

# 1. Introduction

We were assigned to test team Bravo app. This report contains only examples of output from each tool. Check the report files for each tool for accurate results.

# 2. Automated security helper

The tool found two problems of low severity.

```
-----
./API/Properties/launchSettings.json
-----
[31m| FAIL FATAL[0m
[31m|[0m
[31m| #<ArgumentError: invalid byte sequence in US-ASCII>[0m

Failures count: 1
Warnings count: 0
-----
./API/appsettings.Development.json
-----
[31m| FAIL FATAL[0m
[31m|[0m
[31m| Illegal cfn - no Resources[0m

Failures count: 1|
Warnings count: 0
-----
./API/appsettings.json
-----
[31m| FAIL FATAL[0m
[31m|[0m
[31m| Illegal cfn - no Resources[0m

Failures count: 1
```

# 3. Betterscan

Tool found several problems. One of the warnings told us about possibility of hard coded password.

DescriptionPossible hardcoded password: 'mysecretpassword'	
Severity	Warning
Line	102

## 4. SpotBugs

We had some problems with this tool but it's build in plugin in the SonarQube SCA and as a plugin it worked well and found 19 bugs. One shown below was classified as major bug and the rest as minor.

My IssuesAll

Filters

Clear All Filters

Period

New code

TypeBUG

Clear

Bug1

Vulnerability0

Code Smell4

Press Ctrl to add to selection

SeverityMAJOR

Clear

Blocker0

Critical0

Major1

Minor18

Info0

Press Ctrl to add to selection

Bulk Change

1 / 1 issues2min effort

API/Views/Home/Movie.cshtml

Add "<th>" headers to this "<table>".

7 minutes agoL39accessibility, wcag2-a

BugMajorOpenNot assigned2min effortComment

1 of 1 shown

## 5. Horusec

This tool found 64 vulnerabilities in the app, and 17 of them were critical.

```
Language: Leaks
Severity: CRITICAL
Line: 83
Column: 51
SecurityTool: HorusecEngine
Confidence: MEDIUM
File: /home/przemek/Downloads/MovieServiceMobileAPI-master/SQLQuery/createDB.py
Code: sword='mysecretpassword', host='127.0.0.1', port= '5432'
RuleID: HS-LEAKS-26
Type: Vulnerability
ReferenceHash: 39c41e1ea8cbec7964ed3f44761f707bd301c1005d91e7a20e3fd4abaf291bc5
Details: (1/1) * Possible vulnerability detected: Hard-coded password
The software contains hard-coded credentials, such as a password or cryptographic key, which it uses for its own inbound authentication, outbound communication to external components, or encryption of internal data. For more information checkout the CWE-798 (https://cwe.mitre.org/data/definitions/798.html) advisory.
```

## 6. Mobile Security Frameworks

App scored 55 out of 100 points and was classified as medium risk.

### FINDINGS SEVERITY

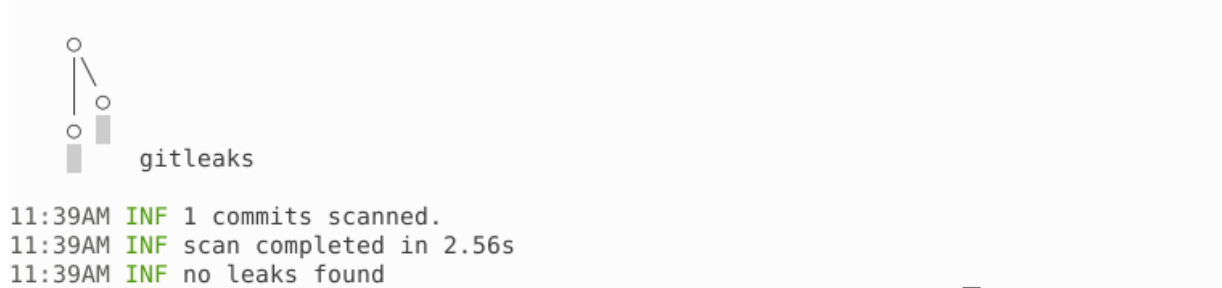
🚨 HIGH	⚠️ MEDIUM	i INFO	✓ SECURE	🔍 HOTSPOT
1	2	2	1	1

android.permission.WRITE_EXTERNAL_STORAGE	dangerous	read/modify/delete external storage contents	Allows an application to write to external storage.
---	-----------	--	---

## 7. GitLeaks

Gitleaks didn't find any leaks in the app.

```
przemek@DESKTOP-628E750:~/Downloads/MovieServiceMobileAPImaster1$ gitleaks detect
```



## 8. SonarQube SCA

The tool found 2 risks shown below and also 19 bugs which were presented in SpotBug section.

2 Security Hotspots to review

Review priority: **LOW**

Encryption of Sensitive Data

"usesCleartextTraffic" is implicitly enabled for older Android versions. Make sure allowing clear-text traffic is safe here.

...Android/Properties/AndroidManifest.xml

Others

Make sure backup of application data is safe here.

...Android/Properties/AndroidManifest.xml

2 of 2 shown

Where is the risk?

What's the risk?

Assess the risk

How can I fix it?

Client/.../MobileServiceMobileApp.Android/Properties/AndroidManifest.xml

Open in IDE

Get Permalink

1 <?xml version="1.0" encoding="utf-8"?>

2 <manifest xmlns:android="http://schemas.android.com/apk/res/android" android:versionCode="1" android:versionName="1.0"

3 package="com.companyname.mobileservicemobileapp">

4 <uses-sdk android:minSdkVersion="21" android:targetSdkVersion="31" />

5 <application android:label="MobileServiceMobileApp.Android" android:theme="@style/MainTheme"></application>

6 </manifest>

7

Make sure backup of application data is safe here. Comment

Comment:

Formatting Help : "Bold" "Code" \* Bulleted point

Comment

2 Security Hotspots to review

Review priority: **LOW**

Encryption of Sensitive Data

"usesCleartextTraffic" is implicitly enabled for older Android versions. Make sure allowing clear-text traffic is safe here.

...Android/Properties/AndroidManifest.xml

Others

Make sure backup of application data is safe here.

...Android/Properties/AndroidManifest.xml

2 of 2 shown

Where is the risk?

What's the risk?

Assess the risk

How can I fix it?

Client/.../MobileServiceMobileApp.Android/Properties/AndroidManifest.xml

Open in IDE

Get Permalink

1 <?xml version="1.0" encoding="utf-8"?>

2 <manifest xmlns:android="http://schemas.android.com/apk/res/android" android:versionCode="1" android:versionName="1.0"

3 package="com.companyname.mobileservicemobileapp">

4 <uses-sdk android:minSdkVersion="21" android:targetSdkVersion="31" />

5 <application android:label="MobileServiceMobileApp.Android" android:theme="@style/MainTheme"></application>

6 <uses-permission android:name="android.permission.ACCESS\_NETWORK\_STATE" />

7 </manifest>

8

"usesCleartextTraffic" is implicitly enabled for older Android versions. Make sure allowing clear-text traffic is safe here. Comment

Comment: