CompTIA

Exam ADR-001

CompTIA Mobile App Security+ Certification Exam (Android Edition)

Version: 6.0

[Total Questions: 102]

Question No : 1

An Intent Sniffing attack is where:

A. a malicious app intercepts network communications to capture Intent traffic.
B. cached Intent messages are read from storage by an attacker.
C. Intent declarations are read from the manifest in order to construct spoof Intents.
D. a malicious app registers to receive public broadcasts in order to intercept data.

Answer: D

Question No : 2

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

Question No : 3

A file with Unix permissions '700' allows:

A. all users to read, write and execute.
B. full access to the app that created it and no other apps.
C. only the system and root access.
D. for protected storage on the shared SD card.

Answer: B

Question No : 4

In the AndroidManifest.xml file which element is used to define the permissions an app is

requesting access to?

A. <uses-permission>
B. <permission>
C. <grant-uri-permissions>
D. <activity>

Answer: A

Question No : 5

Which of the following BEST describes the responsibility of a TrustManager object when used in an Android application with SSL?

A. The TrustManager verifies that a Certificate Authority truly did issue a server's SSL certificate by using the Online Certificate Status Protocol (OCSP).
B. The TrustManager manages the client-side SSL certificate that the Android application will present to a server for mutual authentication.
C. The TrustManager makes decisions on if a server's SSL certificate should be trusted, by allowing the developer to specify which certificates should be allowed.
D. The TrustManager verifies that a server's SSL certificate has not been revoked by checking the Certificate Authority's Certificate Revocation List (CRL).

Answer: C

Question No : 6

A developer is designing a very sensitive web application that will be accessed by both desktop web browsers and mobile Android applications. What is one way the developer can implement a multi-factor authentication system for these users?

A. Have the user memorize a PIN in addition to their password and require them to supply both when attempting to log in.
B. Have the user answer a security question once they authenticate using their username and password.
C. Require a one-time-use code sent via an SMS message in addition to a username and password.
D. Have the user supply their last password in addition to their current password when they attempt to log in.

Answer: C

Question No : 7

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 : 8

When an app "logs out" of a back end system the developer should also ensure:

A. app jumps to device home screen, clearing the data from the previous session.
B. GUI components displaying data while logged in are destroyed as Android does not do this.
C. app switches back to login screen forcing the user to re-login to view the data.
D. app maintains the state of the session ID in the key chain.

Answer: B

Question No : 9

Which of the following is a disadvantage of using a static embedded API Key for client authentication to a web service?

A. API Keys require the use of a certificate issued by a commercial Certificate Authority.
B. API Keys are used with asymmetric cryptography, which is slow and can negatively impact the performance of the client application.
C. API Keys cannot be transmitted over HTTPS, so they are open to compromise.
D. API Keys can be discovered and abused by an attacker.

Answer: D

Question No : 10

When applying PBKDF2 to a password, what would be the MORE secure number of iterations to use?

A. 100
B. 1,000
C. 2,000
D. 10,000

Answer: D

Question No : 11

Adding an Intent Filter to an Activity could cause a security issue because:

A. activities with Intent Filters are unprivileged by default.
B. it bypasses Android's default filters.
C. activities with Intent Filters are exported by default.
D. it violates the Android sandbox security model.

Answer: C

Question No : 12

Which of the following describes why a developer should define private wrappers around native and public native methods?

A. To prevent untrusted callers from invoking native methods.
B. To filter data that is sent to the native methods.
C. Because native methods cannot be called directly.
D. To impose naming convention on methods.

Answer: A

Question No : 13

How does HTTP Basic Authentication work?

A. A client-specific secret value is combined with a server-specific secret value to form a master secret, which is then used to sign all communications.
B. A one-time use token (nonce) is generated by the server and sent to the client, where it is then returned on each subsequent request.
C. A digital signature is generated of the request using the client's private key and sent to the server.
D. A username and password are combined into a string on the client, base 64 encoded, and then sent to the server as an HTTP header.

Answer: D

Question No : 14

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

Question No : 15

Which of the following is TRUE regarding permissions?

