KINGDOM OF SAUDI ARABIA
Ministry of Education
Al-Imam Mohammad University
College of Computer & Information Sciences

المملكة العربية السعودية
وزارة التعليم
جامعة الامام محمد بن سعود الإسلامية
كلية علوم الحاسب والمعلومات

Quality Assessment for Alinma Bank

Workshop 1

Abdullah Jamaan Baskran 440012378
Fahad Al Thenayyan 440012726
Mohammed Alawashiz 438020893

Supervisor
Dr. Sultan S. Alqahtnai

Table of Contents

1-Introduction: 3
1.1 Purpose: 3
1.2 Goals: 3
1.3 Tools Used 3
2- Static analysis: 4
2.1 Bugs: 4
2.1.1- Ignore the return operation status code from method 4
2.1.2-Identical expressions used on both sides of a binary operator 4
2.1.3-Check equality between two object using operator '=' 4
2.1.4-Variables begin self-assigned 5
2.2 Vulnerability: 5
2.2.1-Using a fixed Initialization Vector (IV) 5
2.2.2 -Allow to use a weak SSL/TLS protocol 5
2.2.3 - Cryptographic Algorithm usage of 'MD5' 6
2.2.4-Contents Provider 6
2.2.5- Insecure Random Number Generator 6
2.3 Potential Unsafe code 7
2.4 Documentation 8
2.5 Obfuscate in the code: 9
2.6 Permissions 10
2.7 Checkstyle 10
3- Discussion: 12
3.1 Bugs: 12
3.1.1- Ignore the return operation status code from the method 12
3.1.2-Identical expressions used on both sides of a binary operator 12
3.1.3- Check equality between two object using operator '=' 12
3.1.4-Variables begin self-assigned 13
3.2 Vulnerability: 13
3.2.1-Using a fixed Initialization Vector (IV) 13
3.2.2 -Allow to use a weak SSL/TLS protocol: 13
3.2.3- Cryptographic Algorithm usage of 'MD5' 14
3.2.4- Content Provider 14
3.2.5-Insecure Random Number Generator 15
4- Conclusion 16
5- References 17

1-Introduction:

1.1 Purpose:

The aim of this workshop is to discover methods for determining the quality of delivered programs, identifying vulnerabilities and security gaps, and determining how to prevent, solve, and make programs as safe as possible.

1.2 Goals:

The goal is to identify vulnerabilities and security gaps which include in points.

1- Determine the app's weaknesses.
2- Find bugs in the source code.
3- Obfuscate in the source code.

Finally, we'll talk about how to avoid and fix them.

1.3 Tools Used

- Mobsf
- SonarQube
- VisualCodeGrepper
- Checkstyle
- PMD

2- Static analysis:

By using a SonarQube, mobsf and Visual Code Grepper tool we perform a static analysis for source code, apk file that what we found.

2.1 Bugs:

Bugs is error in program that causes to unexpected behavior. The following found in code.

2.1.1- Ignore the return operation status code from method

Ignoring return value may yield to arise in security risks when the invoking method fails to take suitable action Consequently, programs must not ignore method return values.

Evidence:

com\pushwoosh\inapp\j\k\c.java line 32

com/google/android/gms/common/util/SharedPreferencesUtils.java line 19

2.1.2-Identical expressions used on both sides of a binary operator

Using the same value on both side of binary operators is almost always mistake which lead to dead code.

Evidence:

com\google\android\gms\internal\location\zzo.java line 31

com/google/android/gms/location/places/PlaceReport.java line 58

2.1.3-Check equality between two object using operator '='

It's mistake to compare between tow Object by using binary operator since doesn't compare the actual value it compares the memory location.

Evidence:

com\google\android\gms\measurement\internal\zzjg.java line 3098

2.1.4-Variables begin self-assigned

There is no reason to re-assign a variable to itself, the re-assignment is a mistake, and some other value or variable was intended for the assignment instead.

