.

Lesson 09 Demo 03

Installing and Configuring ZAP Plugin on Jenkins

Objective: To install and configure the OWASP ZAP plugin on Jenkins to automate security testing of web applications during the build process

Tools required: Jenkins

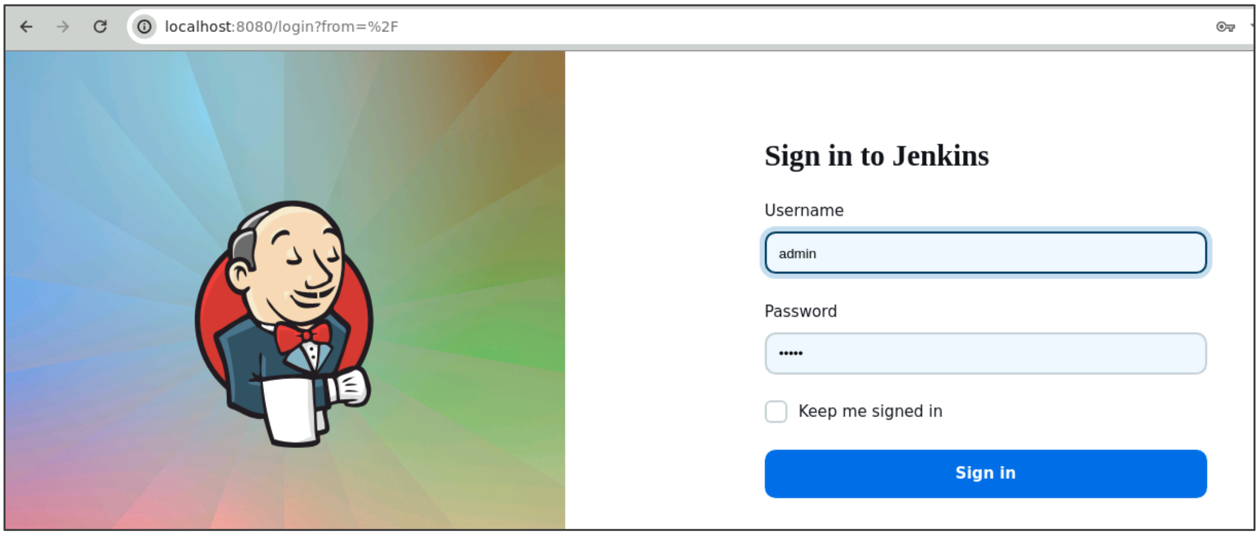
Prerequisites: You need to have a Jenkins up and running.

Steps to be followed:

1. Configure OWASP ZAP tool in Jenkins
2. Create a Jenkins pipeline job to integrate the vulnerability scan tool

Step 1: Configure OWASP ZAP tool in Jenkins

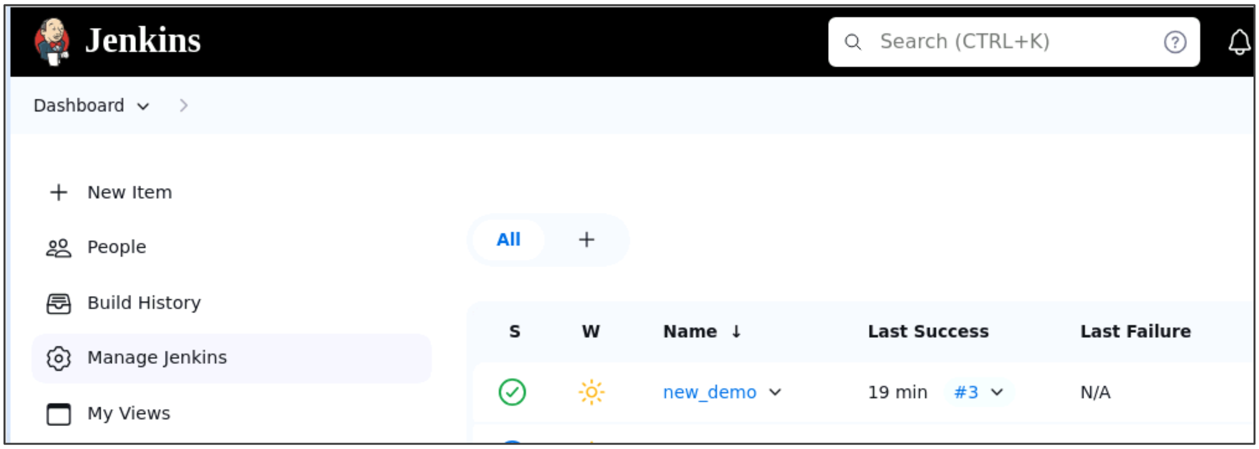
1.1 Log in to **Jenkins** using your credentials



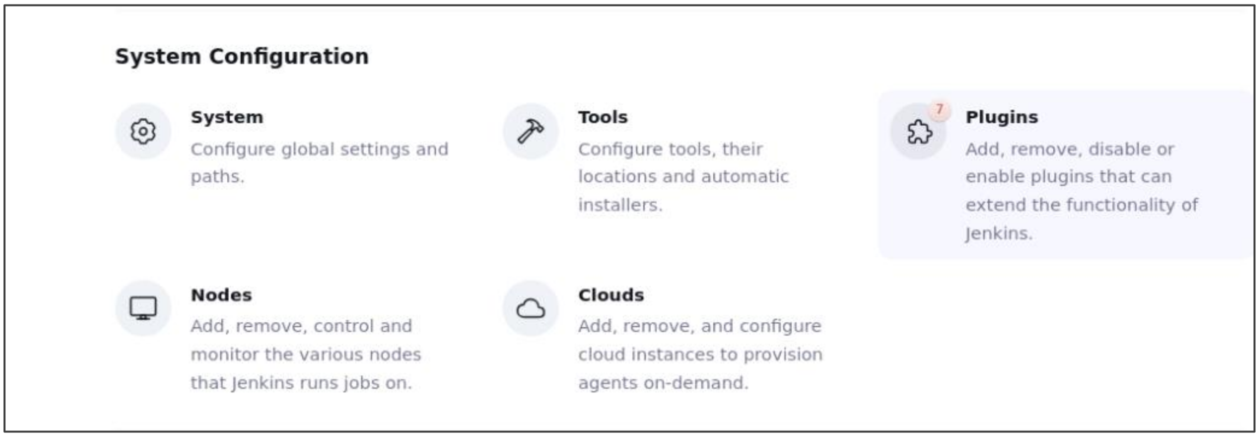
Note: The credentials for accessing Jenkins in the lab are Username: **admin** and Password: **Root123$**.