A. Users cannot review permissions before installing an app
B. Android permissions do not change between versions
C. Over-permissioned apps increase the risk to the end user
D. Apps are granted access to contacts data without requesting permissions

Answer: C

Question No : 16

Which of the following describes what is wrong with the following sample code?

public class MyActivity extends Activity{

public void onCreate(Bundle myBundle){

foo( );

}

}

A. The method onCreate must be private.
B. A developer cannot extend Activity.
C. A call is missing to super.onCreate(mybundle).
D. The class MyActivity must be private.

Answer: C

Question No : 17

Which of the following is true about methods that receive an array as a parameter?

A. The developer should never use an array as a parameter because it will cause a buffer overflow.
B. The developer should expose the array so it can be modified outside the class.
C. The developer should clear the array first.
D. The developer should clone the array object and store the copy.

Answer: D

Question No : 18

Why is it necessary to pass session tokens over a secure, encrypted channel?

A. Revealing the session token over an unsecured channel would allow an attacker to determine the private key used to generate the token.
B. Session tokens can be used to reveal the physical location of the Android device.
C. Session tokens contain the user password.
D. Session tokens can be presented to the application allowing an attacker to impersonate

a valid user.

Answer: D

Question No : 19

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

Question No : 20

Which of the following BEST describes a process or mechanism to thwart reverse engineering through software fault injection?

A. Dumping stack trace information
B. Handling of program exceptions
C. Altering of class names and/or method names
D. Eliminating dead, i.e. unreachable, code

Answer: B

Question No : 21

Session keys are useful because:

A. they temporarily provide a mechanism to maintain the state of user interaction.
B. they are generated on the Android device locally upon startup.
C. there is only one key to generate.
D. they are more secure than public/private keys.

Answer: A

Question No : 22

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 No : 23

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 No : 24

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

Question No : 25

Which of the following describes the purpose of the HTTPOnly cookie attribute?

A. This attribute ensures that such cookies are only sent over HTTP connections and not over SSL making them unusable.
B. This attribute requests that clients use the cookie only for HTTP connections and not expose it to client-side scripting.
C. This attribute requests that other protocols cannot access such cookies.
D. This attribute ensures that such cookies are only transmitted over an encrypted connection.

Answer: B

Question No : 26

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 No : 27

Which of the following defines the difference between static and dynamic analysis of an application?

A. Static analysis can be used against encrypted code and is able to determine the actual instructions running on a device, while dynamic analysis is easily fooled when code is encrypted.
B. Static analysis consists of examining an application's code as it is provided, while dynamic analysis consists of examining the application as it runs on an emulator or other debugging environment.
C. Static analysis is focused solely on the recovery of string and hardcoded values while

dynamic analysis aims to understand the function of the code itself.
D. Static analysis requires a dataflow-modeling tool to examine all data paths, while dynamic analysis can be conducted using only an Android device.

Answer: B

Question No : 28

Which of the following statements is TRUE about session tokens?

A. Session tokens should be unpredictable and be short to derive a maximum security benefit with minimal storage.
B. Session tokens should be reused every time a particular user logs in.
C. Session tokens should be an obfuscated or encrypted version of the user's ID.
D. Session tokens should be unpredictable, of sufficient length and contain no information about the user.

Answer: D

Question No : 29

Why are file permissions important to security?

A. They prevent files from being transmitted to another device.
B. They hide files in the file system.
C. They provide links to files outside the sandbox.
D. They determine which processes can read files.

Answer: D

Question No : 30

On an unencrypted rooted Android device, which of the following BEST describes which data is recoverable?

A. Active data and some deleted data.
B. Active data and none of the deleted data.

C. Only some active data and no deleted data.
D. Only some active data and some deleted data.

Answer: A

Question No : 31

If a Java package contains sensitive data in one or more classes, and the data is declared public, what attacks does that expose?

A. Public data can be intercepted in transit using network sniffing tools.
B. Malicious code can declare itself as part of the same package, and directly access the public data with no means of protection.
C. Public data can be accessed (read-write) via HTTP POST/POST arguments.
D. The sensitive public data gets cached on the Java server, and is thus searchable using traditional enterprise intranet search tools.

