

Installing Sonatype IQ Server and integrating with Fortify SSC & SCA

Fortify SSC 20.x

Author: [Vikas Johari](#)
Date: 15 February 2021
Document Version: v0.1

Contents

Contents	2
Introduction	3
Installing CentOS 8	4
Installing and Configuring Docker on CentOS 8	4
Installing Portainer (Optional).....	5
Installing Sonatype IQ Server	7
Downloading the default policies	9
Testing the Sonatype IQ Server with a Sample Code	10
Installing Sonatype SSC plugin	18
Installing SourceAndLibScanner	21
Using SourceAndLibScanner	22
Scanning WebGoat via SourceAndLibScanner	22
Manual invocation of SCA and the Fortify / Sonatype Open Source Scanning Service.....	23
Scanning WebGoat via Sonatype only.....	27
Scanning Riches.Net Code with Sonatype IQ Server and SCA.....	30
Log Files	32
Deploy Integration Service on Sonatype IQ Server	33

Introduction

This document is written to guide Pre-Sales and Partners to install SonaType Nexus IQ Server and integrating with Fortify 20.2.0 SSC and SCA. Best way to install SonaType Nexus IQ Server using the Docker image, I have used the same.

This document is not written to install SonaType Nexus IQ Server in a Production Environment. However, this document can be used to setup SonaType Nexus IQ Server in a controlled environment like Lab or PoC or CoE Environment.

The Hardware and Software requirements are given in the link –

<https://help.sonatype.com/igserver/product-information/system-requirements>

https://www.microfocus.com/documentation/fortify-software-security-center/2020/Fortify_Sys_Reqs_20.2.0/index.htm#SSC/SSC_Reqs.htm?TocPath=Fortify%2520Software%2520Security%2520Center%2520Server%2520Requirements%257C____0

https://www.microfocus.com/documentation/fortify-static-code-analyzer-and-tools/2020/Fortify_Sys_Reqs_20.2.0/index.htm#SCA/SCA_Reqs.htm?TocPath=Fortify%2520Static%2520Code%2520Analyzer%2520Requirements%257C____0

Detailed SSC 20.2.0 User Guide is given in https://www.microfocus.com/documentation/fortify-software-security-center/2020/SSC_Help_20.2.0/index.htm

Detailed SCA 20.2.0 User Guide is given in https://www.microfocus.com/documentation/fortify-static-code-analyzer-and-tools/2020/SCA_Help_20.2.0/index.htm

I have used a two VMs with the below hardware configuration –

SonaType Nexus IQ Server:

CPU: 2 vCPU

RAM: 8 GB RAM

Disk: 60 GB Thin Provisioned

CentOS 8: Download link http://isoredirect.centos.org/centos/8/isos/x86_64/

Internet Connection

Fortify SSC & SCA Server:

CPU: 4 vCPU

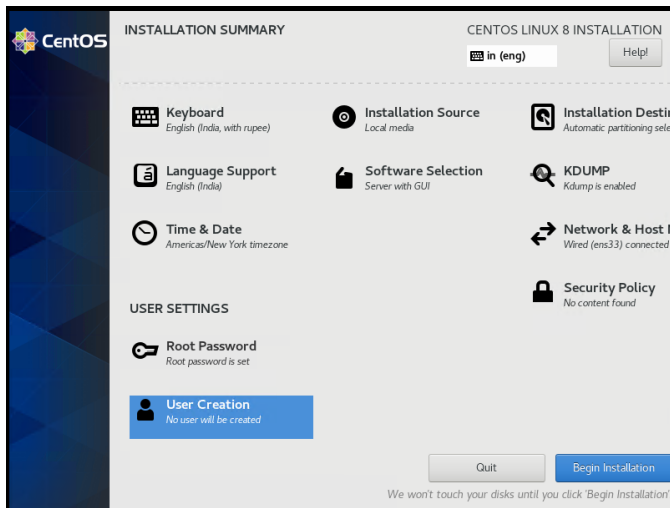
RAM: 16 GB RAM

Disk: 100 GB Thin Provisioned

Windows 2019 Server with MS SQL 2019 Server

Internet Connection

Installing CentOS 8



Install and Configure CentOS 8 64 bit. Install all the patches.

Download and install Oracle JDK 11 i.e. `jdk-11.0.10_linux-x64_bin.rpm` file using –
`# rpm -ivh jdk-11.0.10_linux-x64_bin.rpm`

Verify the installation –

```
# java -version
java version "11.0.10" 2021-01-19 LTS
Java(TM) SE Runtime Environment 18.9 (build 11.0.10+8-LTS-162)
Java HotSpot(TM) 64-Bit Server VM 18.9 (build 11.0.10+8-LTS-162, mixed mode)
# javac -version
javac 11.0.10
```

Installing and Configuring Docker on CentOS 8

Add Docker CE Repo

```
# dnf config-manager --add-repo=https://download.docker.com/linux/centos/docker-ce.repo
```

Removing Conflicting Packages

```
# yum erase podman buildah -y
```

Installing `rpm-build` which is required for SCA. Just in case we have to install SCA on this server.

```
# yum install rpm-build -y
```

Install Containerd.IO

Run the below command as root –

```
# dnf install https://download.docker.com/linux/centos/7/x86_64/stable/Packages/containerd.io-1.4.3-3.1.el7.x86_64.rpm -y
```

Its time to Install Docker

```
# dnf install docker-ce -y
```

Configure Docker Services

```
# systemctl enable docker
# systemctl start docker
# systemctl status docker
```

Verify docker is install and running

Installing Portainer (Optional)

Portainer is easy web based Container management tool.

Ref: <https://documentation.portainer.io/v2.0/deploy/ceinstalldocker/>

Run the below commands as root –

```
# docker volume create portainer_data

# docker run -d -p 8000:8000 -p 9000:9000 --name=portainer --
restart=always -v /var/run/docker.sock:/var/run/docker.sock -v
portainer_data:/data portainer/portainer-ce
```

Verify portainer is running in docker –

```
# docker ps
```


```
[root@iq ~]# docker ps
CONTAINER ID   IMAGE                  COMMAND                  CREATED        STATUS        PORTS                               NAMES
e557b7410534   portainer/portainer-ce "/portainer"            About a minute ago Up About a minute   0.0.0.0:8000->8000/tcp, 0.0.0.0:9000->9000/tcp   portainer
```

```
# netstat -anp | grep :9000
```

```
[root@iq ~]# netstat -anp | grep :9000
tcp        0      0 0.0.0.0:9000          0.0.0.0:*              LISTEN      3690/docker-proxy
```

Use Browser to connect on port 9000


Not secure | 172.17.5.224:9000/#/init/admin




Please create the initial administrator user.

Username

Password

Confirm password 


 The password must be at least 8 characters long

[Create user](#)


☒ Allow collection of anonymous statistics. You can find more information about this in our [privacy policy](#).


Enter a new password for admin user. Click "Create user" button.


Not secure | 172.17.5.224:9000/#/init/endpoint



Connect Portainer to the container environment you want to manage.

 **Docker**
Manage the local Docker environment

 **Kubernetes**
Manage the local Kubernetes environment

 **Agent**
Connect to a Portainer agent

Information

Manage the Docker environment where Portainer is running.

Ensure that you have started the Portainer container with the following Docker flag:

```
-v "/var/run/docker.sock:/var/run/docker.sock" (Linux).
```


or

```
-v "\\.\pipe\docker_engine:\\.\pipe\docker_engine" (Windows).
```

[Connect](#) [Skip](#)

Click on "Docker" option. Then click Connect button.

← → C Not secure | 172.17.5.224:9000/#/home



Home


SETTINGS

Users


Endpoints

Registries

Settings

Home 



Endpoints

Latest News From Portainer 

Portainer CE 2.1.1 is here. Now with support for Compose >3 in standalone hosts, and Compose 3.8 for Swarm. Upgrade today! <https://bit.ly/3p4DO5>


[Refresh](#)

Search by name, group, tag, status, URL...

 **local**  2020-02-15 10:55:11

0 stacks 1 container - 1 0 / 0 0 0 1 volume 1 image

8.1 GB - No tags

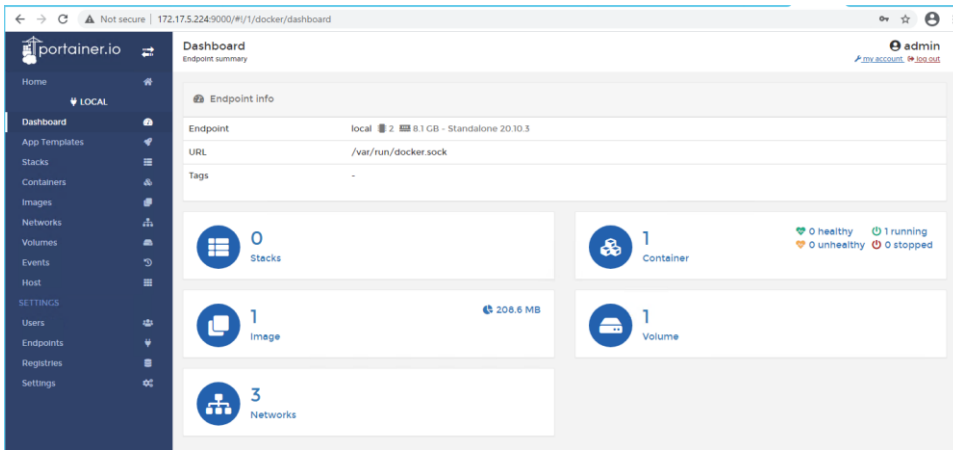
Group: Unassigned 

Standalone 20.10.3

/var/run/docker.sock

Items per page 10

Click on Docker icon.



Looks good.

Installing SonaType IQ Server

Docker version of IQ Server is available in <https://hub.docker.com/r/sonatype/nexus-iq-server>
Run the below command to pull SonaType Nexus IQ Server.

```
# docker pull sonatype/nexus-iq-server
```

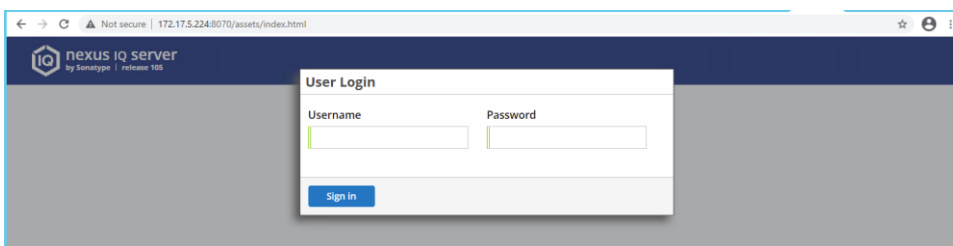
Deploy the image.

```
# docker run -d -p 8070:8070 -p 8071:8071 --name nexus-iq-server sonatype/nexus-iq-server
```

