POZNAN UNIVERSITY OF TECHNOLOGY

FACULTY OF COMPUTING AND TELECOMMUNICATION
Cybersecurity

Application Security

Warehouse Management - security analysis

Natalia Czyżewska 141207
Wojciech Koszela 141251
Joaquin Cerdan

November 26, 2022

Contents

1 Introduction

The project ”Warehouse Management” consists of a client Android application which communicates with a backend written in Python using the Flask framework. Its functionalities are limited due to it being unfinished which significantly reduced the scope of possible tests. However, some features such as login were partially implemented on feature branches.

Static analysis was performed using 7 different tools, the results from which are presented in the following sections. Additionally, the source code was examined according to OWASP Mobile App Security Checklist.

2 Tools

2.1 Automated Security Helper

ASH scanned the project directory and found issues related mostly with running app in debug mode and unsecured Docker configuration.

```
#############################################
Start of ./cdk_report_result.txt
#############################################

#############################################
End of ./cdk_report_result.txt
#############################################


#############################################
Start of ./git_report_result.txt
#############################################
fatal: detected dubious ownership in repository at ’/app’
To add an exception for this directory, call:

       git config --global --add safe.directory /app
#############################################
End of ./git_report_result.txt
#############################################


#############################################
Start of ./grype_report_result.txt
#############################################
No vulnerabilities found
[0000] WARN found package with empty ID while adding to the catalog: Pkg
    (name="gradle-wrapper" version="" type="java-archive" id="")
NAME          VERSION TYPE
gradle-wrapper        java-archive
#############################################
End of ./grype_report_result.txt
```

```
#############################################


#############################################
Start of ./py_report_result.txt
#############################################
[main] INFO   profile include tests: None
[main] INFO   profile exclude tests: None
[main] INFO   cli include tests: None
[main] INFO   cli exclude tests: None
[main] INFO   running on Python 3.11.0
Run started:2022-11-26 16:52:57.787465

Test results:
>> Issue: [B201:flask_debug_true] A Flask app appears to be run with
    debug=True, which exposes the Werkzeug debugger and allows the
    execution of arbitrary code.
   Severity: High Confidence: Medium
   CWE: CWE-94 (https://cwe.mitre.org/data/definitions/94.html)
   Location: ./backend/app.py:14:4
   More Info: https://bandit.readthedocs.io/en/1.7.4/plugins/
       b201_flask_debug_true.html
13      if __name__ == '__main__':
14          app.run(debug=True) ### REMOVE BEFORE DEPLOY
15

--------------------------------------------------

Code scanned:
        Total lines of code: 118
        Total lines skipped (#nosec): 0
        Total potential issues skipped due to specifically being disabled
             (e.g., #nosec BXXX): 0

Run metrics:
        Total issues (by severity):
                Undefined: 0
                Low: 0
                Medium: 0
                High: 1
        Total issues (by confidence):
                Undefined: 0
                Low: 0
                Medium: 1
                High: 0
Files skipped (0):
#############################################
End of ./py_report_result.txt
#############################################
```