Evidence:

com\google\android\gms\measurement\internal\zzjg.java line 551

2.2 Vulnerability:

a vulnerability is a weakness that can be exploited by cybercriminals to gain unauthorized access to a computer system, that what we found by using SonarQube, mobsf, Visual Code Grepper.

2.2.1-Using a fixed Initialization Vector (IV)

When encrypting data with the Cipher Block Chaining (CBC) mode an Initialization Vector (IV) is used to randomize the encryption. When using fixed size, it's make it predicable.

Evidence:

com\scottyab\aescrypt\AESCrypt.java line 19, 34, 47.

2.2.2 -Allow to use a weak SSL/TLS protocol

Using or allowing of insecure TLS protocols like (TLS 1.0, TLS 1.1) could open the door to downgrade attacks, a malicious actor who is able to intercept the connection could modify the requested protocol version and downgrade it to a less secure version.

Evidence:

com\pushwoosh\internal\network\h.java line 17

2.2.3 - Cryptographic Algorithm usage of 'MD5'

The cryptographic algorithm in use is MD5 which is a weak hash known to have hash collisions. MD5 is considered weak and insecure; an attacker can easily use an MD5 collision to forge valid digital certificates. The most well-known example of this type of attack is when attackers forged a Microsoft Windows code-signing certificate and used it to sign the Flame malware.

Evidence:

com/pushwoosh/internal/platform/utils/GeneralUtils.java Line 136

com/pushwoosh/internal/utils/d.java Line 449

2.2.4-Contents Provider

A Content Provider is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device.

Evidence:

com/pushwoosh/PushwooshSharedDataProvider.java

com/pushwoosh/firebase/FirebaseInitProvider.java

com/pushwoosh/PushwooshInitProvider.java

com/pushwoosh/amazon/AmazonInitProvider.java

2.2.5- Insecure Random Number Generator

Instances of java. util. Random are not cryptographically secure. And the Package is flawed and produces predictable values for any given seed which are reproducible once the starting seed is identified

Evidence:

com/pushwoosh/internal/c/d.java Line 4

2.3 Potential Unsafe code

We found with Visual Code Grepper some potential unsafe code which list here

1-The code appears to have classes that contain public variables which may be accessed and modified by other classes without the use of getter/setter methods. It is considered unsafe to have public fields or methods in a class as any method, field, or class that is not private is a potential avenue of attack. It is safer to provide accessor methods to variables in order to limit their accessibility.

2- The code appears to have public classes that are not declared as final as per OWASP recommendation, it is consider best practice to make classes final. Non-Final classes can allow an attacker to extend a class in a malicious manner. its values can be maliciously manipulated by any function that has access to it in order to extend the application code or acquire critical information about the application.

Some example evidence:

com\google\android\gms\internal\measurement\zzdk.java Line: 8

com\google\android\gms\common\api\internal\RegistrationMethods.java Line: 23

com\bumptech\glide\load\resource\gif\GifDrawable.java Line: 23

com\bumptech\glide\manager\SupportRequestManagerFragment.java Line: 17

2.4 Documentation

The system is not documented in the source code after pulling all the comments we found that none of them describes methods or classes with that in mind we can assume that the application is either not documented which is unlikely to be the case of it is externally documented and separated from the source code we analyzed. See figure 1.