.

1.2 In the Jenkins dashboard, navigate to **Manage Jenkins**, and under **System Configuration**, click on **Plugins**



S	W	Name ↓	Last Success	Last Failure
✓	☀	new_demo	19 min #3	N/A



System Configuration

System
Configure global settings and paths.

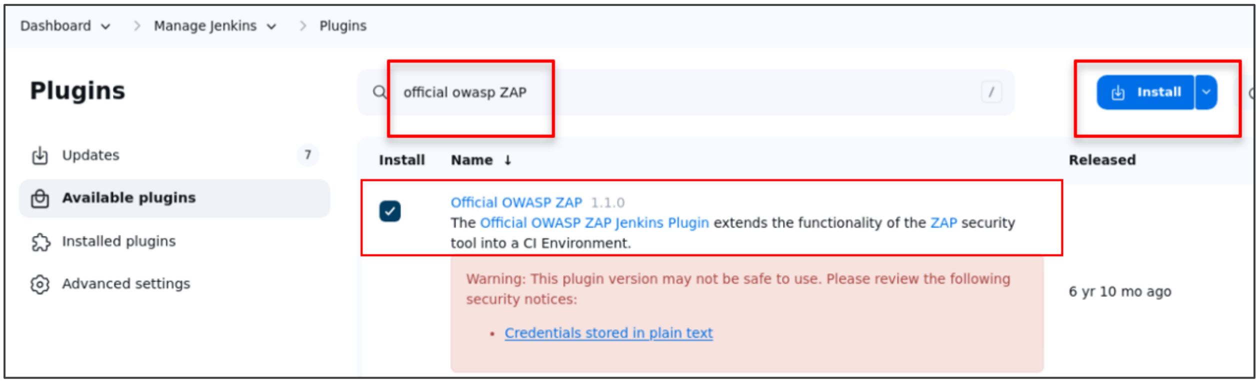
Tools
Configure tools, their locations and automatic installers.

Plugins
Add, remove, disable or enable plugins that can extend the functionality of Jenkins.

Nodes
Add, remove, control and monitor the various nodes that Jenkins runs jobs on.

Clouds
Add, remove, and configure cloud instances to provision agents on-demand.

1.3 In the **Available plugins**, search for the **Official OWASP ZAP** plugin and click on **Install**

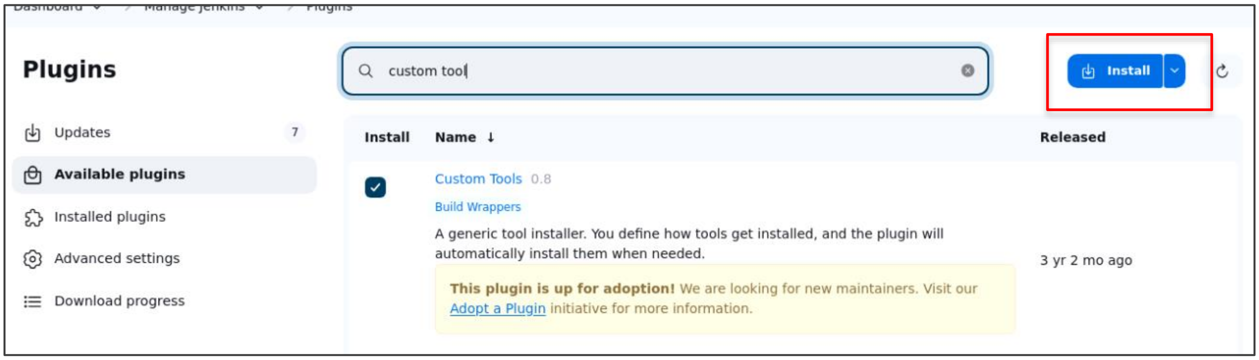


Search: official owasp ZAP

Install	Name ↓	Released
☑	Official OWASP ZAP 1.1.0 The Official OWASP ZAP Jenkins Plugin extends the functionality of the ZAP security tool into a CI Environment. Warning: This plugin version may not be safe to use. Please review the following security notices: • Credentials stored in plain text	6 yr 10 mo ago

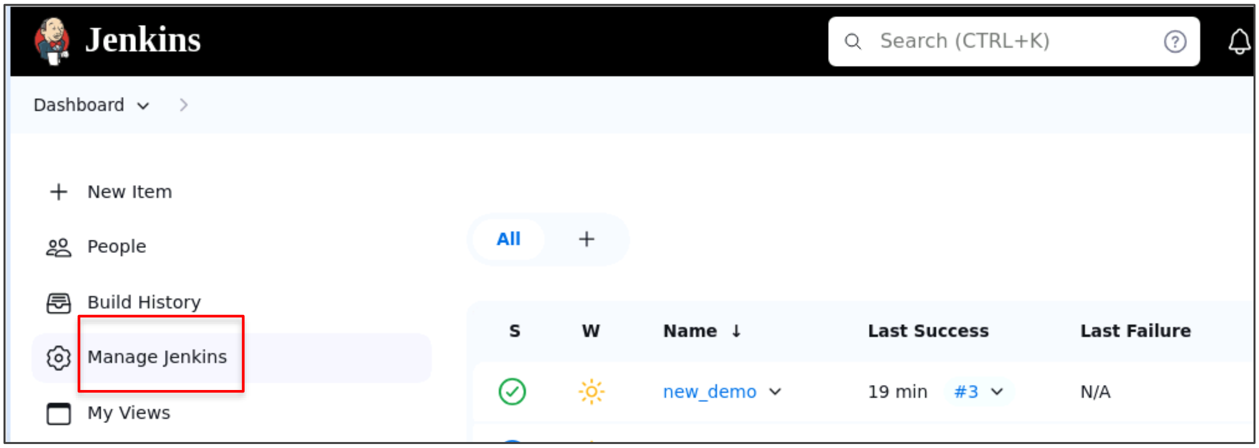
.

