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
```

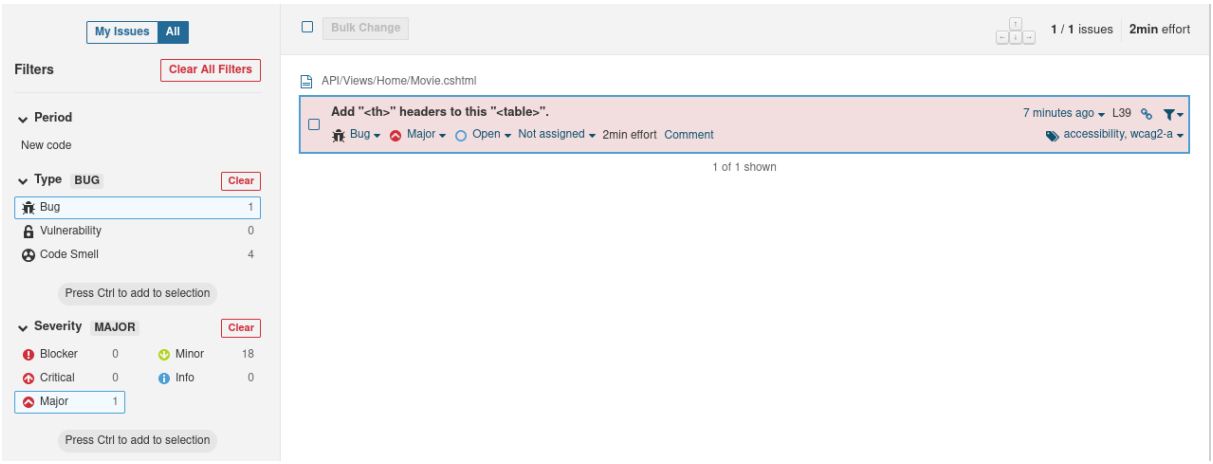
3. Betterscan

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

Description	Possible 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.



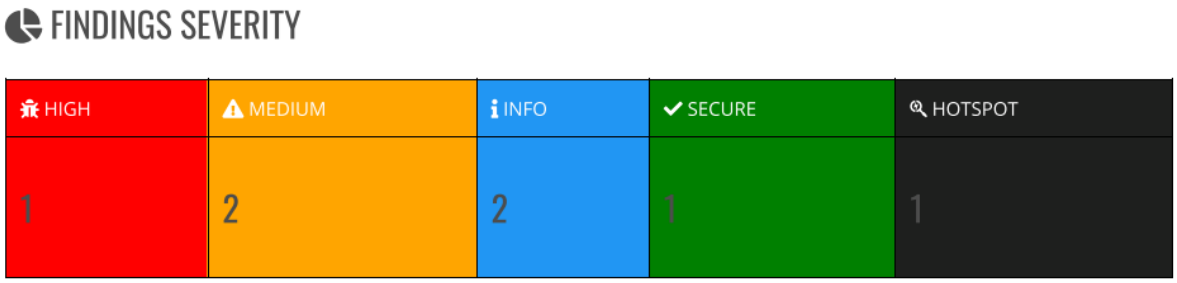
5. Horusec

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/MovieServiceMobileAPImaster/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.



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 fin any leaks in the app.

```
przemek@DESKTOP-628E750:~/Downloads/MovieServiceMobileAPImaster1$ gitleaks detect
    ○
    │╲
    ○ ○
    ▮ ▮  gitleaks

11:39AM INF 1 commits scanned.
11:39AM INF scan completed in 2.56s
11:39AM INF no leaks found
```

8. SonarQube SCA

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