Sure! Here are 100 advanced multiple-choice questions on mobile application penetration testing, including the OWASP Top 10 and other vulnerabilities. The correct options are in bold.

Mobile Application Penetration Testing MCQs

1. Which OWASP Top 10 risk includes insecure data storage?
 - A) Security Misconfiguration
 - *B) Insecure Data Storage*
 - C) Insufficient Logging & Monitoring
 - D) Broken Authentication

2. What is the main purpose of the Mobile Security Testing Guide (MSTG)?
 - A) To provide coding standards
 - *B) To offer a comprehensive security testing framework*
 - C) To outline network security protocols
 - D) To list vulnerabilities in web applications

3. Which of the following is a common tool for mobile application penetration testing?
 - *A) Burp Suite*
 - B) Metasploit
 - C) Nessus
 - D) Wireshark

4. What does "code obfuscation" in mobile apps primarily aim to prevent?
 - A) SQL Injection
 - *B) Reverse engineering*
 - C) Cross-Site Scripting
 - D) Buffer overflow

5. In the context of mobile applications, what does the term "sandboxing" refer to?
- A) Data encryption
- *B) Isolation of app processes*
- C) User authentication
- D) Network segmentation

6. Which OWASP Top 10 vulnerability deals with improper authentication?
- A) Security Misconfiguration
- B) Sensitive Data Exposure
- *C) Broken Authentication*
- D) Insufficient Cryptography

7. What does the term "jailbreaking" refer to?
- A) Securing a device
- *B) Removing OS restrictions*
- C) Updating software
- D) Encrypting data

8. Which of the following is a key step in the mobile application testing process?
- A) Static analysis only
- B) Manual code review only
- *C) Both static and dynamic analysis*
- D) Network analysis only

9. What is the risk of hardcoding sensitive information in mobile apps?
- A) Increased app size
- B) Improved performance
- *C) Exposure to reverse engineering*

- D) Reduced user experience

10. Which OWASP risk focuses on insufficient security controls for API calls?
- A) Insecure Data Storage
- B) Security Misconfiguration
- *C) Insecure Communication*
- D) Broken Access Control

11. What is the purpose of SSL pinning in mobile applications?
- A) Increase performance
- B) Prevent application crashes
- *C) Mitigate man-in-the-middle attacks*
- D) Improve data storage

12. Which of the following tools can be used for dynamic analysis of mobile applications?
- A) Apktool
- *B) Frida*
- C) Burp Suite
- D) Nessus

13. What type of vulnerability is reflected XSS?
- A) Server-side
- B) Client-side
- *C) Both A and B*
- D) None of the above

14. What does the term "rooting" refer to?
- A) Enhancing security

- *B) Gaining superuser access*
- C) Installing antivirus software
- D) Updating firmware

15. Which OWASP vulnerability involves the app exposing sensitive data to unauthorized users?
- A) Insufficient Logging & Monitoring
- *B) Sensitive Data Exposure*
- C) Broken Access Control
- D) Injection

16. Which mobile platform is known for its strict security policies?
- *A) iOS*
- B) Android
- C) Windows Mobile
- D) Blackberry

17. What is the main risk associated with improper session management?
- A) Performance degradation
- *B) Session hijacking*
- C) Increased server load
- D) User confusion

18. Which vulnerability allows an attacker to execute arbitrary code in a mobile app?
- A) XSS
- B) CSRF
- C) *Code Injection*
- D) SQL Injection

19. What is an example of a local data storage mechanism in mobile apps?
 - A) API calls
 - B) Cloud storage
 - *C) SQLite database*
 - D) HTML5 storage

20. Which of the following is a common method for securing sensitive data in transit?
 - A) Using plain text
 - *B) TLS/SSL encryption*
 - C) File system encryption
 - D) Data masking

21. In mobile app testing, what does the term "data leakage" refer to?
 - *A) Unauthorized data exposure*
 - B) Slow application response
 - C) Poor user interface
 - D) High battery consumption

22. Which tool is commonly used to perform reverse engineering on Android applications?
 - A) Burp Suite
 - B) Wireshark
 - *C) JADX*
 - D) Nmap

23. What is the primary goal of an attacker exploiting the "Insecure Communication" vulnerability?
 - A) Modify application behavior
 - *B) Intercept sensitive data*
 - C) Increase app speed
 - D) Gain admin access

24. Which type of attack can exploit broken access controls in mobile apps?
 - A) Denial of Service
 - *B) Privilege escalation*
 - C) XSS
 - D) Man-in-the-middle

