**Mobile Application Security Testing Report**

**Conducted by Brendan Murphy**

**4/7/2019**

Contents

[1. Executive Summary 2](#_Toc460775092)

[2. Test Parameters 2](#_Toc460775093)

[3. Targets 3](#_Toc460775094)

[4. Analysis 4](#_Toc460775095)

[5. Appendix – Documentation 5](#_Toc460775096)

# Executive Summary

The purpose of this document is to capture activities from a Mobile Application Security Assessment of the **InsecureBankv2** Android Application.

# Test Parameters

The Objective of this evaluation is to conduct a Mobile Application Security Testing of the InsecureBankv2 Android Application. The Scope of this evaluation is the **com.android.insecurebankv2-1.apk**. This Application Security Testing conducted an analysis of the device against the following [OWASP Top 10 Mobile Risks](https://www.owasp.org/index.php/OWASP_Mobile_Security_Project#tab=Top_10_Mobile_Risks) client side vulnerabilities:

* [M1: Improper Platform Usage](https://www.owasp.org/index.php/Mobile_Top_10_2016-M1-Improper_Platform_Usage)
* [M2: Insecure Data Storage](https://www.owasp.org/index.php/Mobile_Top_10_2014-M2)
* [M3: Insufficient Transport Layer Protection](https://www.owasp.org/index.php/Mobile_Top_10_2014-M3)
* [M4: Unintended Data Leakage](https://www.owasp.org/index.php/Mobile_Top_10_2014-M4)
* [M5: Poor Authorization and Authentication](https://www.owasp.org/index.php/Mobile_Top_10_2014-M5)
* [M6: Broken Cryptography](https://www.owasp.org/index.php/Mobile_Top_10_2014-M6)
* [M7: Client Side Injection](https://www.owasp.org/index.php/Mobile_Top_10_2014-M7)
* [M8: Security Decisions via Untrusted Inputs](https://www.owasp.org/index.php/Mobile_Top_10_2014-M8)
* [M9: Improper Session Handling](https://www.owasp.org/index.php/Mobile_Top_10_2014-M9)
* [M10: Lack of Binary Protections](https://www.owasp.org/index.php/Mobile_Top_10_2014-M10)

# Testing Activities

The evaluation will include ***Automated Testing*** and a ***Manual Testing***. Automated Testing will be conducted using a Scanner. Manual Testing (and corresponding tools) is restricted to verification of findings identified in the Automated Testing.

* 1. **Automated Testing**

|  |  |  |
| --- | --- | --- |
| **OWASP TOP 10 MOBILE RISK** | **TEST STEPS** | **TOOLS** |
| [M1: Improper Platform Usage](https://www.owasp.org/index.php/Mobile_Top_10_2016-M1-Improper_Platform_Usage) | Automated | Quixxi |
| [M2: Insecure Data Storage](https://www.owasp.org/index.php/Mobile_Top_10_2016-M2-Insecure_Data_Storage) | Automated | Quixxi |
| [M3: Insecure Communication](https://www.owasp.org/index.php/Mobile_Top_10_2016-M3-Insecure_Communication) | Automated | Quixxi |
| [M4: Insecure Authentication](https://www.owasp.org/index.php/Mobile_Top_10_2016-M4-Insecure_Authentication) | Automated | Quixxi |
| [M5: Poor Cryptography](https://www.owasp.org/index.php/Mobile_Top_10_2016-M5-Insufficient_Cryptography) | Automated | Quixxi |
| [M6: Poor Authorization](https://www.owasp.org/index.php/Mobile_Top_10_2016-M6-Insecure_Authorization) | Automated | Quixxi |
| [M7: Client Code Quality](https://www.owasp.org/index.php/Mobile_Top_10_2016-M7-Poor_Code_Quality) | Automated | Quixxi |
| [M8: Code Tampering](https://www.owasp.org/index.php/Mobile_Top_10_2016-M8-Code_Tampering) | Automated | Quixxi |
| [M9: Reverse Engineering](https://www.owasp.org/index.php/Mobile_Top_10_2016-M9-Reverse_Engineering) | Automated | Quixxi |
| [M10: Extraneous Activity](https://www.owasp.org/index.php/Mobile_Top_10_2016-M10-Extraneous_Functionality) | Automated | Quixxi |

