Android

AND-802

Android Security Essentials

Version: 7.0

[Total Questions: 45]

Web: www.examsvce.com

Email: support@examsvce.com

IMPORTANT NOTICE

Feedback

We have developed quality product and state-of-art service to ensure our customers interest. If you have any suggestions, please feel free to contact us at feedback@examsvce.com

Support

If you have any questions about our product, please provide the following items:

- exam code
- screenshot of the question
- login id/email

please contact us at support@examsvce.com and our technical experts will provide support within 24 hours.

Copyright

Question #:1

Releasing updates of an application into Google Play requires signing it with the same certificate, or else all the previous users will not be notified of the update and eventually are lost.

A. True

B. False

[redacted]

Question #:2

Android SQLite database files are stored under the..... directory.

A. /data/database/<application-path>/databases/

B. /data/mydata/<application path>/databases/

C. /data/data/<applicabon-path>/databases/

D. /datatiles/<application-path>/databases/

[redacted]

Question #:3

Which of the following choices is one of the different levels of permission protection? (Select four)

A. Normal

B. Dangerous

C. Signature

D. Sharing

E. System

[redacted]

Question #:4

getExternalFilesDir( ) method is used to get the directory of the external storage.

A. True

B. False

[redacted]

Question #:5

Permissions required for an application to perform its operations are called application level permissions. Which are the types of application level permissions a developer can use? (Select two)

A. System-defined permissions.

B. Application-defined permissions.

C. GPS - defined permissions.

D. Payment - defined permissions.

[redacted]

Question #:6

Android stores cache files in the filesystem and sandboxes along with the application. Cache files are created under directory ……..

A. /data/data/<application-path>/cache/

B. /data/files/<application-path>/cache/

C. /data/personal/<application-path>/cache/

D. /data/cache/<application-path>/cache/

[redacted]

Question #:7

Your app receives location updates from NETWORK_PROVIDER or from GPS_PROVIDER. If your app receives location information from either of these location provider sources, you need to declare that the app uses these hardware features in your app manifest. Which of the following tags gives the location information to your app?

A. <uses-permission android:name=”android.permission.ACCESS_FINE_GPS” />

B. <uses-permission android:name=”android.permission.INTERNET” />

C. <uses-permission android:name=”android.permission.ACCESS_FINE_LOCATION” />

D. <uses-permission android:name=”android.permission.ACCESS_GPS_LOCATION” />

[redacted]

Question #:8

Android cache is Not considered as an Android application storage.

A. False

B. True

[redacted]

Question #:9

Which level of permissions is related to READ_CALENDAR, WRITE_CALENDAR, CAMERA, and READ_CONTACTS?

A. Normal Permissions or Level-Zero Permissions.

B. Dangerous Permissions or Level-one Permissions.

C. Signature Permission or Level-two Permissions.

D. Signature and System Permissions or Level-three Permissions.

[redacted]

Question #:10

Which of the following choices represent the flow of states of data within any app? (Select three)

A. Stored data

B. Data under processing

C. Data in transit

D. Printed Data

[redacted]

Question #:11

The Logcat window in Android Studio displays system messages, such as when a garbage collection occurs, and messages that you added to your app with the Log class. It displays messages in real time and keeps a history so that you can view older messages.

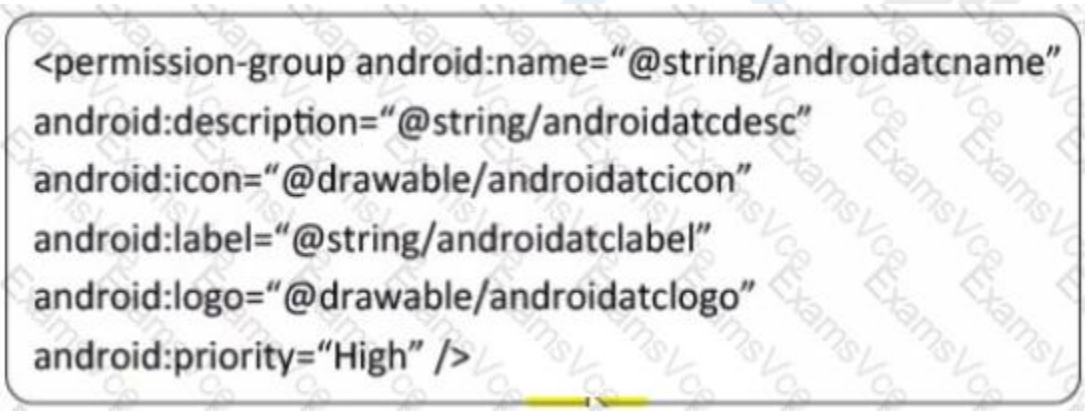
A. True

B. False

[redacted]

Question #:12

The following image includes a code of permission group. Where this code will be written in the Android app?



