

SHIP-HATS 2.0. Configuring SHIP-HATS 101 (Part 2) - Alternative Tools

GovTech Services Group CTMO

17th July 2023



Agenda

- QUICK RECAP OF FORTIFY ON DEMAND
- FORTIFY ON DEMAND CHECKLIST
- QUICK RECAP OF NEXUS IQ
- NEXUS IQ CHECKLIST
- QUICK RECAP OF SONARQUBE
- SONARQUBE CHECKLIST
- WHAT'S NEXT

Fortify on Demand

A Quick Recap



What is Fortify on Demand

An **Application Security as a Service** providing security testing, vulnerability management, expertise and support. On SHIP-HATS, the following security testing are available:

- SAST*
- DAST (Website/Web API) (**Internet-facing only**)

[SHIP-HATS pipeline templates](#) for FOD SAST/DAST scans are available.

*Refer to [FOD documentation](#) for supported languages/compilers/libraries/frameworks

Applications and Releases

Your Applications

All 7 Microservice 0 Non-Microservice 7

KEYWORD: TESTLAB X

2 found

[SELECT ALL](#)

	NAME	PRODUCTION RISK & POLICY COMPLIANCE ⓘ	SCAN & SECURITY STATUS ⓘ
☐	testlab-web 11 RELEASES Business Criticality: HIGH	FAIL ★☆☆☆☆ CRITICAL 22 HIGH 55 MEDIUM 60 LOW 102	STATIC OPEN SOURCE DYNAMIC
☐	testlab-app 2 RELEASES Business Criticality: HIGH	FAIL ★☆☆☆☆ CRITICAL 4 HIGH 5 MEDIUM 0 LOW 1	STATIC OPEN SOURCE DYNAMIC



Do you know?

There is a system-wide policy that requires ratings of releases to be at least **3 stars i.e. 0 critical and high issues**. Otherwise, the given release will FAIL. This also means that the scan will fail (a SAST scan can fail even if all critical/high issue for the release are for DAST)



Balance cost with concurrency

To save cost, you can potentially create multiple releases for the same application to scan multiple components in your application. However, this can impact agility if pipelines for these components can be triggered in parallel.



Separate app for DAST API

To use FOD DAST for APIs, you will have to raise a service request. Note that this service request will require you to create another application.

Overview

- An application can have multiple releases, which can be of different technology stack (e.g. Java, C#, JS).
- The unique identifier for a scan (e.g. for a Maven project, .NET solution) is the Release ID, which can be found in the FOD Portal or SHIP-HATS Portal.
- SAST and DAST scans for the same Release ID will be integrated.
- Only 1 active scan for each application. Subsequent scan requests will be queued for SAST and failed for DAST.

Set Up DAST Scan (To be Done Before Trigger)

sgp.fortify.com/Releases/829/DynamicScanSetup

Dynamic Site URL

Fortify on Demand assessments will occur from IP ranges and networks: 18.142.73.216/32, 18.140.167.117/32, 18.142.98.230/32

Entitlement

731 Unit(s) Available

18 - Subscription (6 Units)



Time Zone

(Choose One)



Environment Facing

(Choose One)



▼ Scope

Fortify on Demand may scan the entire host of the designated URL. Other domains and subdomains will not be scanned during the assessment.

☒ Scan entire host ☐ Restrict scan to URL directory and subdirectories [?]

☒ Allow HTTP (:80) and HTTPS (:443)

☒ Allow form submissions during crawl [?]

Exclude URLs which contain



▼ Authentication

☒ Forms Authentication Required

Primary Username

Primary Password



Do you know?

1. URL, Scope, Authentication values **cannot be edited** once the first DAST scan is started for the given release.
2. FOD DAST include both active and passive scans. An active scan may attempt to exploit a potential vulnerability it detects. This might have severe impact if you run FOD DAST scan in production (e.g. bring down your website).

Vulnerability Management

testlab-web > netapp-v1.0

Release Issues

22 30 6 4 37

Group By
Category

Dynamic Code Evaluation: Insecure T... 1

index.html:19

Open Redirect 4

Password Management: Hardcoded Pas... 16

SQL Injection 2

27239 WebApplicationMVC/index.html : 19

netapp-v1.0 Critical Dynamic Code Evaluation: Insecure Transport SMART FIX

Vulnerability Recommendations Code Diagram More Evidence History

Summary

The file `index.html` on line 19 loads a script over an unencrypted channel. The file loads a script over an unencrypted channel.

Explanation

Including executable content from a website over an unencrypted channel enables an attacker to perform a man-in-the-middle (MITM) attack. This enables an attacker to load their own content that is executed as if it was part of the original website.

Example: Consider the following `script` tag:

```
<script src='http://www.example.com/js/fancyWidget.js'></script>
```

If an attacker is listening to the network traffic between the user and the server, the attacker can imitate or manipulate the content from `www.example.com` to load their own JavaScript.

Instance ID: E19611872D6EB69B9CB94E4FD67FD46A

Primary Rule ID: 0E8690E1-10AE-440C-8315-7F7DE80E7A6A

Standards and Best Practices

Audit

Status Existing

Introduced Date 2022/10/06

Last Found Date 2023/07/06

Assigned User (Not Set)

Developer Status Open

Auditor Status Pending Review

Severity Critical

Comment

SHOW

Fixed

Suppressed

Example Flow

1. Developer go through issues and update analysis in comment and developer status

Developer Status

Open

Open

Open

In Remediation

Closed

Remediated

Will Not Fix

Third Party Component

2. Security Lead review analysis and update auditor status.

Auditor Status

Pending Review

Pending Review

Not Suppressed

Remediation Required

Remediation Deferred

Risk Mitigated

Suppressed

Risk Accepted

Not an Issue



“Closed” or “Suppressed” issues may be hidden in “Issues” page

Check the “Show” dropdown to verify if “Fixed” (i.e. “Closed”) or “Suppressed” issues are selected to be shown.