* 1. **Manual Testing**

|  |  |  |
| --- | --- | --- |
| **OWASP TOP 10 MOBILE RISK** | **TEST STEPS** | **TOOLS** |
| [M1: Improper Platform Usage](https://www.owasp.org/index.php/Mobile_Top_10_2016-M1-Improper_Platform_Usage) | [Unintended Data Leakage Testing](https://canvas.harvard.edu/files/7222852/download?download_frd=1) | adb  sqlite3 |
| [M2: Insecure Data Storage](https://www.owasp.org/index.php/Mobile_Top_10_2016-M2-Insecure_Data_Storage) | [Insecure Data Storage Testing](https://canvas.harvard.edu/files/7222828/download?download_frd=1) | ByteCodeViewer |
| [M3: Insecure Communication](https://www.owasp.org/index.php/Mobile_Top_10_2016-M3-Insecure_Communication) | [Insufficient Transport Layer Protection Testing](https://canvas.harvard.edu/files/7222833/download?download_frd=1) | BurpSuite |
| [M4: Insecure Authentication](https://www.owasp.org/index.php/Mobile_Top_10_2016-M4-Insecure_Authentication) | [Insecure Authentication](https://canvas.harvard.edu/files/7683061/download?download_frd=1) | BurpSuite |
| [M5: Poor Cryptography](https://www.owasp.org/index.php/Mobile_Top_10_2016-M5-Insufficient_Cryptography) | [Broken Cryptography Testing](https://canvas.harvard.edu/files/7222838/download?download_frd=1) | ByteCodeViewer |
| [M6: Poor Authorization](https://www.owasp.org/index.php/Mobile_Top_10_2016-M6-Insecure_Authorization) | [Poor Authorization](https://canvas.harvard.edu/files/7683050/download?download_frd=1) | ByteCodeViewer |
| [M7: Client Code Quality](https://www.owasp.org/index.php/Mobile_Top_10_2016-M7-Poor_Code_Quality) | [Client Side Injection Testing](https://canvas.harvard.edu/files/7222824/download?download_frd=1) | BurpSuite (Optional) |
| [M8: Code Tampering](https://www.owasp.org/index.php/Mobile_Top_10_2016-M8-Code_Tampering) | [Weak Authorization](https://github.com/dineshshetty/Android-InsecureBankv2/blob/master/Walkthroughs/Android%20Application%20patching%20+%20Weak%20Auth.docx?raw=true) | ByteCodeViewer  SignAPK (Optional)  Dex2Jar (Optional) |
| [M9: Reverse Engineering](https://www.owasp.org/index.php/Mobile_Top_10_2016-M9-Reverse_Engineering) | [Lack of Binary Protections Testing](https://canvas.harvard.edu/files/7222840/download?download_frd=1) | ByteCodeViewer |
| [M10: Extraneous Activity](https://www.owasp.org/index.php/Mobile_Top_10_2016-M10-Extraneous_Functionality) | [Extraneous Activity](https://canvas.harvard.edu/files/7683009/download?download_frd=1) | ByteCodeViewer |

# Targets

The Scope of the evaluation is as follows:

* 1. **com.android.insecurebankv2-1.apk**

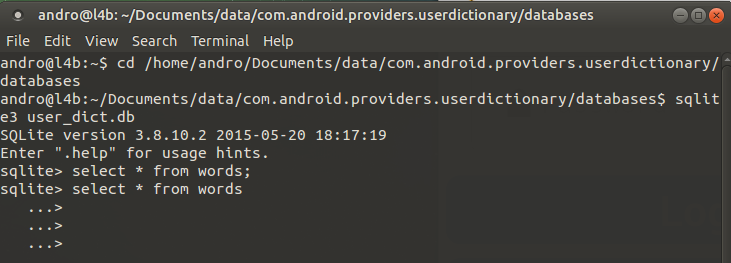
# Analysis

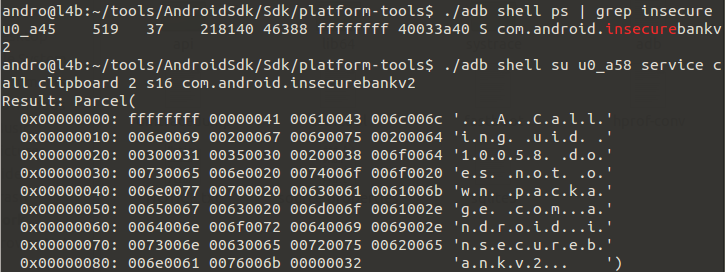
Table 1: Automated Analysis with Manual Verification