1.4 In the **Available plugins**, search for **Custom Tools** and click on **Install**

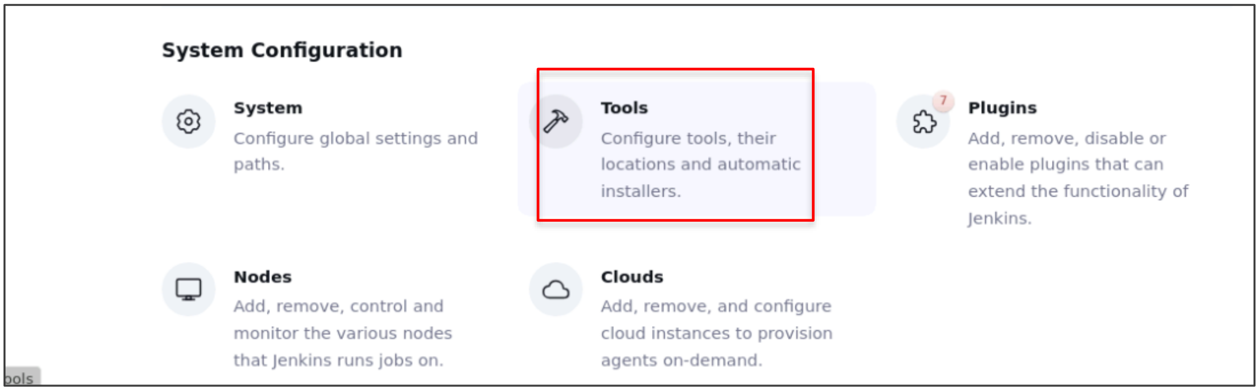


Install	Name ↓	Released
☑	Custom Tools 0.8 Build Wrappers A generic tool installer. You define how tools get installed, and the plugin will automatically install them when needed. **This plugin is up for adoption!** We are looking for new maintainers. Visit our Adopt a Plugin initiative for more information.	3 yr 2 mo ago

1.5 Navigate back to the **Manage Jenkins**, click on **Tools**, and under **Custom tools installations**, click on **Add Custom tool**



S	W	Name ↓	Last Success	Last Failure
✓	☀	new_demo	19 min #3	N/A


System Configuration

System
Configure global settings and paths.

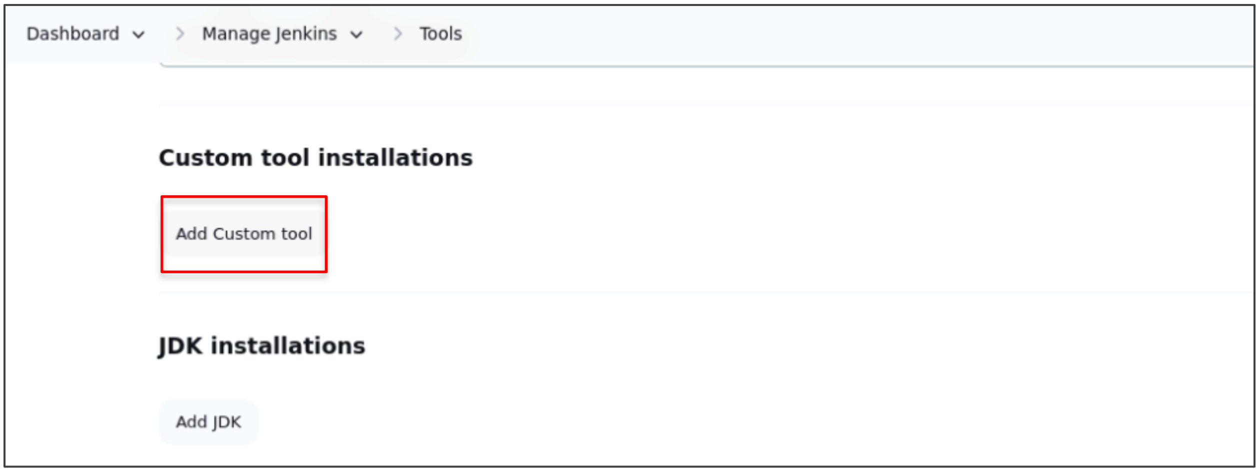
Tools
Configure tools, their locations and automatic installers.

Plugins
Add, remove, disable or enable plugins that can extend the functionality of Jenkins.

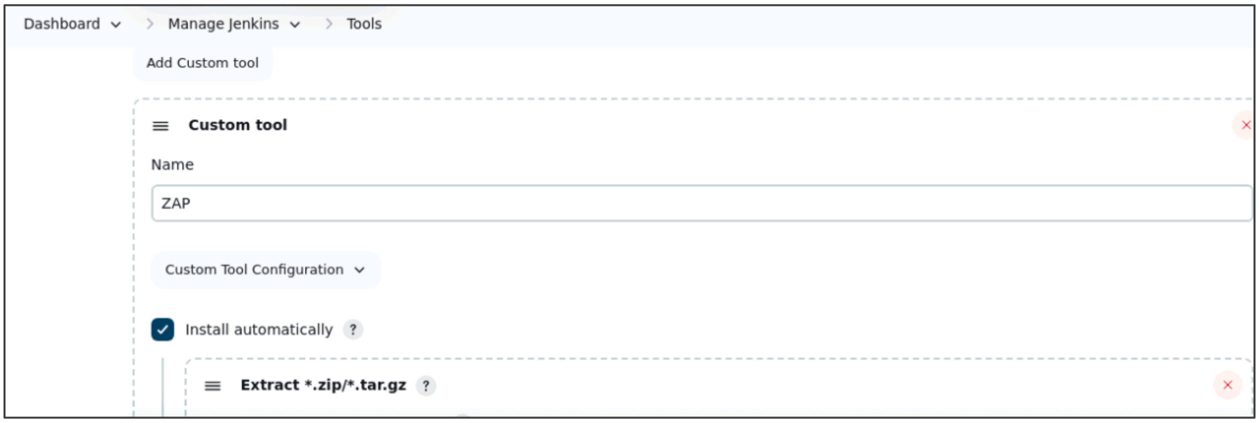
Nodes
Add, remove, control and monitor the various nodes that Jenkins runs jobs on.

Clouds
Add, remove, and configure cloud instances to provision agents on-demand.

.