25. What is a common defense against SQL Injection in mobile apps?
 - A) Input sanitization only
 - B) Prepared statements
 - *C) Parameterized queries*
 - D) Use of stored procedures only

26. What does "session fixation" vulnerability allow?
 - *A) Attackers to hijack user sessions*
 - B) Decrease app performance
 - C) Access admin features
 - D) Inject malware

27. In mobile penetration testing, what does the term "black-box testing" refer to?
 - A) Analyzing source code
 - B) Reviewing network architecture
 - *C) Testing without prior knowledge of the application*
 - D) Testing with full access to the app

28. Which vulnerability involves exploiting unvalidated redirects and forwards?
 - A) Injection
 - *B) Open Redirect*
 - C) CSRF

- D) XSS

29. What is the potential risk of using third-party libraries in mobile applications?
- A) Improved performance
- *B) Introduction of vulnerabilities*
- C) Better user experience
- D) Easier maintenance

30. What is the purpose of a "Content Security Policy" in mobile applications?
- A) Increase load time
- *B) Prevent XSS attacks*
- C) Control access to files
- D) Secure API calls

31. Which OWASP vulnerability allows attackers to manipulate application logic through unexpected inputs?
- A) Insecure Data Storage
- B) Insufficient Logging & Monitoring
- *C) Injection*
- D) Security Misconfiguration

32. What is the main objective of using a Mobile Application Security Assessment (MASA)?
- A) Improve app design
- B) Analyze network traffic
- *C) Identify security vulnerabilities*
- D) Optimize database queries

33. Which method can be used to secure local data on mobile devices?
- *A) Data encryption*

- B) Data obfuscation
- C) Network segmentation
- D) Input validation

34. What does the term "Man-in-the-Middle" (MitM) attack refer to?
- *A) Intercepting communication between two parties*
- B) Gaining unauthorized access to an app
- C) Altering server responses
- D) Injecting malware into an application

35. Which of the following is a common sign of a broken authentication vulnerability?
- *A) Session tokens are predictable*
- B) High server load
- C) Frequent app crashes
- D) Slow response times

36. What does "API security testing" focus on?
- A) User interface design
- *B) Assessing the security of APIs*
- C) Performance optimization
- D) Network analysis

37. Which OWASP risk is concerned with security misconfigurations?
- A) Insecure Data Storage
- *B) Security Misconfiguration*
- C) Insufficient Logging & Monitoring
- D) Broken Authentication

38. What is the primary purpose of using the "WebView" component in mobile apps?
 - *A) To display web content*
 - B) To handle database transactions
 - C) To manage user sessions
 - D) To encrypt data

39. What is a common consequence of poor session management?
 - A) Improved app performance
 - *B) User account compromise*
 - C) Data loss
 - D) Increased load times

40. Which of the following is an example of a static analysis tool for mobile apps?
 - A) Burp Suite
 - B) Frida
 - *C) Checkmarx*
 - D) Wireshark

41. What does the term "credential stuffing" refer to?
 - *A) Using stolen credentials to gain unauthorized access*
 - B) Encrypting user data

 - C) Storing credentials securely
 - D) Improving authentication methods

42. Which technique can help prevent reverse engineering of mobile applications?
 - A) Using open-source libraries

- B) Writing simple code
- *C) Code obfuscation*
- D) Hardcoding sensitive data

43. What is the risk of exposing sensitive APIs in mobile applications?
- A) Increased user engagement
- *B) Unauthorized data access*
- C) Improved app functionality
- D) Lower development costs

44. What is a "Cross-Site Request Forgery" (CSRF) attack?
- *A) Forcing a user to execute unwanted actions on a web application*
- B) Stealing user credentials
- C) Intercepting network traffic
- D) Injecting malicious scripts

45. Which mobile platform is more susceptible to malware?
- *A) Android*
- B) iOS
- C) Windows Mobile
- D) Blackberry

46. What does "security by obscurity" mean?
- A) Using complex algorithms
- B) Hiding vulnerabilities
- *C) Relying on secrecy for security*
- D) Ensuring high visibility of security controls

47. What is the purpose of using a VPN for mobile applications?
 - A) Increase app performance
 - *B) Secure data transmission over public networks*
 - C) Improve user experience
 - D) Bypass network restrictions

48. Which type of testing is performed to identify security vulnerabilities in the backend API?
 - A) Static testing
 - B) Manual testing
 - *C) API security testing*
 - D) Performance testing