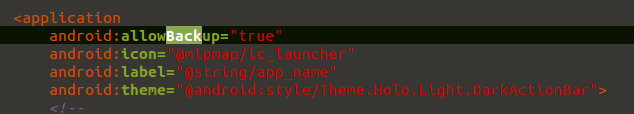
|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **VULNERABILITY** | **YES** | **NO** | **MANUAL VERIFICATION** | **DESCRIPTION** | **RISK RATING** | **MITIGATION TECHNIQUE** | **EVIDENCE** |
| [**M1: Improper Platform Usage**](https://www.owasp.org/index.php/Mobile_Top_10_2016-M1-Improper_Platform_Usage) |  | **✓** | **Verified using Unintended data leakage testing tools** |  |  |  | **Appendix** |
| [**M2: Insecure Data Storage**](https://www.owasp.org/index.php/Mobile_Top_10_2016-M2-Insecure_Data_Storage) | **✓** |  | **Verified using Insecure data storage testing** | **The application will log username and password to the console during user login** | **HIGH** | **Patch software to never log secure data to the console or log files** | **Appendix** |
| [**M3: Insecure Communication**](https://www.owasp.org/index.php/Mobile_Top_10_2016-M3-Insecure_Communication) | **✓** |  | **I was not able to verify with burp - may have been due to a proxy issue. However, I did discover that debugable is set to true in a decoded manifest file.** | **By setting debug to true, the application is vulnerable to allowing unnecessary connections to the debug port.** | **HIGH** | **Set debug to false** | **Appendix** |
| [**M4: Insecure Authentication**](https://www.owasp.org/index.php/Mobile_Top_10_2016-M4-Insecure_Authentication) | **✓** |  | **Verified using Insecure data storage testing** | **The application will log username and password to the console during user login** | **HIGH** | **Patch software to never log secure data to the console or log files** | **Appendix** |
| [**M5: Poor Cryptography**](https://www.owasp.org/index.php/Mobile_Top_10_2016-M5-Insufficient_Cryptography) | **✓** |  | **META-INF file reveals references to deprecated crypt algorithm SHA1** | **Use of outdated/deprecated encryption algorithms are a security risk** | **HIGH** | **Implement updated encryption** | **Appendix** |
| [**M6: Poor Authorization**](https://www.owasp.org/index.php/Mobile_Top_10_2016-M6-Insecure_Authorization) |  | **✓** |  |  |  |  |  |
| [**M7: Client Code Quality**](https://www.owasp.org/index.php/Mobile_Top_10_2016-M7-Poor_Code_Quality) |  | **✓** |  |  |  |  |  |
| [**M8: Code Tampering**](https://www.owasp.org/index.php/Mobile_Top_10_2016-M8-Code_Tampering) | **✓** |  | **Verified using weak authorization testing** | **Admin credentials are hard coded in the application and can be overwritten and recompiled into the application** | **HIGH** | **Use dynamic variables and enhanced security to prevent admin access** | **Appendix** |
| [**M9: Reverse Engineering**](https://www.owasp.org/index.php/Mobile_Top_10_2016-M9-Reverse_Engineering) | **✓** |  | **Verified using ByteCodeViewer** | **The file com.android.insecurebankv2-1. is availble for viewing in ByteCodeViewer** | **HIGH** | **Implement security software like DashO to prevent source code modification** | **Appendix** |