Roles and Responsibilities

Role	Permissions	Key Responsibility
View Only	View - General information of the application - Application releases	-
GT-Report-Upload-And-Generate-SAST-and-DAST Assigned to token generated via SHIP-HATS Portal and cannot be assigned to users	Invoke SAST/DAST scan and download reports	Invoke scan and download report in the pipeline
GT-Application Security Tester	View Only + - Edit Issues - Create Reports - Configure DAST scans	Review findings and update analysis
GT-Security Lead	GT-Application Security Tester + - Audit Issues	Review finding analysis and suppress false positives
GT-Manager Assigned to SHIP-HATS Project Admins by default	GT-Security Lead + - Manage applications	Manage users and applications



Do you know?

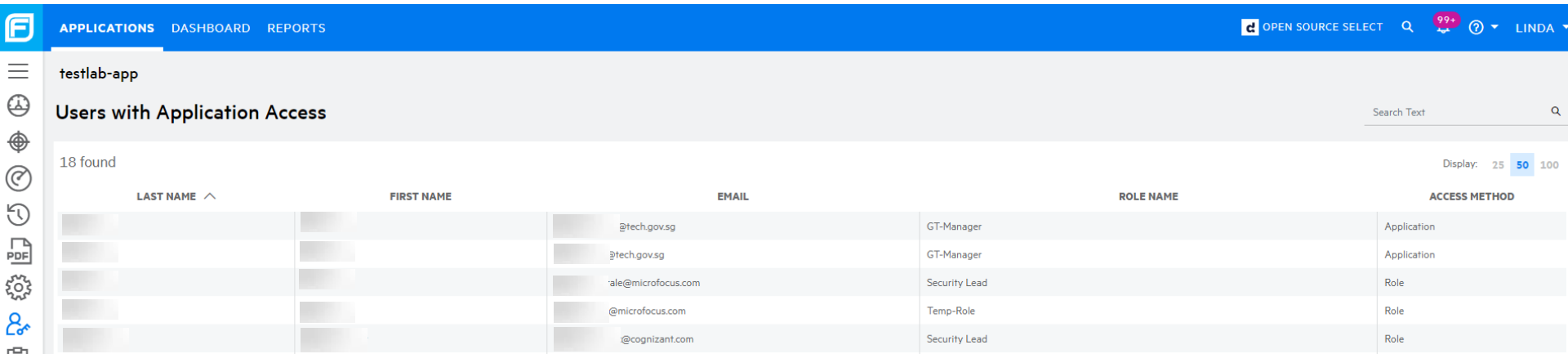
1. Role is global in FOD i.e. the role is applicable to **ALL** FOD apps that the user has access to
2. A user will require Gitlab/Atlassian/SONATYPE license before he/she can be added to a FOD app.
3. FOD does not support assignment of role to groups.

FOD Checklist



Access Control

✓ Validate users for each application.



The screenshot shows the 'testlab-app' page in the GovTech Applications system. The header includes navigation tabs for 'APPLICATIONS', 'DASHBOARD', and 'REPORTS'. The main title is 'testlab-app' and the subtitle is 'Users with Application Access'. A search bar is present on the right. Below the title, it indicates '18 found' and a 'Display' dropdown set to '50'. The table lists users with columns for 'LAST NAME', 'FIRST NAME', 'EMAIL', 'ROLE NAME', and 'ACCESS METHOD'. The visible data rows are as follows:

LAST NAME	FIRST NAME	EMAIL	ROLE NAME	ACCESS METHOD
		@tech.gov.sg	GT-Manager	Application
		@tech.gov.sg	GT-Manager	Application
		'ale@microfocus.com	Security Lead	Role
		@microfocus.com	Temp-Role	Role
		@cognizant.com	Security Lead	Role

Open and Suppressed Issues



Validate issues for each release are open or suppressed as intended.

testlab-app > testlab-app-v1

Release Issues [↓](#)

AUDITOR STATUS: RISK ACCEPTED X

SAVE QUERY CLEAR FILTERS

2 0 0 0 2

Group By
Auditor Status

☐ Risk Accepted 2

☒ ApplicationController.java : 96

☐ AuthenticationController.java : 26

25036 src/main/java/sg/tech/testlab/controller/ApplicationController.java : 96

testlab-app-v1 Critical Privacy Violation SMART FIX

Vulnerability Recommendations Code Diagram More Evidence History

Summary

The method `getById()` in `ApplicationController.java` mishandles confidential information, which can compromise user privacy and is often illegal. Mishandling private information, such as customer passwords or social security numbers, can compromise user privacy and is often illegal.

Explanation

Privacy violations occur when:

1. Private user information enters the program.
In this case, the data comes from in `User.java` on line 95.
2. The data is written to an external location, such as the console, file system, or network.
In this case, the data is passed to `debug()` in `ApplicationController.java` on line 96.

Example 1: The following code contains a logging statement that tracks the records added to a database by storing the contents in a log file.