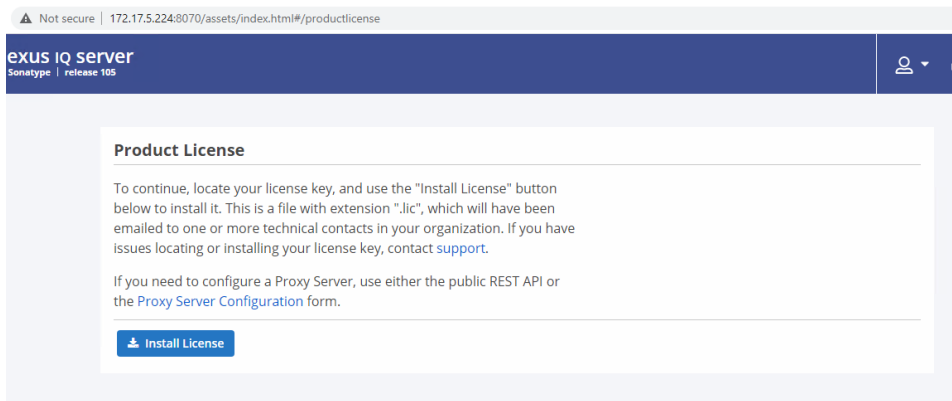
Verify using docker ps command –

```
[root@iq ~]# docker ps
CONTAINER ID   IMAGE                                COMMAND                  CREATED        STATUS        PORTS                                                                                               NAMES
1a0bdef8bd04   sonatype/nexus-iq-server            "sh ./start.sh"         About a minute ago    Up About a minute (healthy)    8080/tcp, 8443/tcp, 0.0.0.0:8070-8071->8070-8071/tcp, 8778/tcp    nexus-iq-server
e557b7410534   portainer/portainer-ce              "/portainer"            13 minutes ago      Up 13 minutes                  0.0.0.0:8080->8080/tcp, 0.0.0.0:9000->9000/tcp                    portainer
```

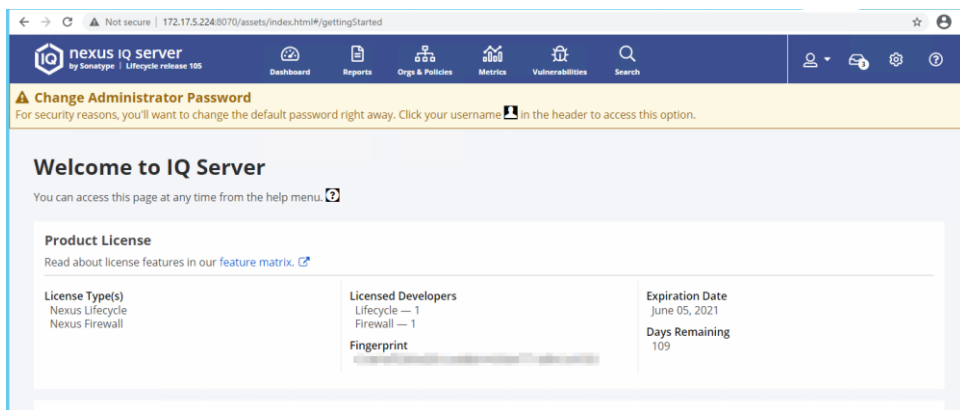
Now connect to port 8070 using browser. SonaType IQ Server runs on port 8070.



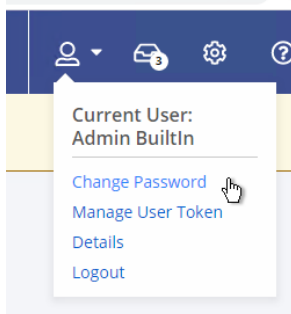
Enter the credentials, username **admin** and password **admin123**. Click Sign In.



Click Install License button. Select the upload the license file.



Change the admin user's password.



Click on Change Password.

A screenshot of the 'Change Password' form. It contains three input fields: 'Current Password', 'New Password', and 'Confirm New Password'. Each field has a green indicator bar on the left. At the bottom of the form are two buttons: 'Change' (in blue) and 'Cancel' (in gray).

Enter the old password and new password then click on Change button.

Reboot the Server.

Verify the Nexus-IQ-Server is running, if not then start the service using –
docker start nexus-iq-server

Downloading the default policies

Click on "Orgs & Policies" -> "Root Organization", if you don't see default policies on the right panel. Then you have to download and install default policies.

THREAT	NAME	PROXY	DEVELOP	BUILD	STAGE	RELEASE	OPERATE
License-Banned		no act...	no action	no act...	no act...	no action	no action
Security-Critical		no act...	no action	no act...	no act...	no action	no action
Security-Malicious		no act...	no action	no act...	no act...	no action	no action
License-None		no act...	no action	no act...	no act...	no action	no action
Security-High		no act...	no action	no act...	no act...	no action	no action

Open the URL <https://help.sonatype.com/iqserver/managing/policy-management#PolicyManagement-DownloadingtheReferencePolicySet> using Browser.

Downloading the Reference Policy Set

You can download the reference policy set into an organization from here:

For IQ Server release 97 or newer

- [reference-policies-v5.json](#)

For IQ Server release 91 to 96: ([more info](#))

- [reference-policies-v4.json](#)

For IQ Server release 50 to 90:

- [reference-policies-v3.json](#)

For IQ Server version 1.22 to 1.49:

- [reference-policies-v2.json](#)

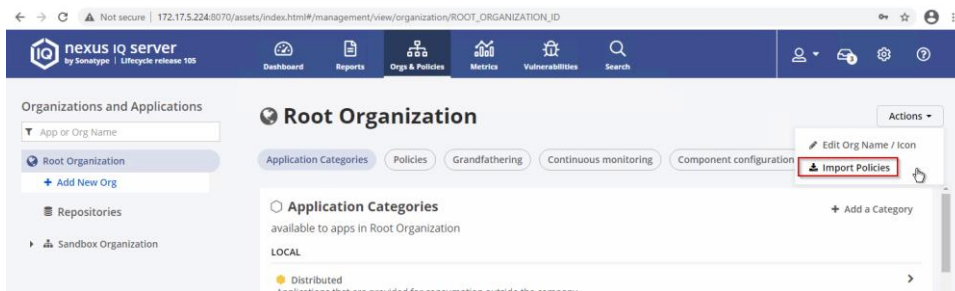
For IQ Server version 1.21 or older:

- [reference-policies-v1.json](#)

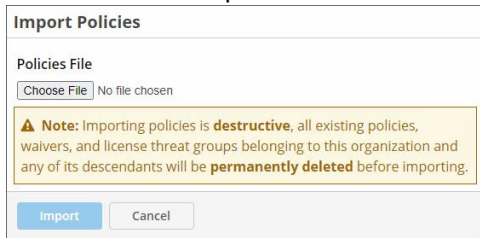
Once the Reference Policy Set is downloaded, you can import it by following the instructions in the next section.

Download the latest json file i.e. "reference-policies-v5.json".

Make sure your IQ server can connect to internet, configure proxies if needed.



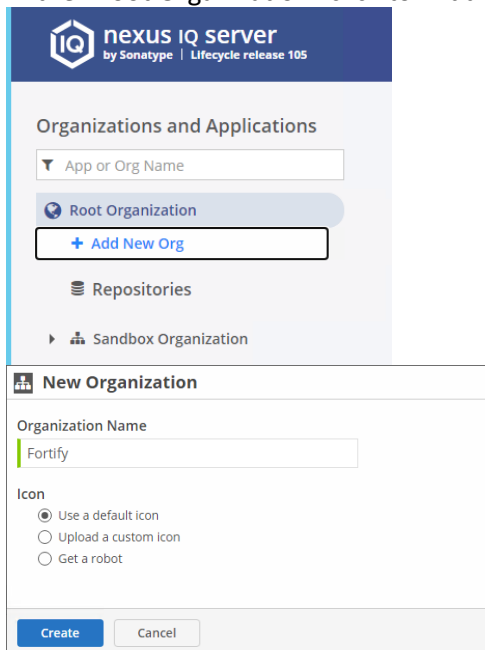
Click Actions -> Import Policies.



Select the downloaded reference-policies-v5.json file and click Import.

Testing the Sonatype IQ Server with a Sample Code

In the "Root Organization" click to "Add New Org".



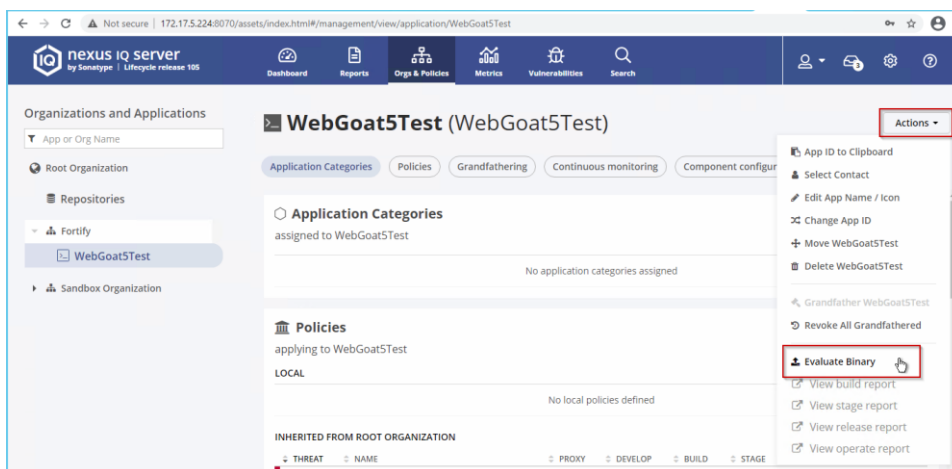
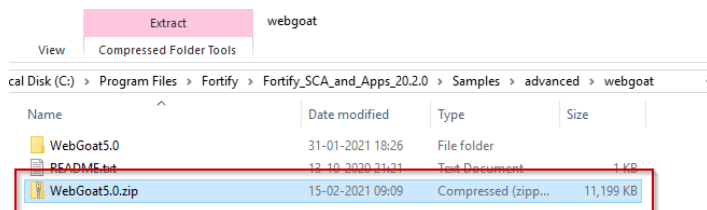
Give a name to your organization i.e. Fortify, click Create.



Click "Add New App".

Create a Test Application name "WebGoat5Test" and its application ID will be "WebGoat5Test".

Open the folder WebGoat 5.0 folder in SCA machine and zip the entire WebGoat 5.0 source code as a Zip file.



In IQ Server's WebGoat5Test application, click Actions -> Evaluate Binary.

Evaluate a Binary

Select the file you want evaluated

Choose file

WebGoat5.0.zip

Which stage should this evaluation be associated with?

Build

Should notifications be sent if this application violates any policies?

☒ Yes

☐ No

Upload

Cancel

Select the WebGoat5.0.zip file and stage as Build. Click Upload.

Evaluation Status

Closing this panel will not interrupt the evaluation. It will still progress until it is complete. When the evaluation has been completed you can view the results by clicking on the button below.

File:

WebGoat5.0.zip

Application:

WebGoat5Test

Stage:

Build

Fingerprinting components

View Report

Close

The IQ Server will start evaluation.

Evaluation Status

Closing this panel will not interrupt the evaluation. It will still progress until it is complete. When the evaluation has been completed you can view the results by clicking on the button below.

File:

WebGoat5.0.zip

Application:

WebGoat5Test

Stage:

Build

Done

View Report

Close

Click View Report.

WebGoat5Test Build Report

2021-02-15 11:37:34 UTC+0530

21 64 12 97 VIOLATIONS Affecting 31 components 51 COMPONENTS 88% of all components identified 0 GRANDFATHERED violations

THREAT	POLICY	COMPONENT
10	Security-Critical	apache-collections : commons-collections : 3.1
10	Security-Critical	apache-log4j : log4j : 1.2.8
10	Security-Critical	log4j : log4j : 1.2.9
9	Security-High	apache-taglibs : standard : 1.1.2
9	Security-High	axis : axis : 1.2
9	Security-High	struts : struts : 1.2.8
9	Security-High	tomcat : catalina : 5.5.4
9	Security-High	tomcat : catalina-optional : 5.5.4
9	Security-High	tomcat : jasper-runtime : 5.0.25

Options menu:

- Generate PDF
- View raw data
- View vulnerabilities
- View legacy report

Click Options -> View Vulnerabilities.

