Analyse de Projet

sonarqube

Date de création : 13/12/2022 Date de modification : 09/01/2023

Sommaire

Présentation de la solution		
Création du Projet		4
Installation du Scanner de SonarQube		8
Téléchargement du Scanner		8
Ajout de la Variable d'environnement		8
Exécution du scanner sur le projet	<u> </u>	
Affichage des informations du projet		
Exemple d'affiche d'information		
Bugs		
Vulnérabilités		
Points Sensibles	\	

PRESENTATION DE LA SOLUTION

SonarQube est un logiciel libre permettant d'aider à la détection, la classification et la réslution de défaut dans le code source d'un projet afin d'obtenir du code propre. Il est applicable sur des projets contenant du Java, C, C++, C#, PHP, Python et encore bien d'autres langages. Ces principales fonctionnalités sont :

- Identifier la duplication de code
- Mesurer le niveau de documentation
- Respecter les règles de programmation
- Détection de vulnérabilités, bugs

SonarQube est aussi extensible grâce à des plugins permettant d'ajouter des règles de programation à l'analyse du projet, ou de supporter un nouveau langage non supporté par le logiciel.

CREATION DU PROJET

Connectez-vous au SonarQube à partir c	le cette IP : 172.20.34.23	6
Vous arriverez sur la page de connexion	:	v - 6 x
← → C ▲ Non sécurisé 1722034236/session	s/new?return_to=%2F	* 整论☆ \$ == □ ● :
	Log In to SonarOute	
	Log in to SonarQube	
	Login	
	Password	
	Log in Cancel	
Entrez ces identifiants : - Login : admin - Password : adminadmin Puis cliquez sur Log in :		
	Log In to SonarQube	
	admin	
	••••••	
	Log in Cancel	

Vous arriverez sur la page d'affichage des projets. Pour créer un projet cliquez sur Create project, puis cliquez sur More.

Si aucune projet n'a été créé auparavant, passez à l'explication suivante

sonarqube Proje	ects Issues Rules	Quality Profiles Quality Gates Administration	Q Search for projects A
My Favori	ites All	Q Search by project name or key	Create Project ~
Filters		1 project(s)	Perspective: Overall Status 👻 Sort by: 1 🗘 Manually
			··· More
Quality Gate		☆ Group2Web Passed	Last analysis: 23 days ano
Passed	1		
Failed	0		
Reliability (🏦 Bugs)		The bugs to vulnerabilities V Hotspots Reviewed	Coverage Dupications Lines
A rating	0		0.0% 14.0% 403 x3 Phr, 033,
B rating	0		
C rating	1		1 of 1 shown
D rating	0		
E rating	0		
Security (🔒 Vulnerabi	ilities)		
A rating	0		
B rating	0		
C rating	0		
D rating	0		
E rating	1		
Security Review (🕲	Security Hotspots)		
A ≥ 80%	0		
B 70% - 80%	0		
50% - 70%	0		
30% - 50%	0		
(30%)	1		
Maintainability (🐼 C	ode Smells)		
A rating	1		
B rating	0	SonarQube™ te Community Edition - Version 9.7.1 (build 62	ecnology is powered by SonarSource SA 2043) - LGPL v3 - Community - Documentation - Plugins - Web API

Ce qui vous affichera cette page, puis Cliquez sur Manally

$\leftarrow \rightarrow \mathbf{C}$ A Non sécuri	sé 172.20.34.236/projects/crea	ate			\$ € ☆	≱ ≕	🔲 🌒 i
sonarqube Projects Iss	sues Rules Quality Profiles	a Quality Gates Administra	ation	0 Q	Search for projects		А
How do you want to create	your project?						
Do you want to benefit from all of First, you need to set up a DevO	f SonarQube's features (like reposi ps platform configuration.	itory import and Pull Request deco	oration)? Create your project from	a your favorite DevOps platform.			
4		0	₩				
From Azure DevOps	From Bitbucket	From GitHub	From GitLab				
Set up global configuration	Set up global configuration	Set up global configuration	Set up global configuration				
Are you just testing or have an a	dvanced use-case? Create a proje	ct manually.					
0							
Manually							

Donnez un nom à votre projet, puis cliquez sur Set Up :

