Static Code Analysis Exercise

For this exercise, you will run SonarQube to analyze your Java project code and SonarScanner to analyze your TypeScript code. There is a deliverable due by end of class and another for Sprint 4.

With the generated reports, you will put together a plan to address issues that were flagged in your Java or TypeScript code.

Note: Make SonarQube is **running**, which you should have verified in the setup document.

Analyzing code with SonarQube

We will use SonarQube to analyze our Java code

1. Go to your project directory where you would run maven to build and test your code and enter the following placeholder incomplete command but **don't run it yet**:

mvn clean test sonar:sonar -D sonar.token=

Should look something like this:



NOTE: in some literature you may see the DEPRECATED **DO NOT USE:**

mvn clean test sonar:sonar -D sonar.login=admin -D sonar.password=admin password

2. Instead you have to first MAKE a token by going to <u>http://localhost:9000</u>

ded database should be	e used for evaluation p	purposes only. It doesn't support scaling, upgrading to a new SonarQube Server version, or migration to another database engine. Learn more 🛽	Administrat
	â		My Account
My Favorites All			Crea Log out
ing ronoidos - rin		Q Search for projects Perspective Overall Status ~ Sort by Name ~ Et	2 project(s)
ilters			
uality Gate		☆ ufund-api public	✓ Passed
✓ Passed	2	Last analysis: 24 hours ago - 1.1k Lines of Code - Java, XML	
× Failed	0 1	A 0 B 1 A 135 A - () 99.5% · 1.8%	
ecurity		Security Reliability Maintainability Hotspots Reviewed Coverage Duplications	
A ≥ 0 info issues	2		
B ≥ 1 low issue	0 =	☆ Ufund-UI PUBLIC	✓ Passed
C ≥ 1 medium issue	0	Last analysis: 24 hours ago - 1.5k Lines of Code - TypeScript, CSS,	
D ≥ 1 high issue	0 =		
E ≥ 1 blocker issue	0	A 0 C 6 A 44 A - 0 0.0% 0.0%	
eliability		evenity minimum minimum receptor referred everyge september	
A ≥ 0 info issues	0	2 of 2 shown	
B ≥ 1 low issue	1		
C ≥ 1 medium issue	1		
D ≥ 1 high issue	0 =		
E > 1 blocker issue	0		

- 3. Click on the little **A** in the top right, and click the "My Account option"
- 4. That should bring you to this page:

Community Projects Issues Rules Quality Profiles Quality Gates Administration More ~	Q 🖉 🛕
Learn m	Iore 2
A Administrator Profile Security Notifications Projects	
Profile	
Login: admin	
Groups sonar-administrators sonar-users	
SCM Accounts 7 admin	
Preferences Enable Keyboard Shortcuts Some actions can be performed using keyboard shortcuts. If you do not want to use these shortcuts, you can disable them here (this wort disable navigation shortcuts, which include the arrows, escape, and enter keys). For a list of available keyboard shortcuts, use the question mark shortcut (hit 2 on your keyboard).	

5. Click on the "Security" tab. **NOTE**: there probably won't be any token initially

Security f you want to enforce se vill increase the security	curity by not providing crede of your installation by not le	entials of a real Sonar tting your analysis us	Qube user to run your code er's password going throug	scan or to invoke web services h your network.	, you can provide a User Tol	ken as a replacement of the	user login. This
Generate Tokens							
lame	Туре	Expires in					
Enter Token Name	Select Token Type	30 days 🗸 G	enerate				
Name		Туре	Project	Last use	Created	Expiration	
Maven Project		Global		24 hours ago	March 26, 2025	April 24, 2025	Revoke
Ufund-UI-token		Project	Ufund-UI	24 hours ago	March 26, 2025	June 23, 2025	Revoke

6. Fill in the token parameters in the Generate Tokens section. Select "Global" type of token. Then click on "Generate" as shown below:

Generate Tokens			
Name	Туре	Expires in	
NAME OF TOKEN	Global Analysis Token	30 days 🗸	Generate

7. This should produce a new token as such:





11. Go back to <u>http://localhost:9000</u> and you should see your SonarQube report for project called Ufund-Api

☆ ufun Last analy	d-api PUBLIC	s ago - 1.1k Lines of	Code - Java, XML						✓ P	assed
A 0 Security	B 1 Reliability	A 135 Maintainability	A — Hotspots Reviewed	O 99.5% Coverage	• 1.8% Duplications					

12. It might take a while to analyze it the **first time**, **so be patient** if docker doesn't show you the project immediately

