**

77. What is "reverse engineering" in cybersecurity?
  - A) Analyzing software to discover vulnerabilities
  - B) Hiding code to prevent access
  - C) Encrypting sensitive information
  - D) None of the above
  - **A) Analyzing software to discover vulnerabilities**

78. What does "user training" help prevent?
  - A) Application performance issues
  - B) Human errors leading to security breaches
  - C) Data loss

- D) None of the above
- **B) Human errors leading to security breaches**

79. What does "security incident response" involve?
- A) Detecting and responding to security breaches
- B) Encrypting sensitive data
- C) Improving application performance
- D) None of the above
- **A) Detecting and responding to security breaches**

80. What is the purpose of "vulnerability management"?
- A) To exploit vulnerabilities
- B) To identify, assess, and prioritize vulnerabilities
- C) To enhance user experience
- D) None of the above
- **B) To identify, assess, and prioritize vulnerabilities**

81. What does "malware analysis" entail?
- A) Analyzing malware to understand its behavior
- B) Encrypting malware
- C) Ignoring malware threats
- D) None of the above
- **A) Analyzing malware to understand its behavior**

82. What does "application hardening" refer to?
- A) Making applications more resistant to attacks
- B) Encrypting sensitive information
- C) Ignoring security measures
- D) None of the above

- **A) Making applications more resistant to attacks**

83. What is "identity theft"?
  - A) Stealing personal information to impersonate someone
  - B) Gaining unauthorized access to accounts
  - C) Modifying user data
  - D) None of the above
  - **A) Stealing personal information to impersonate someone**

84. What does "token-based authentication" provide?
  - A) Simplified user experience
  - B) Secure access without storing passwords
  - C) Increased server load
  - D) None of the above
  - **B) Secure access without storing passwords**

85. What is the role of "firewalls" in network security?
  - A) Encrypting data
  - B) Monitoring and controlling incoming and outgoing traffic
  - C) Managing user permissions
  - D) None of the above
  - **B) Monitoring and controlling incoming and outgoing traffic**

86. What does "user access control" ensure?
  - A) Only authorized users can access specific resources
  - B) Increased application speed
  - C) Data encryption
  - D) None of the above
  - **A) Only authorized users can access specific resources**

87. What is "zero-day vulnerability"?
- A) A vulnerability that has been discovered and patched
- B) A vulnerability that is unknown to the software vendor
- C) A vulnerability that is common in many applications
- D) None of the above
- **B) A vulnerability that is unknown to the software vendor**

88. What is the impact of "malicious insiders"?
- A) Unauthorized access to sensitive data
- B) Increased application performance
- C) Enhanced user experience
- D) None of the above
- **A) Unauthorized access to sensitive data**

89. What does "patch management" involve?
- A) Ignoring software updates
- B) Regularly applying updates to software to fix vulnerabilities
- C) Encrypting sensitive information
- D) None of the above
- **B) Regularly applying updates to software to fix vulnerabilities**

90. What is "ransomware"?
- A) A type of malware that demands payment to restore access
- B) Software that improves security
- C) A method of data encryption
- D) None of the above
- **A) A type of malware that demands payment to restore access**

91. What does "network monitoring" involve?
  - A) Observing and analyzing network traffic
  - B) Encrypting data in transit
  - C) Ignoring security threats
  - D) None of the above
  - **A) Observing and analyzing network traffic**

92. What is "data masking" used for?
  - A) Protecting sensitive data by replacing it with anonymized data
  - B) Encrypting data
  - C) Ignoring security measures
  - D) None of the above
  - **A) Protecting sensitive data by replacing it with anonymized data**

93. What does "automated vulnerability scanning" achieve?
  - A) Finding vulnerabilities without human intervention
  - B) Exploiting vulnerabilities
  - C) Ignoring security measures
  - D) None of the above
  - **A) Finding vulnerabilities without human intervention**

94. What is "cloud security"?
  - A) Protecting data stored in cloud environments
  - B) Improving cloud performance
  - C) Ignoring security threats in the cloud
  - D) None of the above
  - **A) Protecting data stored in cloud environments**

95. What is "two-factor authentication" (2FA)?

- A) A method of securing accounts with two verification steps
- B) Storing passwords securely
- C) Encrypting sensitive data
- D) None of the above
- **A) A method of securing accounts with two verification steps**

96. What does "privilege escalation" involve?
- A) Gaining higher access rights than intended
- B) Lowering user access permissions
- C) Ignoring security measures
- D) None of the above
- **A) Gaining higher access rights than intended**

97. What is the primary goal of "incident response planning"?
- A) To prepare for potential security breaches
- B) To improve application performance
- C) To manage user sessions
- D) None of the above
- **A) To prepare for potential security breaches**

98. What does "web application hardening" focus on?
- A) Making web applications more resistant to attacks
- B) Ignoring vulnerabilities
- C

) Increasing application speed
- D) None of the above
- **A) Making web applications more resistant to attacks**

99. What is "cyber threat intelligence"?
  - A) Information about potential threats to cybersecurity
  - B) Enhancing application performance
  - C) Managing user data
  - D) None of the above
  - **A) Information about potential threats to cybersecurity**

100. What does "risk assessment" involve?
  - A) Identifying and analyzing potential risks to an organization
  - B) Enhancing user experience
  - C) Ignoring security measures
  - D) None of the above
  - **A) Identifying and analyzing potential risks to an organization**

These questions and answers cover various aspects of cybersecurity, including threats, vulnerabilities, security measures, and best practices, providing a comprehensive overview of essential concepts in the field.