

**UNIVERSIDAD PRIVADA DE TACNA
FACULTAD DE INGENIERÍA
ESCUELA DE INGENIERÍA DE SISTEMAS**



Informe de Laboratorio

Laboratorio 02 “Auditoría de seguridad y hallazgos”

Que se presenta para el curso:
“Auditoría de sistemas”

Integrante(s):

- Cano Sucso Anthony Alexander

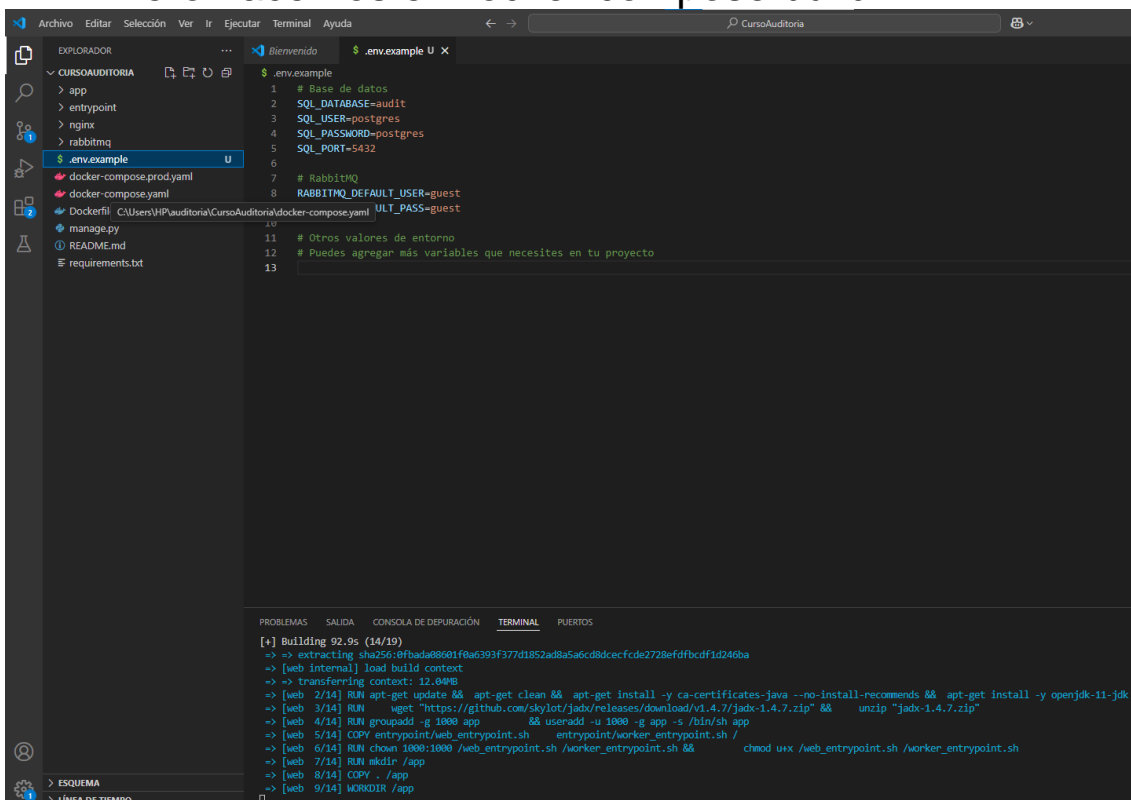
2020067573

Docente:

Dr. Oscar Juan Jimenez Flores

TACNA – PERÚ
2025

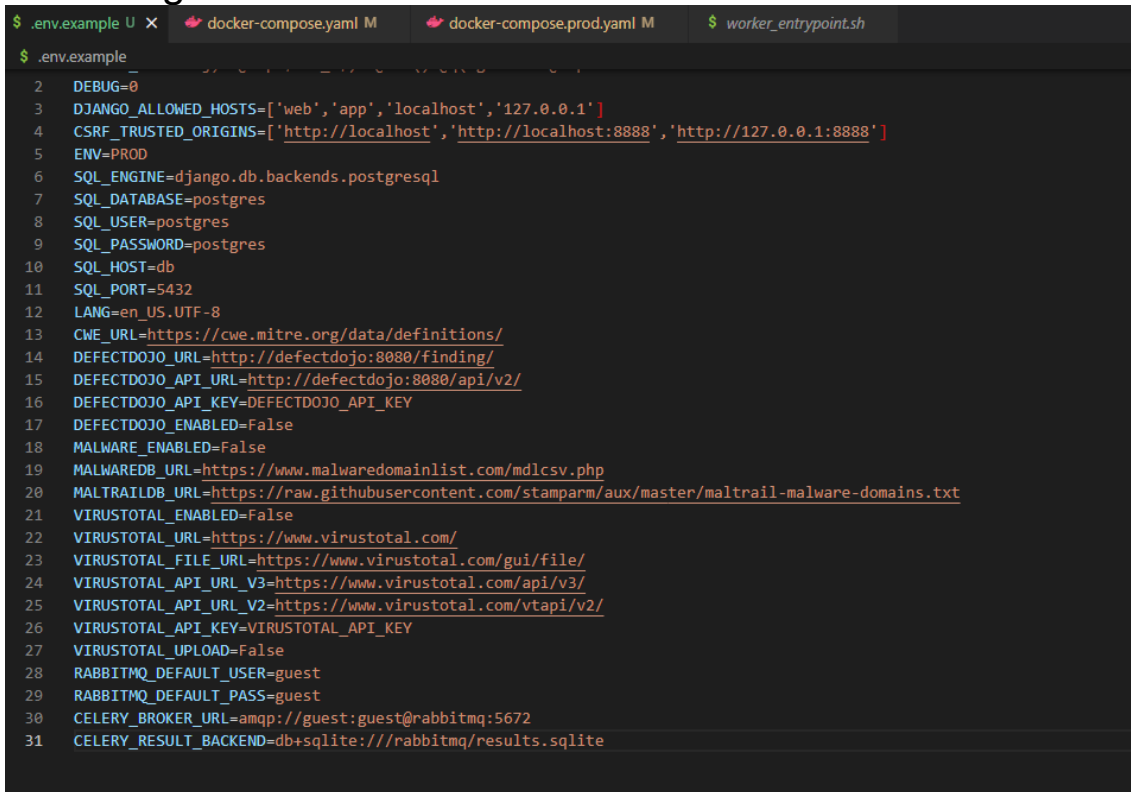
1.-Primero hacemos el Docker-compose build



```
1 # Base de datos
2 SQL_DATABASE=audit
3 SQL_USER=postgres
4 SQL_PASSWORD=postgres
5 SQL_PORT=5432
6
7 # RabbitMQ
8 RABBITMQ_DEFAULT_USER=guest
9 RABBITMQ_DEFAULT_PASS=guest
10
11 # Otros valores de entorno
12 # Puedes agregar más variables que necesites en tu proyecto
13
```

```
[*] Building 92.9s (14/19)
=> extracting sha256:8fbada8801f0a6393f377d1852ad8a5a6cd8dcecfde2728efdfbcd1d246ba
=> [web internal] load build context
=> transferring context: 12.00kB
=> [web 2/14] RUN apt-get update && apt-get clean && apt-get install -y ca-certificates-java --no-install-recommends && apt-get install -y openjdk-11-jdk
=> [web 3/14] RUN wget "https://github.com/skylot/jadx/releases/download/v1.4.7/jadx-1.4.7.zip" && unzip "jadx-1.4.7.zip"
=> [web 4/14] RUN groupadd -g 1000 app && useradd -u 1000 -g app -s /bin/sh app
=> [web 5/14] COPY entrypoint/web_entrypoint.sh entrypoint/worker_entrypoint.sh /
=> [web 6/14] RUN chown 1000:1000 /web_entrypoint.sh /worker_entrypoint.sh && chmod u+x /web_entrypoint.sh /worker_entrypoint.sh
=> [web 7/14] RUN mkdir /app
=> [web 8/14] COPY . /app
=> [web 9/14] WORKDIR /app
```

2.-Corregimos el archivo ENV



```
2 DEBUG=0
3 DJANGO_ALLOWED_HOSTS=['web', 'app', 'localhost', '127.0.0.1']
4 CSRF_TRUSTED_ORIGINS=['http://localhost', 'http://localhost:8888', 'http://127.0.0.1:8888']
5 ENV=PROD
6 SQL_ENGINE=django.db.backends.postgresql
7 SQL_DATABASE=postgres
8 SQL_USER=postgres
9 SQL_PASSWORD=postgres
10 SQL_HOST=db
11 SQL_PORT=5432
12 LANG=en_US.UTF-8
13 CWE_URL=https://cwe.mitre.org/data/definitions/
14 DEFECTDOJO_URL=http://defectdojo:8080/finding/
15 DEFECTDOJO_API_URL=http://defectdojo:8080/api/v2/
16 DEFECTDOJO_API_KEY=DEFECTDOJO_API_KEY
17 DEFECTDOJO_ENABLED=False
18 MALWARE_ENABLED=False
19 MALWAREDB_URL=https://www.malwaredomainlist.com/mdlcsv.php
20 MALTRAILDB_URL=https://raw.githubusercontent.com/stamparm/aux/master/maltrail-malware-domains.txt
21 VIRUSTOTAL_ENABLED=False
22 VIRUSTOTAL_URL=https://www.virustotal.com/
23 VIRUSTOTAL_FILE_URL=https://www.virustotal.com/gui/file/
24 VIRUSTOTAL_API_URL_V3=https://www.virustotal.com/api/v3/
25 VIRUSTOTAL_API_URL_V2=https://www.virustotal.com/vtapi/v2/
26 VIRUSTOTAL_API_KEY=VIRUSTOTAL_API_KEY
27 VIRUSTOTAL_UPLOAD=False
28 RABBITMQ_DEFAULT_USER=guest
29 RABBITMQ_DEFAULT_PASS=guest
30 CELERY_BROKER_URL=amqp://guest:guest@rabbitmq:5672
31 CELERY_RESULT_BACKEND=db+sqlite:///rabbitmq/results.sqlite
```


















3.- Volvemos a hacer build

```
[+] Building 28.0s (13/18)
=> CACHED [web 6/14] RUN chown 1000:1000 /web_entrypoint.sh /worker_entrypoint.sh &&      chmod u+x /web_entrypoint.sh /worker_entrypoint.sh
=> CACHED [web 7/14] RUN mkdir /app
=> [web 8/14] COPY . /app
=> [web 9/14] WORKDIR /app
=> [web 10/14] RUN pip install --upgrade pip && pip install -r requirements.txt
=> => # Downloading six-1.16.0-py2.py3-none-any.whl (11 kB)
=> => # Downloading soupsieve-2.5-py3-none-any.whl (36 kB)
=> => # Downloading sqlparse-0.5.0-py3-none-any.whl (43 kB)
=> => # Downloading stack_data-0.6.3-py3-none-any.whl (24 kB)
=> => # Downloading traitlets-5.14.1-py3-none-any.whl (85 kB)
=> => # Downloading uritemplate-4.1.1-py2.py3-none-any.whl (10 kB)
```

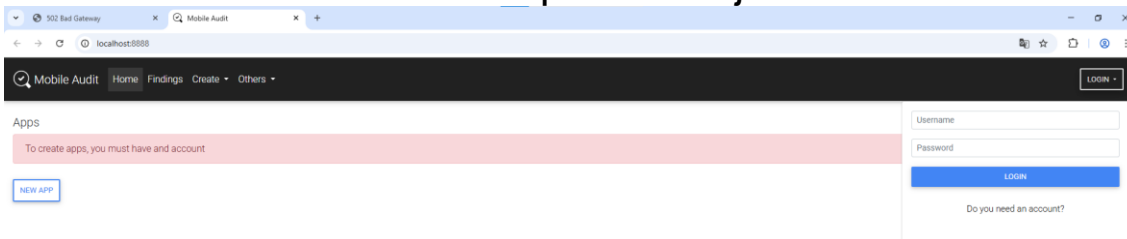
4.-Y ahora levantamos el contenedor

```
PS C:\Users\HP\auditoria\CursoAuditoria> docker-compose up -d
[+] Running 4/6
✔ Network cursoauditoria_default      Created
✔ Container cursoauditoria-db-1       Started
✔ Container cursoauditoria-web-1      Started
- Container cursoauditoria-rabbitmq-1 Starting
- Container cursoauditoria-nginx-1    Starting
✔ Container cursoauditoria-worker-1   Created
```

5.-Revisamos el Docker

<input type="checkbox"/>	cursoauditoria-main	-	-	0%	2 seconds ago			
<input type="checkbox"/>	db-1	5ca5845a4036	postgres:16-bullseye	0%	2 seconds ago			
<input type="checkbox"/>	web-1	6b06109a868a	mobile_audit	0%	2 seconds ago			
<input type="checkbox"/>	nginx-1	db7a10c46b61	nginx:stable-bullseye	8888.8888 C	0%	2 seconds ago		
<input type="checkbox"/>	rabbitmq-1	dc2d4650f127	rabbitmq:3.13.0-management	0%	2 seconds ago			
<input type="checkbox"/>	worker-1	76571dff284b	mobile_audit	0%	2 seconds ago			

6.-Nos creamos una cuenta para trabajar



502 Bad Gateway Mobile Audit

localhost:8888/accounts/register/

Mobile Audit Home Findings Create Others

← BACK

Username

Anthonycs04

First name

Anthony

Last name

Cano

Email

sucsoanthony@gmail.com

Password

.....

Password confirmation

.....

SIGN UP

7.-Haremos un primer análisis

502 Bad Gateway

Mobile Audit

localhost:8888/app/create

Mobile Audit Home Findings Create Others

BACK

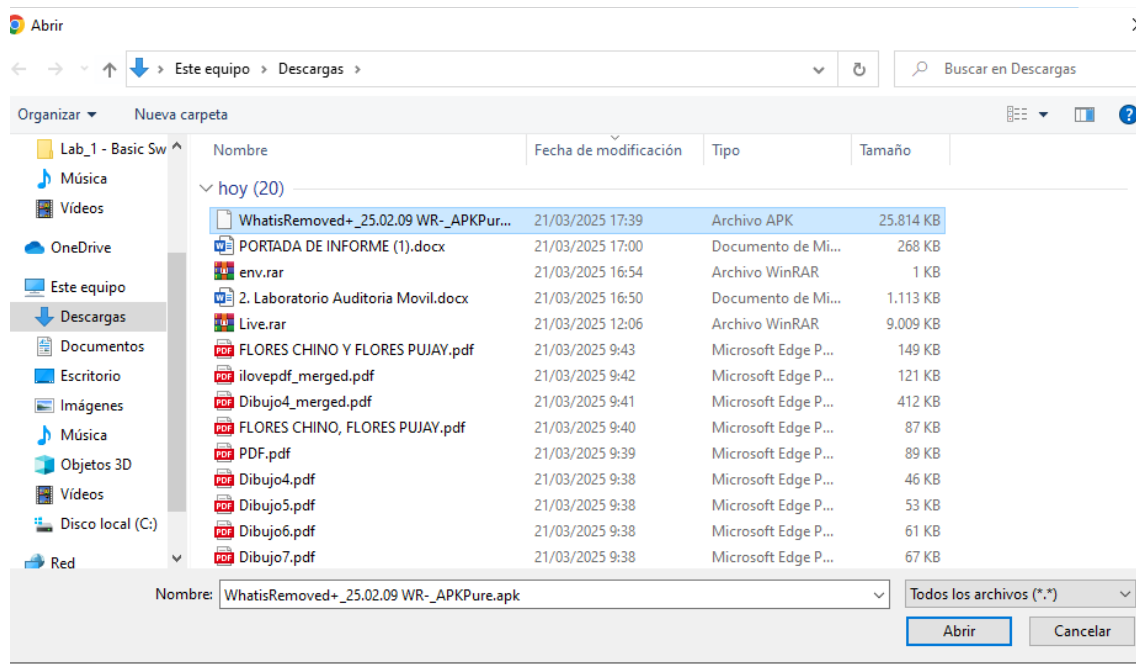
Name

WhatsRemoved+

Description

App para ver mensaje eliminados

CREATE

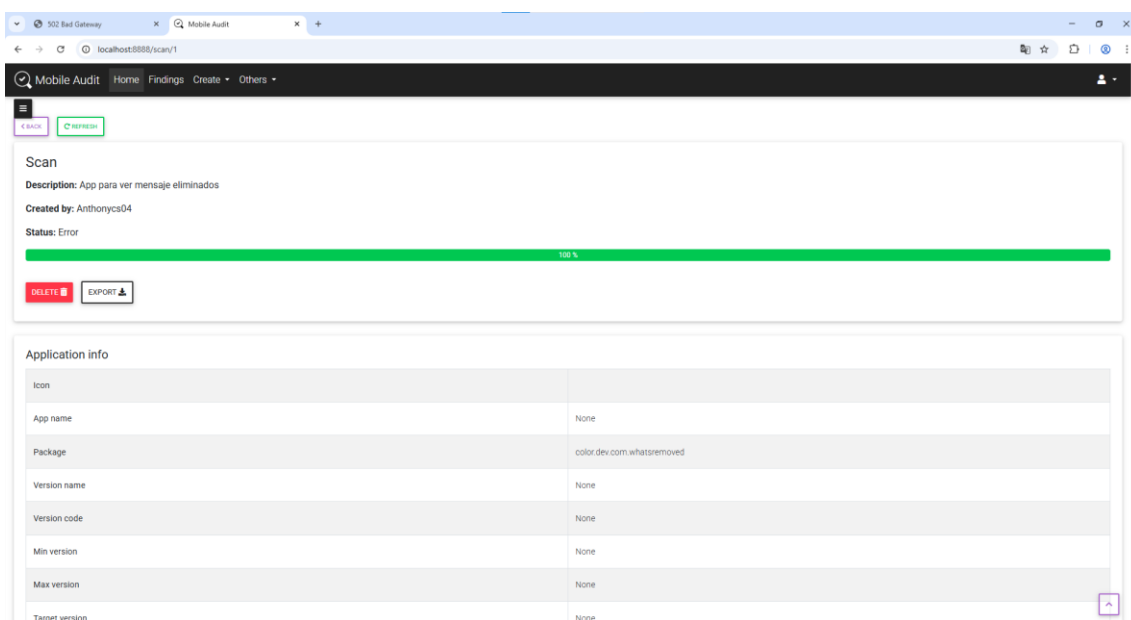


The screenshot shows a web browser with two tabs: '502 Bad Gateway' and 'Mobile Audit'. The address bar shows 'localhost:8888/scan/create/1'. The application has a dark navigation bar with 'Mobile Audit', 'Home', 'Findings', 'Create', and 'Others'. Below the navigation bar is a purple 'BACK' button. The main content area has a 'Description' section with a light blue box containing the text 'App para ver mensaje eliminados'. Below this is an 'Apk' section with a 'Seleccionar archivo' button and the text 'WhatisRemoved+_25.02.09 WR-_APKPure.apk'. Underneath is an 'App' section with a light blue box containing 'Application #1 - WhatsRemoved+'. At the bottom is a green 'UPLOAD' button.