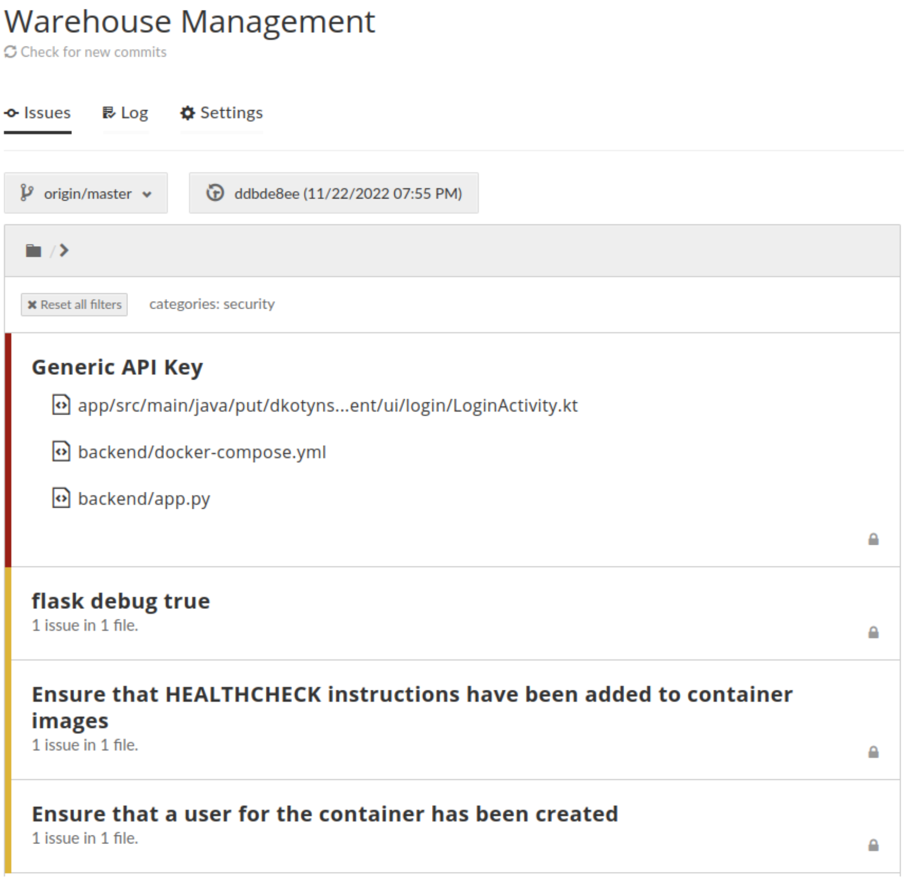
```
#############################################
Start of ./yaml_report_result.txt
#############################################
2022-11-26 16:54:35,705 [MainThread ] [ERROR] Cannot read file contents:
    ./app/build/intermediates/data_binding_base_class_log_artifact/debug
    /out/put.dkotynski.warehouse.management-binding_classes.json
2022-11-26 16:54:35,709 [MainThread ] [ERROR] Cannot read file contents:
    ./app/build/intermediates/incremental/dataBindingGenBaseClassesDebug
    /base_builder_log.json
2022-11-26 16:54:35,710 [MainThread ] [ERROR] Cannot read file contents:
    ./app/build/intermediates/data_binding_base_class_log_artifact/debug
    /out/put.dkotynski.warehouse.management-binding_classes.json
2022-11-26 16:54:35,730 [MainThread ] [ERROR] Cannot read file contents:
    ./app/build/intermediates/incremental/dataBindingGenBaseClassesDebug
    /base_builder_log.json


       _              _
   ___| |__  ___  ___| | _______ __
  / __| ’_ \ / _ \/ __| |/ / _ \ \ / /
 | (__| | | | __/ (__|  < (_) \ V /
  \___|_| |_|\___|\___|_|\_\___/ \_/

By bridgecrew.io | version: 2.2.96

terraform_plan scan results:

Passed checks: 0, Failed checks: 0, Skipped checks: 0, Parsing errors: 2

Error parsing file put.dkotynski.warehouse.management-binding_classes.
    json
Error parsing file base_builder_log.json
dockerfile scan results:

Passed checks: 5, Failed checks: 2, Skipped checks: 0

Check: CKV_DOCKER_11: "Ensure From Alias are unique for multistage builds
    ."
       PASSED for resource: /backend/Dockerfile.
       File: /backend/Dockerfile:1-11
       Guide: https://docs.bridgecrew.io/docs/ensure-docker-from-alias-
           is-unique-for-multistage-builds
Check: CKV_DOCKER_7: "Ensure the base image uses a non latest version tag
    "
       PASSED for resource: /backend/Dockerfile.
       File: /backend/Dockerfile:1-11
       Guide: https://docs.bridgecrew.io/docs/ensure-the-base-image-uses
           -a-non-latest-version-tag
Check: CKV_DOCKER_5: "Ensure update instructions are not use alone in the
     Dockerfile"
```

```
       PASSED for resource: /backend/Dockerfile.
       File: /backend/Dockerfile:1-11
       Guide: https://docs.bridgecrew.io/docs/ensure-update-instructions
           -are-not-used-alone-in-the-dockerfile
Check: CKV_DOCKER_9: "Ensure that APT isn't used"
       PASSED for resource: /backend/Dockerfile.
       File: /backend/Dockerfile:1-11
       Guide: https://docs.bridgecrew.io/docs/ensure-docker-apt-is-not-
           used
Check: CKV_DOCKER_1: "Ensure port 22 is not exposed"
       PASSED for resource: /backend/Dockerfile.
       File: /backend/Dockerfile:1-11
       Guide: https://docs.bridgecrew.io/docs/ensure-port-22-is-not-
           exposed
Check: CKV_DOCKER_2: "Ensure that HEALTHCHECK instructions have been
    added to container images"
       FAILED for resource: /backend/Dockerfile.
       File: /backend/Dockerfile:1-11
       Guide: https://docs.bridgecrew.io/docs/ensure-that-healthcheck-
           instructions-have-been-added-to-container-images

              1  | FROM python:3.6-slim-buster
              2  |
              3  | COPY requirements.txt .
              4  |
              5  | RUN pip install -r requirements.txt
              6  |
              7  | COPY . .
              8  |
              9  | EXPOSE 80
              10 |
              11 | CMD ["flask", "run", "--host=0.0.0.0", "--port=80"]
Check: CKV_DOCKER_3: "Ensure that a user for the container has been
    created"
       FAILED for resource: /backend/Dockerfile.
       File: /backend/Dockerfile:1-11
       Guide: https://docs.bridgecrew.io/docs/ensure-that-a-user-for-the
           -container-has-been-created

              1  | FROM python:3.6-slim-buster
              2  |
              3  | COPY requirements.txt .
              4  |
              5  | RUN pip install -r requirements.txt
              6  |
              7  | COPY . .
              8  |
              9  | EXPOSE 80
              10 |
              11 | CMD ["flask", "run", "--host=0.0.0.0", "--port=80"]
```

```
------------------------------------------------------------
./backend/docker-compose.yml
------------------------------------------------------------------------------------------------------

| FAIL FATAL
|
| Illegal cfn - no Resources

Failures count: 1
Warnings count: 0
#############################################
End of ./yaml_report_result.txt
#############################################
```

2.2 Betterscan

Betterscan found 6 issues, including 3 of critical severity and 3 minor.



