

Universidad del Valle de Guatemala
Facultad de ingeniería



Proyecto Análisis Sonarcloud

Cayetano Molina 20211
Estefanía Elvira 20725
Priscilla Gonzalez 20689

Guatemala 22 de mayo del 20224

Resultados del análisis

Lines of Code Bugs Vulnerabilities Code Smells Security Hotspots Coverage Duplications							
sonarcloud-analysis							
main.py	49	0	0	0	0	0.0%	0.0%

Imagen no.1: Resultados del código sin ninguna vulnerabilidad

Lines of Code Bugs Vulnerabilities Code Smells Security Hotspots Coverage Duplications							
sonarcloud-analysis							
main.py	34	0	0	1	2	0.0%	0.0%

Imagen no. 2: Resultados con Code Smells y Security Hostpots

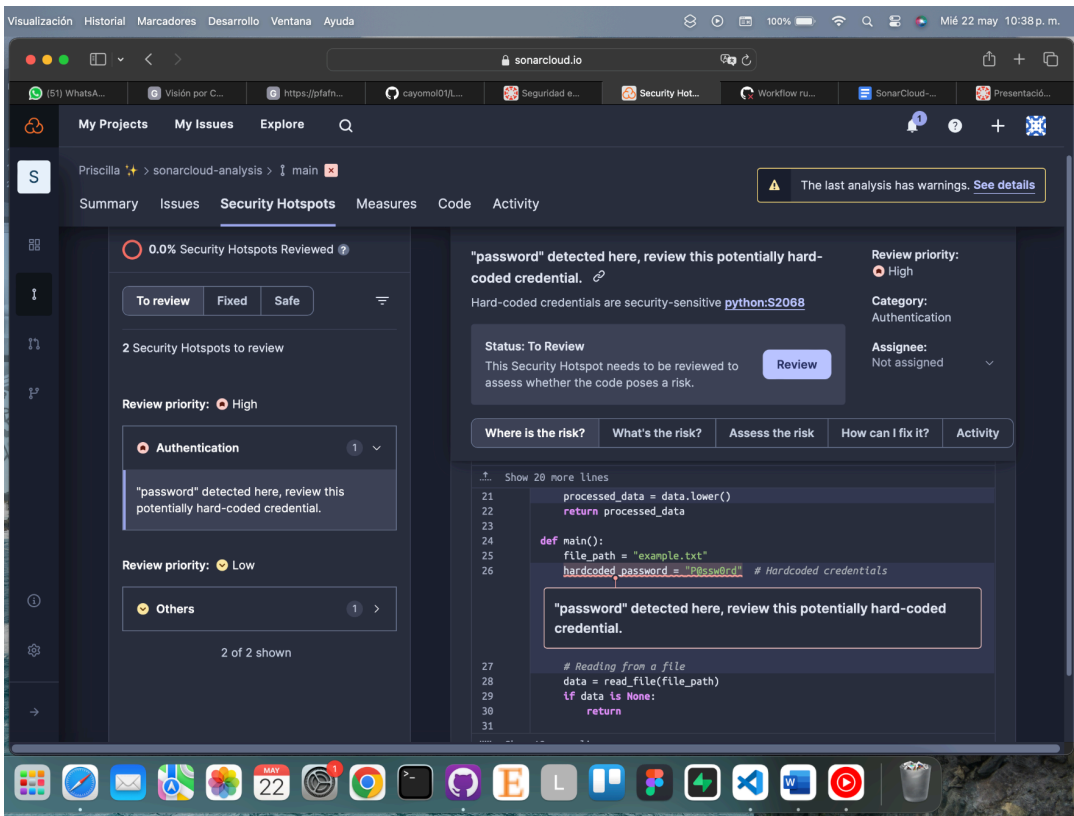


Imagen no. 3: Main branch

Some checks were not successful

1 successful and 1 failing checks

✖

 **SonarCloud Code Analysis**

Failing after 14s - Quality Gate failed

Details

✔

 **SonarCloud / sonarcloud (push)**

Successful in 28s

Details

Imagen no. 4: Referencia desde Github

Main Branch Status

✖

Quality Gate

Some Quality Gate conditions on New Code were ignored because of the small number of New Lines

Failed

1 failed condition

○

0.0% Security Hotspots Reviewed on ...