A. MainActivity.java or MainActivity.kt

B. AndroidManifest.xml

C. activity_main.xml

D. string.xml

[redacted]

Question #:13

You must use permissions to prevent unauthorized access to your application data.

A. False

B. True

[redacted]

Question #:14

A permission group is the concept of creating a group of all similar types of permissions, which will be presented together to the user during the installation time for approval.

A. False

B. True

[redacted]

Question #:15

By default, all Android applications have no permission to access any protected resource that would have adverse effects on the system or on other applications.

A. True

B. False

[redacted]

Question #:16

In the following image of code, what is the purpose of using MODE_PRIVATE in the method getPreferences( )?

```
class MainActivity : AppCompatActivity() {

    override fun onCreate(savedInstanceState: Bundle?) {
        super.onCreate(savedInstanceState)
        setContentView(R.layout.activity_main)
        save.setOnClickListener({
            savePreferences("save", enter_data.text.toString())
            show.isEnabled = true
        })
        show.setOnClickListener({
            load_data.setText(loadPreferences())
        })
        show.isEnabled = false

        /*
        * If there is no data currently stored then the
        * show button will be shown as disabled when
        * application is launched.
        */

        if (loadPreferences().isNotEmpty())
            show.isEnabled = true
    }

    private fun savePreferences(key: String, value: String) {

        val sharedPreferences = getPreferences(MODE_PRIVATE)
        val editor = sharedPreferences.edit()
        editor.putString(key, value)
editor.commit()
    }

    private fun loadPreferences(): String {
        val sharedPreferences = getPreferences(MODE_PRIVATE)
        val savedData = sharedPreferences.getString("save", "")
        return savedData
    }
}
```

A. This allows you to store data and make it private to this application. Also, No other applications can access your saved data.

B. This allows you to share your data with other applications which have the same mode.

C. This allows you to run your apps in Android API 27 or higher.

D. This allows you to run your app with minimum use of device battery.

[redacted]

Question #:17

Any application which would like to receive a message can receive the broadcast. Which of the following mechanisms can be used to protect broadcasts? (Select two)

A. Broadcast receiver decides which broadcast it will receive.

B. Broadcast receiver cannot decide which broadcast it will receive.

C. Broadcast decides which receiver can receive its broadcast.

D. Broadcast receiver does not decide which broadcast it will receive.

[redacted]

Question #:18

Android stores cache files in the filesystem and sandboxes along with the application. Cache files are created under directory ……..

A. /data/data/<application-path>/cache/

B. /data/files/<application-path>/cache/

C. /data/personal/<application-path>/cache/

D. /data/cache/<application-path>/cache/

[redacted]

Question #:19

What is the purpose of adding the following permission tag to your app's AndroidManifest.xml file?