8.-Esperamos a ver el análisis completo


The screenshot shows the 'Scan' results page in the Mobile Audit application. It includes a 'Description' section with the text 'App para ver mensaje eliminados', 'Created by: Anthonycs04', and 'Status: In Progress'. Below this is a progress bar showing 3% completion. There is a 'DELETE' button. The 'Application info' section contains a table with the following data:

Application info	
Icon	
App name	None
Package	None
Version name	None
Version code	None
Min version	None
Max version	None
Target version	None



Se podrá ver el reporte completo en APK1_report.pdf

9.-Haremos un segundo scanero

 Mobile Audit [Home](#) [Findings](#) [Create](#) [Others](#)

[< BACK](#)

Description

Escuchar musica


Apk

[Seleccionar archivo](#) Tap Tool_1.4.4_APKPure.apk

App

Application #3 - Tap Tool

[UPLOAD](#)

 Mobile Audit [Home](#) [Findings](#) [Create](#) [Others](#)

[BACK](#) [REFRESH](#)

Scan

Description: Escuchar musica


Created by: Anthony04

Status: Finding vulnerabilities

40%

[DELETE](#) [EXPORT](#)

Application info

Icon	
App name	TapTool
Package	com.onethousandmoons.taptool
Version name	1.4.4
Version code	10404
Min version	21
Max version	None

localhost:8888/scan/2

Mobile Audit Home Findings Create Others

BACK REFRESH

Scan

Description: Escuchar musica

Created by: Anthonycs04

Status: Finished

100 %

DELETE EXPORT

Application info

Icon	embedded
App name	TapTool
Package	com.onethousandmoons.taptool
Version name	1.4.4
Version code	10404
Min version	21
Max version	None
Tamrnet version	51

El reporte se podrá ver en APK2_report.pdf