Answer: B

Question No : 32

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 : 33

Which of the following is the primary reason for web services to output encode all data sent to Android application clients?

Microsoft Exams List

70-246 Dump PDF VCE	70-485 Dump PDF VCE	70-742 Dump PDF VCE	98-366 Dump PDF VCE
70-247 Dump PDF VCE	70-486 Dump PDF VCE	70-743 Dump PDF VCE	98-367 Dump PDF VCE
70-331 Dump PDF VCE	70-487 Dump PDF VCE	70-744 Dump PDF VCE	98-368 Dump PDF VCE
70-332 Dump PDF VCE	70-488 Dump PDF VCE	70-761 Dump PDF VCE	98-369 Dump PDF VCE
70-333 Dump PDF VCE	70-489 Dump PDF VCE	70-762 Dump PDF VCE	98-372 Dump PDF VCE
70-334 Dump PDF VCE	70-490 Dump PDF VCE	70-765 Dump PDF VCE	98-373 Dump PDF VCE
70-339 Dump PDF VCE	70-491 Dump PDF VCE	70-768 Dump PDF VCE	98-374 Dump PDF VCE
70-341 Dump PDF VCE	70-492 Dump PDF VCE	70-980 Dump PDF VCE	98-375 Dump PDF VCE
70-342 Dump PDF VCE	70-494 Dump PDF VCE	70-981 Dump PDF VCE	98-379 Dump PDF VCE
70-345 Dump PDF VCE	70-496 Dump PDF VCE	70-982 Dump PDF VCE	MB2-700 Dump PDF VCE
70-346 Dump PDF VCE	70-497 Dump PDF VCE	74-343 Dump PDF VCE	MB2-701 Dump PDF VCE
70-347 Dump PDF VCE	70-498 Dump PDF VCE	74-344 Dump PDF VCE	MB2-702 Dump PDF VCE
70-348 Dump PDF VCE	70-499 Dump PDF VCE	74-409 Dump PDF VCE	MB2-703 Dump PDF VCE
70-354 Dump PDF VCE	70-517 Dump PDF VCE	74-678 Dump PDF VCE	MB2-704 Dump PDF VCE
70-383 Dump PDF VCE	70-532 Dump PDF VCE	74-697 Dump PDF VCE	MB2-707 Dump PDF VCE
70-384 Dump PDF VCE	70-533 Dump PDF VCE	77-420 Dump PDF VCE	MB2-710 Dump PDF VCE
70-385 Dump PDF VCE	70-534 Dump PDF VCE	77-427 Dump PDF VCE	MB2-711 Dump PDF VCE
70-410 Dump PDF VCE	70-640 Dump PDF VCE	77-600 Dump PDF VCE	MB2-712 Dump PDF VCE
70-411 Dump PDF VCE	70-642 Dump PDF VCE	77-601 Dump PDF VCE	MB2-713 Dump PDF VCE
70-412 Dump PDF VCE	70-646 Dump PDF VCE	77-602 Dump PDF VCE	MB2-714 Dump PDF VCE
70-413 Dump PDF VCE	70-673 Dump PDF VCE	77-603 Dump PDF VCE	MB2-715 Dump PDF VCE
70-414 Dump PDF VCE	70-680 Dump PDF VCE	77-604 Dump PDF VCE	MB2-716 Dump PDF VCE
70-417 Dump PDF VCE	70-681 Dump PDF VCE	77-605 Dump PDF VCE	MB2-717 Dump PDF VCE
70-461 Dump PDF VCE	70-682 Dump PDF VCE	77-881 Dump PDF VCE	MB2-718 Dump PDF VCE
70-462 Dump PDF VCE	70-684 Dump PDF VCE	77-882 Dump PDF VCE	MB5-705 Dump PDF VCE
70-463 Dump PDF VCE	70-685 Dump PDF VCE	77-883 Dump PDF VCE	MB6-700 Dump PDF VCE
70-464 Dump PDF VCE	70-686 Dump PDF VCE	77-884 Dump PDF VCE	MB6-701 Dump PDF VCE
70-465 Dump PDF VCE	70-687 Dump PDF VCE	77-885 Dump PDF VCE	MB6-702 Dump PDF VCE
70-466 Dump PDF VCE	70-688 Dump PDF VCE	77-886 Dump PDF VCE	MB6-703 Dump PDF VCE
70-467 Dump PDF VCE	70-689 Dump PDF VCE	77-887 Dump PDF VCE	MB6-704 Dump PDF VCE
70-469 Dump PDF VCE	70-692 Dump PDF VCE	77-888 Dump PDF VCE	MB6-705 Dump PDF VCE
70-470 Dump PDF VCE	70-695 Dump PDF VCE	77-891 Dump PDF VCE	MB6-884 Dump PDF VCE
70-473 Dump PDF VCE	70-696 Dump PDF VCE	98-349 Dump PDF VCE	MB6-885 Dump PDF VCE
70-480 Dump PDF VCE	70-697 Dump PDF VCE	98-361 Dump PDF VCE	MB6-886 Dump PDF VCE
70-481 Dump PDF VCE	70-698 Dump PDF VCE	98-362 Dump PDF VCE	MB6-889 Dump PDF VCE
70-482 Dump PDF VCE	70-734 Dump PDF VCE	98-363 Dump PDF VCE	MB6-890 Dump PDF VCE
70-483 Dump PDF VCE	70-740 Dump PDF VCE	98-364 Dump PDF VCE	MB6-892 Dump PDF VCE
70-484 Dump PDF VCE	70-741 Dump PDF VCE	98-365 Dump PDF VCE	MB6-893 Dump PDF VCE