Warehouse Management

Check for new commits

Issues Log Settings

origin/master

ddbde8ee (11/22/2022 07:55 PM)

Reset all filters   categories: security

Generic API Key

app/src/main/java/put/dkotyns...ent/ui/login/LoginActivity.kt

backend/docker-compose.yml

backend/app.py

flask debug true

1 issue in 1 file.

Ensure that HEALTHCHECK instructions have been added to container images

1 issue in 1 file.

Ensure that a user for the container has been created

1 issue in 1 file.

Figure 1: Betterscan security analysis

2.3 Fluid Attack's Scanner

Fluid Attack's Scanner was used to scan the APK. It found some obvious issues like the lack of obfuscation, but also some more hidden ones such as insecure communication over HTTP or allowBackup being enabled.

```
finding,kind,what,where,cwe,stream,title,description,snippet,method
F046,inputs,app/release/app-release.apk (Warehouse),android/support/v4/os
    /ResultReceiver$1 is not obfuscated,1269,"home,apk,bytecodes",046.
    Missing secure obfuscation - APK,android/support/v4/os/
    ResultReceiver$1 is not obfuscated,"
> 1 | package android.support.v4.os;
  2 |  class ResultReceiver$1 implements android.os.Parcelable$Creator {
   3 |
   4 |     ResultReceiver$1()
   5 |     {
   6 |         return;
   7 |     }
   8 |
   9 |     public android.support.v4.os.ResultReceiver createFromParcel(
       android.os.Parcel p2)
  10 |     {
  11 |         return new android.support.v4.os.ResultReceiver(p2);
  12 |     }
  13 |
  14 |     public bridge synthetic Object createFromParcel(android.os.
      Parcel p1)
  15 |     {
  16 |         return this.createFromParcel(p1);
  17 |     }
  18 |
  19 |     public android.support.v4.os.ResultReceiver[] newArray(int p1)
  20 |     {
  21 |         android.support.v4.os.ResultReceiver[] v1_1 = new android.
      support.v4.os.ResultReceiver[p1];
     ^ Col 0
",analyze_bytecodes.no_obfuscation
F207,inputs,app/release/app-release.apk (Warehouse),Missing res/xml/
    network_security_config.xml,295,"home,apk,bytecodes",207. Security
    controls bypass or absence - SSLPinning,Missing res/xml/
    network_security_config.xml,"
   1 | $ python3.8
   2 |
   3 | >>> # We'll use the version 3.3.5 of ""androguard""
   4 | >>> from androguard.core.bytecodes.apk import APK
   5 |
   6 | >>> # This object represents the APK to analyze
   7 | >>> apk = APK('app/release/app-release.apk')
   8 |
   9 | >>> # List all files in the APK
  10 | >>> apk_files = apk.zip.nameslist()
> 11 | >>> ""res/xml/network_security_config.xml"" in apk_files
  12 | False # No network security config exists
     ^ Col 0
",analyze_bytecodes.no_certs_pinning
F103,inputs,app/release/app-release.apk (Warehouse),Not signed,325,"home,
    apk,bytecodes",103. Insufficient data authenticity validation - APK
    signing,Not signed,"
   1 | $ python3.8
   2 |
   3 | >>> # We'll use the version 3.3.5 of ""androguard""
   4 | >>> from androguard.core.bytecodes.apk import APK
   5 |
   6 | >>> # This object represents the APK to analyze
   7 | >>> apk = APK('app/release/app-release.apk')
   8 |
   9 | >>> # Check the META-INF/ folder and retrieve signature pairs
  10 | >>> # with extensions: .DSA & .DF, .EC & .DF, or .RSA & .DF
  11 | >>> apk.get_signature_names()
> 12 | [] # Empty list means no signatures exist
     ^ Col 0
",analyze_bytecodes.apk_unsigned
F055,inputs,app/release/app-release.apk (Warehouse),application.android:
    allowBackup enabled,530,"home,apk,bytecodes",055. Insecure service
    configuration - ADB Backups,application.android:allowBackup enabled
    ,"
   1 | <manifest android:compilesdkversion=""32"" android:
       compilesdkversioncodename=""12"" android:versioncode=""1"" android
       :versionn
     | ame=""1.0"" package=""put.dkotynski.warehouse.management""
         platformbuildversioncode=""32"" platformbuildversionname=""12""
         xmlns
     | :android=""http://schemas.android.com/apk/res/android"">
   2 |  <uses-sdk android:minsdkversion=""28"" android:targetsdkversion
       =""32"">
   3 |  </uses-sdk>
   4 |  <uses-permission android:name=""android.permission.INTERNET"">
   5 |  </uses-permission>
>  6 |  <application android:allowbackup=""true"" android:
    appcomponentfactory=""androidx.core.app.CoreComponentFactory""
    android:da
     | taextractionrules=""@7F130001"" android:extractnativelibs=""false
         "" android:fullbackupcontent=""@7F130000"" android:icon=""@7F0
     | D0000"" android:label=""@7F100021"" android:roundicon=""@7F0D0001
         "" android:supportsrtl=""true"" android:theme=""@7F110248"" andr
     | oid:usescleartexttraffic=""true"">
   7 |   <activity android:exported=""false"" android:name=""put.
       dkotynski.warehouse.management.EditProductDetailsActivity"">
   8 |    <meta-data android:name=""android.app.lib_name"" android:value
       ="""">
   9 |    </meta-data>
  10 |   </activity>
  11 |   <activity android:exported=""false"" android:name=""put.
      dkotynski.warehouse.management.ProductDetailsActivity"">
  12 |    <meta-data android:name=""android.app.lib_name"" android:value
      ="""">
  13 |    </meta-data>
  14 |   </activity>
  15 |   <activity android:exported=""false"" android:label=""@7F1000AC""
       android:name=""put.dkotynski.warehouse.management.MainActi
     | vity"" android:theme=""@7F11024A"">
     ^ Col 0
",analyze_bytecodes.apk_backups_enabled
```

```
F372,inputs,app/release/app-release.apk (Warehouse),The given APK
    references HTTP (not HTTPS) resources.,650,"home,apk,bytecodes",372.
     Use of an insecure channel - HTTP,The given APK references HTTP (
    not HTTPS) resources.,"
   1 | $ python3.8
   2 |
   3 | >>> # We'll use the version 3.3.5 of ""androguard""
   4 | >>> from androguard.misc import AnalyzeAPK
   5 |
   6 | >>> # Parse all Dalvik Executables (classes*.dex) in the APK
   7 | >>> dex = AnalyzeAPK('app/release/app-release.apk')[2]
   8 |
   9 | >>> # Get the method names from all classes in each .dex file
> 10 | >>> sorted(set(method.name for method in dex.get_methods()))
  11 | # HTTP resources found
  12 | >>> ['http://localhost:5000']
     ^ Col 0
",analyze_bytecodes.uses_http_resources
```