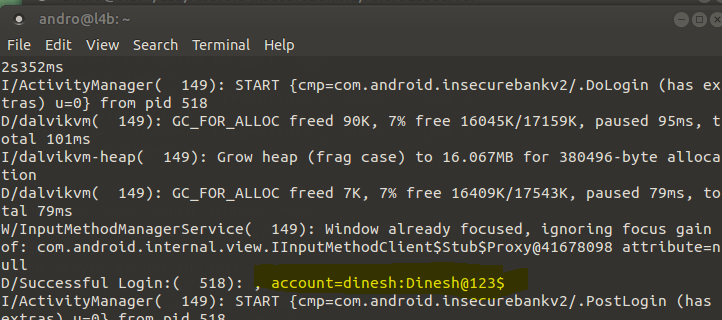
# 

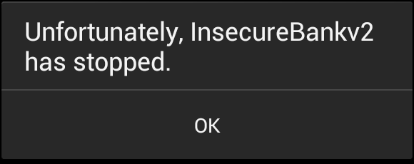
# Appendix – Documentation

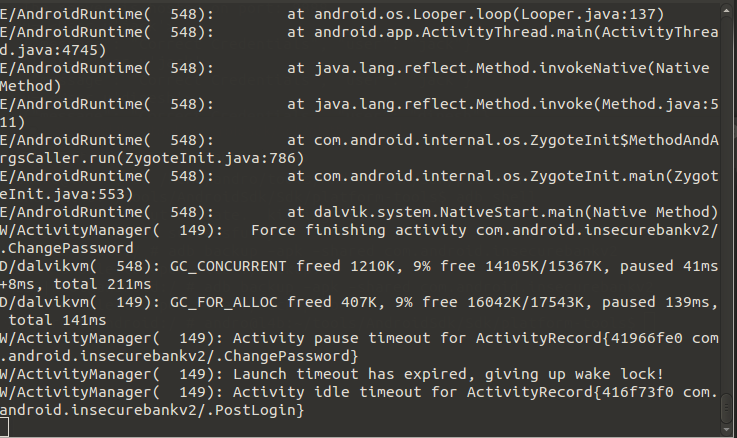
****

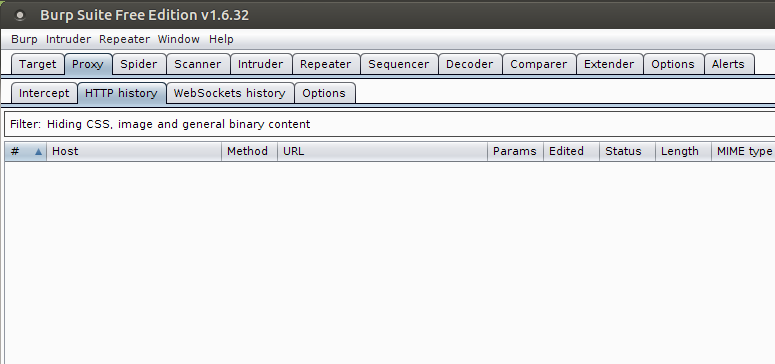