Create a project
All fields marked with * are required Project display name * Group2Web v Up to 255 characters. Some scanners might override the value you
provide. Project key * Group2Web The project key is a unique identifier for your project. It may contain up to 400 characters. Allowed characters are alphanumeric, '-' (dash), '' (underscore), '.' (period) and '.' (colon), with at least one non-digit.
Set Up

quez sur Locally :				
	لب ليب Locally			
sur Generate :				
Provide a token Generate a project token				
Token name @	Expires in			
Analyze "Group2Web" 1	30 days 💌	Generate]	
 Please note that this toker to use the same token to a in your <u>user account</u>. See 	n will only allow you to analyze multiple proje the <u>documentation</u> fo	o analyze th cts, you nee or more infor	e current project. If you want ed to generate a global token mation.	
 Use existing token 				
The token is used to identify you when revoke it at any point in time in your u	n an analysis is perforn ser account.	ned. If it has	been compromised, you can	
sur Continuer :				
Provide a token				
Analyze "Group2Web": sqp_26469	b8714061a2d844cb2	79657a2c6f	63287843 🍵	
The token is used to identify you when revoke it at any point in time in your us	an analysis is performe er account.	ed. If it has be	een compromised, you can	
Continue				
	quez sur Locally : sur Generate : Provide a token Generate a project token Token name O Analyze "Group2Web" 1 Please note that this toker to use the same token to a in your user account. See Use existing token The token is used to identify you when revoke it at any point in time in your user sur Continuer : Provide a token Analyze "Group2Web": sqp_26469 The token is used to identify you when revoke it at any point in time in your user Continue	quez sur Locally : Image: sur Generate : Image: sur Continuer :	quez sur Locally : Locally Locally Esur Generate : Provide a token	quez sur Locally : Locally Locally Locally Locally Locally Locally Locally Issur Generate : Provide a token Senerate a project token Token name Expires in Analyze "Group2Web" 1 30 days Generate Please note that this token will only allow you to analyze the current project. If you want to use the same token to analyze multiple projects, you need to generate a global token in your user account. See the documentation for more information. O Use existing token The token is used to identify you when an analysis is performed. If it has been compromised, you can revoke it at any point in time in your user account. Forvide a token Analyze "Group2Web": sgp_26469b8714061a2d844cb279657a2c6f63287843 The token is used to identify you when an analysis is performed. If it has been compromised, you can revoke it at any point in time in your user account.

Vous pouvez choisir la forme de construction de votre projet. Cliquez sur Other :

2	Run ana	alysis on	your p	roject			
	What option best describes your build?						
	Maven	Gradle	.NET	Other (for JS, TS, Go, Python, PHP,)			
			λ.				

Vous pouvez choisir l'OS présent sur votre ordinateur. Cliquez sur Windows



La commande étant générée, votre analyse est désormais prête à être lancé.



INSTALLATION DU SCANNER DE SONARQUBE

Téléchargement du Scanner

Cliquez sur le lien vers la documentation du Scanner : Download and unzip the Scanner for Windows

Visit the 🗷 official documentation of the Scanner to (

Cliquez sur Windows 64-bit pour télécharger le zip

4.7		Show more versions
2022-02-22		
Ease import of custom certific	cates with the Docker imag	ge, update embedded JRE 11

ézippez le dossier :				
e PC > Disque local (C:) > AnalyseSonarQube			ٽ ~	
Nom	Modifié le	Туре	Taille	
sonar-scanner-cli-4.7.0.2747-windows.zip	13/12/2022 13:51	Dossier compressé	42 253 Ko	

Ajout de la Variable d'environnement

Dans ce dossier précédemment extrait, ouvrez le dossier bin :

sona	ar-scanner-cli-4.7.0.2747-windows > sonar-scan	ner-4.7.0.2747-windows >	bin	~	õ	$ \mathcal{P} $ Rechercher dans : bin
^	Nom	Modifié le	Туре	Taille		
	sonar-scanner.bat	22/02/2022 07:18	Fichier de comma		3 Ko	
	log sonar-scanner-debug.bat	22/02/2022 07:18	Fichier de comma		1 Ko	

Copiez le chemin d'accès du dossier bin :

A A	No.	Ma 100 4 1 -	Turne	T-10-
¥	Nom	iviodifie le	iype	laille
۰.	💿 sonar-scanner.bat	22/02/2022 07:18	Fichier de comma	
e i i	sonar-scanner-debug.bat	22/02/2022 07:18	Fichier de comma	

