

# INFORME DE ANÁLISIS ESTÁTICO

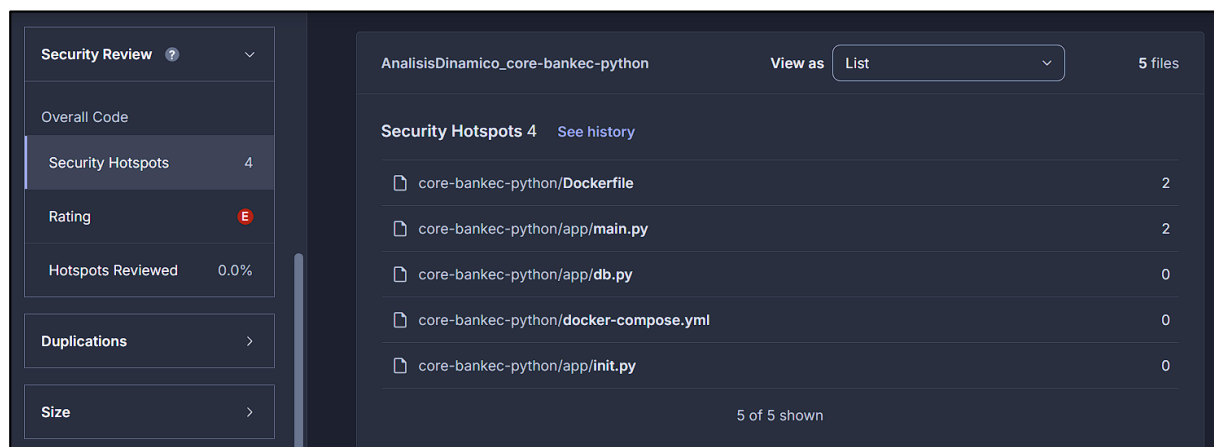
## Grupo 4

### *Elaborado por:*

- Miguel Guilca
- Mateo Dueñas
- Pamela Cruz
- Christopher Zambrano

### *Resumen ejecutivo:*

Para este caso se utilizó la herramienta SonarQube Cloud, la cual fue conectada a un repositorio con el código fuente del aplicativo, la misma encontró 4 puntos críticos de seguridad visibles en el siguiente gráfico.



La puntuación de severidad fue obtenida utilizando la calculadora “Common Vulnerability Scoring System Version 4.0 Calculator” ubicada en la página web de FIRST en el siguiente enlace: <https://www.first.org/cvss/calculator/4-0>.

Considerando las rubricas de puntuación que la misma página web facilita, visibles en el siguiente enlace: <https://www.first.org/cvss/v4-0/user-guide#Scoring-Rubrics>

Hallazgos:

Identificador	PCRIT-001: Desactivación del CSRF
Descripción	Un ataque de falsificación de solicitud entre sitios (CSRF) ocurre cuando un atacante puede obligar a un usuario confiable de una aplicación web a realizar acciones sensibles que no pretendía, como actualizar su perfil o enviar un mensaje, o más generalmente cualquier cosa que pueda cambiar el estado de la aplicación.
Severidad	<div>Common Vulnerability Scoring System Version 4.0 Calculator</div> <div>CVSS:4.0/AV:N/AC:L/AT:P/PR:N/UI:A/VC:H/VI:H/VA:N/SC:N/SI:N/SA:N</div> <div>CVSS v4.0 Score: 7.4 / High</div>
Referencias	<ul style="list-style-type: none"><li>CWE - <a href="#">CWE-352 - Cross-Site Request Forgery (CSRF)</a></li><li>OWASP - <a href="#">Cross-Site Request Forgery</a></li></ul>
Recomendación	<p>Ya que esta es una aplicación <b>Flask</b>, el módulo “<b>CSRFProtect</b>” debe ser utilizado y no deshabilitado con “<b>WTF_CSRF_ENABLED</b>” configurado en <i>false</i>, además de evitar deshabilitarlo en vistas o forms específicos.</p> <pre>app = Flask(__name__) csrf = CSRFProtect() csrf.init_app(app)  @app.route('/example/', methods=['POST']) # Compliant def example():     return 'example '  class unprotectedForm(FlaskForm):     class Meta:         csrf = True  name = TextField('name') submit = SubmitField('submit')</pre>

Evidencia:

0.0% Security Hotspots Reviewed

Cross-Site Request Forgery (CSRF)

1

Make sure disabling CSRF protection is safe here.

