⍰ EASY (Q1–Q10)

Q1. OWASP Mobile Top 10 focuses on:
A. Desktop OS vulnerabilities
B. Mobile application security risks
C. Network hardware issues
D. Cloud infrastructure

Q2. Insecure data storage mainly affects:
A. Availability
B. Confidentiality
C. Performance
D. Usability

Q3. Weak authentication allows attackers to:
A. Encrypt data
B. Bypass login mechanisms
C. Improve security
D. Patch apps

Q4. Insecure communication occurs when apps:
A. Use TLS
B. Transmit data without encryption
C. Use certificates
D. Validate servers

Q5. Client-side injection in mobile apps is similar to:
A. Buffer overflow
B. XSS in web applications
C. SQL backup
D. Port scanning

Q6. Reverse engineering of APKs allows attackers to:
A. Improve app performance
B. Understand app logic and secrets
C. Patch vulnerabilities
D. Encrypt code

Q7. Code tampering modifies:
A. Network traffic
B. Application binaries
C. Device firmware
D. DNS records

Q8. Extraneous functionality refers to:
A. Extra security features
B. Hidden or debug features in production apps
C. App permissions
D. Network services

Q9. Improper platform usage means:
A. Using OS APIs incorrectly
B. Using strong encryption
C. Enabling SELinux
D. Following best practices

Q10. Smishing attacks are delivered via:
A. Email
B. SMS messages
C. Voice calls
D. Bluetooth

□ MEDIUM (Q11–Q25)

Q11. Insecure data storage examples include:
A. Encrypted SharedPreferences
B. Plaintext credentials in files
C. Secure keystore usage
D. Encrypted databases

Q12. Weak authentication often results from:
A. Multi-factor authentication
B. Poor session management
C. Secure tokens
D. Certificate pinning

Q13. Insufficient cryptography refers to:
A. Strong encryption algorithms
B. Incorrect or weak encryption usage
C. Certificate validation
D. Hashing passwords

Q14. Insecure authorization allows attackers to:
A. Access unauthorized features or data
B. Encrypt files
C. Improve availability
D. Patch vulnerabilities

Q15. Intent abuse occurs when:
A. Intents are encrypted
B. Components are exported without restriction
C. Permissions are validated
D. SELinux blocks access

Q16. Reverse engineering attacks are easier when apps:
A. Use obfuscation
B. Lack code obfuscation
C. Use ProGuard
D. Use R8

Q17. Repackaging attacks involve:
A. Updating apps
B. Modifying and redistributing apps
C. Encrypting APKs
D. Signing apps securely

Q18. Runtime manipulation attacks modify apps:
A. Before installation
B. During execution
C. Only at compile time
D. Only in storage

Q19. WebView vulnerabilities arise when:
A. JavaScript is disabled
B. Unsafe JavaScript interfaces are exposed
C. TLS is used
D. Certificates are pinned

Q20. Smishing attacks primarily exploit:
A. Cryptographic flaws
B. User trust and urgency
C. Kernel bugs
D. Network latency

Q21. Android app attack surface includes:
A. Activities and Services
B. Broadcast Receivers
C. Content Providers
D. All of the above

Q22. Code obfuscation helps defend against:
A. Network attacks
B. Reverse engineering
C. SQL injection
D. MITM attacks

Q23. Improper platform usage can lead to:
A. Secure execution
B. Data leakage and privilege escalation
C. Faster performance
D. Better UX

Q24. Static mobile testing focuses on:
A. Runtime behavior
B. Source code and APK analysis
C. Network traffic only
D. User actions

Q25. Dynamic mobile testing focuses on:
A. APK signing
B. App behavior during execution
C. Source code review
D. Build process

HARD (Q26–Q40)

Q26. Insecure data storage becomes critical when:
A. Device is encrypted
B. Device is rooted
C. TLS is enabled
D. SELinux is enforcing

Q27. Weak authentication combined with insecure storage enables:
A. DoS attacks
B. Account takeover
C. Network scanning
D. IDS evasion

Q28. Certificate pinning prevents:
A. SQL injection
B. Man-in-the-Middle attacks
C. Reverse engineering
D. Root detection

Q29. Client-side injection is dangerous because:
A. Server validates input
B. Attacker controls execution context
C. Encryption is used
D. Permissions are restricted

Q30. Reverse engineering threatens intellectual property by:
A. Encrypting binaries
B. Exposing business logic
C. Improving security
D. Increasing performance

Q31. Runtime manipulation tools can bypass:
A. Network firewalls
B. Client-side security checks
C. IDS rules
D. Kernel security

Q32. Improper export of Android components leads to:
A. Secure IPC
B. Unauthorized access by other apps
C. Encryption
D. OS crash

Q33. Smishing is harder to detect because:
A. SMS is encrypted
B. Messages appear legitimate
C. IDS blocks it
D. Firewalls prevent it

Q34. Repackaged malware apps often include:
A. Improved UI
B. Additional malicious payloads
C. Stronger encryption
D. Signed certificates

Q35. Reverse engineering countermeasures include:
A. Hardcoding secrets
B. Code obfuscation and tamper detection
C. Debug flags
D. Exported components

Q36. WebView JavaScript bridges are dangerous if:
A. Properly validated
B. Exposed without access control
C. TLS is enabled
D. Cookies are secure

Q37. OWASP Mobile Top 10 differs from Web Top 10 because:
A. Mobile apps lack backend
B. Mobile apps involve client-side risks
C. Web apps are secure
D. Networks differ

Q38. Static analysis may miss vulnerabilities because:
A. Code is visible
B. Runtime behavior is unknown
C. APK is encrypted
D. Permissions are declared

Q39. Dynamic analysis limitations include:
A. No execution
B. Malware detecting test environment
C. No reports
D. No logs

Q40. Secure mobile app defense requires:
A. One control
B. Secure coding + testing + platform security
C. Antivirus only
D. User ignorance