Appuyez sur la touche Windows de votre clavier et tapez : variable Ouvrez le panneau de configuration ci-dessous :

Modifier les va d'environneme Panneau de confi	r iables nt système guration			
Paramètres Modifier les varia d'environnement	bles >	Modifie	er les variables d'environ système Panneau de configuration	nement
Cliquez sur Variable d'enviro	nnement :			
	Nom de l'ordinateur Paramètres système avancés	Protection du système	Matériel Utilisation à distance	
	Vous devez ouvrir une session ces modifications. Performances Effets visuels, planification du mémoire virtuelle	d'administrateur pour effe processeur, utilisation de	ctuer la plupart de la mémoire et <u>Paramètres</u>	
	Profil des utilisateurs Paramètres du Bureau liés à v	otre connexion	P <u>a</u> ramètres	
	Démarrage et récupération Informations de démarrage du débogage	système, de défaillance (du système et de Para <u>m</u> ètres	
		<u>V</u> ariables d'	environnement	

Double cliquez sur la variable Path :

Variable	Valeur	^
ComSpec	C:\Windows\system32\cmd.exe	
DriverData	C:\Windows\System32\Drivers\DriverData	
JAVA_HOME	C:\Program Files\Java\jdk-18.0.1.1	
NUMBER_OF_PROCESSORS	12	
OS	Windows_NT	
Path	C:\Program Files\Common Files\Oracle\Java\javapath;C:\Windows	
PATHEXT	.COM:.EXE:.BAT:.CMD:.VBS:.VBE:.JS:.JSE:.WSF:.WSH:.MSC	~

Cliquez sur Nouveau, puis collez le chemin d'accès enregistré.

Puis cliquez sur Ok et fermez les panneaux de configurations ouvert :

Nouvelle variable système		×
Nom de la variable :	sonar-scanner	
Valeur de la variable :	C:\Users\MartinC\Desktop\sonar-scanner-4.7.0.2747-windows\bin	
Parcourir le répertoire	Parcourir le fichier OK Annuler	



Exécution du scanner sur le projet

Ajoutez le dossier de votre projet dans le fichier bin :

Dis	que local (C:) > AnalyseSonarQube > s	onar-scanner-4.7.0.2747-window	s > bin >	∨ טֿ ,
^	Nom	Modifié le	Туре	Taille
Ŀ.	Groupe3web	13/12/2022 16:21	Dossier de fichiers	
	💿 sonar-scanner.bat	22/02/2022 07:18	Fichier de comma	3 Ko
	💿 sonar-scanner-debug.bat	22/02/2022 07:18	Fichier de comma	1 Ko

Ouvrez une Invite de commandes et allez dans votre fichier via la commande cd :

Invite de commandes	- 🗆 ×
icrosoft Windows [version 10.0.19044.1889] c) Microsoft Corporation. Tous droits réservés.	
:\Users\MartinC>cd C:\AnalyseSonarQube\sonar-scanner-4.7.0.2747-windows\bin_	
De retour sur le site de SonarQube, copiez la commande :	
sonar-scanner.bat -D"sonar.projectKey=Group2Web" -D"sonar.sources=." -D"sonar.host.url=http://172.20.34.236" -D"sonar.login=sqp_26469b8714061a2c	d844cb279657a2c6f6. ▶ Copy
Invite de commande, collez la commande puis executez la :	- 🗆 X
icrosoft Windows [version 10.0.19044.1889] c) Microsoft Corporation. Tous droits réservés.	
:\Users\MartinC>cd C:\AnalyseSonarQube\sonar-scanner-4.7.0.2747-windows\bin	
:\AnalyseSonarQube\sonar-scanner-4.7.0.2747-windows\bin≻sonar-scanner.bat -D"sonar.projectKey=Group2 s=." -D"sonar.host.url=http://172.20.34.236" -D"sonar.login=sqp_26469b8714061a2d844cb279657a2c6f6328	Web" -D"sonar.sourc 7843"

Dès que la commande a finis de s'exécuter, retourner sur le site de SonarQube. Votre page s'est actualisé.

AFFICHAGE DES INFORMATIONS DU PROJET

L'analyse du projet étant terminé, vous pouvez maintenant voir quels sont les problèmes afin de rendre votre projet propre.