100% required

[See Full Analysis](#)

Main Branch Evolution since 2 hours ago

1 Issues  1

Issues

Coverage

Duplications

0 Issues



Issues

New Code

[See full history](#)

Imagen no. 5: Overview

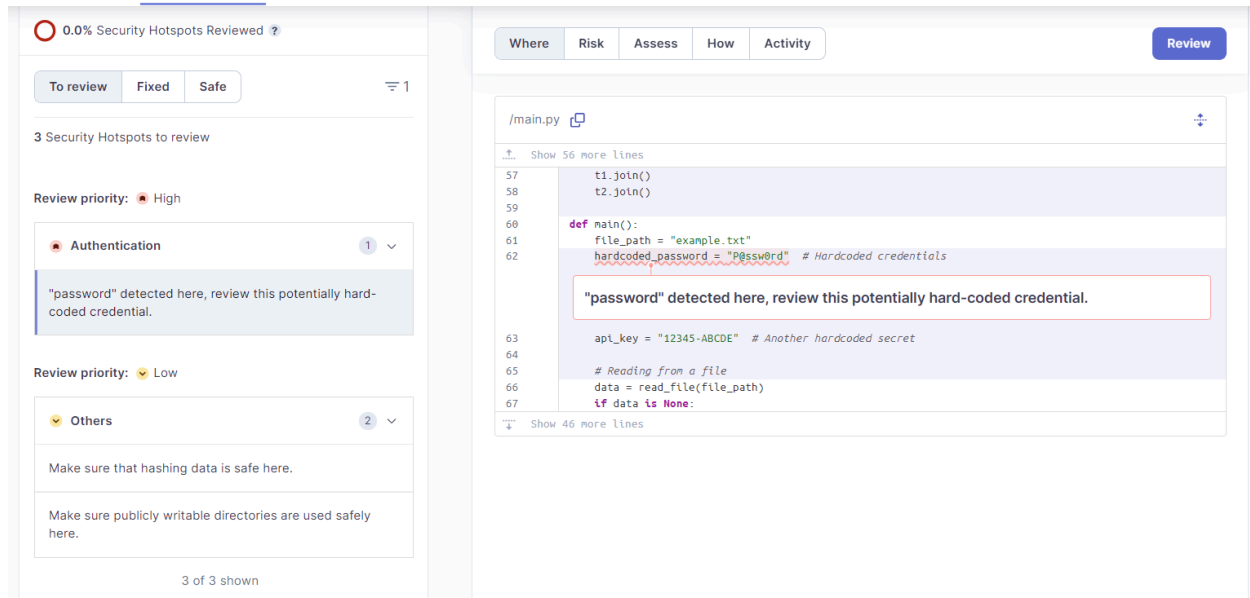


Imagen no. 6: Problemas en el código

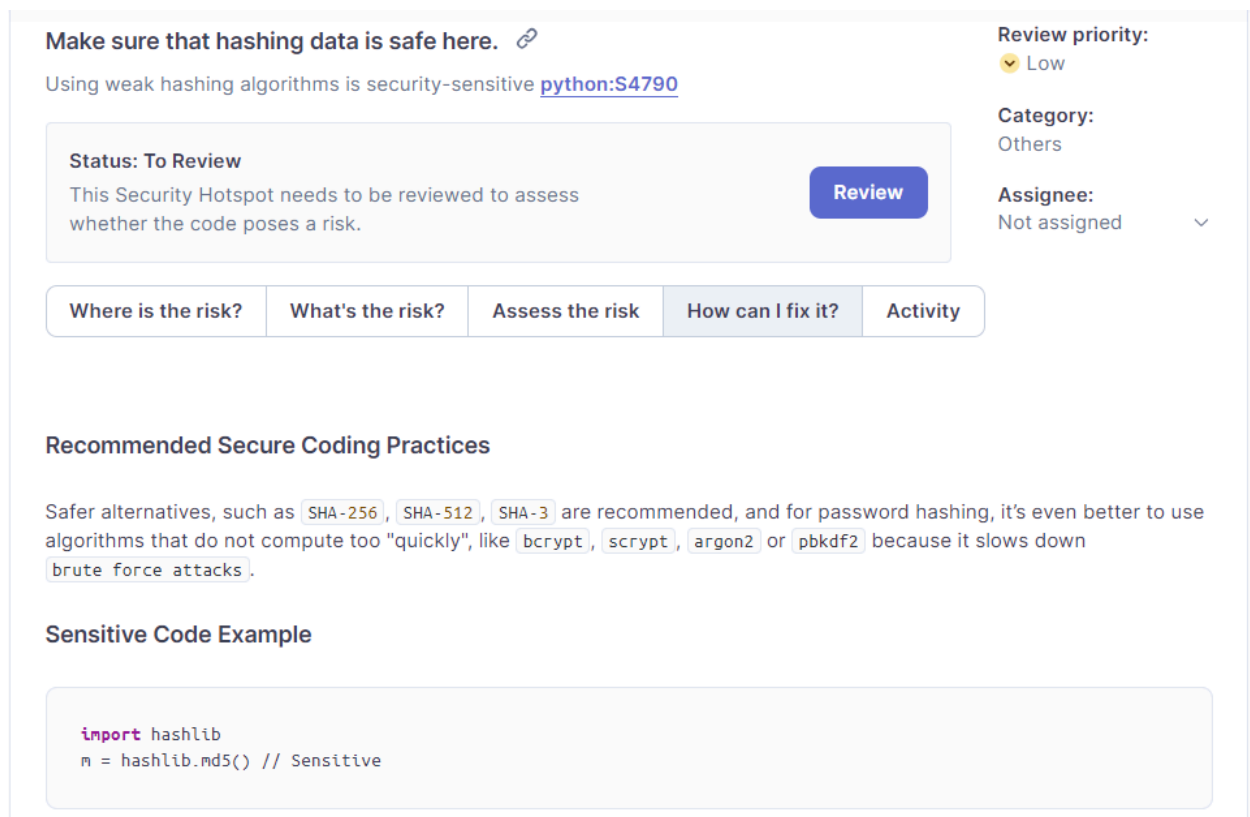


Imagen no. 7: Vulnerabilidades en el código (hashing)

Make sure publicly writable directories are used safely here. [🔗](#)

Using publicly writable directories is security-sensitive [python:S5443](#)

Status: To Review

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

Review

Review priority:

👇 Low

Category:

Others

Assignee:

Not assigned

Where is the risk?

What's the risk?

Assess the risk

How can I fix it?

Activity

```

86     security_vulnerability()
87     # Unrestricted eval usage
88     eval(user_input) # This is dangerous and should be avoided
89
90     # Writing to a potentially insecure temporary file
91     temp_file_path = "/tmp/tempfile.txt"
92
93     with open(temp_file_path, 'w') as temp_file:
94         temp_file.write("This is a temporary file.")
95         # Security risk demonstration
96

```

Make sure publicly writable directories are used safely here.

Imagen no. 8: Sensitive code Vulnerabilidad

20 workflow runs		Event	Status	Branch	Actor
✅	add function security_vulnerability	SonarCloud #20: Commit 8f0a54b pushed by Estef072	main	18 hours ago 🕒 50s	...
✅	api	SonarCloud #19: Commit c919928 pushed by Estef072	main	18 hours ago 🕒 56s	...
✅	ahora si api harcode	SonarCloud #18: Commit c6abd29 pushed by Estef072	main	18 hours ago 🕒 39s	...
✅	api harcode error	SonarCloud #17: Commit 0bbee14 pushed by Estef072	main	18 hours ago 🕒 37s	...
✅	Code update 2	SonarCloud #16: Commit d2d3ca7 pushed by cayomol01	main	19 hours ago 🕒 39s	...
✅	Code Update 1	SonarCloud #15: Commit 9349c3a pushed by cayomol01	main	19 hours ago 🕒 39s	...
✅ ❌	Add more errors	SonarCloud #14: Commit 156360e pushed by Priscigs	main	19 hours ago 🕒 36s	...