1.6 Under **Custom tool**, provide **ZAP** as the **Name**

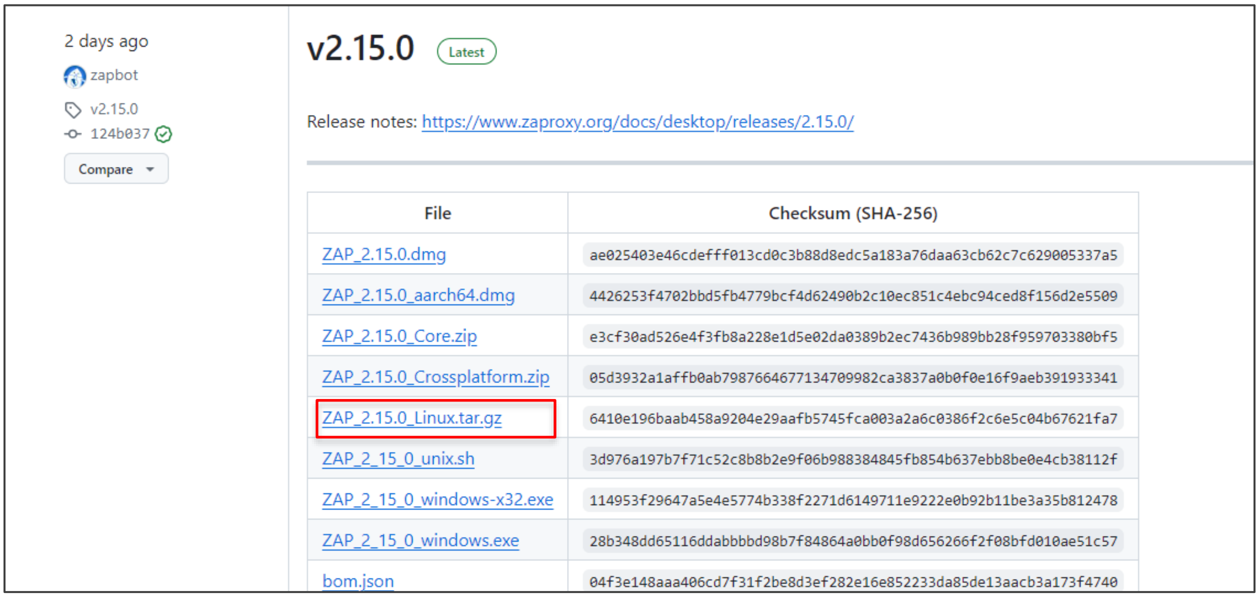


Name: ZAP

☑ Install automatically

.

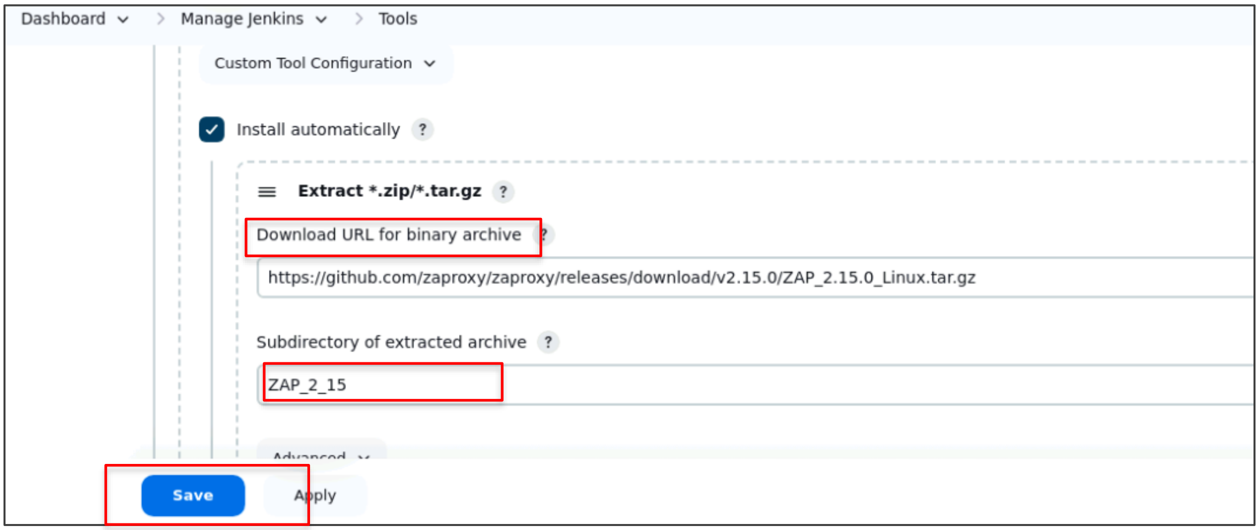
1.7 Navigate to **https://github.com/zaproxy/zaproxy/releases**, copy the URL highlighted in the screenshot, paste it into the **Download URL for binary archive**, enter **ZAP_2_15** for the **Subdirectory of extracted archive** field, and then click **Save**



v2.15.0

Release notes: https://www.zaproxy.org/docs/desktop/releases/2.15.0/

File	Checksum (SHA-256)
ZAP_2.15.0.dmg	ae025403e46cdefff013cd0c3b88d8edc5a183a76daa63cb62c7c629005337a5
ZAP_2.15.0_aarch64.dmg	4426253f4702bbd5fb4779bcf4d62490b2c10ec851c4ebc94ced8f156d2e5509
ZAP_2.15.0_Core.zip	e3cf30ad526e4f3fb8a228e1d5e02da0389b2ec7436b989bb28f959703380bf5
ZAP_2.15.0_Crossplatform.zip	05d3932a1affb0ab7987664677134709982ca3837a0b0f0e16f9aeb391933341
ZAP_2.15.0_Linux.tar.gz	6410e196baab458a9204e29aafb5745fca003a2a6c0386f2c6e5c04b67621fa7
ZAP_2_15_0_unix.sh	3d976a197b7f71c52c8b8b2e9f06b988384845fb854b637ebb8be0e4cb38112f
ZAP_2_15_0_windows-x32.exe	114953f29647a5e4e5774b338f2271d6149711e9222e0b92b11be3a35b812478
ZAP_2_15_0_windows.exe	28b348dd65116ddabbbbd98b7f84864a0bb0f98d656266f2f08bfd010ae51c57
bom.json	04f3e148aaa406cd7f31f2be8d3ef282e16e852233da85de13aacb3a173f4740



☑ Install automatically ?

Extract *.zip/*.tar.gz ?

