Imam Mohammad Ibn Saud Islamic University
College of Computer and Information Sciences
Information Systems Department

Project Title:	**Workshop 1**
Section	**171**

Course Title:	Software Engineering 2
Course Code:	CS 392
Course Instructor:	Sultan S. Alqahtani

Agreement:

1- It was me and my team members -NOT external party- who performed this project.
2- I participated with the group members to accomplish this project effectively and almost equally.
3- This project is totally free from copy and any type of cheating from other students' works and projects.
4- This project is free from illegal copy from any resources and intellectual property breaches.

Based on above I sign below and I accept any corrective action taken in case I breach or don't fulfil the above commitments.

Group 1

Student Name	Student ID
Turki Alqahtani	440016263
Abdullah Alqahtani	440018317
Faisal Alkhalifah	440025849
Abdullah Alrasheed	439027348

14/10/2021

Table of Contents

Introduction

In this workshop, we are going to inspect and analyze an android bank application. We are going to take a deep dive into multiple aspects of this bank application such as Security, Code quality,implementation and documentation.The whole idea behind SoftWare Engineering is that you will be working in a shared environment (in a team), as a team member you will have to follow certain rules and standards. The output Product and its implementation and functionality will reflect upon these rules and standards.We are going to look at the bank application app from different perspectives.

Sections of the report

In the introduction we are going to take a look at each section of the report and the purpose of that section and its part of making the application.

- Security
  - APIS
  - DataBase
  - Manifest analysis
  - Source code security analysis

- Code Quality
  - Clean code
  - Code Structure
  - Code documentation
  - design pattern
  - bugs

Security

The source code of a project is the core on which every aspect of the project stands on , which makes it vulnerable to cyber attacks . Therefore the level of security must be at a high level and ensures security measurements and protocols are meeting high standards.This will include the set of APIs and

libraries that are used in the project along with the DataBase that is being used to store data.

Code Quality

One of the topics that we are going to analyze in this project is code quality. Code quality is a set of standards and rules that a programmer should follow in order to achieve quality in their code, this will significantly improve reusability,and will make the maintenance process easier and overall will make the code easy to read for all parties included in the development.

There are methods of code analysis, including static and dynamic code analysis.

Static analyzes the code without executing it, and its task is to discover errors and problems in the code

In dynamic, you analyze the code using real-time data

Bugs

In order to have a fully functional bank application or any kind of application the number of bugs are needed to be as minimum as possible.In software projects there are always more bugs and the Term that we are going to use “bug free” does not necessarily mean that the bank application has zero bugs, It means that the application was tested thoroughly within the time constraints of this report.

The tools that we are going to use

The main tool that will be used to analyze and view the source code is Mobile Security Framework. Mobile Security Framework is an open source framework that is used to analyze mobile applications, it can run malware analysis and is also capable of performing static and dynamic analysis. The tool will also provide us with the source code on which we can base our report on .

PMD

it's a source code analyzer, used to find unused code, Bugs, Errors, Design problems, etc we are going to use it to analyze STCPay source code, for example, we run the tool on a small sample from the source code and we got several problems some of them could be positive errors like naming a class. in this problem, we have several things like where the problem begins and where it ends, description and the priority of the problem, and link for more information.


```
{
  "beginline": 276,
  "begincolumn": 11,
  "endline": 277,
  "endcolumn": 9,
  "description": "Avoid empty catch blocks",
  "rule": "EmptyCatchBlock",
  "ruleset": "Error Prone",
  "priority": 3,
  "externalInfoUrl": "https://pmd.github.io/pmd-6.39.0/pmd_rules_java_errorprone.html#emptycatchblock"
},
```


```
268     public boolean hasValue() {
269         boolean z;
270         boolean z2 = this.g.getKeyAndEncryptedValue() != null;
271         try {
272             if (this.g.getUnencryptedValue() == null) {
273                 z = false;
274                 return !z2 || z;
275             }
276         } catch (CryptException unused) {
277         }
278         z = true;
279         if (!z2) {
280         }
281     }
```

Our Goal

Our goal is to output a fully well documented report about the STC Pay application. The report will contain multiple sections as mentioned . The status that will be given to the application will be unbiased.Every step that we took towards analyzing the application will be well thought out and documented. In general our approach is to play the role of the receiving end, and ask ourselves was this report useful? This approach will help us understand and achieve our goal for this report.