✅ 🔄	Another one	SonarCloud #13: Commit 00fec7 pushed by Priscigs	main	20 hours ago 🕒 39s	...
✅ 🔄	More Modifications	SonarCloud #12: Commit 8884fb6 pushed by Priscigs	main	20 hours ago 🕒 38s	...
✅ 🔄	Malicious	SonarCloud #11: Commit 75e98a7 pushed by Priscigs	main	yesterday 🕒 49s	...
✅ 🛑	Disable Automatic Analysis	SonarCloud #10: Commit f552cad pushed by Priscigs	main	yesterday 🕒 42s	...

Imagen no. 9: Workflow de Github

Discusión

Se marca un problema grave en el código el cual dice que es de autenticación. En este problema se está escribiendo una contraseña completamente dentro del código lo cual puede llevar a problemas más adelante. La solución sería utilizar variables de entorno o variables que no se suban al repositorio pues pueden quedar grabadas en algún lado. O bien, si se desea guardar una contraseña, se puede utilizar una función de hashing para solo tener que comprobar los caracteres y no tener que revelar las contraseñas en ningún momento.

Por otra parte, se observa que la condición del `if = _main_` está escrita de forma incorrecta. Para resolverlo, simplemente se debería de escribir así `if = __main__`. También, se encuentra el `eval()` que contiene la entrada de usuario que puede llegar a ser bastante peligroso al ejecutar código de forma no restringida. Para poder solucionar esta parte del código, lo más simple que se puede hacer es borrar esa línea del código, ya que no es necesaria en este código. O de igual forma, se podría reemplazar con otro código dependiendo las necesidades que se tengan

Otras de las vulnerabilidades o riesgos que se pueden observar es que se está escribiendo código en un directorio temporal ya que los permisos pueden llegar a afectar. Para solucionar esto, se podría hacer la escritura de código en otro directorio o aplicar restricciones de acceso adecuadas.

Por último, existen en el código variables que se definen, pero nunca se usan. Entonces lo ideal podría ser que se comenten o simplemente se borren las variables que no están siendo utilizadas.