****

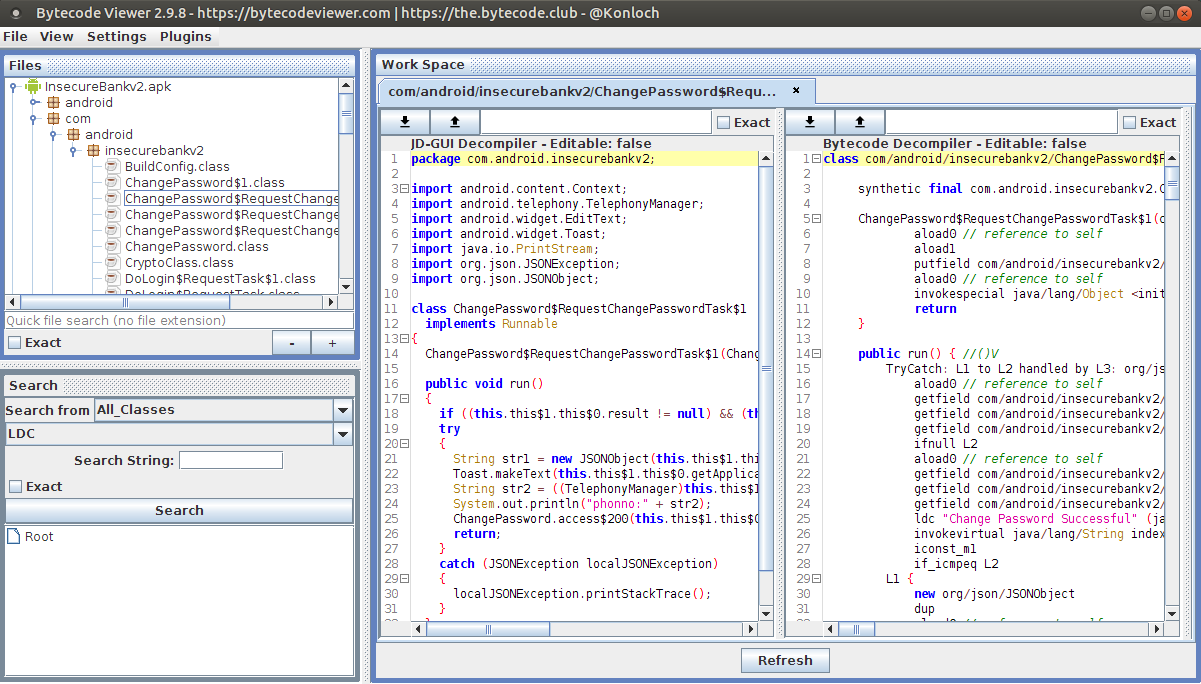
****

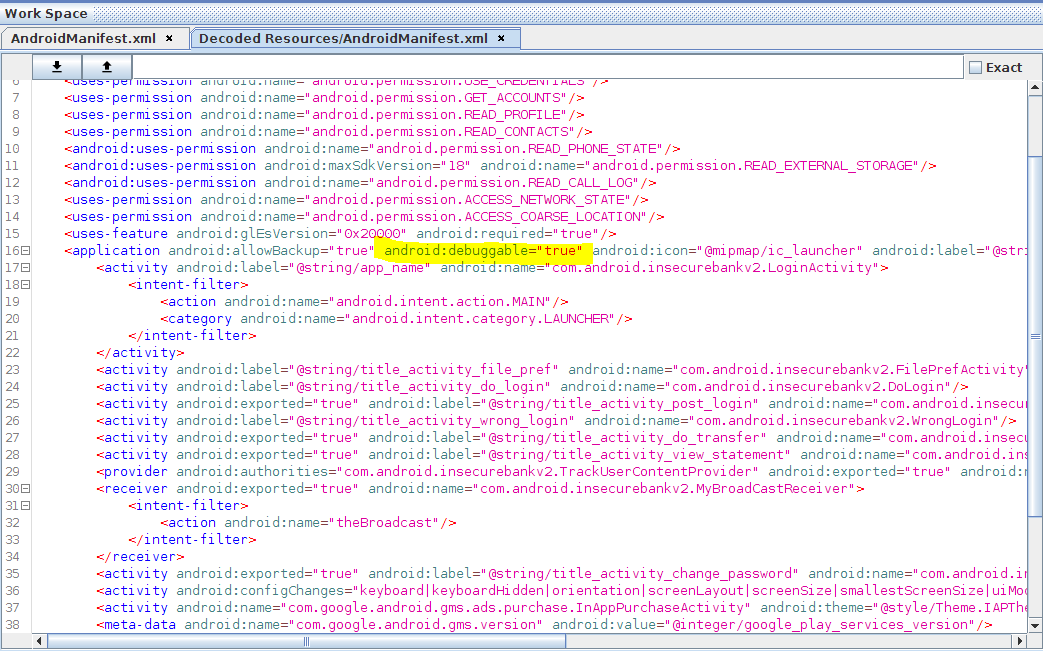
****

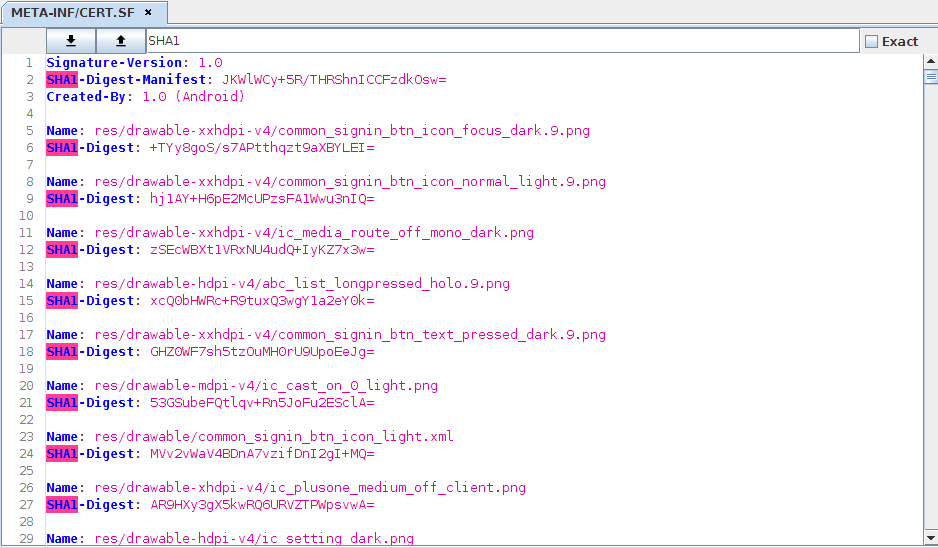
****

****

****

****

****

****