Audit

Status
Existing

Introduced Date
2022/03/31

Last Found Date
2023/07/07

Assigned User
(Not Set)

Developer Status
Open

Auditor Status
Risk Accepted

Severity
Critical

Scan Coverage

✓ Validate that the scan covers the intended code.

</

Scan Summary

File Count	42
Total LOC	1371
Payload Size	32,130.37 KB
Technology Stack	JAVA/J2EE/Kotlin
Language Level	1.8

Scan Manifest

72514_manifest.txt - Notepad				
File	Edit	Format	View	Help
"/Libs/java/1945862116/tomcat-juli-8.5.16.jar" 45047 2023-07-07				
"/Src/testlab-app/src/main/java/sg/tech/testlab/repository/SequenceRepository.java" 319 2023-07-07				
"/Src/testlab-app/src/main/java/sg/tech/testlab/service/ApplicationService.java" 1360 2023-07-07				
"/Src/testlab-app/src/main/java/sg/tech/testlab/service/CodeService.java" 280 2023-07-07				
"/Libs/java/-144557816/mysql-connector-java-6.0.6.jar" 2001778 2023-07-07				
"/Libs/java/630684808/aopalliance-1.0.jar" 4467 2023-07-07				
"/Src/testlab-app/src/main/java/sg/tech/testlab/repository/JobRepository.java" 265 2023-07-07				

Nexus IQ

A Quick Recap



What is Nexus IQ

A **Software Composition Analysis** solution* providing intelligence on open source components used within the application, as well as the associated metadata, such as security vulnerabilities and licenses.

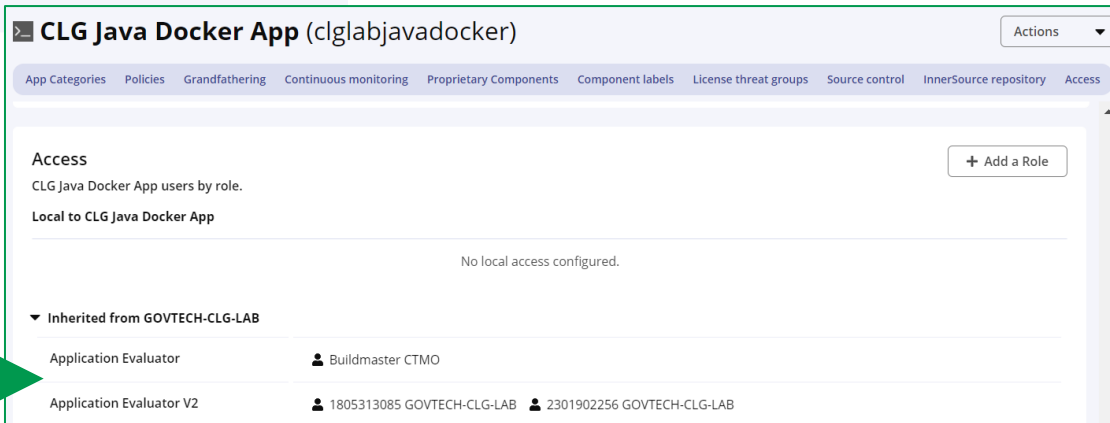
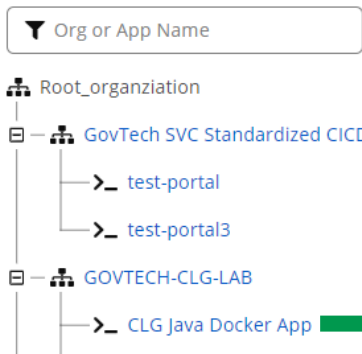
[SHIP-HATS pipeline templates](#) for Nexus IQ scans are available.

*Refer to [Sonatype documentation](#) for supported languages/package

Organizations and Applications

Root_organiziation

View all organizations and applications on which you have permissions. Click on the link for the org or app below to access details.



Overview

- An organization can have multiple applications, which can be of different technology stack (e.g. Java, C#, JS).
- Each application will inherit settings (e.g. access) from its organization.
- The unique identifier for a scan (e.g. for a jar) is the App ID, which can be found in the Nexus IQ Portal or SHIP-HATS Portal.

Policies

Govern the components used. There are policies already defined at the Root that are inherited by all Orgs.

INHERITED FROM ROOT_ORGANIZATION

THREAT NAME

License-Banned

Security-Critical

License-None

Security-High

License-Copyleft

Component-Similar

License-Commercial

License-Threat Not Assigned

Security-Medium

License-Modified Weak Copyleft

License-Non Standard

Security-Low

Component-Unknown

Architecture-Cleanup

Architecture-Quality

Constraints

High risk CVSS score

Is in violation if all of the following are true:

- Security Vulnerability Severity greater than or equals 7
- Security Vulnerability Severity less than 9

Add Constraint

Actions

Action overrides have been disabled for this policy.

Override Status

☒ Inherit parent actions

☐ Override parent actions

	PROXY	DEVELOP	SOURCE	BUILD	STAGE	RELEASE	OPERATE
No Action	☒	☒	☒	☒	☒	☒	☒
Warn	☐	☐	☐	☐	☐	☐	☐
Fail	☐	☐	☐	☐	☐	☐	☐

Notifications

Notification overrides have been disabled for this policy.