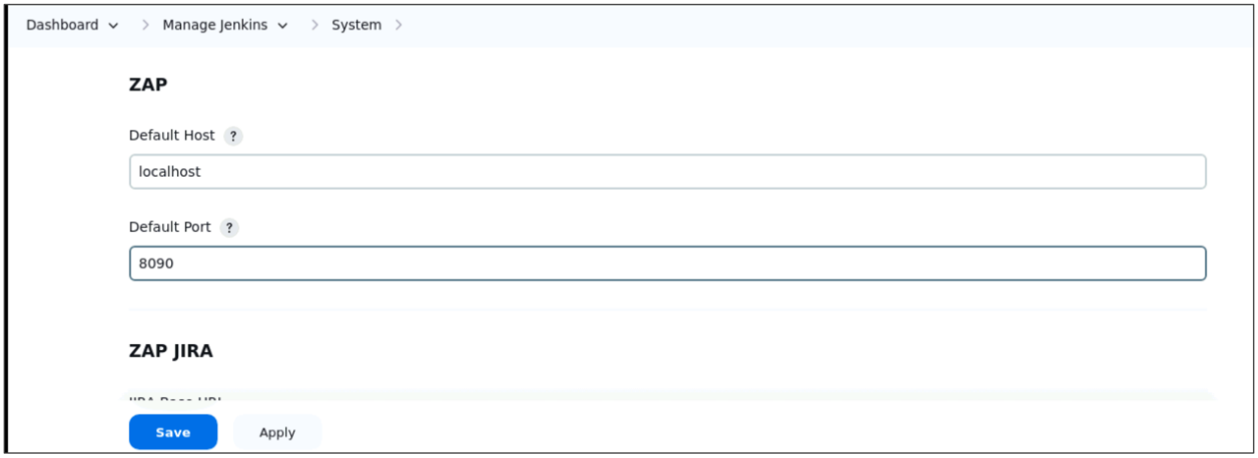
Download URL for binary archive ?

https://github.com/zaproxy/zaproxy/releases/download/v2.15.0/ZAP_2.15.0_Linux.tar.gz

Subdirectory of extracted archive ?

ZAP_2_15

1.8 Navigate back to the **Manage Jenkins** and select **Configure System**, scroll down to **ZAP**, and fill the **Default Host** as **localhost** and **Default Port** as **8090**



ZAP

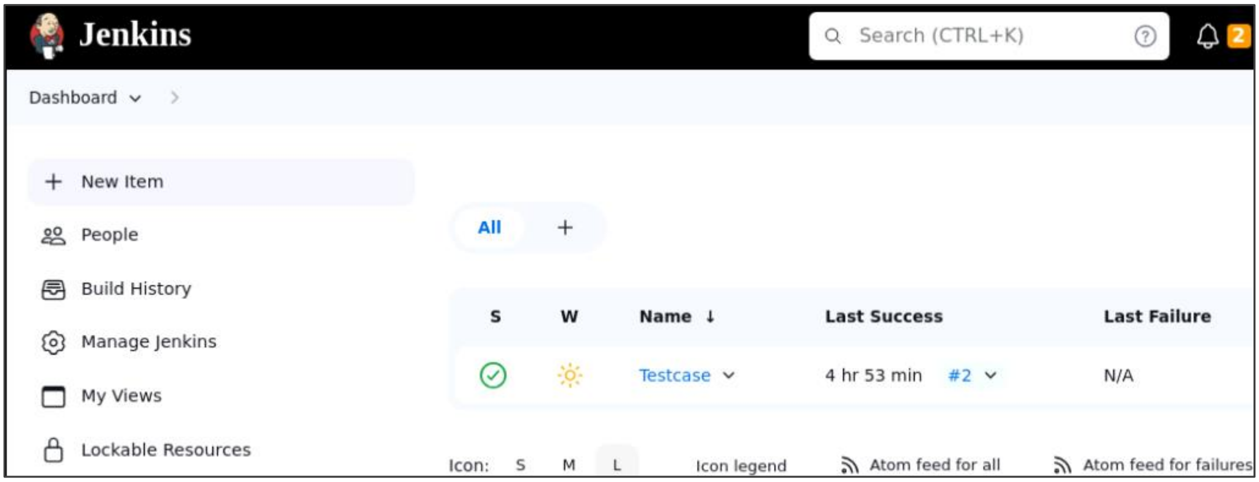
Default Host: localhost

Default Port: 8090

ZAP JIRA

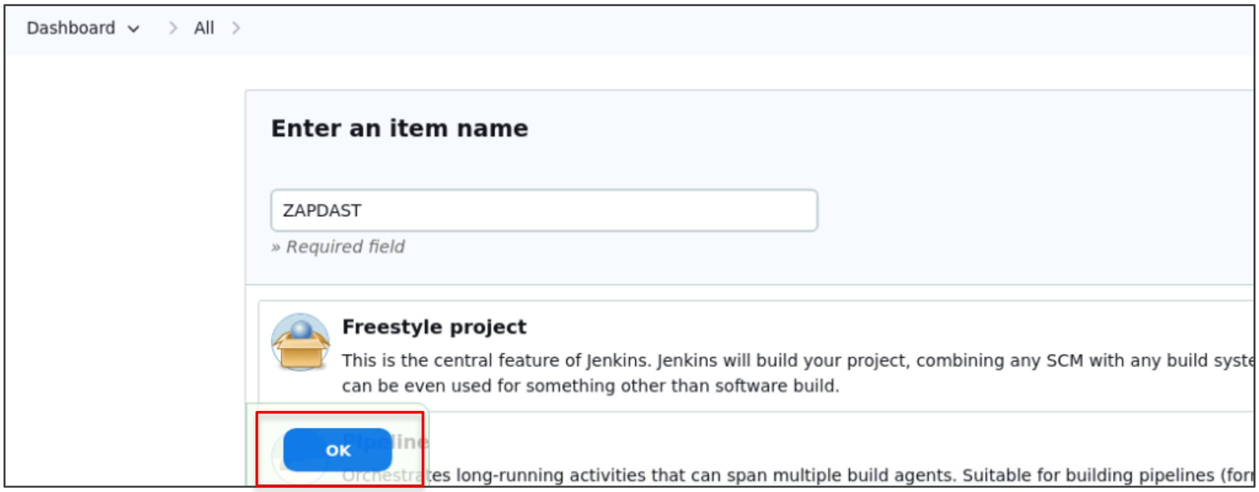
Step 2: Create a Jenkins pipeline job to integrate the vulnerability scan tool