49. What does "clickjacking" vulnerability allow attackers to do?
 - A) Steal user credentials
 - *B) Trick users into clicking on malicious links*
 - C) Redirect users to phishing sites
 - D) Inject malware into the app

50. Which of the following vulnerabilities involves improper validation of user input?
 - *A) Injection*
 - B) Insecure Data Storage
 - C) Broken Access Control
 - D) Insufficient Logging & Monitoring

51. What is the primary risk associated with "Insecure Data Storage"?
 - A) Increased performance
 - *B) Unauthorized access to sensitive data*
 - C) Data corruption
 - D) Poor user experience

52. Which OWASP risk focuses on insufficient logging and monitoring?
- A) Security Misconfiguration
- *B) Insufficient Logging & Monitoring*
- C) Sensitive Data Exposure
- D) Broken Authentication

53. What is the potential risk of using HTTP instead of HTTPS for data transmission?
- A) Increased latency
- *B) Data interception by attackers*
- C) Reduced app performance
- D) Compatibility issues

54. Which of the following is a common method to secure sensitive data at rest?
- A) Storing data in plain text
- B) Using insecure databases
- *C) Encrypting data*
- D) Disabling data storage

55. What is the impact of insecure API design?
- A) Enhanced user experience
- *B) Increased vulnerability to attacks*
- C) Reduced server costs
- D) Improved performance

56. What does "reflected XSS" allow attackers to do?
- A) Execute scripts on the server
- *B) Execute scripts in the user’s browser*
- C) Access sensitive server data

- D) Manipulate database records

57. What is the primary function of "two-factor authentication"?
- A) Increase app speed
- B) Simplify user registration
- *C) Enhance account security*
- D) Store user data securely

58. What type of vulnerability is "buffer overflow"?
- A) Input validation
- *B) Memory corruption*
- C) Logic flaw
- D) Authentication issue

59. Which OWASP risk involves users being able to perform unauthorized actions?
- A) Security Misconfiguration
- B) Sensitive Data Exposure
- *C) Broken Access Control*
- D) Insecure Data Storage

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

61. Which mobile application framework has built-in security features?
- A) Flutter

- B) Ionic
- *C) React Native*
- D) Apache Cordova

62. What type of attack is a "Denial of Service" (DoS)?
- A) Data theft
- *B) Service disruption*
- C) Unauthorized access
- D) Code injection

63. What is the risk of using outdated third-party libraries in mobile apps?
- A) Enhanced features
- *B) Vulnerabilities due to known exploits*
- C) Improved user experience
- D) Reduced app size

64. Which of the following is a technique to prevent SQL Injection?
- *A) Using prepared statements*
- B) Input sanitization only
- C) Hardcoding SQL queries
- D) Storing queries in plain text

65. What does "insufficient logging" mean in a mobile application?
- A) Improved performance
- *B) Lack of audit trails for security incidents*
- C) Reduced app size
- D) Increased user engagement

66. What is the risk of enabling debug mode in a mobile application?
 - A) Improved performance
 - *B) Exposure of sensitive information*
 - C) Reduced battery consumption
 - D) Increased security

67. What does the term "API Rate Limiting" refer to?
 - A) Allowing unlimited access to APIs
 - B) Speeding up API responses
 - *C) Restricting the number of requests to an API*
 - D) Making APIs accessible to all users

68. Which of the following is a common mobile app attack vector?
 - A) Physical access to devices
 - *B) Network-based attacks*
 - C) Denial of Service
 - D) Social engineering

69. What is the main focus of mobile application hardening?
 - *A) Reducing the attack surface*
 - B) Improving user experience
 - C) Enhancing performance
 - D) Increasing app size

70. Which vulnerability allows attackers to execute scripts on behalf of users?
 - A) SQL Injection
 - B) CSRF
 - *C) Cross-Site Scripting (XSS)*
 - D) Clickjacking

71. What is the risk of using sensitive data in URLs?
 - A) Improved SEO
 - *B) Data exposure in logs and referrer headers*
 - C) Increased performance
 - D) Easier tracking

72. Which of the following is a best practice for securing mobile applications?
 - *A) Regular security updates*
 - B) Using unsecured APIs
 - C) Storing sensitive data in plain text
 - D) Disabling authentication

73. What is a common method for conducting mobile application security testing?
 - A) Manual code review only
 - B) User experience testing only
 - *C) Automated and manual testing combined*
 - D) Network testing only

74. What is the impact of enabling insecure permissions in mobile apps?
 - A) Improved functionality
 - *B) Increased risk of data breaches*
 - C) Faster app performance
 - D) Enhanced user interface