Override Status

☒ Inherit parent notifications

☐ Override parent notifications

	PROXY	DEVELOP	SOURCE	BUILD	STAGE	RELEASE	OPERATE	CONTINUOUS MONITORING
No notifications configured								

No Action

Warn

Fail

No Notification

e.g. you cannot configure email to be sent if a new critical vulnerability is disclosed for an OSS library used by the app

"No Action" for most policies

e.g. you cannot configure your pipeline to fail if the Nexus IQ evaluation has a high finding



Create Custom Policies to configure rules, action and/or notification

Vulnerability Management

Reports					
q: clg					
APPLICATION	ORGANIZATION	SOURCE	BUILD	STAGE RELEASE	RELEASE
CLG Lab App	GOVTECH-CLG-LAB		110 92 8 3 hours ago View Report		110 92 12 2 hours ago View Report
CLG MS App	GOVTECH-CLG-LAB		14 42 10 6 minutes ago View Report		14 42 10 15 hours ago View Report
CLG MS Docker	GOVTECH-CLG-LAB		4 28 608 21 hours ago View Report		4 28 608 15 hours ago View Report

Example Flow

1. Pipeline invoke the scan for a given stage e.g. default “BUILD” for CI and “RELEASE” for CD to PROD
2. Developers review the report to understand the components used and to review policy violations
3. Developers resolve policy violations (e.g. fixing the security vulnerability in code)
4. SHIP-HATS Project Admin
 - waive policy violations (e.g. after mitigation is applied outside of code)
 - claim components for application artifacts
 - add proprietary component matcher for proprietary components

CLG Java Docker App Build Report

Triggered by CLI on 2023-07-11 13:36:17 UTC+0800 - Commit 926d1d19e061bdae4796454bfe06071a061bb982

230

179

76

485 VIOLATIONS
Affecting 93 components

227 COMPONENTS
85% of all components identified

0 GRANDFATHERED
violations

☒ Aggregate by component

THREAT	POLICY	COMPONENT
9	GT-SVC-Security-High	org.springframework.boot : spring-boot-autoconfigure : 2.1.3.RELEASE
7	Component-Similar	com.xenoamess : nashorn : jdk8u265-b01-x1
7	Component-Similar	org.openjvm : jsse : 1.0.4.1
7	GT-SVC-Security-Medium	ch.qos.logback : logback-classic : 1.2.3

com.fasterxml.jackson.core : jackson-databind : 2.8.11.3

GOVTECH-CLG-LAB > CLG Java Docker App > Build Report 2023-07-11 18:32:44

☒ Maven ☒ Transitive Dependency

Overview

Policy Violations

Security

Legal

Labels

Audit Log

Component Information				
Match State	Identification Source	Occurrences	Website	Category
Exact	Sonatype	1 File	-	Other

Risk Remediation

Recommended Remediation

The direct dependencies that brought in this component are listed below. Clicking on a component will take you to its Component Details Page.

[org.springframework.boot : spring-boot-starter-actuator : 2.1.3.release](#)

[org.springframework.cloud : spring-cloud-starter-eureka : 1.3.6.release](#)

[org.springframework.cloud : spring-cloud-starter-hystrix : 1.3.6.release](#)

Recommended Versions

Upgrade to 2.12.7.1

Next version with no policy violation

Compare

Roles and Responsibilities

Role	Permissions	Key Responsibility
Developer	View assigned organizations, applications and reports	-
Application Evaluator Assigned to token generated via SHIP-HATS Portal and should not be assigned to users	Invoke Nexus IQ evaluation	Invoke evaluation in the pipeline
Application Security Tester v2	Developer + - Change security vulnerabilities	Review policy violations and update vulnerability status/comment
Owner with Claim Components Assigned to SHIP-HATS Project Admins by default	Application Security Tester + - Manage assigned organizations, applications - Waive policy violations - Claim components	Manage organizations, applications, users, policies and policy violations



Assign roles to groups instead of users to simplify permission management



Assign Owner wisely.

They can

- Change policy constraints and actions
- Waive policy violations
- Change organization/app users



Confine role assignment to organization

While SHIP-HATS Portal assign role at the organization level only, Owner can assign role at the app level. It will not be trivial to check access for every app in every organization.

Nexus IQ Checklist



Access Control

✓ Validate users and groups for each organization and application.

Access

+ Add a Role

CLG Java Docker App users by role.

Local to CLG Java Docker App

No local access configured.

▼ Inherited from GOVTECH-CLG-LAB

Application Evaluator	 Buildmaster CTMO
Application Evaluator V2	 1805313085 GOVTECH-CLG-LAB  2301902256 GOVTECH-CLG-LAB
Application Security Tester V2	 Jianrong Wang
Component Evaluator	 9556e43b-119a-44f2-9f40-6ca1b8ec8f69  gt-ctmo
Developer	 Ramanathan Anu  Debbie Ang  Jianrong Wang
Owner With Claim Components	 Ramanathan Anu  Debbie Ang  Jackson LAW FROMCOGNIZANT  Jianrong Wang  Kin Yeap Liu  Linda Chang

Open and Waived Policy Violations

✓ Validate policy violations are open or waived as intended.

The screenshot shows the Sonatype Lifecycle web application. On the left is a dark sidebar with navigation links: Dashboard, Orgs and Policies, Reports, Success Metrics, Vulnerability Lookup, Advanced Search, Firewall, and Data Insights (with a 'Labs' badge). The main content area is titled 'Results' and has tabs for 'Violations', 'Components' (61), 'Applications' (1), and 'Waivers' (2). A blue information box states: 'This list shows all existing waivers applied at the same or higher hierarchy level, based on your filter selections. [Learn more about waivers.](#)' Below this is a table of waivers.