2.1 Navigate the **Jenkins Dashboard** and click on **New Item**



S	W	Name ↓	Last Success	Last Failure
✓	☼	Testcase	4 hr 53 min #2	N/A

2.2 Click on **Freestyle project** and put **ZAPDAST** under **Enter an item name**, then click on **OK**



Enter an item name

ZAPDAST

» Required field

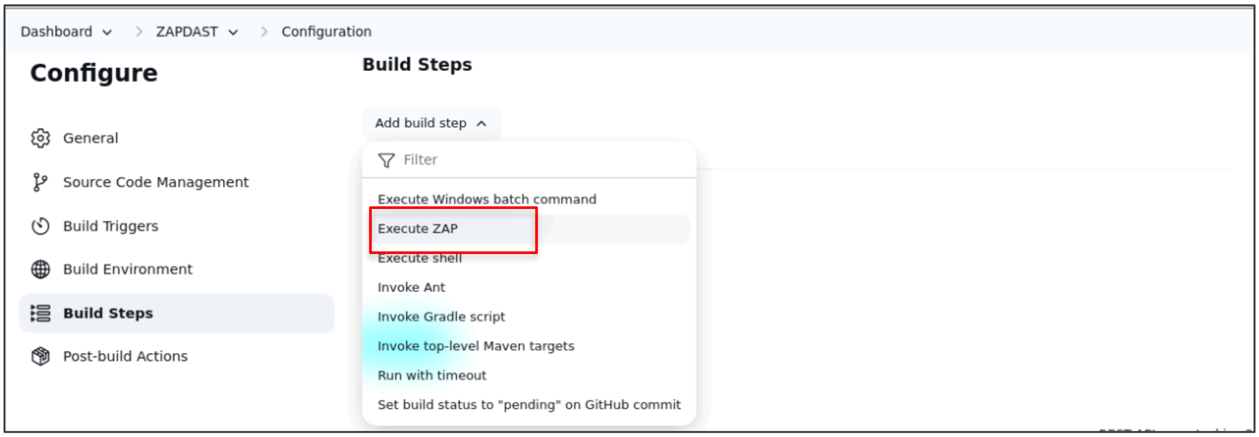
Freestyle project

This is the central feature of Jenkins. Jenkins will build your project, combining any SCM with any build syste
can be even used for something other than software build.

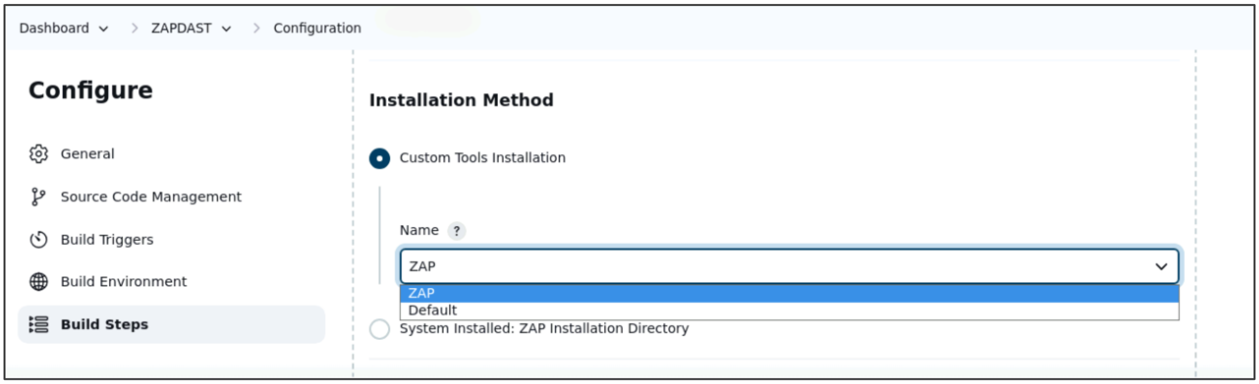
Pipeline

Orchestrates long-running activities that can span multiple build agents. Suitable for building pipelines (for

2.3 Navigate to the **Build Steps**, click on **Add build step**, and select **Execute ZAP**



2.4 Scroll down to the **Installation Method** and select **ZAP** as the **Name**



Installation Method

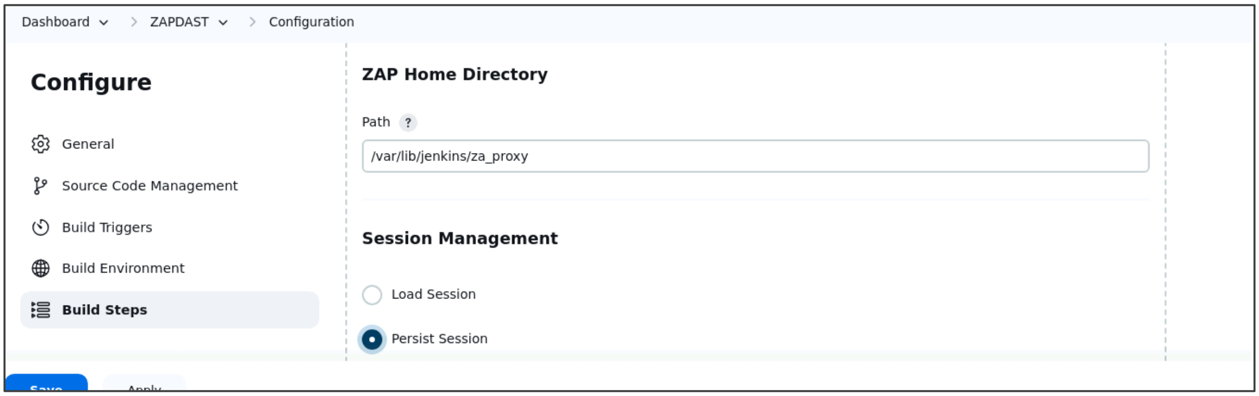
● Custom Tools Installation

Name ?

ZAP

○ System Installed: ZAP Installation Directory

2.5 Scroll down to the **ZAP Home Directory** and provide the path **/var/lib/jenkins/za_proxy**



ZAP Home Directory

Path ?

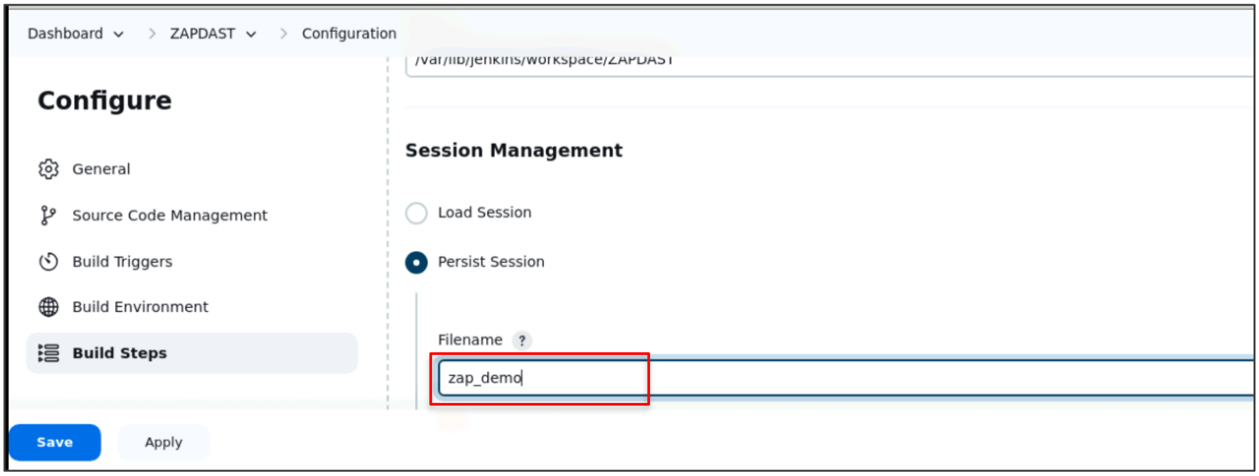
/var/lib/jenkins/za_proxy

Session Management

○ Load Session

● Persist Session

2.6 In the **Session Management** section, select **Persist Session** and write **Filename** as **zap_demo**



/var/lib/jenkins/workspace/ZAPDAST

Session Management

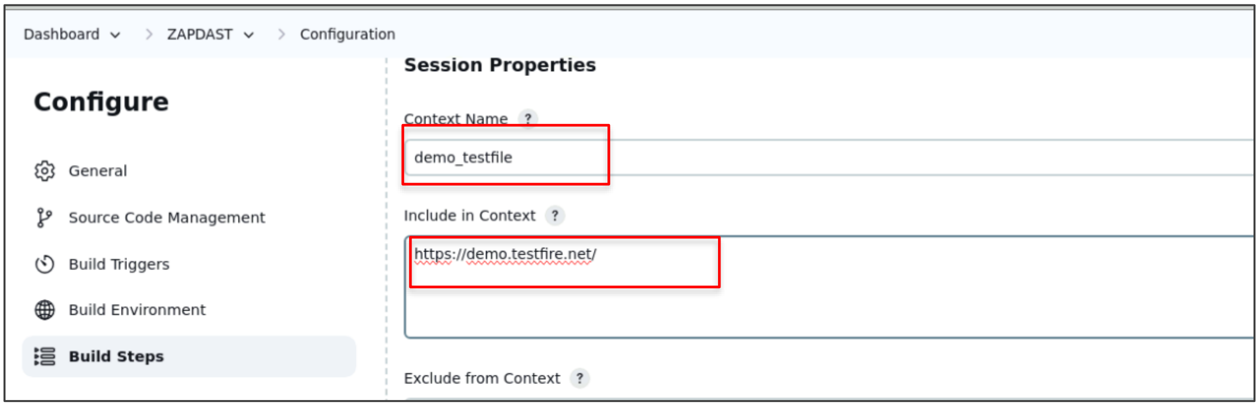
○ Load Session

● Persist Session

Filename ?

zap_demo

2.7 Under **Session Properties**, enter **demo_testfile** as the **Context Name**, provide **https://demo.testfire:net/** for the **Include in Context** field, and enter **^(?:(?!https:\/\/demo.testfire.net/).*).$** for the **Exclude from Context** field



Session Properties

Context Name ?

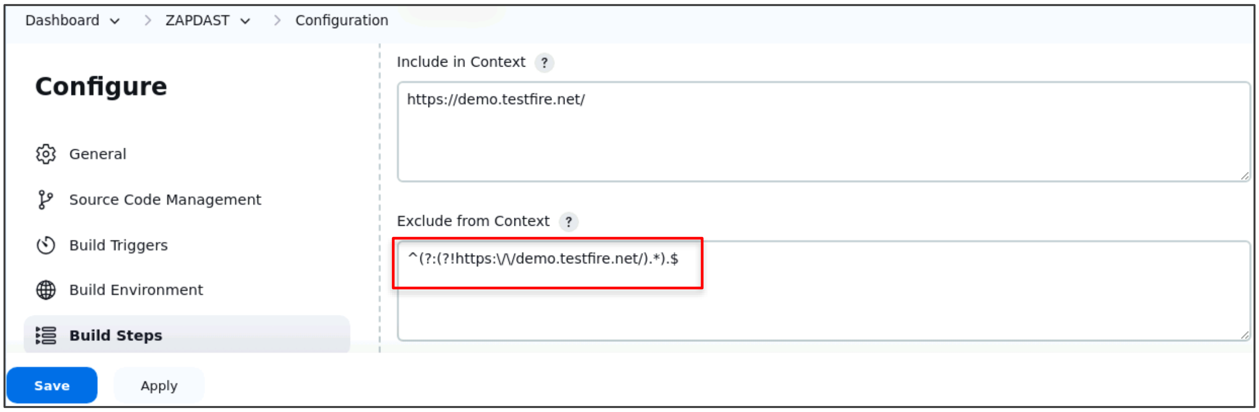
demo_testfile

Include in Context ?

https://demo.testfire.net/

Exclude from Context ?

.



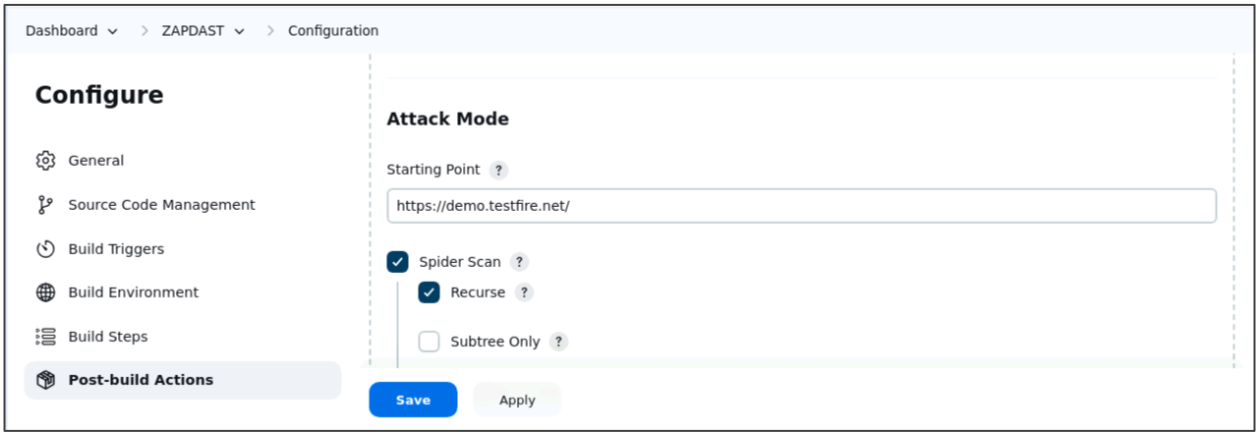
Include in Context ?

https://demo.testfire.net/

Exclude from Context ?