Running SonarScanner

Next, we will run SonarScanner to analyze our TypeScript code

- 1. In SonarQube, click the "Create Project" button in the upper right corner and select "Manually"
- 2. Enter a name for your project and click "Set Up"

sonarqube	Projects	Issues	Rules	Quality Profiles	Quality Gates
Create a	projec	t			
All fields marked	d with * are re	equired			
heroes-app				0	
Up to 255 charac	ters. Some so	canners mig	ght override	e the value you	
Project kov *					
heroes-app					
The project key is 400 characters. A (underscore), '.' (p	a unique ide llowed chara period) and ':'	ntifier for yo cters are al (colon), wi	our project phanumeri th at least (. It may contain up to c, '-' (dash), '_' one non-digit.	
Set Up					

13. Select "Locally"

i i iiiiiiiiiiiiiiiiiiiiiiiiiiiiiiiii

14. For **#1 Provide a Token**, Enter any name for your token and click "Generate"

0	Provide a token Generate a token
	test Generate
	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 of time in your user account.

- 15. Click "Continue"
- 16. For **#2 Run analysis on your project**, select Other (for JS, TS, Go, Python, PHP, ...)
- 17. Select your OS
- 18. You should see something similar to below:

What option best describes your build?
Maven Gradie .NET Other (for JS, TS, Go, Python, PHP,)
What is your OS?
Linux Windows macQS
Bernale and runnin the Decement for meetal
Download and unzip the Scanner for macOS
Visit the official documentation of the Scanner to download the latest version, and add the bin directory to the PATH environment variable
 Visit the official documentation of the Scanner to download the latest version, and add the bin directory to the PATH environment variable
 Visit the official documentation of the Scanner to download the latest version, and add the bin directory to the PATH environment variable Execute the Scanner
Visit the official documentation of the Scanner to download the latest version, and add the bin directory to the PATH environment variable Execute the Scanner Running a SonarQube analysis is straighforward. You just need to execute the following commands in your project's folder.
Visit the official documentation of the Scanner to download the latest version, and add the bin directory to the PATH environment variable Execute the Scanner Running a SonarQube analysis is straightorward. You just need to execute the following commands in your project's folder.
Visit the official documentation of the Scanner to download the latest version, and add the bin directory to the PATH environment variable Execute the Scanner Running a SonarQube analysis is straighforward. You just need to execute the following commands in your project's folder. sonar=scanner \
Visit the official documentation of the Scanner to download the latest version, and add the bin directory to the PATH environment variable Execute the Scanner Running a SonarQube analysis is straightorward. You just need to execute the following commands in your project's folder. sonar-scanner \ -Dsonar.projectKey=heroes-app \ Dsonar.sources \
Visit the official documentation of the Scanner to download the latest version, and add the bin directory to the PATH environment variable Execute the Scanner Running a SonarQube analysis is straighforward. You just need to execute the following commands in your project's folder. Sonar-scanner \ -Dsonar.projectKey=heroes-app \ -Dsonar.host.ur[=http://localhost:9000 \

19. Copy the command under "Execute the Scanner" and go to the directory where your TypeScript code resides and paste this to run. You should see something similar to below:

INFO:	CPD Executor 9 files had no CPD blocks
TNEO	CDD Executor (algulating CDD for 24 files
INFU:	CPD Executor Calculating CPD for 24 files
INF0:	CPD Executor CPD calculation finished (done) time=19ms
INF0:	Analysis report generated in 93ms, dir size=1.2 MB
INF0:	Analysis report compressed in 197ms, zip size=317.4 kB
INF0:	Analysis report uploaded in 181ms
INF0:	ANALYSIS SUCCESSFUL, you can browse http://localhost:9000/dashboard?id=heroes-app
INF0:	Note that you will be able to access the updated dashboard once the server has processed the submitted analysis report
INF0:	More about the report processing at http://localhost:9000/api/ce/task?id=AX3J217VfDrwyKT3wXYQ
INF0:	Analysis total time: 42.204 s
INFO:	
INFO:	EXECUTION SUCCESS
INFO:	
INFO:	Total time: 43.154s
INFO:	Final Memory: 14M/57M
TNEO.	
1111 01	

20. Go back to the SonarQube web page and you should see both your projects listed.

sonarqube Projects Issues Rules	Quality Profiles Quality Gates Administration	Q Search for projects A
My Favorites All	Q. Search by project name or key 2 projects	Create Project - 🔶 Perspective: Overall Status - Sort by: Name - 12
Cuality Gate Passed 2 Falled 0 Reliability (Tr Bugs) A 1	 ☆ heroes-api Passed n Bugs G Vulnerabilities 0 A 0 A - A 	Last analysis: 1 hour ago Code Smells Coverage Duplications Lines 38 (A) 87.9% (C) 0.0% (C) 353 (S) Java, XML
	☆ heroes-app Passed 第 Bugs 월 Vulnerabilities ♥ Hotspots Reviewed 1 0 - A	Last analysis: 3 minutes ago Code Smells 10 () 0.0% () Duplications 0.2% () 803 () TypeScript
B 0 C 0		2 of 2 shown

Take a screen shot of the projects (similar to above) and deposit it in the *Static Code Analysis individual* in the myCourses Assignments by the date shown on your section's schedule.