THREAT	DATE CREATED	EXPIRATION	POLICY	SCOPE	COMPONENTS	UPGRADE
10	2021-05-28	2021-06-04	Security-Critical	Application - CLG Lab App	dom4j : dom4j : 1.6.1	—
9	2020-10-14	Never	GT-SVC-Security-High	Application - CLG Lab App	com.fasterxml,jackson.core : jac...	Available



Do not waive critical/high security policy violations

Even if the vulnerability is currently not applicable due to how it is used or other mitigations, this may not remain the case. Given the potential impact, upgrade to a non-vulnerable version (if available).



Address unknown/similar components

All components should be identified. Modified open source components should be discouraged as they are hard to maintain and the modifications may be vulnerable.

Claimed and Proprietary Components



Validate claimed/proprietary components are app artifacts or proprietary

CLG Java Docker App

Policy Management

▶ Application Categories

▶ Policies

Grandfathering

Continuous Monitoring

Proprietary Components

▶ Component Labels

Source Control

Proprietary Component Configuration

These entries are provided to Sonatype IQ scanners and are used to help identify internal components. If a specified package or file is contained within a component, it will be considered proprietary.

Local

ctmo-helper-1.0.1.jar

Package

Value *

Matcher Type *

Package

CLG Java Docker App Build Report

Triggered by CLI (Re-evaluation) on 2023-07-11 18:32:44 UTC+0800 - Commit 926d1d19e061bdae4796454bfe06071a061bb982

228 129 74

482 VIOLATIONS
Affecting 92 components

227 COMPONENTS
86% of all components identified

0 GRANDFATHERED
violations

Aggregate by component

View

THREAT	POLICY	COMPONENT
0	None	com.xenoamess nashorn jdk8u265-b01-x1
0	None	sg.tech.javadocker : Release 162 Back to Application Report docker-image-danielbryantuk-djproductcatalogue : tar : 2.0.521

Filter

▶ Proprietary 2

▶ InnerSource 2

▼ Component Match State 1 of 3

- ☐ all/none
- ☒ Exact
- ☐ Similar
- ☐ Unknown

▼ Violation State 1 of 4

- ☐ all/none
- ☒ Not Violating
- ☐ Open
- ☐ Waived
- ☐ Grandfathered

▼ Dependency Type 1 of 3

- ☐ all/none
- ☐ Direct Dependencies
- ☐ Transitive Dependencies
- ☒ Unknown

▶ Policy Types 4

▶ Policy Threat Level 9-10

Continuous Monitoring



Validate that continuous monitoring is enabled for prod build

1. Continuous monitoring is enabled for stage used to scan prod builds
2. Add notification for each policy (custom only) when a policy violation (e.g. critical/high/medium security vulnerability) is found during continuous monitoring

Continuous Monitoring
Each day the latest scan from this stage will be evaluated. Notifications for new violations can be configured per policy.

Monitoring Stage

- ☐ Inherit from Govtech SVC (Operate)
- ☐ Develop
- ☐ Build
- ☐ Stage Release
- ☒ Release
- ☐ Operate

Update

NOTIFICATIONS

RECIPIENT	PROXY	DEVELOP	BUILD	STAGE	RELEASE	OPERATE	CONTINUO... MONITORI...
✉ linda_chang@tech.gov.sg	☐	☐	☒	☐	☐	☐	☒

Recipient Type

Email Address

Email

+ Add



Enable continuous monitoring for a stage dedicated to scanning builds deployed to prod

Unless every build in the CI Pipeline goes straight to production, there is a likelihood that the newest build is not the same build that has been deployed to production and that both builds may not be using the exact same components (and versions).

SonarQube

A Quick Recap



What is SonarQube

A **Static Code Analysis** tool* that can be used to find code quality issues. On SHIP-HATS, the following editions are available:

- Community
- Developer

[SHIP-HATS pipeline templates](#) for SonarQube scans are available.

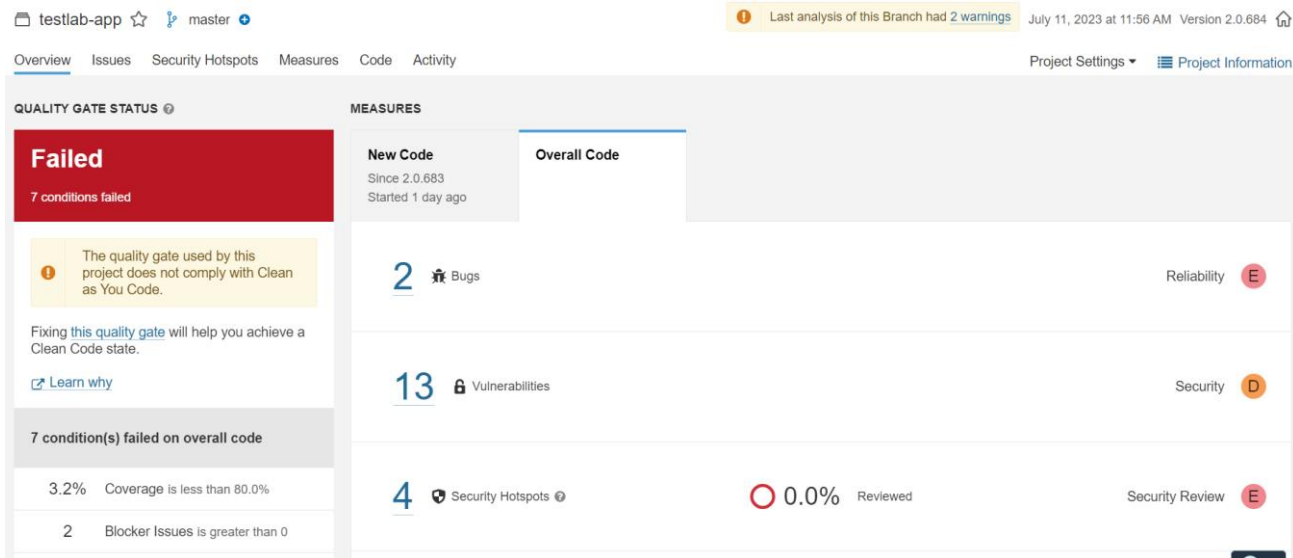
*Refer to [SonarQube documentation](#) for supported languages/package