75. Which of the following is an indicator of a successful SQL Injection attack?
 - A) Application crashes
 - B) Increased latency
 - *C) Unexpected database results*

- D) User authentication failures

76. What is the main goal of a penetration test on a mobile application?
- A) Improve user interface design
- *B) Identify security vulnerabilities*
- C) Optimize performance
- D) Ensure regulatory compliance

77. What does "data at rest" refer to?
- A) Data in transit
- *B) Stored data on devices*
- C) Data in memory
- D) Temporary data

78. Which of the following is a consequence of using weak encryption?
- A) Faster processing
- *B) Data breaches*
- C) Improved user experience
- D) Increased app size

79. What does "client-side validation" help prevent?
- *A) Basic input validation*
- B) SQL Injection
- C) Cross-Site Scripting
- D) Data leakage

80. What is the main concern with hardcoded API keys in mobile apps?
- A) Increased performance

- B) User confusion
- *C) Unauthorized access to APIs*
- D) Reduced functionality

81. Which OWASP risk focuses on the improper handling of sensitive data?
- A) Insecure Data Storage
- *B) Sensitive Data Exposure*
- C) Security Misconfiguration
- D) Broken Authentication

82. What does the term "physical security" refer to in mobile app security?
- A) Network security
- B) Data encryption
- *C) Protecting devices from unauthorized access*
- D) User authentication

83. What is the primary risk of not using secure communication protocols

?
- *A) Data interception*
- B) Increased latency
- C) Application crashes
- D) Performance degradation

84. Which of the following is a characteristic of a well-designed API?
- *A) Proper authentication and authorization*
- B) Unlimited access
- C) Lack of documentation

- D) Inconsistent responses

85. What is the impact of improper session handling in mobile apps?
- A) Increased user engagement
- *B) Session hijacking*
- C) Improved performance
- D) Enhanced security

86. Which technique is used to mitigate CSRF attacks?
- A) User input validation
- *B) Anti-CSRF tokens*
- C) Data encryption
- D) Access control

87. What is the primary risk of using an outdated mobile application framework?
- A) Improved performance
- *B) Exposure to known vulnerabilities*
- C) Increased user engagement
- D) Reduced development time

88. What does "secure coding practices" help prevent?
- A) User confusion
- *B) Security vulnerabilities*
- C) Performance issues
- D) Poor user interface design

89. What is a common tool for API testing in mobile applications?
- A) Wireshark

- B) Nessus
- *C) Postman*
- D) Nmap

90. What does the term "data exfiltration" mean?
- A) Data encryption
- *B) Unauthorized transfer of data*
- C) Data storage
- D) Data processing

91. Which OWASP vulnerability deals with insufficient input validation?
- A) Insecure Data Storage
- *B) Injection*
- C) Broken Access Control
- D) Security Misconfiguration

92. What is the risk of storing sensitive data in the app's local storage?
- *A) Data theft if the device is compromised*
- B) Improved app performance
- C) Increased user engagement
- D) Enhanced user experience

93. What is a common sign of a successful CSRF attack?
- *A) Unauthorized actions performed on behalf of the user*
- B) Increased app crashes
- C) Slower application performance
- D) User confusion

94. What is the impact of using insecure HTTP methods?
 - A) Increased performance
 - *B) Security vulnerabilities*
 - C) Better user experience
 - D) Reduced data size

95. What does "session timeout" refer to?
 - A) Extended session duration
 - *B) Automatic logout after inactivity*
 - C) Improved performance
 - D) Increased user engagement

96. What is the primary goal of data encryption?
 - A) Increase app size
 - *B) Protect sensitive data from unauthorized access*
 - C) Improve performance
 - D) Enhance user experience

97. Which of the following is an indicator of a poorly designed API?
 - A) Comprehensive documentation
 - B) Proper authentication
 - *C) Lack of input validation*
 - D) Consistent responses

98. What does "data integrity" ensure?
 - A) Faster processing
 - B) Improved user experience
 - *C) Accuracy and consistency of data*
 - D) Enhanced performance

99. Which of the following is a common consequence of poor app security?
 - A) Increased performance
 - *B) Data breaches*
 - C) Improved user engagement
 - D) Enhanced user interface

100. What is the purpose of security awareness training for developers?
 - A) Improve coding speed
 - B) Enhance user experience
 - *C) Educate about secure coding practices and vulnerabilities*
 - D) Reduce development costs

Feel free to ask if you need more information on any of these topics! Good luck with your quiz preparation!