Here are 100 more advanced MCQs on mobile application penetration testing, without repeating the previous questions. The correct options are in bold.

Additional Mobile Application Penetration Testing MCQs

1. What is the purpose of "input validation" in mobile apps?
 - A) Increase performance
 - *B) Prevent malicious input*
 - C) Simplify user experience
 - D) Optimize database queries

2. Which tool is used for static analysis of iOS applications?
 - *A) MobSF*
 - B) Frida
 - C) Burp Suite
 - D) Zap

3. What is "client-side encryption" primarily used for?
 - A) Securing API endpoints
 - *B) Protecting user data before sending it to the server*
 - C) Improving server performance
 - D) Data storage optimization

4. What does the term "race condition" refer to in mobile apps?
 - A) Slow app response
 - B) Resource exhaustion
 - *C) Unexpected behavior due to timing issues*
 - D) Memory leaks

5. Which of the following attacks exploits session tokens?
- A) CSRF
- *B) Session fixation*
- C) Clickjacking
- D) XSS

6. What is a common technique used to prevent clickjacking?
- A) Data encryption
- *B) X-Frame-Options header*
- C) Input validation
- D) Access control

7. In mobile app security, what does "rooted" mean?
- *A) Device has been modified to gain superuser access*
- B) Device is securely locked
- C) App is installed without user permission
- D) App runs in a sandbox environment

8. Which type of testing assesses the security of mobile backends?
- A) Static testing
- *B) API security testing*
- C) Manual code review
- D) UI testing

9. What is the main concern with using weak cryptographic algorithms?
- A) Increased processing time
- *B) Data can be easily decrypted*
- C) Compatibility issues

- D) Reduced performance

10. What does "data in transit" refer to?
 - A) Data stored on a device
 - *B) Data being transmitted over networks*
 - C) Data in databases
 - D) Temporary data storage

11. What is a common vulnerability related to improper API authentication?
 - A) Cross-Site Scripting
 - B) SQL Injection
 - *C) Insecure Direct Object References*
 - D) Clickjacking

12. Which of the following is a method to protect against Man-in-the-Middle (MitM) attacks?
 - A) Regular backups
 - *B) Using HTTPS*
 - C) Session timeouts
 - D) Input validation

13. What does the term "local storage" in mobile apps refer to?
 - *A) Data stored on the user's device*
 - B) Data stored on a remote server
 - C) Data stored in a database
 - D) Temporary data during processing

14. What is "path traversal" vulnerability?
 - *A) Accessing files outside the intended directory*

- B) SQL command injection
- C) Unrestricted file upload
- D) Buffer overflow

15. Which of the following is a common sign of poor security practices?
- A) Data encryption
- *B) Use of default credentials*
- C) Regular security audits
- D) Session management

16. What is the purpose of a "honeypot" in security testing?
- A) To improve app performance
- *B) To attract and analyze attackers*
- C) To protect sensitive data
- D) To enhance user experience

17. What type of attack does "dictionary attack" refer to?
- *A) Attempting to guess passwords using a predefined list*
- B) SQL Injection
- C) XSS
- D) CSRF

18. What is the role of "server-side validation"?
- A) Simplify the user interface
- *B) Ensure data integrity and security*
- C) Improve performance
- D) Reduce data storage

19. What is a major risk of using third-party SDKs?
 - A) Improved functionality
 - *B) Introducing vulnerabilities*
 - C) Faster development
 - D) Better user experience

20. What does "credential management" involve?
 - A) Increasing app speed
 - *B) Securely storing and handling user credentials*
 - C) Simplifying user registration
 - D) Monitoring user activity

21. Which OWASP risk is associated with improper API access controls?
 - A) Security Misconfiguration
 - *B) Broken Access Control*
 - C) Insecure Data Storage
 - D) Insufficient Logging & Monitoring

22. What does "mobile app sandboxing" do?
 - *A) Isolates app processes from each other*
 - B) Prevents data storage
 - C) Increases app performance
 - D) Simplifies user interaction

23. What is the consequence of exposing sensitive endpoints in an API?
 - A) Improved app performance
 - *B) Increased risk of unauthorized access*
 - C) Enhanced user experience
 - D) Reduced development time

24. Which technique helps mitigate data leakage?
 - *A) Encrypting sensitive data*
 - B) Using plain text
 - C) Disabling authentication
 - D) Allowing all network traffic