SonarQube est capable de vous afficher :

- Bugs : problèmes critiques ou non visant à rendre le code plus propre
- Vulnérabilités : point à corriger où la sécurité est nécessaire (connexion base de données...)
- Security Hotspots : Erreur lié à une connexion web ou des méthodes de hachage connue

🗇 Group2Web 🏠 🦻 master 💿		Last analysis of this Branch had <u>2 warnings</u>	December 13, 2022 at 4:31 PM Version not provided 🏠
Overview Issues Security Hotspots Measures	Code Activity		Project Settings - Improject Information
To benefit from more of SonarQube's features, s	et up analysis in your favorite CI.		×
QUALITY GATE STATUS @	MEASURES		
Passed	New Code Overall Code		
All conditions passed.	41 A Bugs		Reliability 🧿
	1 & Vulnerabilities		Security 🜔
	5 Security Hotspots @	0.0% Reviewed	Security Review E
	1d Debt	231 & Code Smells	Maintainability 🔥
	O.0% Coverage on <u>300</u> Lines to cover	- () 12 Unit Tests	L.6% 6 Cations on 463 Lines Duplicated Blocks
	ACTIVITY		

La vérification des bugs et problèmes de sécurité est sous forme de pastille colorée contenant une lettre. Celle-ci vont du vert au rouge. Celle-ci indique le niveau critique de sécurité dans l'ordre croissant, donc du moins dangereux au plus dangereux.

EXEMPLE D'AFFICHE D'INFORMATION

Bugs

Cliquez sur le nombre pour afficher les bugs présents dans votre code afin de voir leur degré de dangerosité

<u>41</u> *	é Bugs		Reliability	С	

Vous obtenez ainsi la liste des bugs présent dans votre code. Cliquez sur l'une des erreurs pour afficher ces informations

Groupe3web/BackOffice/ActionsBO/AjouterBO.php	
Replace "include" with "include_once". ∯ Bug ▼ 🤨 Minor ▼ 🔾 Open ▼ Not assigned ▼ 5min effort Comment	7 minutes ago ▾ L61 � ♥▼ ♥ No tags ▼
Groupe3web/BackOffice/ActionsBO/ModifierBO.php	
Replace "include" with "include_once". ∯ Bug ▼ O Minor ▼ O Open ▼ Not assigned ▼ 5min effort Comment	7 minutes ago ▾ L6 � ▼▼ ♥ No tags ▼
Replace "include" with "include_once". ∯ Bug ▼ O Minor ▼ O Open ▼ Not assigned ▼ 5min effort Comment	7 minutes ago ▾ L47 � ▼▼ ♥ No tags ▼
Replace "include" with "include_once". ∯ Bug ▼ O Minor ▼ O Open ▼ Not assigned ▼ 5min effort Comment	7 minutes ago → L81 % ▼• % No tags →
Groupe3web/BackOffice/ActionsBO/ajouter.php	
Replace "require" with "require_once". ∯ Bug ▼ O Minor ▼ O Open ▼ Not assigned ▼ 5min effort Comment	7 minutes ago マ L10 % ▼マ No tags マ
Replace "require" with "require_once". ∯ Bug ▼ 🧿 Minor ▼ 🔘 Open ▼ Not assigned ▼ 5min effort Comment	7 minutes ago ← L37 % ▼. No tags ←
Replace "require" with "require_once". ∯ Bug ▼	7 minutes ago ▼ L61 % ▼▼

Vous obtenez ainsi le fichier dans lequel le bug est présent ainsi la ligne à laquelle elle se trouve.

Replace	"include"	with "include_once".		Get permalink %
'require_ond	ce" and "includ	le_once" should be used instea	d of "require" and "include" php:S2003	11 minutes ago 👻 L61
🙀 Bug 🗸	🕚 Minor 👻	O Open ▼ Not assigned ▼	5min effort 0 comments	🗞 No tags 🛩
Where is	s the issue?	Why is this an issue?		
🛱 Grou	up2Web 🗎 (Groupe3web/BackOffice/Acti	onsBO/AjouterBO.php	See all issues in this file 🕴
÷				
56		<div></div>		
57		<label>Catégorie<</label>	/label>	
58		<select></select>		
59		php</td <td></td> <td></td>		
60				
61		include "//sq	Lconnect.php";	
	j∰n Rep	lace "include" with "includ	e_once".	
62		<pre>\$sql= \$connection</pre>	->prepare("SELECT * FROM categorie") ;	
63		<pre>\$sql->execute();</pre>		
64		\$ligne = \$sql->fe	tchall();	
65				
66				
67		<pre>foreach(\$ligne as</pre>	<pre>\$categorie){</pre>	
68		echo " <option< td=""><td>name=\"categorieEchauff\" value=".\$categor</td><td>ie['id'].">".\$categorie['nom']."";</td></option<>	name=\"categorieEchauff\" value=".\$categor	ie['id'].">".\$categorie['nom']."";
69		}		
70		?>		

