2014 Latest CompTIA ADR-001 Exam Dump Free Download!

QUESTION 1 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 QUESTION 2 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 QUESTION 3 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 QUESTION 4 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 QUESTION 5 The digital certificate used to sign the production release should be: A.   regenerated for each version of the app. B.   stored inside the app package before deployment. C.   stored in a secure location separate from the passphrase. D.   stored with the source code so all developers can build the app. Answer: C QUESTION 6 Which statement about native code in apps is TRUE? A.   Native code is faster because it runs as a separate user ID (UID) giving it direct access to restricted APIs. B.   Native code is run under the same user ID (UID) as the Java app and therefore comes under the same sandbox restrictions. C.   Native code is executed by the kernel with increased privileges and is mainly used for root operations. D.   Native code runs outside the Dalvik VM and therefore is not restricted by the sandbox. Answer: B QUESTION 7 When an app creates a configuration file in its private data directory the developer should ensure: A.   that the file path is determined with getExternalStorageDirectory(). B.   that the file is created world writable. C.   that file ownership is set to system. D.   that the file is not created world readable. Answer: D QUESTION 8 An example of APIs protected by permissions would bE. (Select TWO). A.   SIM card access B.   Telephony functions C.   File handling functions D.   Encryption functions E.   Network/data connections Answer: BE QUESTION 9 An app accessing protected APIs should use which manifest declaration? A.   app-permissions B.   add-permissions C.   grant-permission D.   uses-permission Answer: D QUESTION 10 The MOST likely reason the developer might want to define their own permission in the manifest is because: A.   they wish to ensure that only their app has the permission to launch their activities or access their private data. B.   they wish to prevent the user from granting access to protected functionality by mistake. C.   they wish to define a permission to access system APIs and native libraries. D.   they wish to restrict access to a function in their app to only those apps which are specifically granted access by the user. Answer: D QUESTION 11 Valid permission protection levels are. (Select TWO). A.   private B.   signature C.   user D.   public E.   dangerous Answer: BE QUESTION 12 The checkCallingPermission() method is used when: A.   the app needs to determine what permission is required for it to make a call. B.   the app needs to determine if it should allow an incoming call from another app. C.   the app needs to determine whether it has permission to make a call. D.   the app needs to determine what permissions are required to call a specific API. Answer: B QUESTION 13 Which of the following is a more secure way for a developer to give 3rd party apps temporary access to resources in their app, such as opening attachments in an external editor? A.   Make use of grantTempAccess() B.   Make use of per-URI permissions C.   Temporarily make files world readable D.   Temporarily store files on SD Card Answer: B Passing your CompTIA ADR-001 Exam by using the latest CompTIA ADR-001 Exam Dump Full Version: http://www.braindump2go.com/adr-001.html