Cisco Exams List

010-151 Dump PDF VCE	350-018 Dump PDF VCE	642-737 Dump PDF VCE	650-667 Dump PDF VCE
100-105 Dump PDF VCE	352-001 Dump PDF VCE	642-742 Dump PDF VCE	650-669 Dump PDF VCE
200-001 Dump PDF VCE	400-051 Dump PDF VCE	642-883 Dump PDF VCE	650-752 Dump PDF VCE
200-105 Dump PDF VCE	400-101 Dump PDF VCE	642-885 Dump PDF VCE	650-756 Dump PDF VCE
200-120 Dump PDF VCE	400-151 Dump PDF VCE	642-887 Dump PDF VCE	650-968 Dump PDF VCE
200-125 Dump PDF VCE	400-201 Dump PDF VCE	642-889 Dump PDF VCE	700-001 Dump PDF VCE
200-150 Dump PDF VCE	400-251 Dump PDF VCE	642-980 Dump PDF VCE	700-037 Dump PDF VCE
200-155 Dump PDF VCE	400-351 Dump PDF VCE	642-996 Dump PDF VCE	700-038 Dump PDF VCE
200-310 Dump PDF VCE	500-006 Dump PDF VCE	642-997 Dump PDF VCE	700-039 Dump PDF VCE
200-355 Dump PDF VCE	500-007 Dump PDF VCE	642-998 Dump PDF VCE	700-101 Dump PDF VCE
200-401 Dump PDF VCE	500-051 Dump PDF VCE	642-999 Dump PDF VCE	700-104 Dump PDF VCE
200-601 Dump PDF VCE	500-052 Dump PDF VCE	644-066 Dump PDF VCE	700-201 Dump PDF VCE
210-060 Dump PDF VCE	500-170 Dump PDF VCE	644-068 Dump PDF VCE	700-205 Dump PDF VCE
210-065 Dump PDF VCE	500-201 Dump PDF VCE	644-906 Dump PDF VCE	700-260 Dump PDF VCE
210-250 Dump PDF VCE	500-202 Dump PDF VCE	646-048 Dump PDF VCE	700-270 Dump PDF VCE
210-255 Dump PDF VCE	500-254 Dump PDF VCE	646-365 Dump PDF VCE	700-280 Dump PDF VCE
210-260 Dump PDF VCE	500-258 Dump PDF VCE	646-580 Dump PDF VCE	700-281 Dump PDF VCE
210-451 Dump PDF VCE	500-260 Dump PDF VCE	646-671 Dump PDF VCE	700-295 Dump PDF VCE
210-455 Dump PDF VCE	500-265 Dump PDF VCE	646-985 Dump PDF VCE	700-501 Dump PDF VCE
300-070 Dump PDF VCE	500-275 Dump PDF VCE	648-232 Dump PDF VCE	700-505 Dump PDF VCE
300-075 Dump PDF VCE	500-280 Dump PDF VCE	648-238 Dump PDF VCE	700-601 Dump PDF VCE
300-080 Dump PDF VCE	500-285 Dump PDF VCE	648-244 Dump PDF VCE	700-602 Dump PDF VCE
300-085 Dump PDF VCE	500-290 Dump PDF VCE	648-247 Dump PDF VCE	700-603 Dump PDF VCE
300-101 Dump PDF VCE	500-801 Dump PDF VCE	648-375 Dump PDF VCE	700-701 Dump PDF VCE