25. What does the term "API throttling" refer to?
 - A) Allowing unlimited API calls
 - *B) Limiting the number of requests from a user*
 - C) Speeding up API responses
 - D) Removing API access logs

26. Which tool is commonly used for network analysis in mobile apps?
 - A) Nessus
 - *B) Charles Proxy*
 - C) Metasploit
 - D) Sqlmap

27. What is "SQL Injection" primarily aimed at?
 - A) Compromising user credentials
 - *B) Manipulating database queries*
 - C) Gaining unauthorized access
 - D) Executing scripts in the browser

28. What is the potential risk of allowing unrestricted file uploads?
 - *A) Malware injection*
 - B) Data corruption
 - C) Performance degradation

- D) User confusion

29. What is the purpose of using "HTTPS"?
- A) Improve server performance
- *B) Secure data transmission*
- C) Simplify the user experience
- D) Increase app size

30. What does "data masking" do?
- A) Increases data size
- B) Hides data during processing
- *C) Obscures sensitive information*
- D) Improves performance

31. Which attack exploits a vulnerability in the user interface?
- A) SQL Injection
- B) CSRF
- *C) Clickjacking*
- D) Code Injection

32. What is a common consequence of a successful phishing attack?
- A) Increased user trust
- *B) Credential theft*
- C) Improved security
- D) Enhanced user engagement

33. What is the goal of using "password hashing"?
- *A) To securely store user passwords*

- B) To simplify user authentication
- C) To enhance performance
- D) To reduce data size

34. What does "whitelisting" refer to in security?
- A) Allowing all traffic
- *B) Permitting only approved applications or actions*
- C) Blocking all traffic
- D) Simplifying access controls

35. What is the main objective of using "firewalls" in mobile app security?
- A) Improve performance
- *B) Block unauthorized access*
- C) Simplify user interface
- D) Encrypt data

36. What type of vulnerability does "open redirect" create?
- *A) Redirecting users to malicious sites*
- B) Data leakage
- C) SQL Injection
- D) Cross-Site Scripting

37. What is a "backdoor" in mobile applications?
- *A) A hidden method for bypassing authentication*
- B) An access control mechanism
- C) A performance optimization tool
- D) A standard security feature

38. Which of the following is a characteristic of a secure API?
 - A) No authentication
 - B) Open access to all data
 - *C) Proper access controls and validation*
 - D) Lack of documentation

39. What does "session management" help prevent?
 - A) Improved user experience
 - *B) Session hijacking*
 - C) Data corruption
 - D) Application crashes

40. Which OWASP risk is associated with insufficient logging?
 - A) Insecure Data Storage
 - *B) Insufficient Logging & Monitoring*
 - C) Broken Access Control
 - D) Injection

41. What is the purpose of "secure coding guidelines"?
 - A) Simplify coding
 - *B) Enhance security and reduce vulnerabilities*
 - C) Improve performance
 - D) Increase user engagement

42. Which vulnerability involves executing commands through user inputs

?
 - A) Buffer overflow

- *B) Command Injection*
- C) SQL Injection
- D) Cross-Site Scripting

43. What is the impact of using hardcoded passwords?
- A) Improved performance
- *B) Increased risk of credential exposure*
- C) Enhanced user experience
- D) Simplified authentication

44. Which of the following is a common tool for dynamic application security testing (DAST)?
- A) Veracode
- B) SonarQube
- *C) OWASP ZAP*
- D) Fortify

45. What does the term "supply chain attack" refer to?
- A) Hacking a network
- *B) Compromising third-party services or libraries*
- C) Attacking user devices directly
- D) Phishing for user credentials

46. What is the goal of "security awareness training" for developers?
- A) Improve coding speed
- *B) Educate on secure coding practices*
- C) Enhance user experience
- D) Reduce development costs

47. What is the consequence of failing to sanitize user inputs?
 - *A) Vulnerability to injection attacks*
 - B) Increased performance
 - C) Enhanced user experience
 - D) Data encryption issues

48. What does "cross-origin resource sharing" (CORS) manage?
 - A) Secure data storage
 - *B) Sharing resources between different origins*
 - C) User authentication
 - D) Session management

49. What is the main purpose of "security tokens" in mobile apps?
 - A) Enhance user experience
 - *B) Authenticate users securely*
 - C) Increase app performance
 - D) Simplify data storage

50. What is the risk of exposing the app's source code?
 - *A) Increased chance of reverse engineering*
 - B) Improved performance
 - C) Enhanced user trust
 - D) Data encryption issues