Review priority: Medium

Permission

1

Review priority: Low

Insecure Configuration

1

Others

1

4 of 4 shown

Make sure disabling CSRF protection is safe here.

Disabling CSRF protections is security-sensitive python:S4502

Status: To Review

This Security Hotspot needs to be reviewed to assess whether the code poses a risk.

Review

Where is the risk?

What's the risk?

Assess the risk

How can I fix it?

Activity

core-bankec-python/app/main.py

Show 26 more lines

27

'name': 'Authorization',

28

'description': 'Enter your token in the format \*\*Bearer <token>\*\*

29

}

30

}

31

32

app = Flask(\_\_name\_\_)

Identificador	PCRIT-002: Contenedor ejecutándose con usuario root por defecto
Descripción	<p>Ejecutar contenedores como un usuario con privilegios debilita su seguridad en tiempo de ejecución, lo que permite que cualquier usuario cuyo código se ejecute en el contenedor realice acciones administrativas.</p> <p>En los contenedores de Linux, el usuario con privilegios suele llamarse <i>root</i>. En los contenedores de Windows, el equivalente es <i>ContainerAdministrator</i>.</p>
Severidad	<p><b>Common Vulnerability Scoring System Version 4.0 Calculator</b></p> <p>CVSS:4.0/AV:N/AC:L/AT:N/PR:L/UI:P/VC:H/VI:H/VA:N/SC:L/SI:L/SA:L <span>Reset</span></p> <p>CVSS v4.0 Score: <b>8.5 / High</b> ⊕</p>
Referencias	<ul style="list-style-type: none"> <li>CWE - <a href="#">CWE-284 - Improper Access Control</a></li> <li><a href="#">nginxinc/nginx-unprivileged: Example of a non-root container by default</a></li> </ul>
Recomendación	<p>Crear un nuevo usuario predeterminado y usarlo con la instrucción USER. Algunos administradores de contenedores crean un usuario específico sin configurarlo explícitamente como predeterminado, como postgresql o zookeeper. Se recomienda usar estos usuarios en lugar de root.</p> <pre>FROM alpine  RUN addgroup -S nonroot \     &amp;&amp; adduser -S nonroot -G nonroot  USER nonroot  ENTRYPOINT ["id"]</pre>

### Evidencia:

0.0% Security Hotspots Reviewed

Make sure disabling CSRF protection is safe here.

Review priority: Medium

Permission

The "python" image runs with "root" as the default user. Make sure it is safe here.

Review priority: Low

Insecure Configuration

The "python" image runs with "root" as the default user. Make sure it is safe here.

Running containers as a privileged user is security-sensitive [docker:S6471](#)

Status: To Review

This Security Hotspot needs to be reviewed to assess whether the code poses a risk.

Review

Where is the risk? What's the risk? Assess the risk How can I fix it? Activity

core-bankec-python/Dockerfile

```
1 # Usar imagen base de Python 3.10-slim
2 FROM python:3.10-slim
```

The "python" image runs with "root" as the default user. Make sure it is safe here.

Review priority: Medium

Category: Permission

Assignee: Not assigned

Identificador	PCBIT-003: Modo de depuración activado
Descripción	Las herramientas y los frameworks de desarrollo suelen incluir opciones para facilitar la depuración a los desarrolladores. Si bien estas funciones son útiles durante el desarrollo, nunca deben habilitarse para aplicaciones implementadas en producción. Las instrucciones de depuración o los mensajes de error pueden filtrar información detallada sobre el sistema, como la ruta de la aplicación o los nombres de archivo.
Severidad	<b>Common Vulnerability Scoring System Version 4.0 Calculator</b> <div>CVSS:4.0/AV:N/AC:L/AT:P/PR:L/UI:N/VC:L/VI:L/VA:L/SC:L/SI:L/SA:L <span>Reset</span></div> CVSS v4.0 Score: <b>2.3 / Low</b> ⊕
Referencias	<ul style="list-style-type: none"> <li>CWE - <a href="#">CWE-489 - Active Debug Code</a></li> <li>CWE - <a href="#">CWE-215 - Information Exposure Through Debug Information</a></li> </ul>
Recomendación	No activar las funciones de depuración en servidores de producción o aplicaciones distribuidas a usuarios finales.  <pre>from flask import Flask  app = Flask() app.debug = False app.run(debug=False)</pre>

### Evidencia:

0.0% Security Hotspots Reviewed ?