300-115 Dump PDF VCE	600-199 Dump PDF VCE	648-385 Dump PDF VCE	700-702 Dump PDF VCE
300-135 Dump PDF VCE	600-210 Dump PDF VCE	650-032 Dump PDF VCE	700-703 Dump PDF VCE
300-160 Dump PDF VCE	600-211 Dump PDF VCE	650-042 Dump PDF VCE	700-801 Dump PDF VCE
300-165 Dump PDF VCE	600-212 Dump PDF VCE	650-059 Dump PDF VCE	700-802 Dump PDF VCE
300-180 Dump PDF VCE	600-455 Dump PDF VCE	650-082 Dump PDF VCE	700-803 Dump PDF VCE
300-206 Dump PDF VCE	600-460 Dump PDF VCE	650-127 Dump PDF VCE	810-403 Dump PDF VCE
300-207 Dump PDF VCE	600-501 Dump PDF VCE	650-128 Dump PDF VCE	820-424 Dump PDF VCE
300-208 Dump PDF VCE	600-502 Dump PDF VCE	650-148 Dump PDF VCE	840-425 Dump PDF VCE
300-209 Dump PDF VCE	600-503 Dump PDF VCE	650-159 Dump PDF VCE	
300-210 Dump PDF VCE	600-504 Dump PDF VCE	650-281 Dump PDF VCE	
300-320 Dump PDF VCE	640-692 Dump PDF VCE	650-393 Dump PDF VCE	
300-360 Dump PDF VCE	640-875 Dump PDF VCE	650-472 Dump PDF VCE	
300-365 Dump PDF VCE	640-878 Dump PDF VCE	650-474 Dump PDF VCE	
300-370 Dump PDF VCE	640-911 Dump PDF VCE	650-575 Dump PDF VCE	
300-375 Dump PDF VCE	640-916 Dump PDF VCE	650-621 Dump PDF VCE	
300-465 Dump PDF VCE	642-035 Dump PDF VCE	650-663 Dump PDF VCE	
300-470 Dump PDF VCE	642-732 Dump PDF VCE	650-665 Dump PDF VCE	
300-475 Dump PDF VCE	642-747 Dump PDF VCE	650-754 Dump PDF VCE	

HOT EXAMS

Cisco

100-105 Dumps VCE PDF
200-105 Dumps VCE PDF
300-101 Dumps VCE PDF
300-115 Dumps VCE PDF
300-135 Dumps VCE PDF
300-320 Dumps VCE PDF
400-101 Dumps VCE PDF
640-911 Dumps VCE PDF
640-916 Dumps VCE PDF

Microsoft

70-410 Dumps VCE PDF
70-411 Dumps VCE PDF
70-412 Dumps VCE PDF
70-413 Dumps VCE PDF
70-414 Dumps VCE PDF
70-417 Dumps VCE PDF
70-461 Dumps VCE PDF
70-462 Dumps VCE PDF
70-463 Dumps VCE PDF
70-464 Dumps VCE PDF
70-465 Dumps VCE PDF
70-480 Dumps VCE PDF
70-483 Dumps VCE PDF
70-486 Dumps VCE PDF
70-487 Dumps VCE PDF

CompTIA

220-901 Dumps VCE PDF
220-902 Dumps VCE PDF
N10-006 Dumps VCE PDF
SY0-401 Dumps VCE PDF