51. Which OWASP risk focuses on the insecure storage of sensitive data?
 - A) Insufficient Logging & Monitoring
 - *B) Insecure Data Storage*
 - C) Broken Authentication
 - D) Security Misconfiguration

52. What does "session fixation" attack involve?
 - A) Hijacking user sessions
 - B) Compromising data at rest
 - *C) Forcing a user to use a known session ID*
 - D) Injecting malicious scripts

53. What is a common method to test for XSS vulnerabilities?
 - A) Input sanitization
 - *B) Script injection*
 - C) Static analysis
 - D) Performance testing

54. What does "buffer overflow" vulnerability allow attackers to do?
 - A) Slow down the application
 - *B) Execute arbitrary code*
 - C) Access user credentials
 - D) Increase memory usage

55. What is the purpose of "threat modeling" in mobile security?
 - *A) Identify and mitigate potential security threats*
 - B) Improve user interface design
 - C) Optimize app performance
 - D) Reduce development time

56. Which of the following is a sign of a successful brute force attack?
 - *A) Multiple failed login attempts*
 - B) Increased app performance
 - C) User confusion

- D) Decreased server load

57. What does "network sniffing" do?
- A) Enhance app performance
- *B) Capture and analyze network traffic*
- C) Improve user experience
- D) Encrypt data in transit

58. Which technique helps protect against SQL Injection?
- *A) Parameterized queries*
- B) Input sanitization only
- C) Plain text storage
- D) User authentication

59. What is the risk of enabling verbose error messages in production?
- A) Improved debugging
- *B) Exposure of sensitive information*
- C) Enhanced user experience
- D) Increased app performance

60. What is the function of an "access control list" (ACL)?
- A) Increase app performance
- *B) Define permissions for users or groups*
- C) Simplify user experience
- D) Enhance data encryption

61. What does "security misconfiguration" commonly lead to?
- A) Improved app performance

- *B) Unintended data exposure*
- C) Enhanced user experience
- D) Reduced app size

62. What does "dynamic analysis" in mobile apps involve?
- *A) Testing the application in a running state*
- B) Reviewing source code
- C) Network traffic monitoring
- D) Static code analysis

63. Which of the following is a sign of a poorly configured API?
- A) Robust authentication
- *B) Lack of rate limiting*
- C) Comprehensive logging
- D) Proper input validation

64. What is a common method to prevent unauthorized access to APIs?
- *A) API keys*
- B) Public access
- C) Lack of authentication
- D) Unrestricted access

65. What does "data exfiltration" typically involve?
- A) Data encryption
- *B) Unauthorized transfer of sensitive data*
- C) Data storage
- D) Data processing

66. What is the risk of using hardcoded secrets in code?
 - A) Improved performance
 - *B) Increased exposure if the code is leaked*
 - C) Enhanced user experience
 - D) Reduced functionality

67. What is a common sign of "man-in-the-middle" attack?
 - A) Improved data transfer speed
 - *B) Altered communication between two parties*
 - C) Increased user engagement
 - D) User confusion

68. What does "secure API design" include?
 - A) Open access to all resources
 - *B) Authentication and authorization checks*
 - C) Lack of documentation
 - D) Minimal error handling

69. What is the main concern with "default configurations" in mobile apps?
 - A) Improved performance
 - *B) Security vulnerabilities*
 - C) User confusion
 - D) Increased data size

70. What does "code signing" achieve?
 - A) Increase app performance
 - *B) Verify the integrity and authenticity of code*
 - C) Simplify code distribution
 - D) Improve user experience

71. What is a potential consequence of "insufficient security testing"?
 - A) Enhanced user experience
 - *B) Discovery of unpatched vulnerabilities*
 - C) Increased performance
 - D) Better usability

72. Which of the following is a feature of a secure mobile app?
 - *A) Regular security updates*
 - B) Hardcoded API keys
 - C) Unrestricted access to data
 - D) Lack of error handling

73. What does "social engineering" refer to in security?
 - *A) Manipulating people into divulging confidential information*
 - B) Network-based attacks
 - C) Physical device attacks
 - D) Software vulnerabilities

74. What is the impact of using deprecated libraries in mobile applications?
 - A) Improved performance
 - *B) Increased vulnerability to known exploits*
 - C) Enhanced user engagement
 - D) Reduced app size