<uses-permission android:name='android.permission.ACCESS_WIFI_STATE7>

A. Allows the application to access information about Wi-Fi networks.

B. Allows the application to access cache files' information.

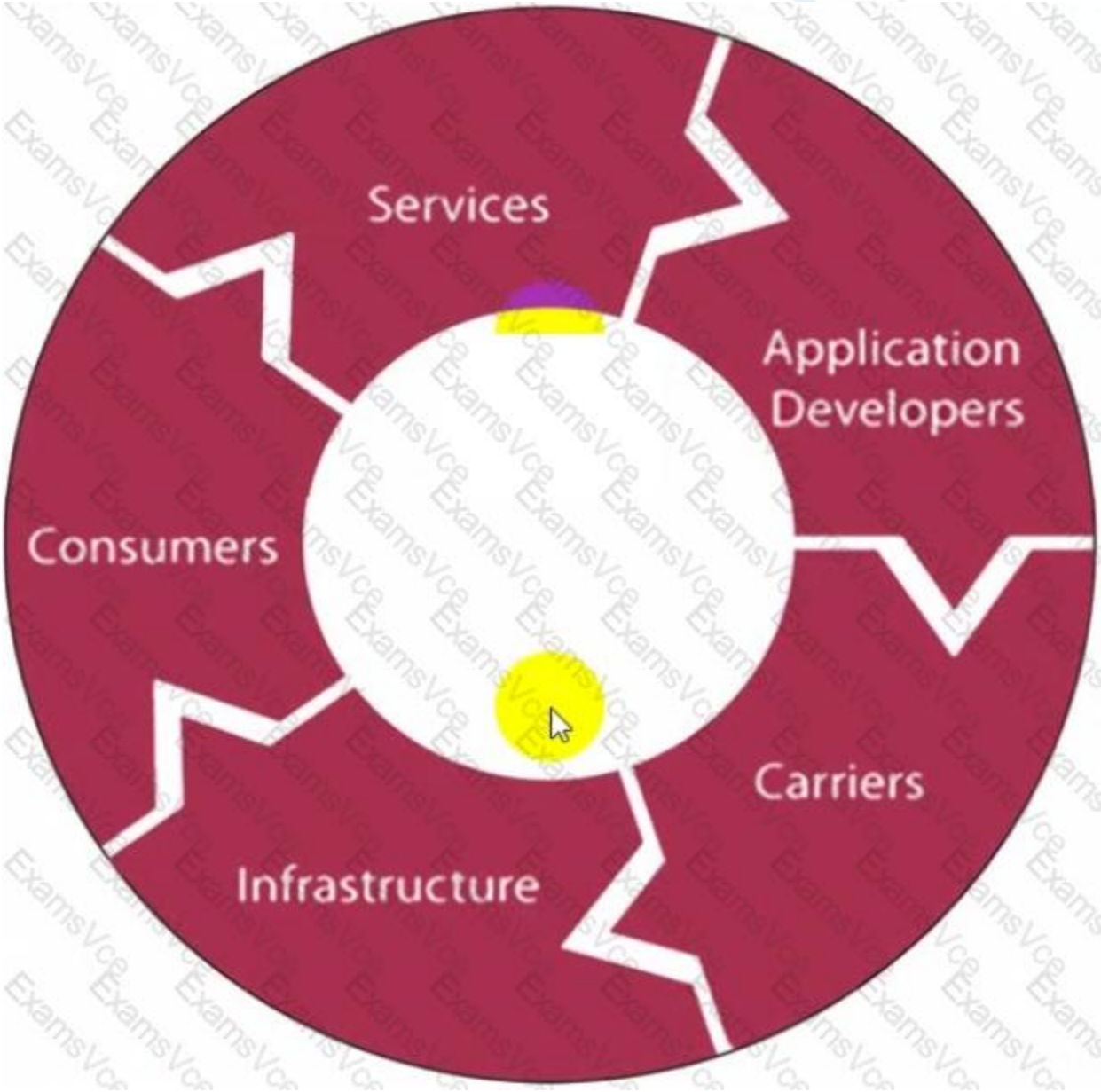
C. Allows the application to access internet .

D. Allows the application to access external storage.

[redacted]

Question #:20

The following image includes some components which you must be aware of to learn about the complexity of the security issue and the fact that software developers can only deal with security issues within their own applications. These components belong to …….



A. Mobile Environment.

B. Android Development.

C. Telephone Land Lines Network.

D. Internet.

[redacted]

Question #:21

If you are developing more than one application that is signed with the same certificate, and you want these applications to share access to each other's data and run in the same process, you need to give them the same ……

A. user ID (sharedUserId).

B. user name and password.

C. app description.

D. Ad unit ID.

[redacted]

Question #:22

Which of the following choices is considered Android application storage? (Select five)

A. SharedPreferences

B. Android's file system

C. External Storage

D. Cache

E. SQLite database

F. Microsoft Access

G. Text file

[redacted]

Question #:23

Android application developers can create custom permissions that should be labeled properly.

A. True

B. False

[redacted]

Question #:24

If you want to configure your app to receive an intent from another app, you should open AndroidManifest.xml file in your app, and then add ……. including the name and category which will be used in the second app's configuration.

A. intent filter.

B. user name and password.

C. certificate key.

D. Android mini version.

[redacted]

Question #:25

What is the purpose of adding the following permission tag to your app's AndroidManifest.xml file?

<uses-permission android:name="android.permission.INTERNET" />

A. Permission to connect the app to internet.

B. Permission to enable cookies' files on your app.

C. Permission to configure Chrome as default web browser.

D. Permission to open hidden internet connection.

[redacted]

Question #:26

What is the result of clicking Button1 in the code which is illustrated in the following image? Assuming that write_to_internal_storage is the name of an activity that allows users to write to internal storage.

```
Button1.setOnClickListener({
        startActivity(Intent(this, write_to_internal_storage::class.java))
    })
```

A. Creates an intent to open an activity that writes to the internal storage.

B. Creates an intent to open an activity that reads from the internal storage.

C. Creates an intent to open an activity that reads from the external storage.

D. Creates an intent to open an activity that writes to the external storage.

[redacted]

Question #:27

Any Android application can protect itself by declaring permissions that can be accessed by other applications. This can be achieved using the <permission> tag in the activity_main.xml file of the Android applications providing the permission.