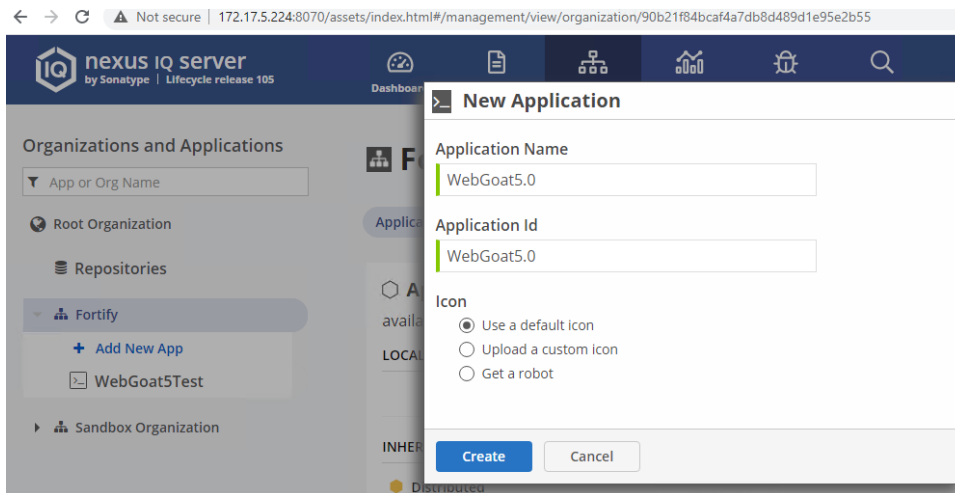
Vulnerabilities for WebGoat5Test Build Report

2021-02-15 11:37:34 UTC+0530

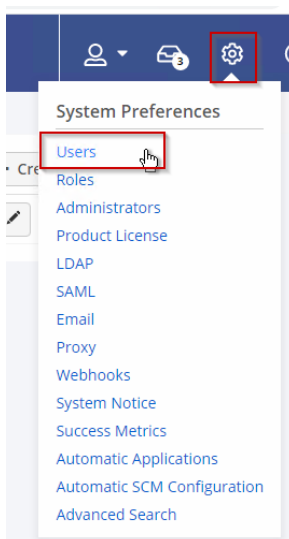
THREAT	SECURITY ISSUE	CVSS SCORE	COMPONENT
10	CVE-2019-17571	9.8	apache-log4j : log4j : 1.2.8
10	CVE-2019-17571	9.8	log4j : log4j : 1.2.9
10	sonatype-2015-0002	9.0	apache-collections : commons-collections : 3.1
9	CVE-2016-1182	8.2	struts : struts : 1.2.8
9	CVE-2016-1181	8.1	struts : struts : 1.2.8
9	CVE-2006-1547	7.8	struts : struts : 1.2.8
9	sonatype-2010-0053	7.8	apache-log4j : log4j : 1.2.8
9	sonatype-2010-0053	7.8	log4j : log4j : 1.2.9

If you are able to see Vulnerabilities report then we are good for next step.

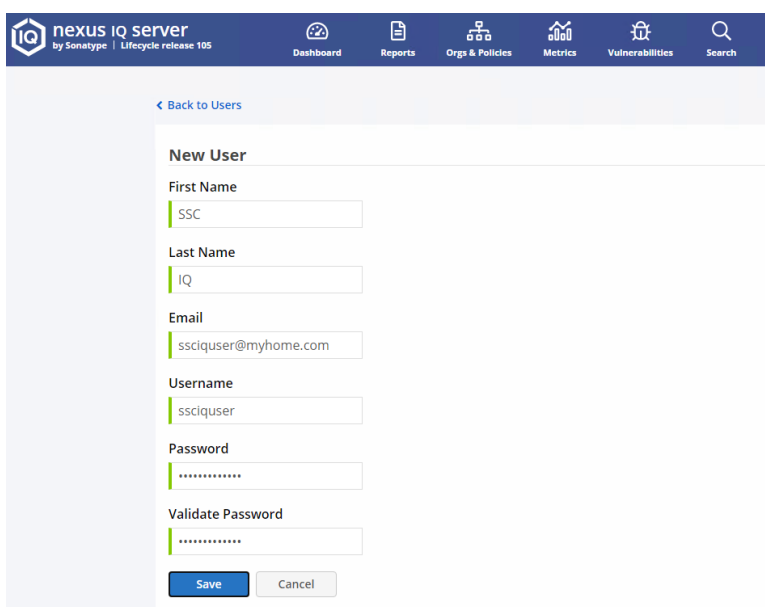
Delete the WebGoat5.0.zip file from Samples folder, this file is no longer needed.



Click on Fortify Organization, and create an Application named "WebGoat5.0" with the Application ID as "WebGoat5.0".

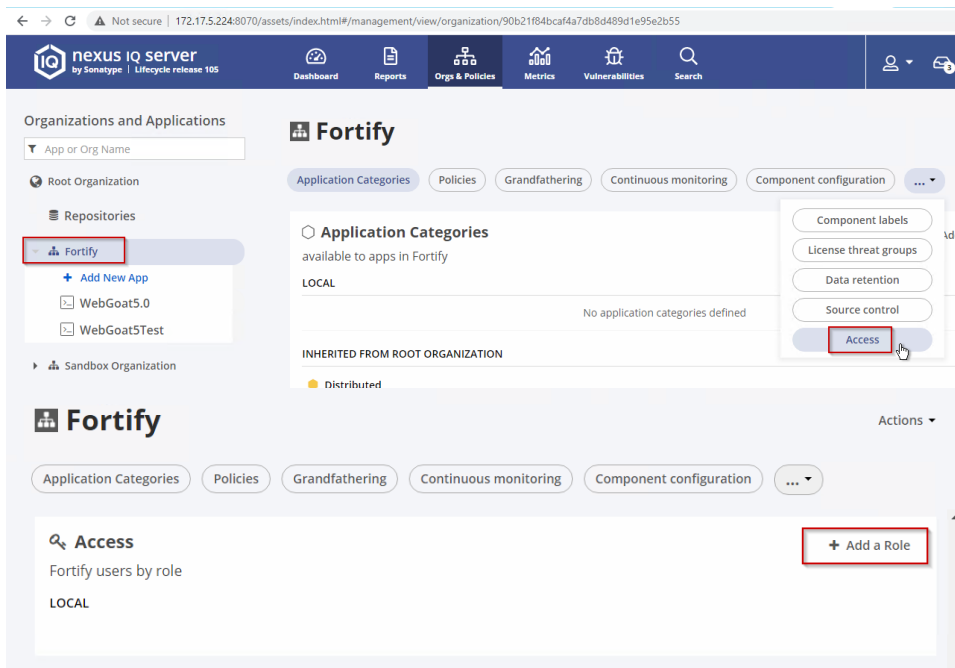


Create a user named "ssciquser" with the password "ssciquser@123" in Settings -> Users -> Create User.

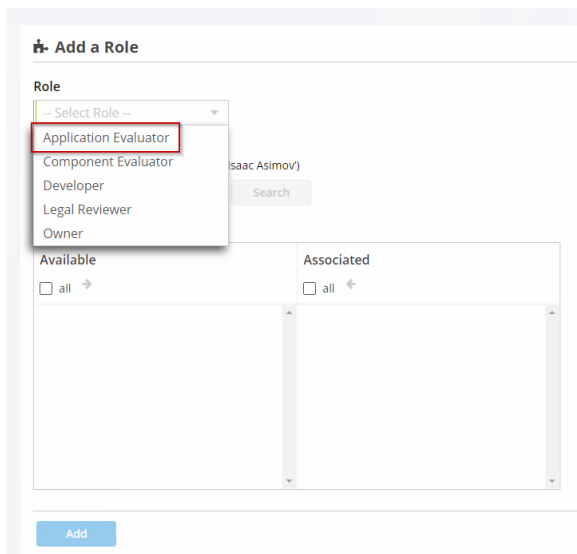


Click Save.

We will use this user in SCA. Lets assign this user in Fortify Organization as "Application Evaluator", "Component Evaluator" and "Developer" role.



Click "Add a Role".



From Role drop down, select "Application Evaluator" role.

Add a Role

Role
Application Evaluator

Search Users
use "*" as wildcard (ex. "Isa*" matches "Isaac Asimov")

* Search

Associated Users

Available	Associated
<input type="checkbox"/> all →	<input type="checkbox"/> all ←
<input type="checkbox"/> Admin BuiltIn <input type="checkbox"/> Authenticated Users <input checked="" type="checkbox"/> SSC IQ	

Add

Enter "*" in Search Users and Click Search, it will display all the users. Select the check box before "SSC IQ" user and click the Right Arrow.

Add a Role

Role
Application Evaluator

Search Users
use "*" as wildcard (ex. "Isa*" matches "Isaac Asimov")

* Search

Associated Users

Available	Associated
<input type="checkbox"/> all →	<input type="checkbox"/> all ←
<input type="checkbox"/> Admin BuiltIn <input type="checkbox"/> Authenticated Users	<input checked="" type="checkbox"/> SSC IQ

Add

Click Add.

Fortify

- Application Categories
- Policies
- Component Labels
- License Threat Groups
- Source Control
- Access
 - Add a Role
 - Application Evaluator

Add a Role

Role
-- Select Role --

Component Evaluator
Developer
Legal Reviewer
Owner

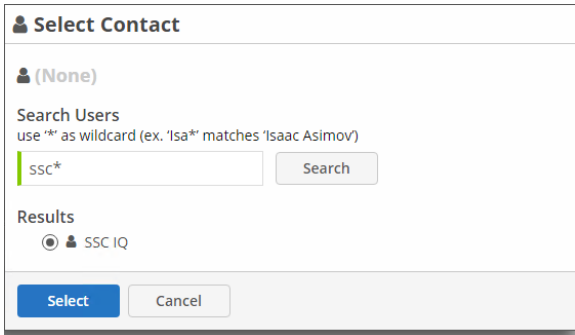
Associated Users

Available	Associated
<input type="checkbox"/> all →	<input type="checkbox"/> all ←

Add

Repeat the same steps for "Component Evaluator" and "Developer" role.

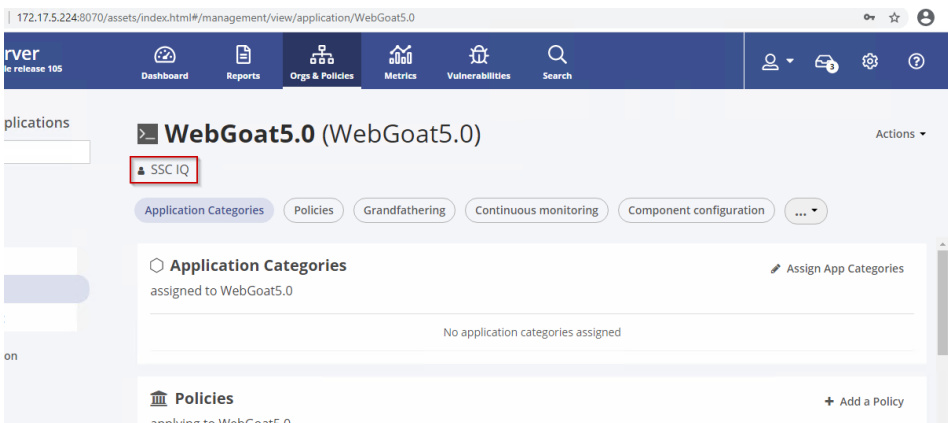
To assign the point of contact for the application. Open WebGoat5.0 Application in Fortify Organization. Click Actions -> Select Contacts.