A breakdown of the code lines

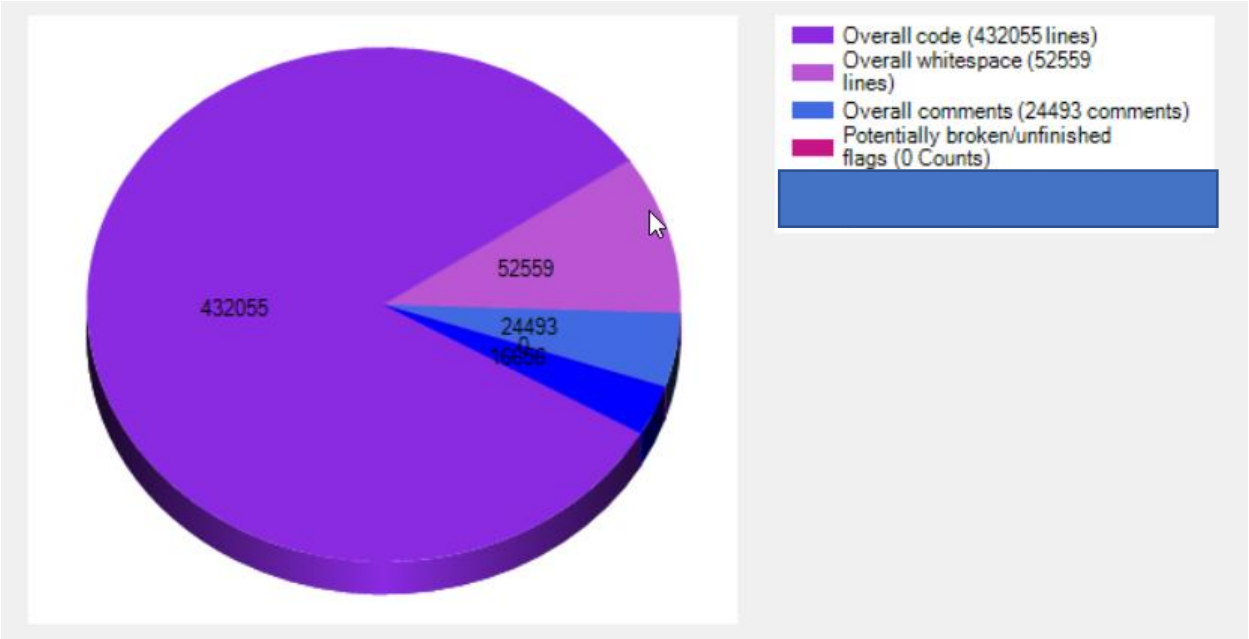

Figure 1, A breakdown of the code lines

There are 509704 lines of which there are:

~4.8% comments (24463)

~10.3% lines of white space (52559)

~84.9% lines of code (432652)

2.5 Obfuscate in the code:

Obfuscation is way to protect your code from reverse engineer by make it difficult to understand, so we made a program written in python to count the percentage of obfuscated file by name of the file, based on if file name contains on only one character so count it as obfuscated file or duplicate character, we except file R.java which it auto-generated file by AAPT (Android Asset Packaging Tool). See figure 1.

Number of files is 4481 files.

Number of obfuscated files is 1508 files.

Number of non-obfuscated files is 2973 files.

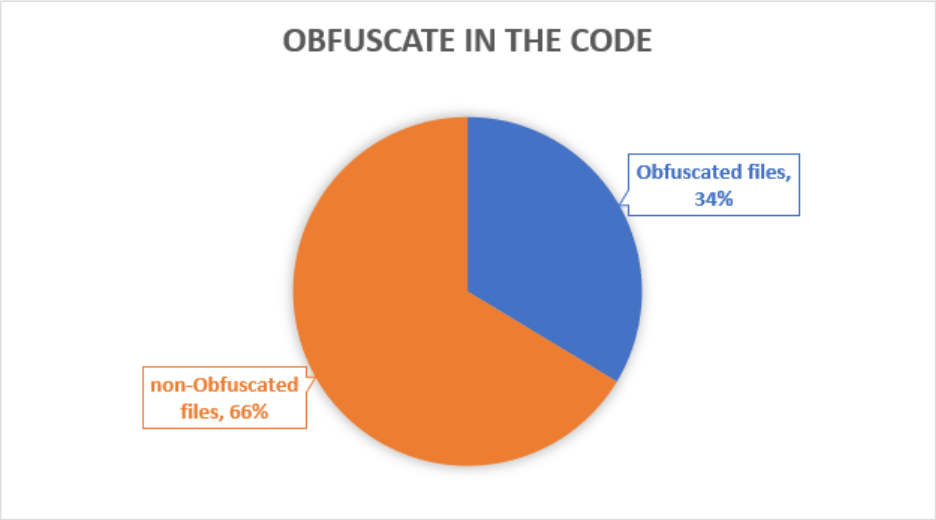

Figure 2. Obfusate in the code

2.6 Permissions

The tools we use showed that the app asking for permission as a security issue:

- Access coarse location sources, such as the mobile network database, to determine an approximate phone location, where available.
- Access fine location sources, such as the Global Positioning System on the phone, where available.
- Allows application to take pictures and videos with the camera.

Those can be seen as a security issue but depend on the app that you deal with it if it is a malicious app than it is considered as security issue because there is a chance of expose your data, but if the app is trusted and the creator is known than may not consider as security issue.

2.7 Checkstyle

It is a development tool to help programmers write Java code that adheres to a coding standard. It automates the process of checking Java code to spare humans of this boring (but important) task. This makes it ideal for projects that want to enforce a coding standard.

1-Problem synopsis:

Utility should not have a public or default constructor.

Solution:

If this class is only a utility class, should make the class final and define a private constructor

Evidence:

com.pushwoosh.firebase.a.java

com.pushwoosh.internal.c.java

com.pushwoosh.inbox.ui.utils.DateExtensionKt.java

2-Problem synopsis:

Boolean expression complexity is more than 3 (max allowed is 3).

operators have to be at most 3 in each statement

Solution:

giving meaningful names to each sub-expression and assign the results to variables and then check between the variables. This will greatly increase readability.

Evidence:

com.google.android.gms.common.internal.BaseGmsClient.zzb.java line 223

com.pushwoosh.internal.utils.JsonUtils.java line81

3-Problem synopsis:

magic number (Unique values with unexplained meaning or multiple that is used directly in the code)

Solution:

use constant to represent values instead of using magic numbers. It improves the readability of code and provides easy modification in the code.

Evidence:

com.pushwoosh.secure.crypt.a.java line 11

com.google.android.material.appbar.AppBarLayout.java line 83

4-Problem synopsis:

Inner Type Last (Fields and methods come after inner classes)

Solution:

Fields and methods should be before inner classes.

Evidence:

com.pushwoosh.e.a.a.a.e.java line12

com.bumptech.glide.request.transition.Transition.java line 18

3- Discussion:

3.1 Bugs:

Here will discuss the result of bug section and the solution of each problem.

3.1.1- Ignore the return operation status code from the method

Ignoring the status code led to a raise in error and security risks

which is undesirable, should avoid this situation, the best way to avoid it is to make sure you test any status code to see whether it is completed successfully or failed. [4][7]

3.1.2-Identical expressions used on both sides of a binary operator

It's almost always a mistake to use the same value on both sides of a binary operator. It's either a copy/paste error and thus a bug with logical operators, or it's just wasted code that could be streamlined. Having the same value on both sides of a bitwise operator, as well as other binary mathematical operators, produces predictable results and should be simplified.[8]

Solution is avoiding any usage of identical expressions that are not required or make sure what you want to make it

3.1.3- Check equality between two object using operator '='

Confusing reference equality and object equality can lead to unexpected results. Because the '==' and '!=' operators compare object references rather than object values, the values of object cannot be directly compared using these operators. The best way is using equals function to check the actual value not the memory location.[1][5][6].