A. True

B. False

[redacted]

Question #:28

Android uses “Intents” to communicate and send data between different components which make it vulnerable to malicious attacks. Which of the following choices are component-level Permissions to protect this type of communication? (Select Four)

A. Activity

B. Service

C. Content Provider

D. Broadcast Receiver

E. Widgets

[redacted]

Question #:29

If your database contains sensitive information, it is recommended not to store it on external storage. If you want to share the database with other applications, then you have to use a ……. to protect your app's data.

A. Separate Storage

B. Content Provider

C. Shared Folder

D. Internal Storage

[redacted]

Question #:30

What is the result of click the Button1 in the code which is illustrated in the following image? Assuming that write_to_external_storage is the name of an activity that allows users to write to external storage.

```
read_file_from_external_storage.setOnClickListener({
            startActivity(Intent(this, read_from_external_storage::class.java))
        })
```

A. Creates an intent to open an activity that writes to the internal storage.

B. Creates an intent to open an activity that reads from the internal storage.

C. Creates an intent to open an activity that reads from the external storage.

D. Creates an intent to open an activity that writes to the external storage.

[redacted]

Question #:31

Which of the following choices was added to AndroidManifest.xml to produce the following dialog below when the app tries to save data to external storage?

A. <usesandrold:name=-android.pemiission.WRITE_EXTERNAL_STORAGE"/>

B. <uses-permlssion android:name-"android.pennission.WRITE_TO_EXTERNAL_2_STORAGE"/>

C. <uses-petnHssion androtd:name-"android.WRITE EXTERNAL STORAGE"/>

D. <usespermlsslonandroid:name-"android.pernii»sion.WRITE_EXTERNAL_STORAGE"/>

E. <uses-permissionandroid:name="android.permission.WRITE_EXTERNAL_STORAGE"/>

[redacted]

Question #:32

It is not necessary that every application installed on an Android device be signed by the developer before being published.

A. True

B. False

[redacted]

Question #:33

Which of the following choices are considered as principles of data security? (Select three)

A. Confidentiality

B. Integrity

C. Availability

D. Independency

[redacted]

Question #:34

A digital certificate is an electronic “passport” that allows a person, computer or organization to exchange information securely over the Internet using the public key infrastructure (PKI).The message is encrypted with the Private key, and can only be decrypted with the Public key.

A. True

B. False

[redacted]

Question #:35

Content providers can help an application manage access to data stored by it or by other apps. They also provide a way to share data with other apps.

A. True

B. False

[redacted]

Question #:36

If two applications are developed by the same developer, they can share each other’s data if they have the same signature and the same android:sharedUserId flag set in their manifest files.

A. True

B. False

[redacted]

Question #:37

What is the message "File Written to external memory" which appeared when the app user clicks "Save" button in the following image?

A. It is <permission> tag added to Manifestfile.xml.

B. This message must appear when the user clicks back button.

C. It is auto message which appears when users use external storage.

D. It is just a Toast message.

[redacted]

Question #:38

The tag of a manifest file is a declaration for the whole application and each application component is declared in a sub-tag inside it.

A. True

B. False

[redacted]

Question #:39

Permission is the right given to an application by Android to allow access to restricted system API (Application Programming Interface) such as Camera, Bluetooth, GPS, etc…

A. True

B. False

[redacted]

Question #:40

A manifest file (AndroidManifest.xml) describes the components of the application, which include the activities, services, broadcast receivers, and content providers that compose the application.

A. False

B. True

[redacted]

Question #:41

Complete the following blank area with one of the following choices:

You can register your app with “Android Backup Service” at:

https://developer.android.com/google/backup/signup.html and get “Android Backup Service key” for your application. This key will be added to ……. tag with its attributes to add them to the manifest file in the next step.