75. What does "fuzz testing" do?
 - A) Enhance performance
 - *B) Identify vulnerabilities through random data input*
 - C) Improve user experience

- D) Simplify coding

76. What is a "zero-day vulnerability"?
- A) A known exploit
- *B) An undisclosed vulnerability*
- C) A minor bug
- D) An outdated feature

77. Which of the following helps ensure data confidentiality?
- A) Public storage
- *B) Data encryption*
- C) Open access
- D) Lack of security measures

78. What is the primary goal of "penetration testing"?
- *A) Identify and exploit vulnerabilities*
- B) Improve app design
- C) Enhance user experience
- D) Reduce development costs

79. What does "multi-factor authentication" (MFA) do?
- A) Simplifies user login
- *B) Provides an additional layer of security*
- C) Reduces server load
- D) Increases performance

80. What is the impact of "insecure data transmission"?
- *A) Potential data interception*

- B) Increased latency
- C) Improved performance
- D) Enhanced user experience

81. What does "API endpoint exposure" risk entail?
- A) Improved functionality
- *B) Unauthorized access to sensitive data*
- C) Enhanced user experience
- D) Reduced development time

82. Which of the following is a sign of a successful denial of service attack?
- A) Improved app performance
- *B) Service unavailability*
- C) Enhanced user engagement
- D) Data corruption

83. What is "data integrity" concerned with?
- A) Data encryption
- *B) Ensuring accuracy and consistency of data*
- C) Data storage
- D) User authentication

84. Which of the following techniques is used to prevent XSS?
- A) Input validation only
- **B) Output

encoding**
- C) Lack of error handling

- D) Session management

85. What is a common consequence of SQL Injection?
- *A) Unauthorized access to database*
- B) Improved performance
- C) Enhanced user experience
- D) Data encryption issues

86. What does "API security testing" focus on?
- A) Performance optimization
- *B) Identifying vulnerabilities in API endpoints*
- C) User interface design
- D) Data storage solutions

87. What does the term "data breach" refer to?
- A) Improved data access
- *B) Unauthorized access to sensitive data*
- C) Enhanced security measures
- D) User confusion

88. What is the role of "encryption keys"?
- *A) To encrypt and decrypt data*
- B) To enhance performance
- C) To simplify coding
- D) To manage user sessions

89. What is the risk of using weak passwords?
- A) Improved performance

- *B) Easier for attackers to guess*
- C) Enhanced user experience
- D) Reduced data size

90. What does "vulnerability scanning" do?
- A) Improve user experience
- *B) Identify security weaknesses*
- C) Enhance app design
- D) Increase performance

91. What is the consequence of failing to implement proper session management?
- A) Improved user experience
- *B) Increased risk of session hijacking*
- C) Enhanced app performance
- D) Reduced development time

92. What does "social engineering" rely on?
- A) Technical exploits
- *B) Human psychology*
- C) Software vulnerabilities
- D) Network attacks

93. What is the purpose of "intrusion detection systems" (IDS)?
- A) Improve performance
- *B) Monitor and analyze network traffic for malicious activity*
- C) Simplify user authentication
- D) Enhance data storage

94. What is the risk of exposing sensitive data in logs?
 - *A) Potential for data breaches*
 - B) Improved debugging
 - C) Enhanced user experience
 - D) Increased performance

95. What does "third-party library" risk entail?
 - A) Improved functionality
 - *B) Introduction of vulnerabilities*
 - C) Enhanced user experience
 - D) Simplified coding

96. What is the impact of "insufficient encryption"?
 - A) Improved performance
 - *B) Increased risk of data theft*
 - C) Enhanced user experience
 - D) Reduced app size

97. What does "network segmentation" do?
 - A) Simplifies coding
 - *B) Isolates different parts of a network for security*
 - C) Enhances performance
 - D) Improves user experience

98. What is a common feature of a secure login process?
 - A) Single-factor authentication
 - *B) Multi-factor authentication*
 - C) Hardcoded passwords
 - D) Lack of error handling

99. What does "pen testing" simulate?
 - *A) Real-world attacks on applications*
 - B) Improved user experience
 - C) Enhanced performance
 - D) Data encryption issues

100. What is the purpose of a "security audit"?
 - *A) Evaluate and improve security measures*
 - B) Increase app performance
 - C) Simplify user experience
 - D) Reduce development costs

Feel free to ask if you need further clarification on any of these questions! Good luck with your quiz preparation!