Permission 1

The "python" image runs with "root" as the default user. Make sure it is safe here.

Review priority: Low

Insecure Configuration 1

Make sure this debug feature is deactivated before delivering the code in production.

Others 1

Make sure automatically installing recommended packages is safe here.

4 of 4 shown

Make sure this debug feature is deactivated before delivering the code in production.

Delivering code in production with debug features activated is security-sensitive [python:S4507](#)

Status: To Review

This Security Hotspot needs to be reviewed to assess whether the code poses a risk.

Review

Where is the risk?

What's the risk?

Assess the risk

How can I fix it?

Activity

core-bankek-python/app/main.py

Show 391 more lines

```

392 @app.before_first_request
393 def initialize_db():
394     init_db()
395
396 if __name__ == "__main__":
397     app.run(host="0.0.0.0", port=8000, debug=True)
```

Make sure this debug feature is deactivated before delivering the code in production

Review priority: Low

Category: Insecure Configuration

Assignee: Not assigned

Identificador	PCRIT-004: Instalación automática de paquetes no estrictamente requeridos
Descripción	<p>Instalar automáticamente los paquetes recomendados puede generar vulnerabilidades en la imagen de Docker, ya que, los paquetes potencialmente innecesarios se instalan mediante un gestor de paquetes Debian conocido. Estos paquetes aumentan la superficie de ataque del contenedor creado, ya que podrían contener vulnerabilidades no identificadas o código malicioso. En general, cuantos más paquetes se instalan en un contenedor, más débil es su seguridad. Dependiendo de las vulnerabilidades introducidas, un atacante que acceda a dicho contenedor podría utilizarlas para escalar privilegios. Eliminar los paquetes no utilizados también puede reducir significativamente el tamaño de la imagen de Docker.</p>
Severidad	<p><b>Common Vulnerability Scoring System Version 4.0 Calculator</b></p> <p>CVSS:4.0/AV:N/AC:H/AT:P/PR:H/UI:N/VC:N/VI:N/VA:N/SC:L/SI:L/SA:L <span>Reset</span></p> <p>CVSS v4.0 Score: <b>2.1 / Low</b> ⊕</p>
Referencias	<ul style="list-style-type: none"> <li>• <a href="#">Debian Documentation</a> - Binary Dependencies</li> <li>• <a href="#">Ubuntu Blog</a> - Container size reduction</li> </ul>
Recomendación	<p>Evitar la instalación de paquetes de dependencias no estrictamente requeridos.</p> <pre>FROM ubuntu:22.04  RUN apt --no-install-recommends install -y build-essential  RUN apt-get --no-install-recommends install -y build-essential  RUN aptitude --without-recommends install -y build-essential</pre>

### Evidencia:

0.0% Security Hotspots Reviewed ?

Permission 1

The "python" image runs with "root" as the default user. Make sure it is safe here.

Review priority: Low

Insecure Configuration 1

Make sure this debug feature is deactivated before delivering the code in production.

Others 1

Make sure automatically installing recommended packages is safe here.

Make sure automatically installing recommended packages is safe here.

Automatically installing recommended packages is security-sensitive `docker:S6500`

Status: To Review

This Security Hotspot needs to be reviewed to assess whether the code poses a risk.

Review

Where is the risk?

What's the risk?

Assess the risk

How can I fix it?

Activity

core-bankec-python/Dockerfile

Show 2 more lines

# Establecer el directorio de trabajo

WORKDIR /app

# Instalar dependencias del sistema (gcc, libpq-dev para compilar psycopg2)

RUN apt-get update && apt-get install -y gcc libpq-dev && rm -rf /var/lib/apt/lists/\*

Make sure automatically installing recommended packages is safe

Review priority: Low

Category: Others

Assignee: Not assigned