2.4 Gitleaks

Gitleaks found a valid jwt token in 7 places within the same file, which was a Postman collection presumably used for testing the API.

```
Finding:    "value": "eyJ0eXAiOiJKV1QiLCJhbGciOiJIUzI1NiJ9.
    eyJwdWJsaWNfaWQiOiI5YWY0NzJiZC1iMjk1LTQ2OTUtOWZkYi1mYTBlMWFlZmJ...,
Secret:     eyJ0eXAiOiJKV1QiLCJhbGciOiJIUzI1NiJ9.
    eyJwdWJsaWNfaWQiOiI5YWY0NzJiZC1iMjk1LTQ2OTUtOWZkYi1mYTBlMWFlZmJ...
RuleID:     jwt
Entropy:    5.420272
File:       backend/Warehouse_management_system.postman_collection.json
Line:       16
Commit:     e85f7aeef717bf369a68169b2a1eac06045f54b6
Author:     Daniel
Email:      danielkotynski@gmail.com
Date:       2022-11-23T01:09:50Z
Fingerprint: e85f7aeef717bf369a68169b2a1eac06045f54b6:backend/
    Warehouse_management_system.postman_collection.json:jwt:16

Finding:    "value": "eyJ0eXAiOiJKV1QiLCJhbGciOiJIUzI1NiJ9.
    eyJwdWJsaWNfaWQiOiI5YWY0NzJiZC1iMjk1LTQ2OTUtOWZkYi1mYTBlMWFlZmJ...,
Secret:     eyJ0eXAiOiJKV1QiLCJhbGciOiJIUzI1NiJ9.
    eyJwdWJsaWNfaWQiOiI5YWY0NzJiZC1iMjk1LTQ2OTUtOWZkYi1mYTBlMWFlZmJ...
RuleID:     jwt
Entropy:    5.420272
File:       backend/Warehouse_management_system.postman_collection.json
Line:       39
Commit:     e85f7aeef717bf369a68169b2a1eac06045f54b6
Author:     Daniel
```

```
Email:      danielkotynski@gmail.com
Date:       2022-11-23T01:09:50Z
Fingerprint: e85f7aeef717bf369a68169b2a1eac06045f54b6:backend/
    Warehouse_management_system.postman_collection.json:jwt:39

Finding:    "value": "eyJ0eXAiOiJKV1QiLCJhbGciOiJIUzI1NiJ9.
    eyJwdWJsaWNfaWQiOiI5YWY0NzJiZC1iMjk1LTQ2OTUtOWZkYi1mYTBlMWFlZmJ...,
Secret:     eyJ0eXAiOiJKV1QiLCJhbGciOiJIUzI1NiJ9.
    eyJwdWJsaWNfaWQiOiI5YWY0NzJiZC1iMjk1LTQ2OTUtOWZkYi1mYTBlMWFlZmJ...
RuleID:     jwt
Entropy:    5.420272
File:       backend/Warehouse_management_system.postman_collection.json
Line:       72
Commit:     e85f7aeef717bf369a68169b2a1eac06045f54b6
Author:     Daniel
Email:      danielkotynski@gmail.com
Date:       2022-11-23T01:09:50Z
Fingerprint: e85f7aeef717bf369a68169b2a1eac06045f54b6:backend/
    Warehouse_management_system.postman_collection.json:jwt:72

Finding:    "value": "eyJ0eXAiOiJKV1QiLCJhbGciOiJIUzI1NiJ9.
    eyJwdWJsaWNfaWQiOiI5YWY0NzJiZC1iMjk1LTQ2OTUtOWZkYi1mYTBlMWFlZmJ...,
Secret:     eyJ0eXAiOiJKV1QiLCJhbGciOiJIUzI1NiJ9.
    eyJwdWJsaWNfaWQiOiI5YWY0NzJiZC1iMjk1LTQ2OTUtOWZkYi1mYTBlMWFlZmJ...
RuleID:     jwt
Entropy:    5.420272