The "Select Contact" dialog box is shown. It has a title bar with a person icon and the text "Select Contact". Below the title bar, there is a section labeled "(None)" with a person icon. Underneath, it says "Search Users" and "use * as wildcard (ex. 'Isa*' matches 'Isaac Asimov')". There is a search input field containing "ssc*" and a "Search" button. Below the search field, there is a "Results" section showing a single result: "SSC IQ" with a person icon and a radio button. At the bottom, there are "Select" and "Cancel" buttons.

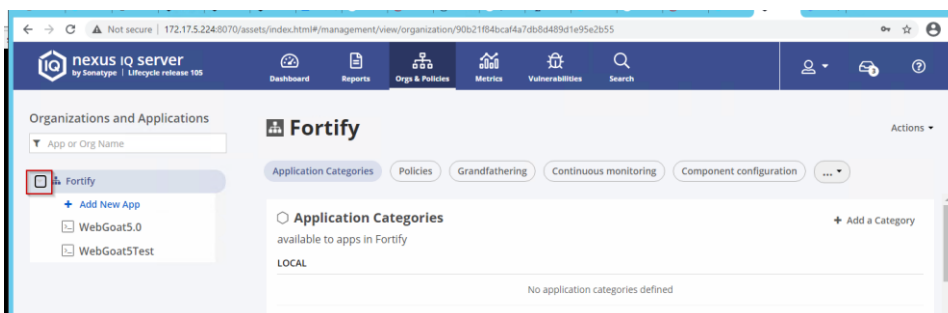
Search for "ssc*" and select "SSC IQ" user which was created for SCA integration.

Click Select.



Notice the change.

Logout from IQ Server and login as "ssciquser" with the password "ssciquser@123"



Expand the Fortify Organization and validate both applications are listed there.

Installing Sonatype SSC plugin

Download the plugin from <https://marketplace.microfocus.com/fortify/content/sonatype-nexus-lifecycle-integration-with-ssc> into Downloads folder.



The image shows a marketplace listing for the Sonatype Nexus Lifecycle integration with SSC. It includes the Sonatype logo, a 'DOWNLOAD V 20.1' button, a 'See previous releases' link, and icons for 'Share' and 'Subscribe'. The description states: 'This bundle contains the parser plugin for Software Security Center and an integration service that can integrate results from Sonatype's Nexus Lifecycle alongside findings from SCA, providing a consolidated view of application vulnerabilities.' It also shows a rating of 2 reviews and 532 downloads. At the bottom, it lists 'PRODUCT COMPATIBILITY: Fortify Software Security Center' and 'CATEGORY: Open Source'.

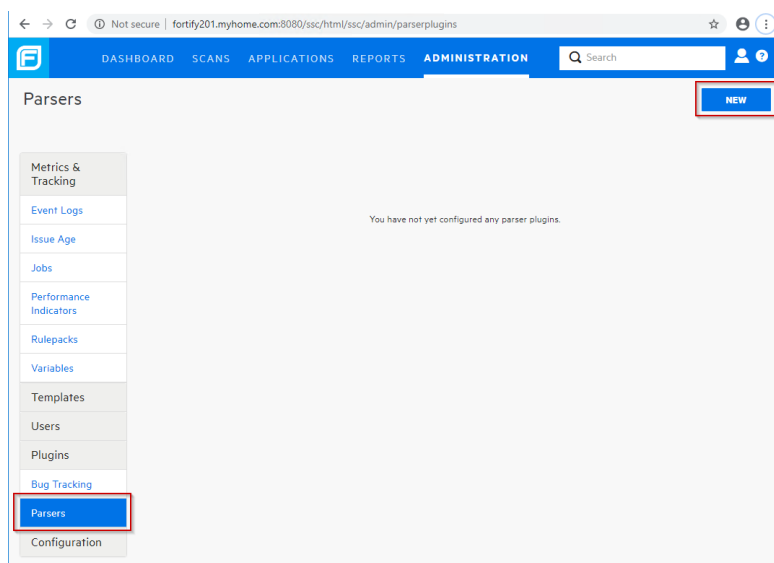
Download and extract the available latest version.

View

Local Disk (C:) > Users > Administrator > Downloads > SonatypeFortifyBundle-20.1 > SonatypeFortifyBundle-20.1

Name	Date modified	Type	Size
IntegrationService	31-01-2021 18:08	File folder	
InstallationGuide-22Oct2019	31-01-2021 18:08	Chrome HTML Do...	321 KB
sonatype-plugin-20.1.20200914	31-01-2021 18:08	Executable Jar File	1,829 KB


Login into SSC as admin -> Administration -> Plugins -> Parsers -> New.



The screenshot shows the Fortify SSC Administration interface. The 'ADMINISTRATION' tab is selected. In the left sidebar, 'Parsers' is highlighted. In the main content area, there is a 'NEW' button in the top right corner. The main area also displays a message: 'You have not yet configured any parser plugins.'

Click New.

UPLOAD PLUGIN WARNING

 You are uploading a plugin that you have written, obtained from a third party, or that was provided to you by Micro Focus Fortify.

Plugins provided by Micro Focus Fortify have been developed securely and are tested to work as described within Software Security Center. Plugins not provided by Micro Focus Fortify should be examined for security defects and tested to ensure they do not contain security vulnerabilities and perform only their advertised features.

Please acknowledge this risk by selecting "OK".

CANCEL **OK**

Click OK on the warning.

UPLOAD PLUGIN BUNDLE

Plugin Bundle jar file*

sonatype-plugin-20.1.20200914.jar

BROWSE...

REMOVE

CANCEL

START UPLOAD

Browse and select the SonaType plugin jar file and click Start Upload.

	Name	Description	Plugin Version	Data Version	Engine Type	Plugin State
Metrics & Tracking	Sonatype Vulnerability Parser	Sonatype scan result parser	20.1.20200914	1		DISABLED
Event Logs						
Issue Age						

Click on the Plugin.

Tracking

Event Logs

Issue Age

Jobs

Performance Indicators

Rulepacks

Variables

Templates

Users

Plugins

Bug Tracking

Parsers

Configuration

Sonatype Vulnerability Parser

Sonatype scan result parser

20.1.20200914

1

DISABLED

Name

Sonatype Vulnerability Parser

Description

Sonatype scan result parser

Properties

Value

Vendor Name

Sonatype

Vendor URL

https://www.sonatype.com/

Plugin Version

20.1.20200914

Supported Engine Versions

Engine Type

Data Version

1

API Version

1.0

Plugin Identifier

com.sonatype.iq.parser

ENABLE

REMOVE

Click Enable.

ENABLE PLUGIN WARNING

⚠ You are enabling a plugin that you have written, obtained from a third party, or that was provided to you by Micro Focus Fortify.

Plugins provided by Micro Focus Fortify have been developed securely and are tested to work as described within Software Security Center. Plugins not provided by Micro Focus Fortify should be examined for security defects and tested to ensure they do not contain security vulnerabilities and perform only their advertised features.

Please acknowledge this risk by selecting "OK".

CANCEL

OK

Click OK on the Warning.

Tracking

Event Logs

Issue Age

Jobs

Performance Indicators

Rulepacks

Workflows

Sonatype Vulnerability Parser

Sonatype scan result parser20.1.202009141

Name

Sonatype Vulnerability Parser

Description

Sonatype scan result parser

Request to enable plugin "Sonatype Vulnerability Parser" version "20.1.20200914" was submitted.

more...

F

DASHBOARDAPPLICATIONSREPORTSADMINISTRATION

Q Search

?

Parsers

NEW

Metrics & Tracking

Event Logs

Issue Age

Name	Description	Plugin Version	Data Version	Engine Type	Plugin State
Sonatype Vulnerability Parser	Sonatype scan result parser	20.1.20200914	1	SONATYPE	ENABLED

Now Plugin is Enabled.

Installing SourceAndLibScanner

Download SourceAndLibScanner CLI Tool from <https://marketplace.microfocus.com/fortify/content/fortify-sourceandlibscanner> into Downloads folder.

The screenshot shows the product page for Fortify SourceAndLibScanner. At the top, there's a navigation bar with links to Fortify Products, Securing DevOps, Digital Transformation, Contact us, and Hi Vikas. Below this, the product name 'Fortify SourceAndLibScanner' is displayed with a 'DOWNLOAD V 20.2.0' button and a link to 'See previous releases'. The product is described as a command-line interface that combines Fortify Static Code Analyzer and Sonatype scan. It has 0 reviews and 393 downloads. There are also 'Share' and 'Subscribe' buttons.

Extract the downloaded zip file.

The screenshot shows a Windows File Explorer window with the path 'PC > Downloads > Fortify_SourceAndLibScanner_20.2.0_x64 > Fortify_SourceAndLibScanner_20.2.0_x64'. The table below lists the contents of this folder.

Name	Date modified	Type	Size
bin	31-01-2021 18:17	File folder	
Core	06-11-2020 08:49	File folder	
LICENSE	31-01-2021 18:17	File folder	
SourceAndLibScanner_20.2.0	31-01-2021 18:17	Chrome HTML Do...	173 KB

Copy all the files from the "bin" folder to "C:\Program Files\Fortify\Fortify_SCA_and_Apps_20.2.0\bin" folder.

The screenshot shows two Windows File Explorer windows. The top window is the 'bin' folder from the previous step, with a red box highlighting the 'sourceandlibscanner' file and its batch file. The bottom window is the destination folder 'C:\Program Files\Fortify\Fortify_SCA_and_Apps_20.2.0\bin', with a red box highlighting the 'sourceandlibscanner' file and its batch file. A red arrow points from the source file to the destination file, indicating the copy operation.

Name	Date modified	Type	Size
sourceandlibscanner	31-01-2021 18:17	File	3 KB
sourceandlibscanner	31-01-2021 18:17	Windows Batch File	2 KB

Name	Date modified	Type	Size
scancentral-worker-service	31-01-2021 18:21	File folder	
auditworkbench	13-10-2020 21:21	Windows Comma...	2 KB
autoupdate-windows	13-10-2020 21:21	Application	9,349 KB
BIRTReportGenerator	13-10-2020 21:21	Windows Comma...	3 KB
CustomRulesEditor	13-10-2020 21:21	Windows Comma...	2 KB
fortifyclient	13-10-2020 21:21	Windows Batch File	2 KB
fortifyupdate	13-10-2020 21:21	Windows Comma...	2 KB
IPRUtility	13-10-2020 21:21	Windows Batch File	2 KB
indmigrator	13-10-2020 21:21	Windows Batch File	2 KB
packageScanner	13-10-2020 21:30	Windows Batch File	2 KB
pwtool	13-10-2020 21:30	Windows Batch File	3 KB
ReportGenerator	13-10-2020 21:21	Windows Batch File	2 KB
scancentral	13-10-2020 21:30	Windows Batch File	3 KB
ScanVizard	13-10-2020 21:21	Windows Comma...	2 KB
scapostinstall	13-10-2020 21:21	Windows Comma...	2 KB
SCAState	13-10-2020 21:21	Windows Comma...	2 KB
sourceanalyzer	13-10-2020 21:21	Application	504 KB
sourceandlibscanner	31-01-2021 18:17	File	3 KB
sourceandlibscanner	31-01-2021 18:17	Windows Batch File	2 KB
update	13-10-2020 21:21	Configuration sett...	0 KB

Also, copy the files and folder from "Core\lib" to "C:\Program Files\Fortify\Fortify_SCA_and_Apps_20.2.0\Core\lib", do not overwrite any file if there is conflict on the files.

Using SourceAndLibScanner

- Scan your code with SCA and Sonatype (via the Open Source Component Scan Service), and then upload both results to SSC
- Scan your code with SCA and Sonatype, then upload both results to SSC and the Sonatype results to an on-premises Lifecycle product (Nexus IQ Server)
- Scan your code with SCA scans of your code OR perform Sonatype scans of your third-party components, for the Sonatype only option, you must use our -bt none option, executed in the top level dir, as we need to pass the libraries to the utility.

```
sourceandlibscanner -h
```

Displays the help of SourceAndLibScanner.

```
sourceandlibscanner -version
```

Displays the version of SourceAndLibScanner.

Scanning WebGoat via SourceAndLibScanner

CREATE NEW APPLICATION VERSION

1. General

STEP 1. GENERAL

Application Setup ⓘ

Application name*

WebGoat via SonaType

Application description

Description of application

☐ Add to existing application ⓘ

Version Setup ⓘ

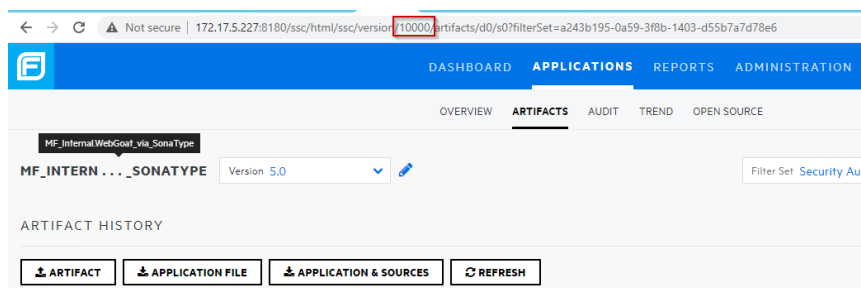
Version name*

5.0

Version description

Description of version

Create a new Application named "MF_Internal.WebGoat_via_SonaType" and version as "5.0".



Identify the version id, as above (it is 10000 for this application) or use fortifyclient to identify the application's version id.

Generate a CIToken Use Administration -> Users -> Token Management -> New. Select Token Type as CI Token.

Note down the CIToken for Tools, we will be using this token in SCA.

Manual invocation of SCA and the Fortify / Sonatype Open Source Scanning Service

Run the below command in "C:\Program

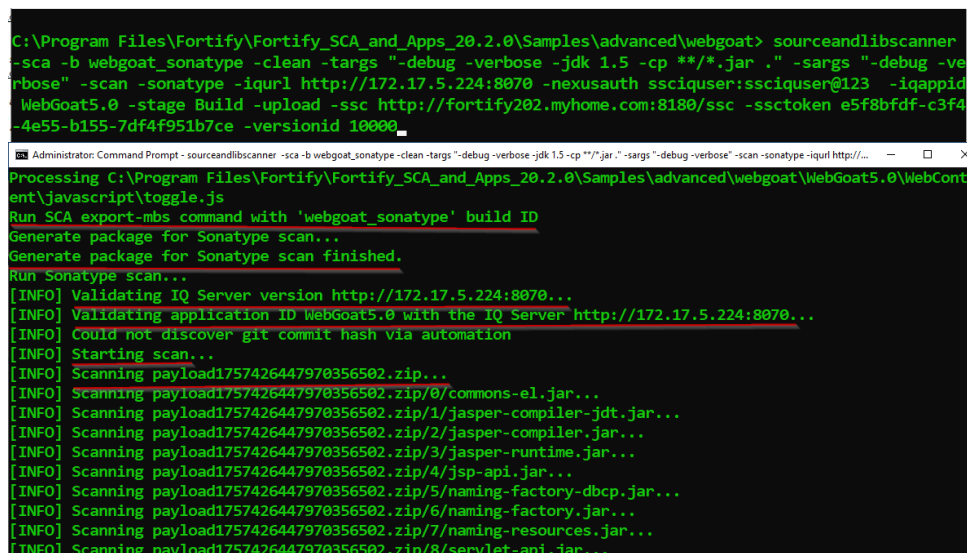
Files\Fortify\Fortify_SCA_and_Apps_20.2.0\Samples\advanced\webgoat" folder.

```
sourceandlibscanner -sca -b webgoat_sonatype -clean -targs "-  
verbose -cp -jdk 1.5 **/*.jar ." -sargs "-verbose" -scan -sonatype  
-libscanurl https://ds.sonatype.com -nexusauth <SonaType_Token> -  
upload -ssc http://fortify202.myhome.com:8080/ssc -ssctoken  
6e057de0-87b8-4430-a606-da2dad049c0d -versionid 10000
```

While using IQ Server (-debug and -verbose is optional)-

```
sourceandlibscanner -sca -b webgoat_sonatype -clean -targs "-debug  
-verbose -jdk 1.5 -cp **/*.jar ." -sargs "-debug -verbose" -scan -  
sonatype -iqurl http://172.17.5.224:8070 -nexusauth  
ssciquser:ssciquser@123 -iqappid WebGoat5.0 -stage Build -upload -  
ssc http://fortify202.myhome.com:8180/ssc -ssctoken e5f8bfdf-c3f4-  
4e55-b155-7df4f951b7ce -versionid 10000
```

Note: Source path must be last command in **targs**



```
C:\Program Files\Fortify\Fortify_SCA_and_Apps_20.2.0\Samples\advanced\webgoat> sourceandlibscanner  
-sca -b webgoat_sonatype -clean -targs "-debug -verbose -jdk 1.5 -cp **/*.jar ." -sargs "-debug -ve  
rbose" -scan -sonatype -iqurl http://172.17.5.224:8070 -nexusauth ssciuser:ssciuser@123 -iqappid  
WebGoat5.0 -stage Build -upload -ssc http://fortify202.myhome.com:8180/ssc -ssctoken e5f8bfdf-c3f4-  
4e55-b155-7df4f951b7ce -versionid 10000  
Administrator: Command Prompt - sourceandlibscanner -sca -b webgoat_sonatype -clean -targs "-debug -verbose -jdk 1.5 -cp **/*.jar ." -sargs "-debug -verbose" -scan -sonatype -iqurl http://...  
Processing C:\Program Files\Fortify\Fortify_SCA_and_Apps_20.2.0\Samples\advanced\webgoat\WebGoat5.0\WebCont  
ent\javascript\toggle.js  
Run SCA export-mbs command with 'webgoat_sonatype' build ID  
Generate package for Sonatype scan...  
Generate package for Sonatype scan finished.  
Run Sonatype scan...  
[INFO] Validating IQ Server version http://172.17.5.224:8070...  
[INFO] Validating application ID WebGoat5.0 with the IQ Server http://172.17.5.224:8070...  
[INFO] Could not discover git commit hash via automation  
[INFO] Starting scan...  
[INFO] Scanning payload1757426447970356502.zip...  
[INFO] Scanning payload1757426447970356502.zip/0/commons-el.jar...  
[INFO] Scanning payload1757426447970356502.zip/1/jasper-compiler-jdt.jar...  
[INFO] Scanning payload1757426447970356502.zip/2/jasper-compiler.jar...  
[INFO] Scanning payload1757426447970356502.zip/3/jasper-runtime.jar...  
[INFO] Scanning payload1757426447970356502.zip/4/jsp-api.jar...  
[INFO] Scanning payload1757426447970356502.zip/5/naming-factory-dbc.jar...  
[INFO] Scanning payload1757426447970356502.zip/6/naming-factory.jar...  
[INFO] Scanning payload1757426447970356502.zip/7/naming-resources.jar...  
[INFO] Scanning payload1757426447970356502.zip/8/servlet-api.jar...
```

During the scan you can see the number of issues identified by IQ Server.

```

Administrator: Command Prompt - sourceandibscanner -sca -b webgoat_sonatype -clean -targs "-debug -verbose -jdk 1.5 -cp ""/"" -sargs "-debug -verbose" -scan -sonatype -iurl http://...
[INFO]
[INFO]
[INFO]
[INFO]
[INFO] *****
[INFO] Policy Action: None
[INFO] Stage: build
[INFO] Number of components affected: 12 critical, 13 severe, 6 moderate
[INFO] Number of open policy violations: 21 critical, 64 severe, 12 moderate
[INFO] Number of grandfathered policy violations: 0
[INFO] The detailed report can be viewed online at http://172.17.5.224:8070/ui/links/application/WebGoat5.0
/report/a035d0a418474df882cee2c861d5033e
[INFO] *****
Sonatype scan finished.
Generate Sonatype based rules...
Sonatype based rules generation failed. See log for details.
Run SCA scan command with 'webgoat_sonatype' build ID
Fortify Static Code Analyzer 20.2.0.0139 (using JRE 1.8.0_181)
Analyzing 190 source file(s)

```

The URL is the direct link of the report.

```

Administrator: Command Prompt
/report/a035d0a418474df882cee2c861d5033e
[INFO] *****
Sonatype scan finished.
Generate Sonatype based rules...
Sonatype based rules generation failed. See log for details.
Run SCA scan command with 'webgoat_sonatype' build ID
Fortify Static Code Analyzer 20.2.0.0139 (using JRE 1.8.0_181)
Analyzing 190 source file(s)
Configuration analysis complete
Rendering 1164 results
Analysis completed in 02:52
SCA execution finished.
Convert Sonatype report for uploading to SSC...
Sonatype report conversion finished.
Start uploading SCA results to SSC...
Uploading SCA results to SSC finished.
Start uploading Sonatype results to SSC...
Uploading Sonatype results to SSC finished.
C:\Program Files\Fortify\Fortify_SCA_and_Apps_20.2.0\Samples\advanced\webgoat>

```

Check the on-screen information.

Open SSC and open the artifacts of the application.

The screenshot shows the Fortify SSC web interface. The top navigation bar includes 'DASHBOARD', 'APPLICATIONS', 'REPORTS', and 'ADMINISTRATION'. The 'APPLICATIONS' tab is active, and the 'ARTIFACTS' sub-tab is selected. The main content area shows a table of artifacts. The first artifact is 'MF_INTERN..._SONATYPE' with a status of 'Complete' and a scan artifact 'ssc-tp3070300013578871016.zip'. Below the table are buttons for 'DOWNLOAD', 'DOWNLOAD WITH SOURCES', 'APPROVE', 'PURGE', and 'DELETE'.

The ZIP file uploaded by Sonatype will be listed in the Artifacts section, click on Audit.

In the Filter select SONATYPE.

MF_INTERN..._SONATYPE Version: 5.0 Filter Set: Security Auditor View

Search issues Group by Select attributes Filter by SONATYPE

20 0 0 0 00 ASSIGN CLAIM SUPPRESS UNSUPPRESS REFRESH EXPORT 0 of 80 issues selected

Category	Primary Location	Analysis Type	Criticality
Vulnerable OSS	jasper-runtime@5.5.4?type=jar	SONATYPE	Critical
Vulnerable OSS	log4j@1.2.8?type=jar	SONATYPE	Critical
Vulnerable OSS	log4j@1.2.8?type=jar	SONATYPE	Critical
Vulnerable OSS	commons-collections@3.1?type=jar	SONATYPE	Critical
Vulnerable OSS	log4j@1.2.9?type=jar	SONATYPE	Critical
Vulnerable OSS	log4j@1.2.9?type=jar	SONATYPE	Critical
Vulnerable OSS	struts@1.2.8?type=jar	SONATYPE	Critical
Vulnerable OSS	struts@1.2.8?type=jar	SONATYPE	Critical
Vulnerable OSS	struts@1.2.8?type=jar	SONATYPE	Critical

Expand the vulnerability identified by Sonatype and check the details provided by Sonatype.

