Exam : **ADR-001**

Title : CompTIA Mobile App Security+ Certification Exam (Android Edition)

Version : DEMO

1.Which of the following is a reason to take mobile app security seriously when developing a social networking app that does NOT accept payments? (Select TWO).
A.PCI-DSS regulations
B.Consumer privacy expectations and regulations
C.HIPAA regulations
D.FIPS compliance
E.Company reputation
Answer: B,E

2.Which of the following accurately explains why many people criticize the use of a unique hardware ID such as IMEI/MEID to identify users? (Select TWO).
A.The hardware ID can be traced to an individual user and help track activity over time and across apps
B.The hardware ID unlocks encryption on the device
C.Companies encode email addresses directly into the hardware ID
D.Hardware ID values are easily predictable
E.Users cannot selectively block apps' access to it
Answer: A,E

3.Which of the following attempts to inhibit an application from being trojanized and proliferating?
A.Tamper protection in code.
B.Encrypting config file.
C.Ensure appropriate permissions are deployed to every component.
D.Login credentials delivered over network with HTTPS.
Answer: A

4.Which of the following is fundamental to MOST transport layer encryption implementations?
A.Device passcode
B.Obfuscation
C.HTTPS
D.Keychain
Answer: C

5.Which of the following can be performed to find security design flaws in mobile apps prior to writing code?
A.Threat modeling
B.Penetration testing
C.Static source code analysis
D.Dynamic validation testing
Answer: A

6.Which of the following methodologies is BEST for a developer to find input validation weaknesses in their own mobile app source code?
A.Disassembly of mobile app executable
B.Threat modeling

C.Fuzz testing an app’s attack surface
D.Single stepping an app through a debugger
Answer: C

7.Which of the following techniques are useful in a secure software development process? (Select TWO).
A.Cross platform compatibility testing with HTML5
B.Using hardware encryption to protect all data on the device
C.Static code analysis
D.Abuse/misuse case analysis
E.Implementation of two-factor authentication
Answer: C,D

8.Which of the following will LEAST likely be detected through source code analysis?
A.Improper certificate validation
B.Buffer overflow vulnerability
C.Improper build process
D.Hardcoded credentials
Answer: C

9.Which of the following is the MOST reliable form of input validation?
A.Positive validation of input data using regular expression processing
B.Base64 encoding of input data
C.Validating the bounds of input data using a character set
D.HTML or URI encoding of input data and ensuring Unicode support
Answer: A

10.When handling sensitive data with Android apps, which of the following storage strategies is MOST secure?
A.Store data on device using encryption, with encryption key managed on the server
B.Prompt users to enable encryption
C.Store sensitive data locally in XML protected with file permissions
D.Store sensitive data on the server
Answer: D

11.Which of the following describes a best practice in a software system?
A.Security through obscurity
B.Hardcoded encryption keys
C.Principle of least privilege
D.Trust session implicitly
Answer: C

12.Which of the following provides an enumeration of software weaknesses to be avoided?
A.Open IOC (MANDIANT)
B.Metasploit Framework (RAPID7)

C.NVD (NIST)
D.CWE (MITRE)
Answer: D

13.A developer is using a third-party cloud service via Web APIs for backup of unencrypted user photos.The use of this service is invisible to the end user.Incorporation of this service into the application introduces which potential key security risk?
A.User data breach on cloud provider’s systems
B.Breaking backward compatibility
C.Reflected XSS
D.Application instability in case of cloud provider outage
Answer: A

14.Which of the following is true regarding DNS?
A.Each DNS request is uniquely encrypted
B.DNS security is by design difficult to tamper
C.Secure host name resolution is assured globally by ICANN
D.DNS on most public Wi-Fi has little security
Answer: D

15.Which of the following is an effective means of confirming data integrity?
A.File access control
B.Set the No execute (NX) bit on data segment in memory
C.Base64 encoding
D.Digital signatures
Answer: D

16.When reviewing the security architecture of a mobile app, which of the following is the MOST important piece of data to start with?
A.UI wireframes and process flows
B.Diagram/flowchart of all app components
C.Source code
D.Test plans
Answer: B

17.An architectural review is BEST for finding which of the following security defects?
A.Malware infection vectors
B.SQL or other injection flaws
C.Design flaws
D.Zero-day vulnerabilities
Answer: C

18.Which of the following describes a security risk that may have to be accepted when using a commercial cross-platform mobile application framework?

A.Allowing code to run outside the app sandbox
B.Installing HTML 5 support on user device
C.Digest authentication without HTTPS
D.Using native code libraries without source code review
Answer: D

19.In an application architecture diagram, what categories of weaknesses are considered using Microsoft's threat modeling process?
A.Man-in-the-middle, Data injection, SQL Injection, Malware, Zero-day exploits
B.Damage, Reproducibility, Exploitability, Affected users, Discoverability
C.Spoofing, Tampering, Repudiation, Information disclosure, Denial of service, Elevation of privilege
D.Cross site scripting, Clickjacking, Data input validation, SSL, RSA security, Buffer overflow, Heap smashing, ARP injection
Answer: C

20.Android's kernel-level app sandbox provides security by:
A.assigning a unique user ID (UID) to each app and running in a separate process.
B.running all apps under an unprivileged group ID (GID).
C.restricting read access to an app's package to the kernel process.
D.preventing an app's data files from being read by any running process.
Answer: A