File:       backend/Warehouse_management_system.postman_collection.json
Line:       81
Commit:     e85f7aeef717bf369a68169b2a1eac06045f54b6
Author:     Daniel
Email:      danielkotynski@gmail.com
Date:       2022-11-23T01:09:50Z
Fingerprint: e85f7aeef717bf369a68169b2a1eac06045f54b6:backend/
    Warehouse_management_system.postman_collection.json:jwt:81

Finding:    "value": "eyJ0eXAiOiJKV1QiLCJhbGciOiJIUzI1NiJ9.
    eyJwdWJsaWNfaWQiOiI5YWY0NzJiZC1iMjk1LTQ2OTUtOWZkYi1mYTBlMWFlZmJ...,
Secret:     eyJ0eXAiOiJKV1QiLCJhbGciOiJIUzI1NiJ9.
    eyJwdWJsaWNfaWQiOiI5YWY0NzJiZC1iMjk1LTQ2OTUtOWZkYi1mYTBlMWFlZmJ...
RuleID:     jwt
Entropy:    5.420272
File:       backend/Warehouse_management_system.postman_collection.json
Line:       108
Commit:     e85f7aeef717bf369a68169b2a1eac06045f54b6
Author:     Daniel
Email:      danielkotynski@gmail.com
Date:       2022-11-23T01:09:50Z
Fingerprint: e85f7aeef717bf369a68169b2a1eac06045f54b6:backend/
    Warehouse_management_system.postman_collection.json:jwt:108
```

```
Finding:    "value": "eyJ0eXAiOiJKV1QiLCJhbGciOiJIUzI1NiJ9.
    eyJwdWJsaWNfaWQiOiI5YWY0NzJiZC1iMjk1LTQ2OTUtOWZkYi1mYTBlMWFlZmJ...,
Secret:     eyJ0eXAiOiJKV1QiLCJhbGciOiJIUzI1NiJ9.
    eyJwdWJsaWNfaWQiOiI5YWY0NzJiZC1iMjk1LTQ2OTUtOWZkYi1mYTBlMWFlZmJ...
RuleID:     jwt
Entropy:    5.420272
File:       backend/Warehouse_management_system.postman_collection.json
Line:       141
Commit:     e85f7aeef717bf369a68169b2a1eac06045f54b6
Author:     Daniel
Email:      danielkotynski@gmail.com
Date:       2022-11-23T01:09:50Z
Fingerprint: e85f7aeef717bf369a68169b2a1eac06045f54b6:backend/
    Warehouse_management_system.postman_collection.json:jwt:141

Finding:    "value": "eyJ0eXAiOiJKV1QiLCJhbGciOiJIUzI1NiJ9.
    eyJwdWJsaWNfaWQiOiI5YWY0NzJiZC1iMjk1LTQ2OTUtOWZkYi1mYTBlMWFlZmJ...,
Secret:     eyJ0eXAiOiJKV1QiLCJhbGciOiJIUzI1NiJ9.
    eyJwdWJsaWNfaWQiOiI5YWY0NzJiZC1iMjk1LTQ2OTUtOWZkYi1mYTBlMWFlZmJ...
RuleID:     jwt
Entropy:    5.420272
File:       backend/Warehouse_management_system.postman_collection.json
Line:       165
Commit:     e85f7aeef717bf369a68169b2a1eac06045f54b6
Author:     Daniel
Email:      danielkotynski@gmail.com
Date:       2022-11-23T01:09:50Z
Fingerprint: e85f7aeef717bf369a68169b2a1eac06045f54b6:backend/
    Warehouse_management_system.postman_collection.json:jwt:165

10:28PM INF 19 commits scanned.
10:28PM INF scan completed in 73.3ms
10:28PM WRN leaks found: 7
```