Vulnerable OSS jasper-runtime@5.5.4?type=jar SONATYPE Critical

SONATYPE COMMENTS & HISTORY ATTACHMENTS SUPPRESS

Vulnerability Description

Recommended Version(s): No recommended versions are available for the current component.

In Apache Tomcat 9.0.0.M1 to 9.0.0.M9, 8.5.0 to 8.5.4, 8.0.0.RC1 to 8.0.36, 7.0.0 to 7.0.70 and 6.0.0 to 6.0.45 a malicious web application was able to bypass a configured SecurityManager via a Tomcat utility method that was accessible to web applications.

Full Sonatype Scan Report

Report URL <http://172.17.5.224:8070/assets/index.html#/applicationReport/WebGoat5.0/a035d0a418474df882cee2c861d5033e/vulnerabilities>

Issue CVE-2016-5018

Source National Vulnerability Database

SONATYPE Threat Level 9

CWE CWE 254

CWE URL <https://cwe.mitre.org/data/definitions/254.html>

CWE ID <https://172.17.5.224:8070/utilities/index.html/CVE-2016-5018>

Component Details

Group tomcat

Artifact jasper-runtime

Version 5.5.4

Click on OPEN SOURCE tab.

Component	CVE	Version	Priority	Type	License
apache-collections/commons-collections	sonatype-2015-0002	3.1	Critical		
apache-log4j/log4j	CVE-2019-17571	1.2.8	Critical		
apache-log4j/log4j	sonatype-2010-0053	1.2.8	Critical		
apache-taglibs/standard	CVE-2015-0254	1.1.2	Critical		
axis/axis	CVE-2007-2353	1.2	Critical		
axis/axis	CVE-2012-5784	1.2	Critical		
axis/axis	CVE-2014-3596	1.2	Critical		
axis/axis	CVE-2019-0227	1.2	Critical		
commons-modeler/commons-modeler	sonatype-2008-0022	1.1	Critical		

Expand the Vulnerability.

Component	CVE	Version	Priority	Type	License
apache-collections/commons-collections	sonatype-2015-0002	3.1	Critical		

File Name	pkg:maven/apache-collections/commons-collections@3.1.1?type=jar	Category	Vulnerable OSS
Priority	Critical	CVE	sonatype-2015-0002
Evidence	None	CWE	CWE-502
Invoked	No	Controllable	No

Analysis Not Set

Comments

Suppress ☐

CANCEL SAVE

Auditing can be done on this page as well.

Login into IQ Server using user as "ssciquser" and the password "ssciquser@123" and click Reports.

APPLICATION NAME	CONTACT	ORGANIZATION	BUILD VIOLATIONS	STAGE RELEASE VIOLATIONS	RELEASE VIOLATIONS
WebGoat5.0	SSC IQ	Fortify	21 64 12 View Report (28 minutes ago)		
WebGoat5Test		Fortify	21 64 12 View Report (2 hours ago)		

Click on View Report.

WebGoat5.0 Build Report
2021-02-15 13:01:53 UTC+0530

97 VIOLATIONS Affecting 31 components
50 COMPONENTS 88% of all components identified
0 GRANDFATHERED violations

THREAT	POLICY	COMPONENT
10	Security-Critical	apache-collections:commons-collections:3.1
10	Security-Critical	apache-log4j:log4j:1.2.8
10	Security-Critical	log4j:log4j:1.2.9
9	Security-High	apache-taglibs:standard:1.1.2
9	Security-High	axis:axis:1.2
9	Security-High	struts:struts:1.2.8
9	Security-High	tomcat:catalina:5.5.4
9	Security-High	tomcat:catalina-optional:5.5.4
9	Security-High	tomcat:jasper-runtime:5.0.25
9	Security-High	tomcat:jasper-runtime:5.5.4

Open the Component listed in the report.

apache-collections:commons-collections:3.1 Direct Dependency

COMPONENT INFO POLICY SIMILAR OCCURRENCES LICENSES **VULNERABILITIES** LABELS AUDIT LOG

Recommended Version(s)
The current version doesn't cause Build failure

Version Graph
Popularity: [Graph showing popularity over time]
Policy Threat: 10 (Critical)

Selected Version: 3.1
Type: maven
Group: apache-collections
Artifact: commons-collections
Version: 3.1
Declared License: Not Declared
Observed License: No Sources
Effective License: Not Declared, No Sources
Highest Policy Threat: 10 within 2 policies
Highest CVSS Score: 9
Integrity Rating: Not Applicable
Cataloged: 4 years ago
Match State: exact
Identification Source: Sonatype
Category: Other

Explore the various options.

The short version of the command is below, where we can use build type to none.

```
sourceandlibscanner -auto -bt none -scan -sonatype -iqurl
http://172.17.5.224:8070 -nexusauth ssciquser:ssciquser@123 -
iqappid WebGoat5.0 -stage build -upload -ssc
http://fortify202.myhome.com:8180/ssc -ssctoken e5f8bfdf-c3f4-4e55-
b155-7df4f951b7ce -versionid 10000
```

Scanning WebGoat via SonaType only

Create a new version "6.0" of Application named "MF_Internal.WebGoat_via_SonaType" and note down the version id.

Run the below command in "C:\Program

Files\Fortify\Fortify_SCA_and_Apps_20.2.0\Samples\advanced\webgoat" folder
notice it is missing "-scan"

```
sourceandlibscanner -sca -b webgoat_sonatype -clean -targs "-debug
-verbose -jdk 1.5 -cp **/*.jar ." -sargs "-debug -verbose" -
sonatype -iqurl http://172.17.5.224:8070 -nexusauth
ssciquser:ssciquser@123 -iqappid WebGoat5.0 -stage Build -upload -
ssc http://fortify202.myhome.com:8180/ssc -ssctoken e5f8bdfd-c3f4-
4e55-b155-7df4f951b7ce -versionid 10001
```

or

```
sourceandlibscanner -auto -bt none -sonatype -iqurl
http://172.17.5.224:8070 -nexusauth ssciuser:ssciuser@123 -
iqappid WebGoat5.0 -stage build -upload -ssc
http://fortify202.myhome.com:8180/ssc -ssctoken e5f8bdfd-c3f4-4e55-
b155-7df4f951b7ce -versionid 10001
```

```
Administrator: Command Prompt - sourceandlibscanner -auto -bt none -sonatype -iqurl http://172.17.5.224:8070 -nexusauth ssciuser:ssciuser@123 -iqappid WebGoat5.0 -stage build -upload -ssc...
C:\Program Files\Fortify\Fortify_SCA_and_Apps_20.2.0\Samples\advanced\webgoat> sourceandlibscanner -auto -bt
none -sonatype -iqurl http://172.17.5.224:8070 -nexusauth ssciuser:ssciuser@123 -iqappid WebGoat5.0 -stage
build -upload -ssc http://fortify202.myhome.com:8180/ssc -ssctoken e5f8bdfd-c3f4-4e55-b155-7df4f951b7ce -vers
ionid 10001
Log files will be stored in "C:\Users\Administrator\AppData\Local\Fortify\sourceandlibscanner-20.2.0\log" dir
ectory.
Start package generation...
Controller URL http://fortify202.myhome.com:8280/scancentral-ctrl found in scancentral.properties
Checking for updates...
No update available or auto update is disabled on the controller.
Log files will be stored in "C:\Users\Administrator\AppData\Local\Fortify\sourceandlibscanner-20.2.0\log" dir
ectory.
Gathering project information...
Packaging project...
Package generation finished.
Run Sonatype scan...
[INFO] Validating IQ Server version http://172.17.5.224:8070...
[INFO] Validating application ID WebGoat5.0 with the IQ Server http://172.17.5.224:8070...
[INFO] Could not discover git commit hash via automation
[INFO] Starting scan...
[INFO] Scanning fortify-sonatype4806807269240225587.zip...
[INFO] Scanning fortify-sonatype4806807269240225587.zip/Libs/java/-1284376651/servlets-webdav.jar...
[INFO] Scanning fortify-sonatype4806807269240225587.zip/Libs/java/-1284376651/servlets-invoker.jar...
[INFO] Scanning fortify-sonatype4806807269240225587.zip/Libs/java/-1284376651/catalina-cluster.jar...
[INFO] Scanning fortify-sonatype4806807269240225587.zip/Libs/java/-1284376651/catalina-optional.jar...
[INFO] Scanning fortify-sonatype4806807269240225587.zip/Libs/java/-1284376651/catalina.jar...
[INFO] Scanning fortify-sonatype4806807269240225587.zip/Libs/java/-1284376651/servlets-default.jar...
[INFO] Scanning fortify-sonatype4806807269240225587.zip/Libs/java/-1284376651/catalina-ant.jar...
[INFO] Scanning webgoat/WebGoat5.0.zip/WebGoat5.0/WebContent/WEB-INF/lib/wsd14j-1.5.1.jar...
[INFO] Scanning webgoat/WebGoat5.0.zip/WebGoat5.0/WebContent/WEB-INF/lib/xercesImpl-2.0.2.jar...
[INFO] Fingerprinting completed in 7 seconds for 146 archives, 7619 total files
[INFO] Could not discover git repository url via automation
[INFO] Waiting for policy evaluation to complete...
[INFO] Assigned scan ID 29f9b6307fe84efe858c267ae8fbfcd
[INFO] Policy evaluation completed in 27 seconds.
[INFO]
[INFO]
[INFO]
[INFO] *****
[INFO] Policy Action: None
[INFO] Stage: build
[INFO] Number of components affected: 12 critical, 13 severe, 7 moderate
[INFO] Number of open policy violations: 21 critical, 64 severe, 13 moderate
[INFO] Number of grandfathered policy violations: 0
[INFO] The detailed report can be viewed online at http://172.17.5.224:8070/ui/links/application/WebGoat5.0/r
eport/29f9b6307fe84efe858c267ae8fbfcd
[INFO] *****
Sonatype scan finished.
Convert Sonatype report for uploading to SSC...
Sonatype report conversion finished.
Start uploading Sonatype results to SSC...
Uploading Sonatype results to SSC finished.
C:\Program Files\Fortify\Fortify_SCA_and_Apps_20.2.0\Samples\advanced\webgoat>
```

In SSC –

← → ↻ ⚠ Not secure | fortify202.myhome.com:8180/ssc/html/ssc/version/10001/artifacts/d0/s0?filterSet=a243b195-0a59-3f8b-1403-d55b7a7d... 🏠 ☆ 👤

DASHBOARD SCANCENTRAL APPLICATIONS REPORTS ADMINISTRATION

OVERVIEW ARTIFACTS AUDIT TREND OPEN SOURCE

MF_INTERN ..._SONATYPE Version 6.0

Filter Set Security Auditor View

ARTIFACT HISTORY

ARTIFACT
 APPLICATION FILE
 APPLICATION & SOURCES
 REFRESH

Upload Date	Status	Uploaded By	Type	Audits	Scan Artifact
02/15/2021 4:13:22 PM	Complete	admin	SONATYPE		ssc-tp7793795653710949031.zip

Upload IP	172.17.5.227	File Name	ssc-tp7793795653710949031.zip			File Size	30.4 KB
Analysis Type	SONATYPE	Analysis Date	02/15/2021 4:11:21 PM			Certification	NOT PRESENT
Engine Version	1.0	Scan Elapsed Time	Not Available			Hostname	isNew,sscliquer

DOWNLOAD
DOWNLOAD WITH SOURCES
APPROVE
PURGE
DELETE

← → 🔒 Not secure | fortify202.myhome.com:8180/ssc/html/ssc/version/10001/artifacts/d0/s0?filterSet=a243b195-0a59-3f8b-1403-d55b7a7d... ☆

FORTIFY DASHBOARD SCANCENTRAL APPLICATIONS REPORTS ARTIFACTS ADMINISTRATION 🔍 Search 👤 ?