A. <permission>

B. <meta-data>

C. <string>

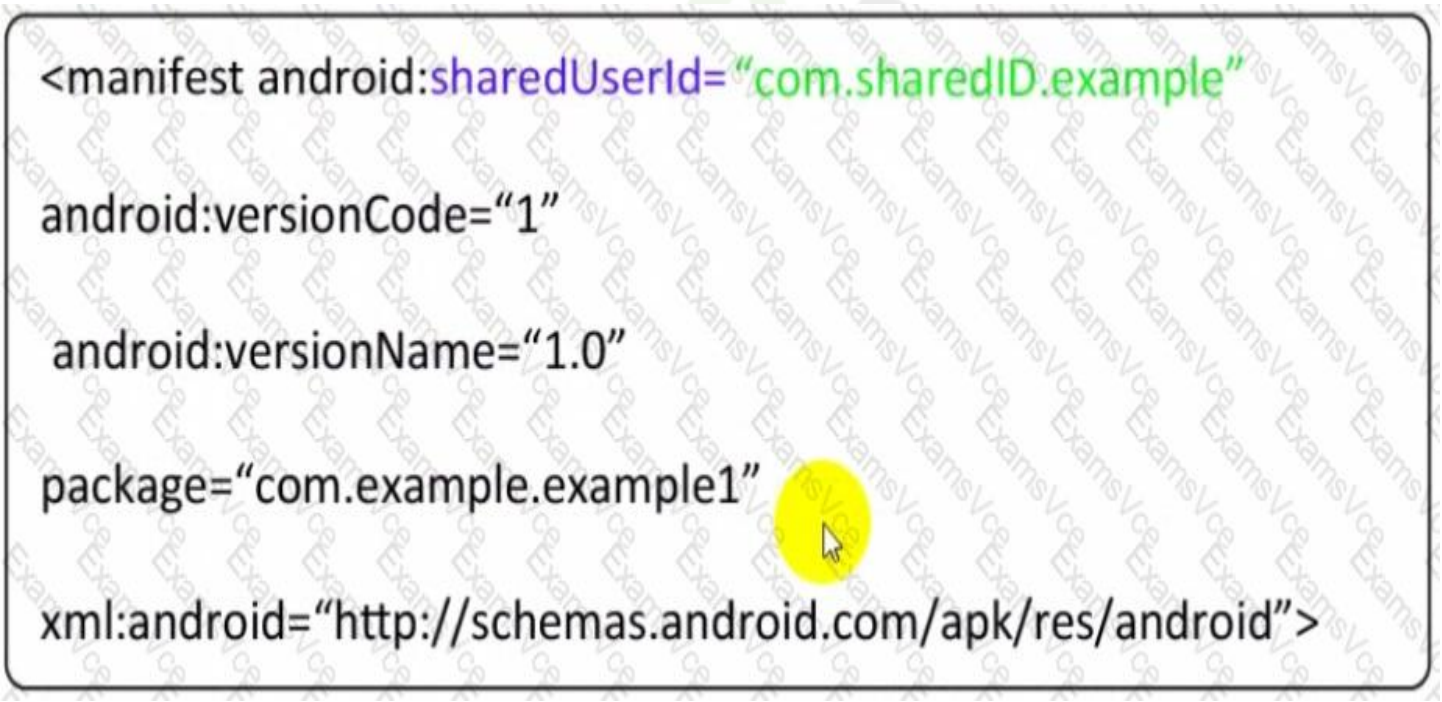
D. <key>

[redacted]

Question #:42

Assume that you have two apps signed with the same certificate and you want them to share access to each other's data. The manifest file in the first app is illustrated in the following image. It has shartedUserId =”com.sharedID.example” .

Which of the following choices is the value of the shartedUserId in the second app?



A. com.sharedID.example

B. com.example.example1

C. app2Name. com.sharedID.example

D. app2. com.sharedID.example

[redacted]

Question #:43

Which of the following Android levels of permissions are granted automatically without the user's approval?

A. Normal Permissions or Level-Zero Permissions.

B. Dangerous Permissions or Level-one Permissions.

C. Signature Permission or Level-two Permissions.

D. Signature and System Permissions or Level-three Permissions.

[redacted]

Question #:44

During an application run-time, permissions may be enforced at a number of places when calling into the system, starting an activity, sending and receiving broadcasts, accessing and manipulating a content provider, and binding to or starting a service.

A. True

B. False

[redacted]

Question #:45

A manifest file (AndroidManifest.xml) is a file that lists the contents of a software package. Not every application must have an AndroidManifest.xml file in its root directory.

A. False

B. True

[redacted]

About ExamsVCE.com

examsvce.com was founded in 2007. We provide latest & high quality IT / Business Certification Training Exam Questions, Study Guides, Practice Tests.

We help you pass any IT / Business Certification Exams with 100% Pass Guaranteed or Full Refund. Especially Cisco, CompTIA, Citrix, EMC, HP, Oracle, VMware, Juniper, Check Point, LPI, Nortel, EXIN and so on.

View list of all certification exams: All vendors

We prepare state-of-the art practice tests for certification exams. You can reach us at any of the email addresses listed below.

- Sales: sales@examsvce.com
- Feedback: feedback@examsvce.com
- Support: support@examsvce.com

Any problems about IT certification or our products, You can write us back and we will get back to you within 24 hours.