2.5 Horusec

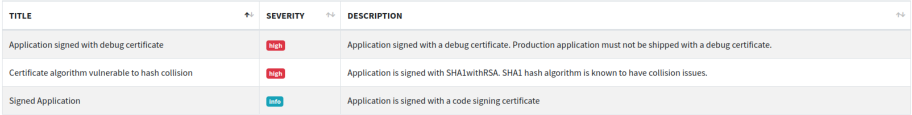
Horusec found 6 possible vulnerabilities. 2 of them were classified with HIGH severity and 4 as CRITICAL.

```
==================================================================================


HORUSEC ENDED THE ANALYSIS WITH STATUS OF "success" AND WITH THE
    FOLLOWING RESULTS:

==================================================================================


Analysis StartedAt: 2022-11-26 13:24:56
Analysis FinishedAt: 2022-11-26 13:25:45

==================================================================================


Language: Leaks
Severity: CRITICAL
Line: 11
Column: 21
SecurityTool: HorusecEngine
Confidence: MEDIUM
File: /home/nir/tools/Warehouse_Management/backend/docker-compose.yml
Code: - DATABASE_URL=postgresql://postgres:postgres@db:5432/postgres
RuleID: HS-LEAKS-27
Type: Vulnerability
ReferenceHash:
    e5fed14d0e173fd1232b39e6a239e95951f783fbfa4ac50ac08c2d32083e9f8c
Details: (1/1) * Possible vulnerability detected: Password found in a
    hardcoded URL
A password was found in a hardcoded URL, this can lead to not only the
    leak of this password but also a failure point to some more
    sophisticated CSRF and SSRF attacks. Check CWE-352 (https://cwe.
    mitre.org/data/definitions/352.html) and CWE-918 (https://cwe.mitre.
    org/data/definitions/918.html) for more details.

==================================================================================


Language: Leaks
Severity: CRITICAL
Line: 19
Column: 12
SecurityTool: HorusecEngine
Confidence: MEDIUM
File: /home/nir/tools/Warehouse_Management/backend/app.py
Code: app.config['SECRET_KEY'] = os.environ.get('SECRET_KEY')
RuleID: HS-LEAKS-25
Type: Vulnerability
ReferenceHash: 578840
    eb3387494b8de9f838ae77bbcf773844979eea2c8ab65fc1b85f8071e2
Details: (1/1) * Possible vulnerability detected: Potential Hard-coded
    credential
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.

==================================================================================
Language: Leaks
Severity: CRITICAL
Line: 61
Column: 70
SecurityTool: HorusecEngine
Confidence: MEDIUM
File: /home/nir/tools/Warehouse_Management/backend/app.py
Code: token = jwt.encode({'public_id': user.public_id}, app.config['
    SECRET_KEY'], 'HS256')
RuleID: HS-LEAKS-25
Type: Vulnerability
ReferenceHash: 1
    cff3ec77823bf0a4586dfea77c9ed52f1b7fce670c5204ad54c094955e26119
Details: (1/1) * Possible vulnerability detected: Potential Hard-coded
    credential
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.

==================================================================================


Language: Leaks
Severity: CRITICAL
Line: 90
Column: 43
SecurityTool: HorusecEngine
Confidence: MEDIUM
File: /home/nir/tools/Warehouse_Management/backend/app.py
Code: data = jwt.decode(token, app.config['SECRET_KEY'], algorithms=['
    HS256'])
RuleID: HS-LEAKS-25
Type: Vulnerability
ReferenceHash:
    bd0ab69a091998ec3f2a60338a3523e750967857e6af8317b13c667c578b1413
Details: (1/1) * Possible vulnerability detected: Potential Hard-coded
    credential
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.

==================================================================================


Language: Python
```

```
Severity: HIGH
Line: 14
Column: 0
SecurityTool: Bandit
Confidence: MEDIUM
File: /home/nir/tools/Warehouse_Management/backend/app.py
Code: 13 if __name__ == '__main__':
14    app.run(debug=True) ### REMOVE BEFORE DEPLOY
15

RuleID: B201
Type: Vulnerability
ReferenceHash: 109382
    acd67c6b27ae7ee647ab3081d2a4cd5c9dadbae781abab071616b8f0c9
Details: (1/1) * Possible vulnerability detected: A Flask app appears to
    be run with debug=True, which exposes the Werkzeug debugger and
    allows the execution of arbitrary code.

==================================================================================


Language: Generic
Severity: HIGH
Line: 0
Column: 0
SecurityTool: Trivy
Confidence: MEDIUM
File: /home/nir/tools/Warehouse_Management/backend/Dockerfile
Code: root user
Type: Vulnerability
ReferenceHash:
    c569629b8e893f2d1b2af676dc20fdb5cb5d866618c8f22298f532f5d5322163
Details: (1/1) * Possible vulnerability detected: MissConfiguration
     Running containers with 'root' user can lead to a container escape
         situation. It is a best practice to run containers as non-root
         users, which can be done by adding a 'USER' statement to the
         Dockerfile.
     Message: Specify at least 1 USER command in Dockerfile with non-
         root user as argument
     Resolution: Add 'USER <non root user name>' line to the Dockerfile
     References: [https://docs.docker.com/develop/develop-images/
         dockerfile_best-practices/ https://avd.aquasec.com/appshield/
         ds002]

==================================================================================


In this analysis, a total of 6 possible vulnerabilities were found and we
     classified them into:
Total of Vulnerability HIGH is: 2
Total of Vulnerability CRITICAL is: 4

==========================================================================
```