SonarQube is NOT a code coverage tool

A separate code coverage tool must be used to generate the code coverage results, which will then be analyzed by SonarQube.

Projects



Overview

- The unique identifier for a scan is the project key, which can be found in the “Project Information” in SonarQube Portal. Do **NOT** confuse this with the project name (e.g. what you see in above screenshot is the project name and not the project key).

Quality Profiles

Collection of rules to apply during an analysis with a default profile for each language.

testlab-app ☆ master +

Overview Issues Security Hotspots Measures Code Activity

Quality Profiles ⓘ

Manage project Quality Profiles

Choose which profile is associated with this project on a language-by-language basis.

Language	Current Quality Profile	Active Rules
JSP	Sonar way BUILT-IN	0
Java	Sonar way BUILT-IN	479
XML	Instance default	24

Q Search for rules...

Language

▼ Type

🐛 Bug 139

🔒 Vulnerability 31

💡 Code Smell 272

🔥 Security Hotspot 37

> Tag

> Repository

> Default Severity

> Status

> Security Category

> Available Since

> Template ⓘ

> Quality Profile ⓘ SONAR ... Clear

⬆️ ".equals()" should not be used to test the values of "Atomic" classes

⬆️ "==" should not be used instead of "=="

🟢 "@CheckForNull" or "@Nullable" should not be used on primitive types

⬆️ "@Controller" classes that use "@SessionAttributes" must call "setComplete" on their "SessionStatus" objects

⬆️ "@Deprecated" code marked for removal should never be used Java

🟢 "@Deprecated" code should not be used Java

🟢 "@NonNull" values should not be set to null

⬆️ "@Override" should be used on overriding and implementing methods

⬆️ "@RequestMapping" methods should not be "private" Java

⬆️ "@SpringBootApplication" and "@ComponentScan" should not be used in the default package



Review “Vulnerability” and “Security Hotspot” rules in quality profile

If you are planning to use SonarQube for SAST, review the quality profile to see if the rules are sufficient to find security vulnerabilities in your source code. Some quality profiles e.g. Sonar way for Go has 0 vulnerability rule.

Quality Gates

Enforce a quality policy, which defines a set of conditions against which projects are measured.
Raise a ticket for custom quality gate (only if necessary).

testlab-app ☆ master +

Overview Issues Security Hotspots Measures Code Activity

Quality Gate ?

Manage project Quality Gate

Choose which quality gate is associated with this project.

☒ Always use the instance default Quality Gate
Current: GT-QualityGates-v0.2

☐ Always use a specific Quality Gate
Select...

Save

Conditions ?		
Conditions on Overall Code		
Metric	Operator	Value
Blocker Issues	is greater than	0
Cognitive Complexity	is greater than	10
Coverage	is less than	80.0%
Critical Issues	is greater than	0
Cyclomatic Complexity	is greater than	15
Duplicated Blocks	is greater than	0
Major Issues	is greater than	0
Skipped Unit Tests	is greater than	0
Unit Test Errors	is greater than	0
Unit Test Failures	is greater than	0

Projects ?
Every project not specifically associated to a quality gate will be associated to this one by default.

Roles and Responsibilities

Permissions

Grant and revoke project-level permissions. Permissions can be granted to groups or individual users.

This project is private. Only authorized users can browse and see the source code.

☐ Public ☒ Private

All

Users

Groups

Q Search for users or groups...

Browse ?

See Source
Code ?

Administer
Issues ?

Administer
Security
Hotspots ?

Administer ?

Execute
Analysis ?

An example for illustration:

Who	Permissions	Responsibilities
SHIP-HATS Project Admin	Browse, Administer	Manage projects and users
Tech Lead	All except Administer, Execute Analysis	Review findings and update analysis
Engineer	Browse, See Source Code	View and fix findings
Token	Browse, Execute Analysis	Upload analysis and check quality gate status



Assign permissions to groups instead of users to simplify permission management



Assign Administer permission wisely.
They can

- Change quality gate
- Change quality profile
- Change permissions

SonarQube Checklist



Access Control



Validate

- Permissions of users and groups for each project
- Project is private

testlab-app ☆ master

1 Last analysis of this Branch had 2 warnings July 11, 2023 at 11:56 AM Version 2.0.684

Overview Issues Security Hotspots Measures Code Activity Project Settings Project Information

Permissions

Grant and revoke project-level permissions. Permissions can be granted to groups or individual users.
This project is private. Only authorized users can browse and see the source code.

