

考試編碼:ADR-001

考試名稱:CompTIA Mobile App  
Security+ Certification Exam (Android  
Edition)

版本: Demo

<http://exam24.net/>

QUESTION NO: 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

QUESTION NO: 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

QUESTION NO: 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

QUESTION NO: 4

Which of the following is fundamental to MOST transport layer encryption implementations?

- A. Device passcode

- B. Obfuscation
- C. HTTPS
- D. Keychain

Answer: C

QUESTION NO: 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

QUESTION NO: 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

QUESTION NO: 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

QUESTION NO: 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

QUESTION NO: 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

QUESTION NO: 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