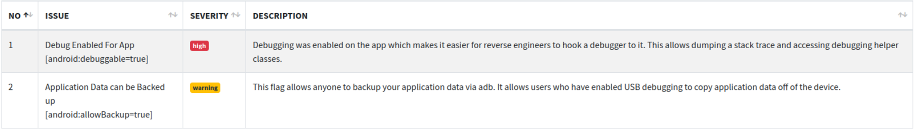
2.6 Mobile Security Framework

MobSF found 3 vulnerabilities with High severity and 1 with Medium one. Two of them classified as High are present solely because no APK was made available to us, so we had to create our own.



TITLE	SEVERITY	DESCRIPTION
Application signed with debug certificate	high	Application signed with a debug certificate. Production application must not be shipped with a debug certificate.
Certificate algorithm vulnerable to hash collision	high	Application is signed with SHA1withRSA. SHA1 hash algorithm is known to have collision issues.
Signed Application	info	Application is signed with a code signing certificate

Figure 2: MobSF Signer certificate analysis

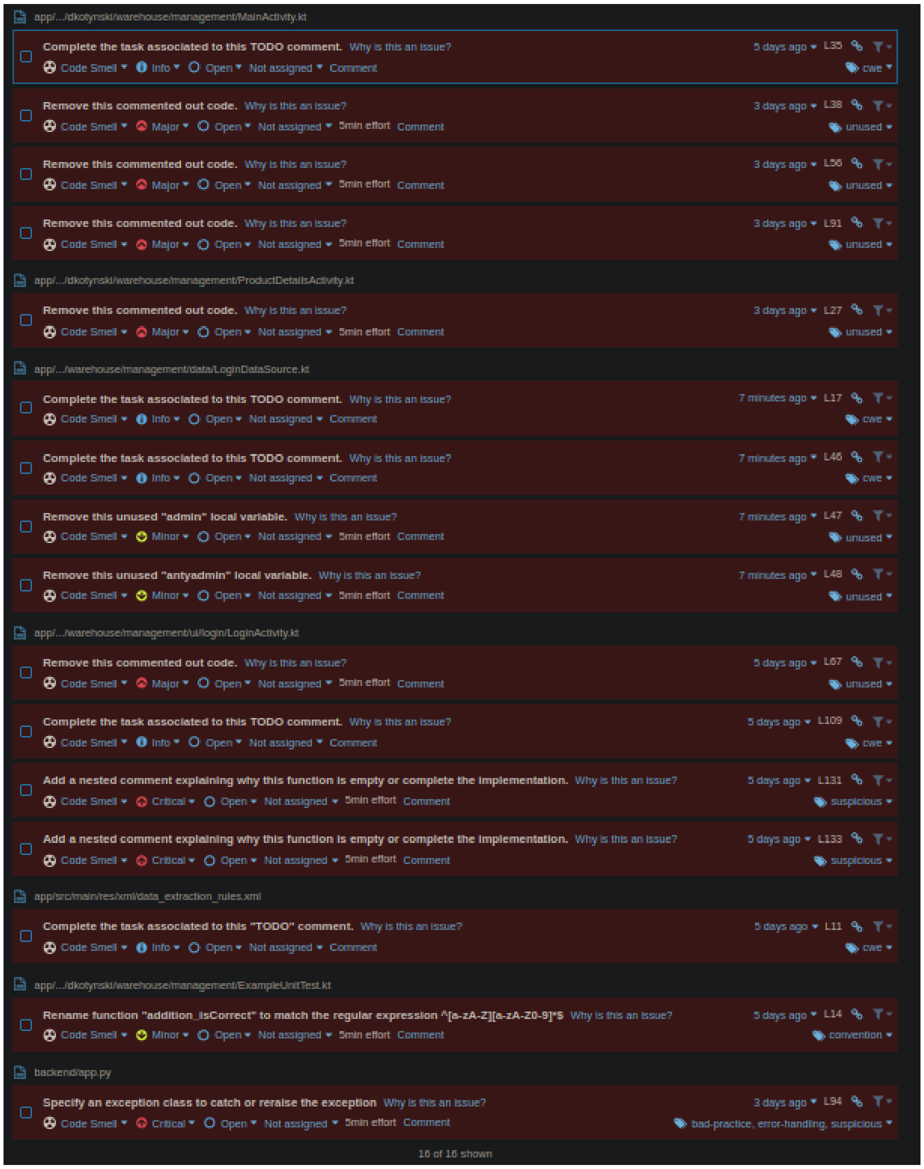


NO	ISSUE	SEVERITY	DESCRIPTION
1	Debug Enabled For App [android:debuggable=true]	high	Debugging was enabled on the app which makes it easier for reverse engineers to hook a debugger to it. This allows dumping a stack trace and accessing debugging helper classes.
2	Application Data can be Backed up [android:allowBackup=true]	warning	This flag allows anyone to backup your application data via adb. It allows users who have enabled USB debugging to copy application data off of the device.

Figure 3: MobSF Manifest analysis

2.7 SonarQube

SonarQube identified 16 code smells, mostly unused or unimplemented features.



app/.../dkotynski/warehouse/management/MainActivity.kt

□ Complete the task associated to this TODO comment. Why is this an issue? — 5 days ago L35
Code Smell · Info · Open · Not assigned · Comment — cwe

□ Remove this commented out code. Why is this an issue? — 3 days ago L38
Code Smell · Major · Open · Not assigned · 5min effort · Comment — unused

□ Remove this commented out code. Why is this an issue? — 3 days ago L56
Code Smell · Major · Open · Not assigned · 5min effort · Comment — unused

□ Remove this commented out code. Why is this an issue? — 3 days ago L91
Code Smell · Major · Open · Not assigned · 5min effort · Comment — unused

app/.../dkotynski/warehouse/management/ProductDetailsActivity.kt

□ Remove this commented out code. Why is this an issue? — 3 days ago L27
Code Smell · Major · Open · Not assigned · 5min effort · Comment — unused

app/.../warehouse/management/data/LoginDataSource.kt

□ Complete the task associated to this TODO comment. Why is this an issue? — 7 minutes ago L17
Code Smell · Info · Open · Not assigned · Comment — cwe