Explore and Analyze Your Reports

Every report will be different based on what the code analysis identified. Clicking on "Issues" (top of screen – see below) will list all the issues across your projects, which can then be categorized by severity (e.g. major, critical, blocker) and type (e.g. bug, vulnerability).

sonarqube Projects Issues	ules Quality Profiles Quality Gates Administration	Q Search for projects A
My Issues All	Bulk Change	, 1 / 49 issues 3h 18min effort
Filters	heroes-api / src//api/heroesapi/controller/HeroController,java	
∨ Туре	Use the built-in formatting to construct this argument. Why is this an issue? Code Smell + Amount A	1 hour ago マ L54 % ▼~ % performance マ
第 Bug 1 G Vulnerability 0 O Code Smell 48	Replace the type specification in this constructor call with the diamond operator ("<>"). ⊖ Why is this an issue? O Code Smell • O Minor • O Open • Not assigned • 1 min effort Comment	1 hour ago ▾ L57 🗞 ▾ � clumsy ▾
✓ Severity e Blocker 2 ♦ Minor 6	Use the built-in formatting to construct this argument. Why is this an issue? Code Smell * O Major * O Open * Not assigned * Smin effort Comment	1 hour ago マ L89 % ▼~ % performance マ
Critical 4 10 Info 22 Major 15	Use the built-in formatting to construct this argument. Why is this an issue? Code Smell * O Major * O Open * Not assigned * Smin effort Comment	1 hour ago + L104 % ▼- % performance +
> Scope > Resolution	Use the built-in formatting to construct this argument. Why is this an issue? O Code Smell + O Major + O Open - Not assigned + Smin effort Comment	1 hour ago ▾ L120 % ་་- % performance ▾
Status Security Category	Use the built-in formatting to construct this argument. Why is this an issue? Code Smell + A Major + O Open + Not assigned + Smin effort Comment	1 hour ago マ L138 % ▼~ % performance マ
> Creation Date	heroes-api / src//com/heroes/api/heroesapi/model/Hero.java	
> Language > Rule	Remove this unused *LOG* private field. Why is this an issue? Q Code Smell • Major • Open • Not assigned • Smin effort Comment	1 hour ago マ L10 % ママ ❤ unused マ
> Tag	heroes-api / src//api/heroesapi/persistence/HeroFileDAO.java	
> Project > Assignee	Reorder the modifiers to comply with the Java Language Specification. Why is this an issue? Q Code Smell • O Minor • O Open • Not assigned • 2min effort Comment	1 hour ago ▼ L57 % ▼~ Societation →
> Author	Make the enclosing method "static" or remove this set. Why is this an issue?	1 hour ago 🕶 L124 💊 🍸 -

Depending on the complexity of your code, certain metrics like **Cognitive Complexity** might get triggered, requiring attention for potentially refactoring:



Other "code smells" may get flagged due to issues with readability or other factors. This may indicate a problem or possibly a false flag.



If a particular issue is not clear, click the "Why is this an issue?", which will provide a description of the issue including code examples of a non-compliant issue and a compliant solution.

Overview Issues Security Hotspots Measures Code	Activity	Project Settings • 📰 Project Information
← <u>'</u>	Replace this if-then-else statement by a single return statement Why is this an issue? Ø Code Smell ♥ Ø Minor ♥ Open Not assigned Pain effort Comment	2 years ago マ L59 % ♥ clumsy マ
Remove this unused "jumped" private field. 60 gwb8.	<pre>return true; } else { return false; } //if # of white pieces == 0, white has lost</pre>	
Code Smell O Minor Curmsy Available Since Dec 17, 2021 SonarQube (Java) Constant/issue: 2min Return of boolean literal statements wrapped into if-then-else ones should be simplified. Similarly, method invocations wrapped into if-then-else differing only from boolean literals should be simplified into a single invocation. Noncompliant Code Example		
<pre>boolean foo(Object param) { if (expression) { // Noncompliant bar(param, true, "qix"); } else { bar(param, false, "qix"); } if (expression) { // Noncompliant return true; } else { return false; } }</pre>		
Compliant Solution		

Project Sprint 4 Deliverable

Identify 3-4 areas within your code that have been flagged by SonarQube and provide your analysis and recommendations. Include any relevant screenshot(s) with each area. This will be part of your final design documentation in your Sprint 4 submission. Be sure to include at least one from both reports (Java and TypeScript).

Stopping SonarQube

Refer to the setup document to stop SonarQube.