3.1.4-Variables begin self-assigned

When a field, a local, or a parameter symbol is assigned to itself. When a local, parameter, or field symbol has a name that is identical to another symbol in scope, this is a typical error. Rather than utilizing distinct symbols on the left and right sides of the assignment, the same symbol was used on both. This results in a duplicate assignment of the value to itself, which is usually a sign of a bug, or the statement is redundant and should be removed if don't have effect.[8]

3.2 Vulnerability:

3.2.1-Using a fixed Initialization Vector (IV)

Using Initialization Vector (IV) in a predictable way that happens when you are using fixed-size, makes it susceptible to a dictionary attack and Chosen-Plaintext Attack which is attacked to gain information that reduces the security of the encryption scheme. To avoid it you must use IV in an unpredictable way. There are two approaches for creating unexpected IVs that are approved. The first way is to encrypt a nonce using the forward cipher function using the same key that was used to encrypt the content. The nonce must be a data block that is different for each encryption operation execution. The nonce might be a counter or a message number, the second option is to use a secure random number generator to produce a random data block.[3][10]

3.2.2 -Allow to use a weak SSL/TLS protocol:

Outdated TLS protocols utilize cipher suites that are no longer maintained or recommended and utilizing earlier TLS versions would necessitate extra effort to keep the libraries up to date, raising product maintenance costs.

TLS 1.0 and 1.1 are vulnerable to downgrade attacks since they rely on the SHA-1 hash to ensure message integrity. Even handshake authentication is done with SHA-1, making it easier for an attacker to impersonate a server in MITM attacks. TLS 1.1 and earlier protocols lack the ability to use more robust hashing

methods, which is available in subsequent protocols, to avoid such kind of problem is recommended to enforce TLS 1.2 as the minimum protocol version and to disallow older versions like TLS 1.0.[2][9]

3.2.3- Cryptographic Algorithm usage of 'MD5'

The MD5 algorithm has weaknesses that allow for output collisions. As a result, attackers can produce cryptographic tokens or other data that look to be legitimate but aren't.[11]

Don’t use 'MD5' instead OWASP recommends the use of one of these algorithms

- Confidentiality algorithms: AES-GCM-256 or ChaCha20-Poly1305
- Integrity algorithms: SHA-256, SHA-384, SHA-512, Blake2, the SHA-3 family
- Digital signature algorithms: RSA (3072 bits and higher), ECDSA with NIST P-384
- Key establishment algorithms: RSA (3072 bits and higher), DH (3072 bits or higher), ECDH with NIST P-384

3.2.4- Content Provider

Because an application's data is private, it is not feasible for an application to access the data of another application by default. When applications want to exchange data with other apps, Content Provider provides a mechanism to do it. It functions as an interface for data sharing across apps.[13][14]

We can either:

- change Set android:exported attribute’s value to false
- Limit access with custom permissions imposing permission-based restrictions by defining custom permissions for an activity.

3.2.5-Insecure Random Number Generator

When a function that can provide predictable values is utilized as a source of randomness in a security-sensitive situation, insecure randomness mistakes arise.

Computers are deterministic machines, which means they can't generate actual randomness. PRNGs (Pseudo-Random Number Generators) are algorithms that approximate randomness by beginning with a seed and calculating subsequent values from it.

PRNGs are classified as statistical or cryptographic. Statistical PRNGs have useful statistical qualities, but their output is extremely predictable and creates an easy to replicate numeric stream, making them inappropriate for application in situations where produced numbers must be surprising.

Instead of using Random use Secure Random to get a cryptographically secure pseudo-random number generator for use by security-sensitive applications.[12]

4- Conclusion

In the end, we achieved the purpose of this workshop using tools that make us discover the quality and security weaknesses of given app. And we have achieved our goals to find bugs that may lead to unexpected behavior and we provide a ways to avoid this kind of bugs and how to overcome of this problem and Vulnerabilities that makes the app vulnerable to attacks and risk of data disclosure and how to overcome this problem, also we find how much of code begin obfuscated in percentage and we show them in detail and we provide a chart to show the percentage of obfuscate in the code, we perform a breakdown of the code lines, white space of the code and we find some of potentially unsafe code.

5- References

[1] Cwe.mitre.org. 2021. *CWE - CWE-597: Use of Wrong Operator in String Comparison (4.6)*. [online] Available at: <https://cwe.mitre.org/data/definitions/597.html> [Accessed 3 November 2021].