□ Complete the task associated to this TODO comment. Why is this an issue? — 7 minutes ago L46
Code Smell · Info · Open · Not assigned · Comment — cwe

□ Remove this unused "admin" local variable. Why is this an issue? — 7 minutes ago L47
Code Smell · Minor · Open · Not assigned · 5min effort · Comment — unused

□ Remove this unused "antyadmin" local variable. Why is this an issue? — 7 minutes ago L48
Code Smell · Minor · Open · Not assigned · 5min effort · Comment — unused

app/.../warehouse/management/ui/login/LoginActivity.kt

□ Remove this commented out code. Why is this an issue? — 5 days ago L67
Code Smell · Major · Open · Not assigned · 5min effort · Comment — unused

□ Complete the task associated to this TODO comment. Why is this an issue? — 5 days ago L109
Code Smell · Info · Open · Not assigned · Comment — cwe

□ Add a nested comment explaining why this function is empty or complete the implementation. Why is this an issue? — 5 days ago L131
Code Smell · Critical · Open · Not assigned · 5min effort · Comment — suspicious

□ Add a nested comment explaining why this function is empty or complete the implementation. Why is this an issue? — 5 days ago L133
Code Smell · Critical · Open · Not assigned · 5min effort · Comment — suspicious

app/src/main/res/xml/data_extraction_rules.xml

□ Complete the task associated to this "TODO" comment. Why is this an issue? — 5 days ago L11
Code Smell · Info · Open · Not assigned · Comment — cwe

app/.../dkotynski/warehouse/management/ExampleUnitTest.kt

□ Rename function "addition_isCorrect" to match the regular expression ^[a-zA-Z][a-zA-Z0-9]*$ Why is this an issue? — 5 days ago L14
Code Smell · Minor · Open · Not assigned · 5min effort · Comment — convention

backend/app.py

□ Specify an exception class to catch or reraise the exception Why is this an issue? — 3 days ago L94
Code Smell · Critical · Open · Not assigned · 5min effort · Comment — bad-practice, error-handling, suspicious

16 of 16 shown

Figure 4: SonarQube security analysis

3 Summary

Despite numerous vulnerabilities having been discovered, a large portion of them exists only because the app is still in development. The most critical ones were found by more than one tool, which is good. Some were also possibly misidentified, for instance the ”hardcoded” secret keys which come from environmental variables and in a production environment would not be stored in the same repository.