STC Pay

STC Pay is a digital wallet to complete daily operations, after the Cabinet approved the transfer of STC Pay to an approved digital bank to become one of the first digital banks in the Kingdom of Saudi Arabia.

The STC Pay digital wallet is designed to make payments, whether personal or local or international money transfers.

One of the main advantages of STC Pay is that it is able to better connect traders with their customers through a secure digital wallet, enabling both sides to complete their transactions quickly, easily and securely.

API

API is a set of definitions and protocols that allow applications to access data with another software.

In our application analysis we found multi APIs and libraries that have been used to improve the application. We will mention some of them and give a brief explanation of their purpose:

Notifications for Android

Notifications are short messages that inform the users of information from your app such as cashback offers. There are types of notifications have been used in STC Pay:

Notification Manger:

To create a new notification and add content into notifications and manage the channels. Also can set a color, the icon for your application by NotificationCompat.

Notifications Channels :

If you have different types of notifications in your app some of the notifications the user is interested in and some of them they didn't want to receive. By the Notifications Channels, the user can turn off the category that controls some of the notifications.

Android Content Provider

In the android system, every application has its own database and files which are stored in the application folder in the system. In android another application cannot access this folder unless the folder is stored in the

content provider, other applications can easily access and make use of this data.

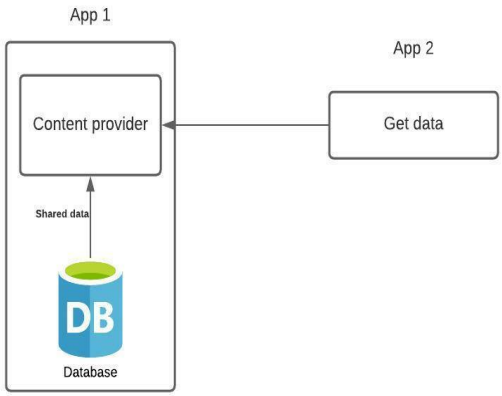
By content provider you can:

- fetch data from a content provider.
- insert, update, or delete data.

Security issue :

If your application shares sensitive data in the content provider may put you at risk.

Applications that are shared in the content provider must grant permission to access data by other applications.



Base64

Base64 is considered as an extra layer of security that helps in encoding string text to Bytes and vice versa and there are two main methods which is Base64 encoding and Base64 decoding

Base64 encoding

When it comes to encoding binary data that needs to be saved and transferred across ASCII-compatible media, Base64 encoding is used. This is done to ensure that the data is not tampered with during transit. Base64 is widely used in a variety of applications, including email and storing complex data in XML.

for example

```
import base64
encoded_data = base64.b64encode("Encode this text")
print("Encoded text with base 64 is")
print(encoded_data)
```

Base64 decoding

it's basically decode encoded a text string into bytes. for example

```
import base64
decoded_data = base64.b64decode("RW5jb2RlIHRoaXMgdGV4dA==")
print("decoded text is ")
print(decoded_data)
```

what is manifest analyses

Manifest analysis is a new form of technique used to dedicate android melicons behaviors by analyzing the manifest file. It mostly focuses on permissions in the applications.

manifest analyses (problems)

- androidx folder under activity folder every class imports"jxbx.x", which is an import call to allow usage from other apps(intent) however these classes don't protect the intent. severity is High

  solution : by making the intent value =false , however this kind of solution does not make sense because in order for this application to work it needs to take orders from other kinds of apps. so we believe the optimal solution is to make the intent value = True and add an intent filter to filter the orders of this intent.