☐ Public ☒ Private

	All	Users	Groups	Search for users or groups...	Browse	See Source Code	Administer Issues	Administer Security Hotspots	Administer	Execute Analysis
2a14b79b-4bc8-4dc9-aeaf-bdcdbd2b18553 1805313085-CI-GROUP					☒	☐	☐	☐	☐	☐
CLG-LAB					☒	☒	☒	☒	☐	☒
sonar-administrators System administrators					☒	☐	☐	☐	☒	☒



SHIP-HATS SonarQube is shared by **ALL** tenants.

Setting a visibility other than “Private” mean that every SHIP-HATS users can access the project.

Quality Profiles



Validate the quality profile selected for each language for each project.

testlab-app master

[Overview](#) [Issues](#) [Security Hotspots](#) [Measures](#) [Code](#) [Activity](#)

Quality Profiles

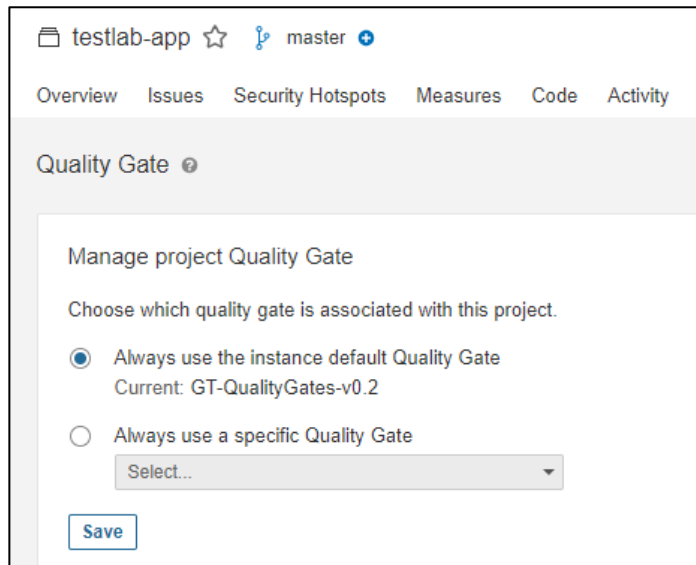
Manage project Quality Profiles

Choose which profile is associated with this project on a language-by-language basis.

Language	Current Quality Profile	Active Rules
JSP	Sonar way BUILT-IN	<u>0</u>
Java	Sonar way BUILT-IN	<u>479</u>
XML	Instance default	<u>24</u>

Quality Gates

- ✓ Validate the quality gates selected for each project



The screenshot shows a web interface for configuring quality gates for a project named 'testlab-app'. At the top, there are navigation tabs: 'Overview', 'Issues', 'Security Hotspots', 'Measures', 'Code', and 'Activity'. Below these is a 'Quality Gate' section with a help icon. The main content area is titled 'Manage project Quality Gate' and contains the instruction 'Choose which quality gate is associated with this project.' There are two radio button options: 'Always use the instance default Quality Gate' (which is selected) and 'Always use a specific Quality Gate'. The first option has a sub-label 'Current: GT-QualityGates-v0.2'. The second option has a dropdown menu labeled 'Select...'. A 'Save' button is located at the bottom left of the configuration area.

testlab-app ☆ master +

Overview Issues Security Hotspots Measures Code Activity

Quality Gate ⓘ

Manage project Quality Gate

Choose which quality gate is associated with this project.

☒ Always use the instance default Quality Gate
Current: GT-QualityGates-v0.2

☐ Always use a specific Quality Gate
Select...

Save

Scan Coverage

✓ Validate that the scan covers the intended code.

testlab-app ☆ master +

ⓘ Last analysis of this Branch had 2 warnings July 11, 2023 at 11:56 AM Version 2.0.684 🏠

Overview Issues Security Hotspots Measures Code Activity

Project Settings ▾ [Project Information](#)

🔍 Search for files...

↑ ↓ to select files ← → to navigate

	Lines of Code	Bugs	Vulnerabilities	Code Smells	Security Hotspots	Coverage	Duplications
testlab-app							
└─ src	1,743	2	13	64	4	3.2%	4.2%
└─ pom.xml	315	0	0	3	0	—	0.0%

Pipeline Checklist



Quality Gates

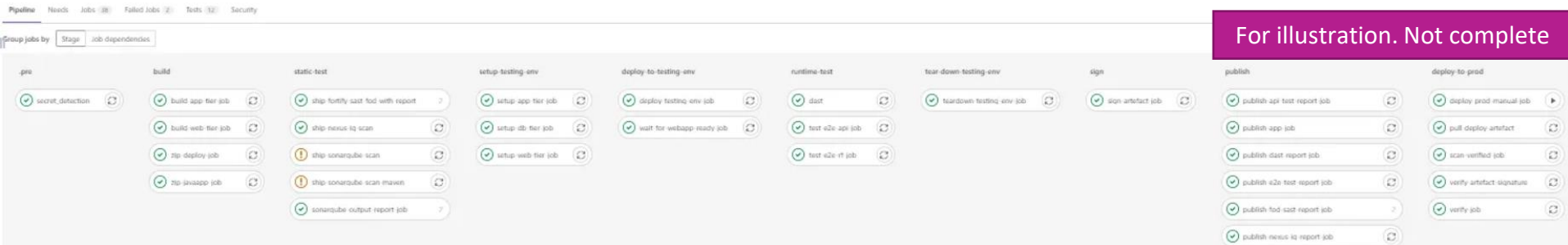
✓ Validate that for each required test/scan

1. The pipeline invokes the test/scan

- Unit Test
- SAST
- Code Quality Scan
- API Test
- DAST
- Container Scanning
- UI Test
- Dependency Scanning
- Secret Detection