[2]2021. *Diagnosing TLS, SSL, and HTTPS*. [online] Available at: <https://blogs.oracle.com/java/post/diagnosing-tls-ssl-and-https> [Accessed 3 November 2021].

[3] Dworkin, M., 2021. *Recommendation for Block Cipher Modes of Operation*. [online] Available at: <https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-38a.pdf> [Accessed 3 November 2021].

[4] Wiki.sei.cmu.edu. 2021. *EXP00-J. Do not ignore values returned by methods - SEI CERT Oracle Coding Standard for Java - Confluence*. [online] Available at: <https://wiki.sei.cmu.edu/confluence/display/java/EXP00-J.+Do+not+ignore+values+returned+by+methods> [Accessed 3 November 2021].

[5] Wiki.sei.cmu.edu. 2021. *EXP03-J. Do not use the equality operators when comparing values of boxed primitives - SEI CERT Oracle Coding Standard for Java - Confluence*. [online] Available at: <https://wiki.sei.cmu.edu/confluence/display/java/EXP03-J.+Do+not+use+the+equality+operators+when+comparing+values+of+boxed+primitives> [Accessed 3 November 2021].

[6] Wiki.sei.cmu.edu. 2021. *EXP50-J. Do not confuse abstract object equality with reference equality - SEI CERT Oracle Coding Standard for Java - Confluence*. [online] Available at: <https://wiki.sei.cmu.edu/confluence/display/java/EXP50-J.+Do+not+confuse+abstract+object+equality+with+reference+equality> [Accessed 3 November 2021].

[7] Wiki.sei.cmu.edu. 2021. *FIO02-J. Detect and handle file-related errors - SEI CERT Oracle Coding Standard for Java - Confluence*. [online] Available at: <https://wiki.sei.cmu.edu/confluence/display/java/FIO02-J.+Detect+and+handle+file-related+errors> [Accessed 3 November 2021].

[8] Wiki.sei.cmu.edu. 2021. *MSC12-C. Detect and remove code that has no effect or is never executed - SEI CERT C Coding Standard - Confluence*. [online] Available at: <https://wiki.sei.cmu.edu/confluence/display/c/MSC12-C.+Detect+and+remove+code+that+has+no+effect+or+is+never+executed> [Accessed 3 November 2021].

[9] GitHub. 2021. *SSL and TLS Deployment Best Practices · ssllabs/research Wiki*. [online] Available at: <https://github.com/ssllabs/research/wiki/SSL-and-TLS-Deployment-Best-Practices#22-use-secure-protocols> [Accessed 3 November 2021].

[10] 2021. *Generation of Predictable IV with CBC Mode*. [online] Available at: <https://cwe.mitre.org/data/definitions/329> [Accessed 3 November 2021].

[11]"owasp-mstg/0x04g-Testing-Cryptography.md at master · OWASP/owasp-mstg", *GitHub*, 2021. [Online]. Available: https://github.com/OWASP/owasp-mstg/blob/master/Document/0x04g-Testing-Cryptography.md. [Accessed: 04- Nov- 2021].

[12]"Insecure Randomness | OWASP", *Owasp.org*, 2021. [Online]. Available: https://owasp.org/www-community/vulnerabilities/Insecure_Randomness. [Accessed: 04- Nov- 2021].

[13]"Android hacking and security, part 2: Content provider leakage - Infosec Resources", *Infosec Resources*, 2021. [Online]. Available: https://resources.infosecinstitute.com/topic/android-hacking-security-part-2-content-provider-leakage/. [Accessed: 04- Nov- 2021].

[14]"Android App Development: Securing Content Providers", *FutureLearn*, 2021. [Online]. Available: https://www.futurelearn.com/info/courses/secure-android-app-development/0/steps/21592. [Accessed: 04- Nov- 2021].