- Broadcast receiver: is an android API that allows sending and receiving android application events such as (valid payment, notify the host). with that being said. Each class that implements this API does not check for permission(AdjustReferrerReceiver) this means that a malicious application can take control of this component and can cause threats to the application. severity is High

- in folder diagnostics : in the class "DiagnosticsReceiver" that extends Broadcastreceiver class which is responsible for dumping out useful diagnostics information.The problem here is the same as the problem mentioned in number two there is no permission checking when creating the instance therefore can be a vulnerability. severity is High

DataBase

STC Pay uses a FireBase. A firebase is a cloud hosted database that allows you to store data and sync it with your users in real time.In general the dissection of picking a certain database for your application is very crucial and it breaks down to multiple aspects.

- Operation and maintenance cost
- service stability
- security

Security

FireBase has no default implementation of security measures.It relies on the development team to implement the security aspect of the Database. however it provides default authentication that includes email and password and as a development team you can add more custom authentication to your database.

Total cost and service stability

In general , a firebase database is not expensive, it does not have a fixed price.Looking at it from a stability standpoint Firebase is a very powerful service that can help with developing applications quickly without having to implement new components or modules. Firebase was built for scalability and performance to put it into perspective the application can go from 1 user to 1million users without having to change any code related to the database.

Source code

In this section, we will talk about the source code. It has some good attributes and some bad security problems that may occur if not addressed; some of these may come under code quality.

Here are some of those problems we found in STC pay app:CWE: or common weakness enumeration is a list of common software weakness types or errors in software code or design that could result in software vulnerability if it was attacked, the CWE list is community developed list that addresses the issues in the source code.

SQL Injection(CWE-89):

Found in (lookout, dynatrace)

SQL databases hold sensitive data and SQL injection allows the attackers to insert a query to make changes to sensitive data that they are not normally allowed to view or belong to some other users.

Prevention: Since the input field is the main gate for the attacker to send these queries we recommend developers to use:

- Input validation.
- Use firewalls.
- Etc.

Use of insecure random(CWE-330):

Found in (lookout, dynatrace)

Software sometimes needs to generate random numbers to use it in any form but when that random number is predictable it is not useful anymore and the attackers can predict or generate that number and access sensitive information.

Prevention: we recommend minimizing the use of random numbers but if it is a must try to use secure randoms.

Incorrect Default Permissions(CWE-276):

Found in (lookout, huawei)

The software reads and writes to external storage which is accessible by any other software, the problem is that the software may get modified, that problem may occur during the installation and corrupt the data or even worse misuse of the software.

Prevention: apply after installation checks to check the safety of the software.

Found in (theartofdev)

The software creates temporary files, temp files may contain sensitive information these information should not be in temporary files.

Prevention: if the files are important or sensitive they must be saved in an organized file or developers must delete these temp files.

Method that exposes the software(CWE-749):

The software uses insecure webview implementation which has exposed method that the attacker can use to exploit to penetrate and get sensitive data or use the software improperly Some methods in webview are never intended to be accessible by any user or to be exposed at all, depending to the behavior of the method that could lead to several critical problems.

Prevention: software developers must examine these methods before using them in their software.

Log of sensitive information(CWE-532):

While logging information is helpful for the maintenance and the development of the software, some of the information is highly sensitive and should never be put in log folders.

Prevention: consider setting logging levels appropriately to prevent exposing sensitive users or server data.

Some good attributes in the code:

Secure Sockets Layer(SSL):

The software uses Secure Sockets Layer(SSL) security protocol to maintain a secure connection and encrypt the communication between the user and the server, which prevents several attacks like man-in-the-middle attack.

Root checker:

The software uses a method that checks if the android device is rooted or not, which makes the android device capable of doing a lot more than what it was intended to do.

Some informational things:

Using clipboard:

Users of the software can copy text to clipboard which is shared by other applications. Some attackers may misuse this feature to their own intentions, the software has security checks that contain this problem but developers must be careful about this problem.