OVERVIEW ARTIFACTS **AUDIT** TREND OPEN SOURCE

MF_INTERN ... _SONATYPE Version: 6.0 🛠️ Filter Set: Security Auditor View ⚙️ +

🔍 Search issues Group by: Select attributes ▼ Filter by: Select attributes ▼

Syntax Guide... Advanced...

80 Critical High Medium Low All

ASSIGN CLAIM SUPPRESS UNSUPPRESS **REFRESH ⓘ** **EXPORT**

0 of 80 issues selected

Category ▾	Primary Location ▾	Analysis Type ▾	Criticality ▴	Tagged ▾	⌂ 🏠 💬
Vulnerable OSS	jasper-runtime@5.5.4?type=jar	SONATYPE	Critical		
Vulnerable OSS	log4j@1.2.87?type=jar	SONATYPE	Critical		
Vulnerable OSS	log4j@1.2.87?type=jar	SONATYPE	Critical		
Vulnerable OSS	commons-collections@3.1.1?type=jar	SONATYPE	Critical		

← → ↻ ⚠ Not secure | fortify202.myhome.com:8180/ssc/html/ssc/version/10001/opensource/d0/s0?filterSet=a243b195-0a59-3f8b-1403-d55b7... 🔑 ☆ 👤

F DASHBOARD SCANCENTRAL APPLICATIONS REPORTS ADMINISTRATION 🔍 Search 👤 ?

OVERVIEW ARTIFACTS AUDIT TREND **OPEN SOURCE**

MF_INTERN ... _SONATYPE Version 6.0 📝 Filter Set Security Auditor View 🔒 +

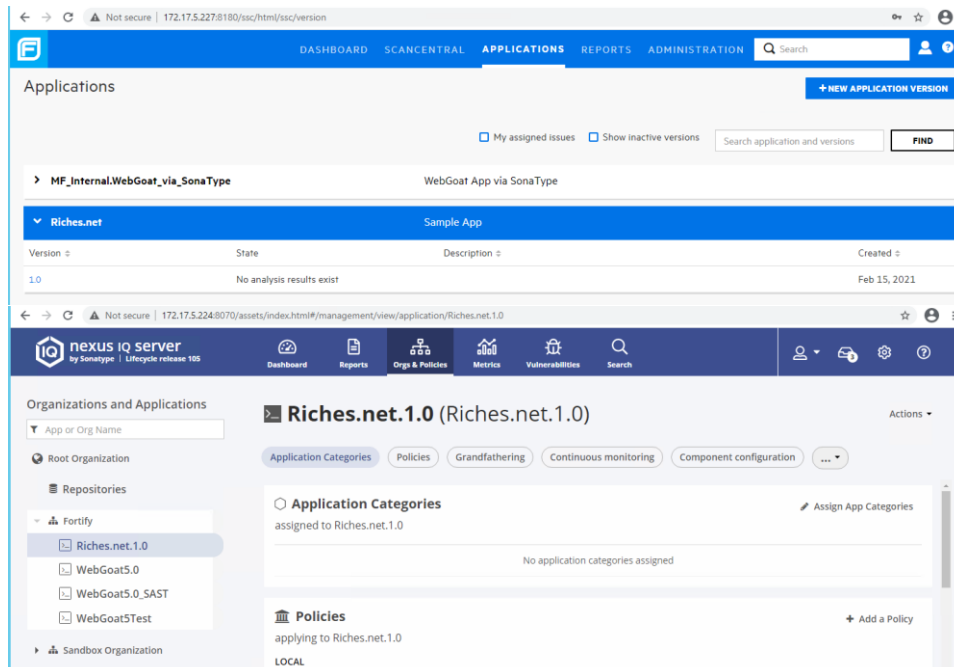
OPEN SOURCE COMPONENTS REFRESH 🔄

▼ SONATYPE					
Component	CVE	Version	Priority	Type	License
> apache-collections/commons-collections	sonatype-2015-0002	3.1	Critical		
> apache-log4j/log4j	CVE-2019-17571	1.2.8	Critical		
> apache-log4j/log4j	sonatype-2010-0053	1.2.8	Critical		
> apache-taglibs/standard	CVE-2015-0254	1.1.2	Critical		
> axis/axis	CVE-2007-2353	1.2	Critical		
> axis/axis	CVE-2012-5784	1.2	Critical		

Scanning Riches.Net Code with Sonatype IQ Server and SCA

Make sure Visual Studio 2019 CE / EE is installed.

Create an application in SSC as "Riches.net" version "1.0" and in IQ Server application name and ID will be "Riches.net.1.0" in Fortify Organization.



Open CMD in C:\Program Files\Fortify\Fortify_SCA_and_Apps_20.2.0\Samples\advanced\riches.net folder. Run the below commands one by one –

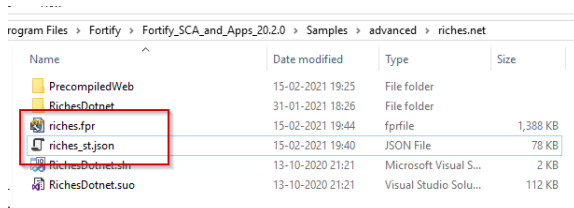
```
MKDIR "C:\hp_la_chouffe\rules\scratch\RichesDotnet\scratch\RichesDotnet"
```

```
"C:\Program Files (x86)\Microsoft Visual  
Studio\2019\Community\Common7\Tools\VsDevCmd.bat"
```

```
sourceandlibscanner -auto -bt msbuild -bf RichesDotnet.sln -scan -  
sonatype -iqurl http://172.17.5.224:8070 -nexusauth  
ssciquser:ssciquser@123 -iqappid Riches.net.1.0 -stage build -f  
riches.fpr -r riches_st.json
```

if everything goes well then you will see two files –

1. riches.fpr containing SCA results
2. riches_st.json containing Sonatype IQ Server results



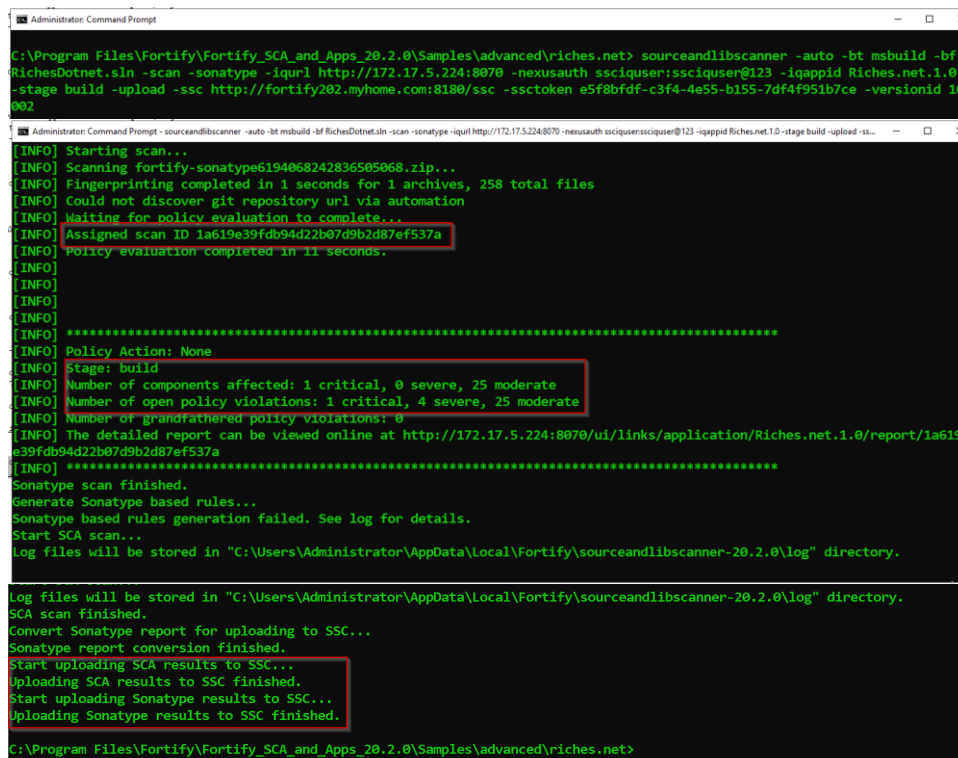
Open these files into respective applications and verify the contents.

Now either delete both files or move it some other folder i.e. Downloads.

Identify the version id of the Riches.net application in SSC or use fortifyclient.

Run the below command after updating the version id.

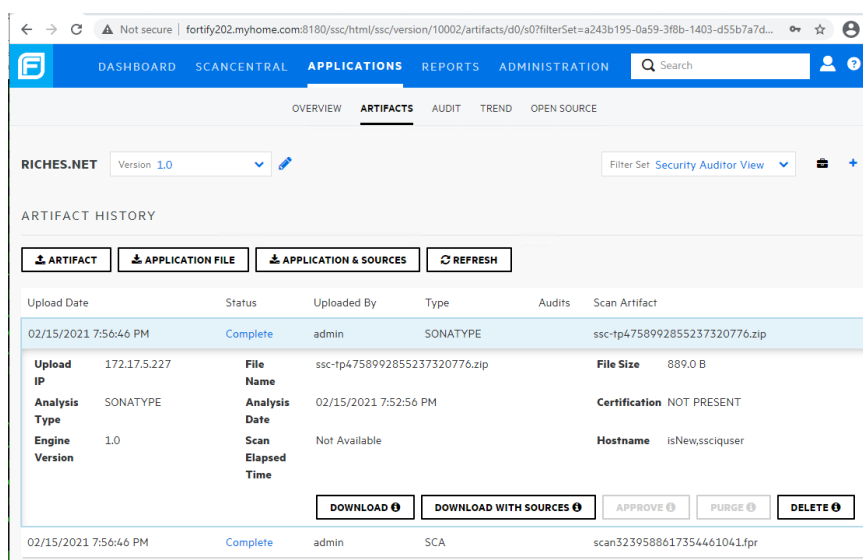
```
sourceandlibscanner -auto -bt msbuild -bf RichesDotnet.sln -scan -  
sonatype -iqurl http://172.17.5.224:8070 -nexusauth  
ssciquser:ssciquser@123 -iqappid Riches.net.1.0 -stage build -  
upload -ssc http://fortify202.myhome.com:8180/ssc -ssctoken  
e5f8bdfd-c3f4-4e55-b155-7df4f951b7ce -versionid 10002
```



```
C:\Program Files\Fortify\Fortify_SCA_and_Apps_20.2.0\Samples\advanced\riches.net> sourceandlibscanner -auto -bt msbuild -bf RichesDotnet.sln -scan -sonatype -iqurl http://172.17.5.224:8070 -nexusauth ssciuser:ssciuser@123 -iqappid Riches.net.1.0 -stage build -upload -ssc http://fortify202.myhome.com:8180/ssc -ssctoken e5f8bdfd-c3f4-4e55-b155-7df4f951b7ce -versionid 10002
```

```
[INFO] Starting scan...  
[INFO] Scanning fortify-sonatype6194068242836505068.zip...  
[INFO] Fingerprinting completed in 1 seconds for 1 archives, 258 total files  
[INFO] Could not discover git repository url via automation  
[INFO] Waiting for policy evaluation to complete...  
[INFO] Assigned scan ID 1a619e39fdb94d22b07d9b2d87ef537a  
[INFO] Policy evaluation completed in 11 seconds.  
[INFO]  
[INFO]  
[INFO]  
[INFO]  
[INFO] Policy Action: None  
[INFO] Stage: build  
[INFO] Number of components affected: 1 critical, 0 severe, 25 moderate  
[INFO] Number of open policy violations: 1 critical, 4 severe, 25 moderate  
[INFO] Number of grandfathered policy violations: 0  
[INFO] The detailed report can be viewed online at http://172.17.5.224:8070/ui/links/application/Riches.net.1.0/report/1a619e39fdb94d22b07d9b2d87ef537a  
[INFO] *****  
Sonatype scan finished.  
Generate Sonatype based rules...  
Sonatype based rules generation failed. See log for details.  
Start SCA scan...  
Log files will be stored in "C:\Users\Administrator\AppData\Local\Fortify\sourceandlibscanner-20.2.0\log" directory.  
Log files will be stored in "C:\Users\Administrator\AppData\Local\Fortify\sourceandlibscanner-20.2.0\log" directory.  
SCA scan finished.  
Convert Sonatype report for uploading to SSC...  
Sonatype report conversion finished.  
Start uploading SCA results to SSC...  
Uploading SCA results to SSC finished.  
Start uploading Sonatype results to SSC...  
Uploading Sonatype results to SSC finished.  
C:\Program Files\Fortify\Fortify_SCA_and_Apps_20.2.0\Samples\advanced\riches.net>
```