2. The test/scan completes successfully

3. The test/scan passes the success criteria

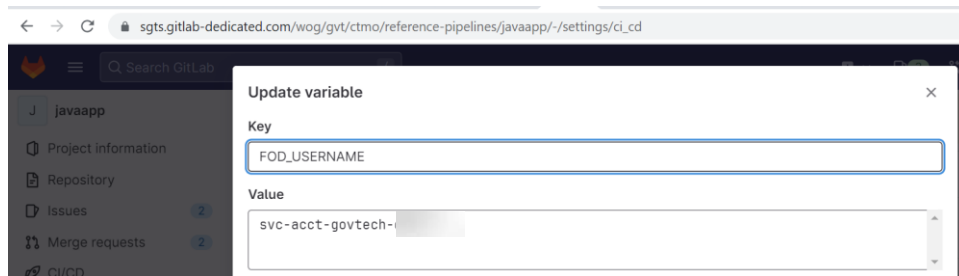


Do you know that a “green tick” can mean that the job completes successfully but test/scan may **NOT** have passed? It is possible to script each test/scan job so that it fails if the success criteria is not met but you will have to review the script to ensure that this hard gating has been implemented.

Tokens

✓ Validate that the project token is used for integration with

- Nexus IQ
- FOD
- Sonarcube



💡 Do you know that using a personal token imply

1. The corresponding user may have additional privileges that he/she should not have (e.g. upload analysis)
2. It may not be possible to differentiate between the pipeline and the user in the tools' audit logs

💡 **Save the project token as a masked group/project variable** (if not using a secret manager)

If you cannot find the project token in the list of group/project variable, it may have been **hardcoded** in the pipeline YAML.

Scan Coverage

✓ Validate that the scan covers the intended code

```
scan-verified-job: # Scanning of verified artefact
# override to enable continuous monitoring
variables:
  NEXUS_IQ_SCAN_OPTIONS: "-t release"
  SCAN_TARGETS: prod/$OUTPUT_ARTEFACT
needs: ["pull-image-job"]
```

```
ship-fortify-sast-fod-with-report: # perform FOD sast scan on web tier code
variables:
  PACKAGE_OPTS: $PACKAGE_OPTS_TESTLABWEB
  FOD_RELEASE: $FOD_RELEASE_TESTLABWEB
  FOD_UPLOADER_OPTS: $FOD_UPLOADER_OPTS_TESTLABWEB
before_script:
  - cd testlab-web/public
artifacts:
  paths:
    - gl-fortify-sast.json
```

```
ship-sonarqube-scan: # perform sonarqube scan on web tier code
# override to change scan directory and projectkey
variables:
  SONAR_PROJECTKEY: $SONAR_PROJECTKEY_TESTLABWEB
  SCAN_DIR: "testlab-web/public"
```

💡 Do you know that some scanners support exclusions? For example, SonarQube allows you to specify the option “sonar.exclusions” to list files or directories to exclude from analysis.

What's Next?



Documentation (Requires SHIP-HATS Access)

- **PM/BA Checklist:** [https://sgts.gitlab-dedicated.com/groups/wog/gvt/ctmo/reference-pipelines/-/wikis/PM-BA-Checklist-\(SHIP-HATS-2.0\)](https://sgts.gitlab-dedicated.com/groups/wog/gvt/ctmo/reference-pipelines/-/wikis/PM-BA-Checklist-(SHIP-HATS-2.0))
- **Considerations for using FOD:** [https://sgts.gitlab-dedicated.com/groups/wog/gvt/ctmo/reference-pipelines/-/wikis/Considerations-for-using-Microfocus-Fortify-on-Demand-\(FoD\)](https://sgts.gitlab-dedicated.com/groups/wog/gvt/ctmo/reference-pipelines/-/wikis/Considerations-for-using-Microfocus-Fortify-on-Demand-(FoD))
- **Considerations for using Nexus IQ:** <https://sgts.gitlab-dedicated.com/groups/wog/gvt/ctmo/reference-pipelines/-/wikis/Considerations-for-using-Nexus-IQ>
- **Considerations for using SonarQube:** <https://sgts.gitlab-dedicated.com/groups/wog/gvt/ctmo/reference-pipelines/-/wikis/Considerations-for-using-Sonarqube>

Upcoming Webinars

<https://go.gov.sg/ship-hats-learning-events>

GitLab Issues, Labels, and Boards

Covers more tips & tricks on issues, labels, and boards.

24 July '23 | 3 PM to 4 PM |
Level 100

Supply Chain Security using SLSA

Covers overview of Supply Chain Levels for Software Artifacts (SLSA), and how to use SHIP-HATS templates to strengthen supply chain security.

7 August '23 | 3 PM to 4:30 PM | Level 200

Innersource in GovTech

Covers what is innersource, how to innersource, and models of innersource.

21 August '23 | 3 PM to 4:30 PM | Level 200

[Sign up here](https://go.gov.sg/ship-hats-learning-events)

All migrations must be completed by
31 December 2023.

Key Timelines

Tool	Decommission Date	Replacement Tool
Fortify WebInspect (OnPrem)	31 July 2023	GitLab SAST/DAST or Fortify On Demand
Fortify SCA (OnPrem)	31 July 2023	GitLab SAST/DAST or Fortify On Demand
Bitbucket	January 2024	GitLab
Bamboo	January 2024	GitLab
Prisma Cloud	January 2024	GitLab

Thank You