Date de création : 13/12/2022 Date de modification : 09/01/2023

Vulnérabilités

Cliquez sur le nombre pour afficher les problèmes de vulnérabilités présent dans votre code

1	6 Vulnerabilities	Security	E

Vous obtenez la liste des alertes de vulnérabilités qui devra être corriger. Cliquez sur l'une des erreurs pour afficher ces informations

Add p	aassword protection to this database. Inerability 🕶 🚯 Blocker 💌 🔿 Open 🖛 Not assigned 🖛 45min effort Comment	1 day ago ▼ L18 % ▼▼ S cwe, owasp-a2, owasp-a3 ▼
	1 of 1 shown	
	; · · · · · · · · · · · · · · · · · · ·	
- no	uvez ainsi savoir quelle est la vulnérabilité et comm	ent la corriger
, po		
pass	sword protection to this database.	Get permalink %
ire pas	ssword should be used when connecting to a database php:S2115	1 day ago 👻 L18
Inerab	nility • 0 Blocker • O Open • Not assigned • 45min effort 0 comments	CWP DWasp-a2 Dwasp-a3
morub		
noro is	the issue? Why is this an issue?	
lere is		
Grou	up2Web 🗎 Groupe3web/sqlconnect.php	See all issues in this file 🛛 👙
3		
4	try{	
5	<pre>\$dns = 'mysql:host=localhost;dbname=workout';</pre>	
6	<pre>\$utilisateur = 'root';</pre>	
7	<pre>\$motDePasse = '';</pre>	
8	<pre>\$connection = new PDO(\$dns, \$utilisateur, \$motDePasse);</pre>	
	Add password protection to this database.	
9	<pre>\$connection->auery("SET NAMES utf8");</pre>	
8		
1	<pre>} catch (Exception \$e) {</pre>	
2	<pre>echo "Connection à MySQL impossible : ", \$e->getMessage();</pre>	
3	<pre>die();</pre>	
4		
5	}	
6		

Points Sensibles

Cliquez sur le nombre pour afficher la liste et la recommandation à suivre pour corriger ces points sensibles

5 Security Hotspots @	O 0.0% Reviewed Securi	ty Review E
s obtenez ainsi la liste	e des erreurs de sécurité à corriger	
5 Security Hotspots to review	Make sure this weak hash algorithm is not used in a sensitive context here.	
view priority: LOW	Status: TO REVIEW This security hotspot needs to be reviewed to assess	no: Not assigned
hers 5 A	whether the code poses a risk.	ee. Not assigned 🥜
Make sure not using resource integrity eature is safe here.	Where is the risk? What's the risk? Assess the risk How can I fix it?	
Groupe3web/Detail_activite.php		
ake sure this weak hash algorithm is ot used in a sensitive context here.	Groupe3web/connexionCompte.php	Get Permalink %
Groupe3web/connexionCompte.php	1 <7php 2	
ike sure this weak hash algorithm is t used in a sensitive context here.	<pre>3 try(4 session_start(); 5 require "sqlconnect.php";</pre>	
Groupe3web/connexionCompte.php	<pre>6 \$psw=SHA1(\$_REQUEST['password']);</pre>	
ake sure this weak hash algorithm is t used in a sensitive context here.	Make sure this weak hash algorithm is not used in a sensitive context here.	Comment
Groupe3web/connexionCompte.php	<pre>\$\$sql= \$connection->prepare("SELECT mail,HDP FROM employer WHERE mail = :mail AND MDP = :HDP");</pre>	
ake sure this weak hash algorithm is ot used in a sensitive context here.	9 10 \$sql->bindParam(':mail', \$_REQUEST["mail"], PDO::PARAM_STR); 11 \$sql->bindParam(':MDP', \$psw, PDO::PARAM_STR);	
Groupe3web/inscriptionCompte.php	12 13 \$sql->execute();	
5 of 5 shown	<pre>14 Sligne = ssql->fetchall(); 15 16 if(!empty(Sligne))</pre>	