Verify in SSC –



Upload Date	Status	Uploaded By	Type	Audits	Scan Artifact
02/15/2021 7:56:46 PM	Complete	admin	SONATYPE		ssc-tp4758992855237320776.zip
Upload IP	172.17.5.227	File Name	ssc-tp4758992855237320776.zip	File Size	889.0 B
Analysis Type	SONATYPE	Analysis Date	02/15/2021 7:52:56 PM	Certification	NOT PRESENT
Engine Version	1.0	Scan Elapsed Time	Not Available	Hostname	isNewssciquser

Buttons: DOWNLOAD, DOWNLOAD WITH SOURCES, APPROVE, PURGE, DELETE

The top screenshot shows the Fortify web interface with the 'AUDIT' tab selected. It displays a table of issues for 'RICHES.NET' version 1.0, filtered by 'SONATYPE'. The table has columns for Category, Primary Location, Analysis Type, Criticality, and Tagged. The issues listed are all 'Vulnerable OSS' with 'jQuery@1.4.1' as the primary location and 'SONATYPE' as the analysis type, all marked as 'Critical'.

The bottom screenshot shows the Fortify web interface with the 'OPEN SOURCE' tab selected. It displays a table of open source components for 'RICHES.NET' version 1.0, filtered by 'SONATYPE'. The table has columns for Component, CVE, Version, Priority, Type, and License. The components listed are all 'pkg-name/jQuery@1.4.1' with various CVEs, all marked as 'Critical'.

Log Files

Log files are located in the following directories:

Windows:

C:\Users\

C:\Users\

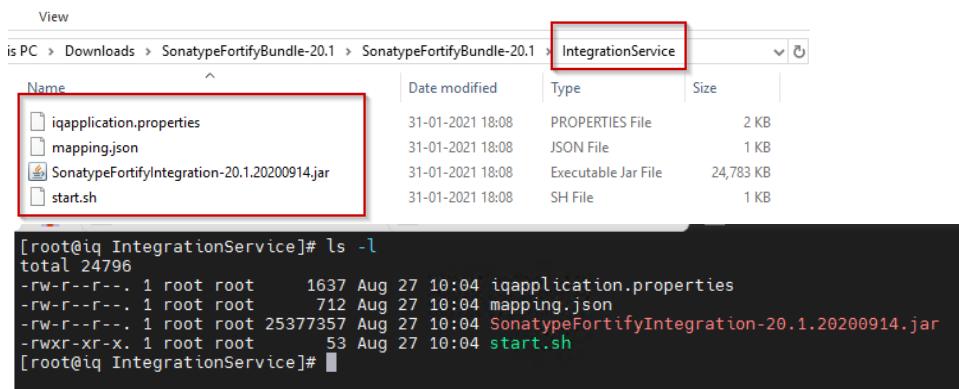
Linux and macOS:

<userhome>/fortify/sca<version>/log

<userhome>/fortify/sourceandlibscanner-<version>/log

Deploy Integration Service on Sonatype IQ Server

Upload the folder "IntegrationService" to IQ Server's / folder.



The screenshot shows a file manager window with the path `is PC > Downloads > SonatypeFortifyBundle-20.1 > SonatypeFortifyBundle-20.1`. The `IntegrationService` folder is highlighted. Below it, a table lists the files in the folder:

Name	Date modified	Type	Size
<code>iqapplication.properties</code>	31-01-2021 18:08	PROPERTIES File	2 KB
<code>mapping.json</code>	31-01-2021 18:08	JSON File	1 KB
<code>SonatypeFortifyIntegration-20.1.20200914.jar</code>	31-01-2021 18:08	Executable Jar File	24,783 KB
<code>start.sh</code>	31-01-2021 18:08	SH File	1 KB

Below the file manager, a terminal window shows the command `ls -l` and its output:

```
[root@iq IntegrationService]# ls -l
total 24796
-rw-r--r--. 1 root root 1637 Aug 27 10:04 iqapplication.properties
-rw-r--r--. 1 root root 712 Aug 27 10:04 mapping.json
-rw-r--r--. 1 root root 25377357 Aug 27 10:04 SonatypeFortifyIntegration-20.1.20200914.jar
-rwxr-xr-x. 1 root root 53 Aug 27 10:04 start.sh
```

Open `iqapplication.properties` file in `vi` and modify it based on your environment –

```
# Default port to listen on, set as needed
server.port=8182

# URL and creds for IQ Server
iqserver.url=http://172.17.5.225:8070/
iqserver.username=admin
iqserver.password=Passw0rd

# URL and creds (CIToken token) to SSC server: see https://www.microfocus.com/documentation/fortify-software-
security-center/2010/SSC_Help_20.1.0/index.htm#SSC_UG/Gen_Auth_Tokens.htm
sscserver.url=http://172.17.5.227:8080/ssc/
sscserver.token=ZTVmOGJmZGYtYzNmNC00ZTU1LWIxNTUtN2RmNGY5NTFiN2Nl

# work directory where JSON files are stored
loadfile.location=.work/
mapping.file=mapping.json

# Update the mapping.file with project values dynamically passed as request parameters
update.mapping.file=true

# Define which report type to view (raw, vulnerabilities, policy = default)
iq.report.type=vulnerabilities

# directory/file where log files are stored
logfile.location=.work/ServiceLog.log
logLevel=info

# cron expression; it consists of 7 fields
# <second> <minute> <hour> <day-of-month> <month> <day-of-week> <year>
# <year> field is optional. Rest all are required
# Some examples are as follows:
# Running every 12 hours starting at 6 - 0 0/720 6 * * ?
# Running every 12 hours starting at midnight - 0 0/720 0 * * ?
# Running every 6 hrs starting at 6 AM - 0 0/360 6 * * ?
# For more details please visit - https://www.baeldung.com/cron-expressions
# Currently scheduled to run at 6 AM and then every 6 hours.
scheduling.job.cron=0 0/360 6 * * ?

# Set it to true if wanted to close the process after next scheduled run or
# leave set to true if you want to use your own scheduler
# also http://localhost/killProcess will stop the process
KillProcess=false
```

Save the file.

Open `mapping.json` file in `vi` and edit as per environment.

```
[
  {
    "sonatypeProject": "petclinic",
    "sonatypeProjectStage": "release",
    "fortifyApplication": "PetClinic",
    "fortifyApplicationVersion": "1.0"
  },
  {
    "sonatypeProject": "petclinic",
    "sonatypeProjectStage": "build",
    "fortifyApplication": "PetClinic",
```

```

    "fortifyApplicationVersion": "2.0"
  },
  {
    "sonatypeProject": "struts-showcase",
    "sonatypeProjectStage": "stage-release",
    "fortifyApplication": "Struts Showcase",
    "fortifyApplicationVersion": "1.0"
  },
  {
    "sonatypeProject": "webgoat8",
    "sonatypeProjectStage": "release",
    "fortifyApplication": "Webgoat8",
    "fortifyApplicationVersion": "1.0"
  },
  {
    "sonatypeProject": "WebGoat5.0",
    "sonatypeProjectStage": "build",
    "fortifyApplication": "MF_Internal.WebGoat_via_SonaType",
    "fortifyApplicationVersion": "5.0"
  }
]

```

Save and Close the file.

Start the service using –

```
# chmod +x start.sh
```

```
# ./start.sh &
```

```

[rooth@iq IntegrationService]# ./start.sh &
[1] 88995
[rooth@iq IntegrationService]#

Spring
v2.3.3.RELEASE

2021-02-15 02:43:29.158 INFO 88995 --- [main] c.s.ssc.ultsvc.SonatypeApplication : Starting SonatypeApplication v20.1.20200914 on iq.myhome.com with PID 88995 (/Integrations
Service/SonatypeFortifyIntegration-20.1.20200914.jar started by root in /IntegrationService)
2021-02-15 02:43:29.171 INFO 88995 --- [main] c.s.ssc.ultsvc.SonatypeApplication : No active profile set, falling back to default profiles: default
2021-02-15 02:43:33.296 INFO 88995 --- [main] o.s.b.w.embedded.tomcat.TomcatWebServer : Tomcat initialized with port(s): 8182 (http)
2021-02-15 02:43:33.299 INFO 88995 --- [main] o.apache.catalina.core.StandardService : Starting service [Tomcat]
2021-02-15 02:43:33.270 INFO 88995 --- [main] org.apache.catalina.core.StandardEngine : Starting Servlet engine: [Apache Tomcat/9.0.37]
2021-02-15 02:43:33.488 INFO 88995 --- [main] o.s.s.c.f.TomcatLocalhost : Initializing Spring embedded WebApplicationContext
2021-02-15 02:43:33.489 INFO 88995 --- [main] w.s.c.ServletWebServerApplicationContext : Root WebApplicationContext: initialization completed in 3909 ms
2021-02-15 02:43:33.657 [main] INFO root : Integration service ready: 20.1.20200914
2021-02-15 02:43:33.844 INFO 88995 --- [main] o.s.s.concurrent.ThreadPoolTaskExecutor : Initializing ExecutorService 'applicationTaskExecutor'
2021-02-15 02:43:34.188 INFO 88995 --- [main] o.s.s.c.ThreadPoolTaskScheduler : Initializing ExecutorService 'taskscheduler'
2021-02-15 02:43:34.256 INFO 88995 --- [main] o.s.b.w.embedded.tomcat.TomcatWebServer : Tomcat started on port(s): 8182 (http) with context path ''
2021-02-15 02:43:34.279 INFO 88995 --- [main] c.s.ssc.ultsvc.SonatypeApplication : Started SonatypeApplication in 7.119 seconds (JVM running for 8.06)

```

It will create a folder named work. Which will contain the log file.

```

[rooth@iq .work]# pwd
/IntegrationService/.work
[rooth@iq .work]# ls -l
total 4
-rw-r--r--. 1 root root 86 Feb 15 02:43 ServiceLog.log
[rooth@iq .work]#

```

< !! End of the Document !! >