^(?:(?!https:\/\/demo.testfire.net/).*).$

2.8 Now, scroll down to **Attack Mode** and enter the **Starting Point** as **https://demo.testfire.net/**, and then select **Spider Scan**, **Recurse**, **AJAX Spider**, and **Active Scan**



Attack Mode

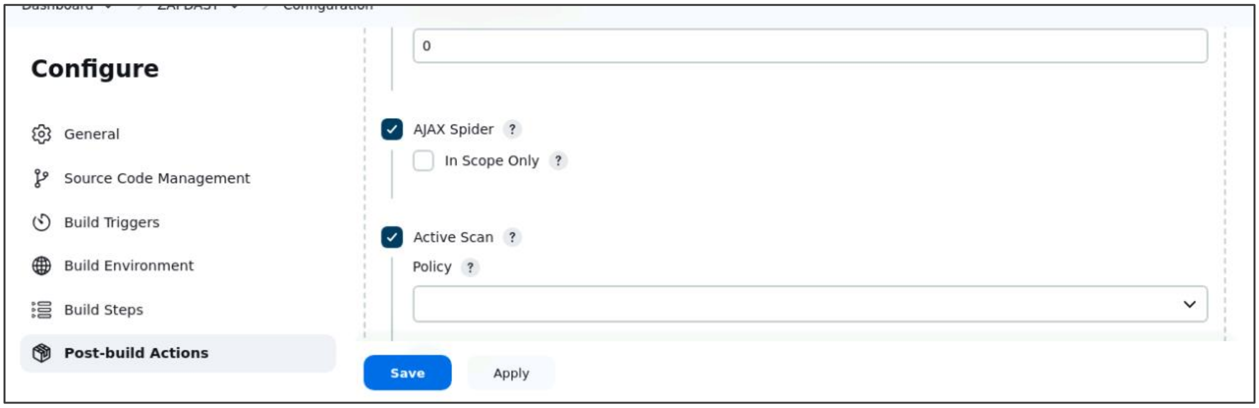
Starting Point ?

https://demo.testfire.net/

☑ Spider Scan ?

☑ Recurse ?

☐ Subtree Only ?



0

☑ AJAX Spider ?

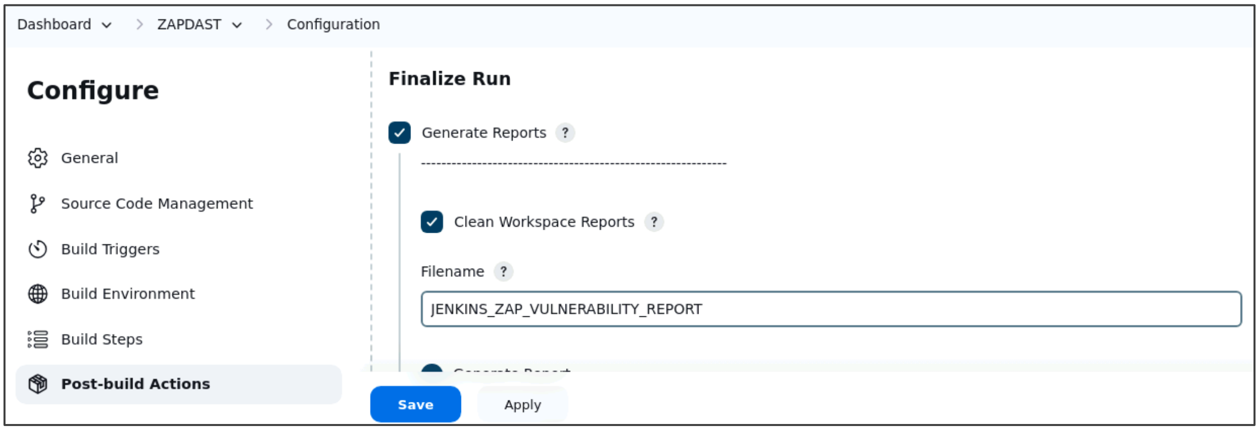
☐ In Scope Only ?

☑ Active Scan ?

Policy ?

.

2.9 Under **Finalize Run**, select **Generate Reports**, **Clean Workspace Reports**, **Generate Reports** and select **HTML** as **format**



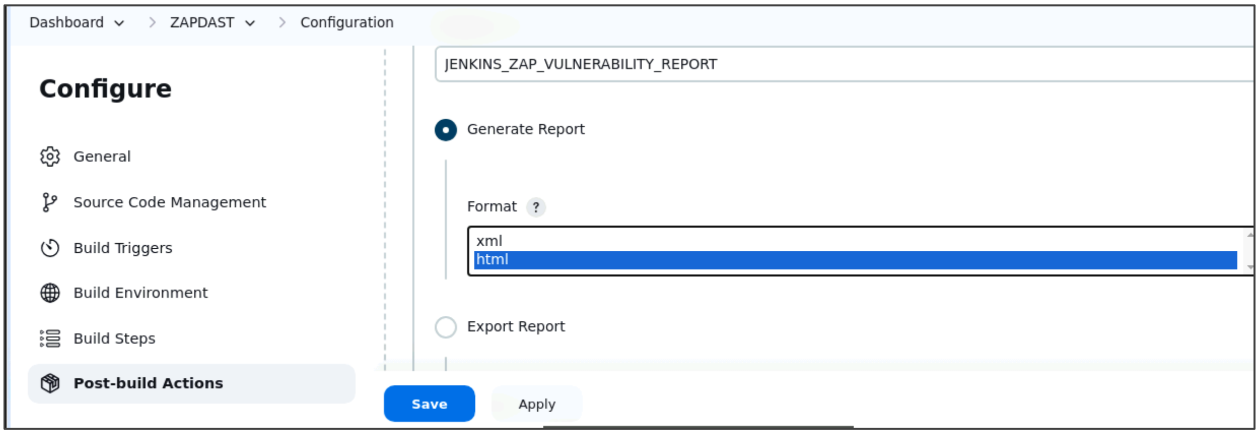
Finalize Run

☑ Generate Reports ?

☑ Clean Workspace Reports ?

Filename ?

JENKINS_ZAP_VULNERABILITY_REPORT



JENKINS_ZAP_VULNERABILITY_REPORT

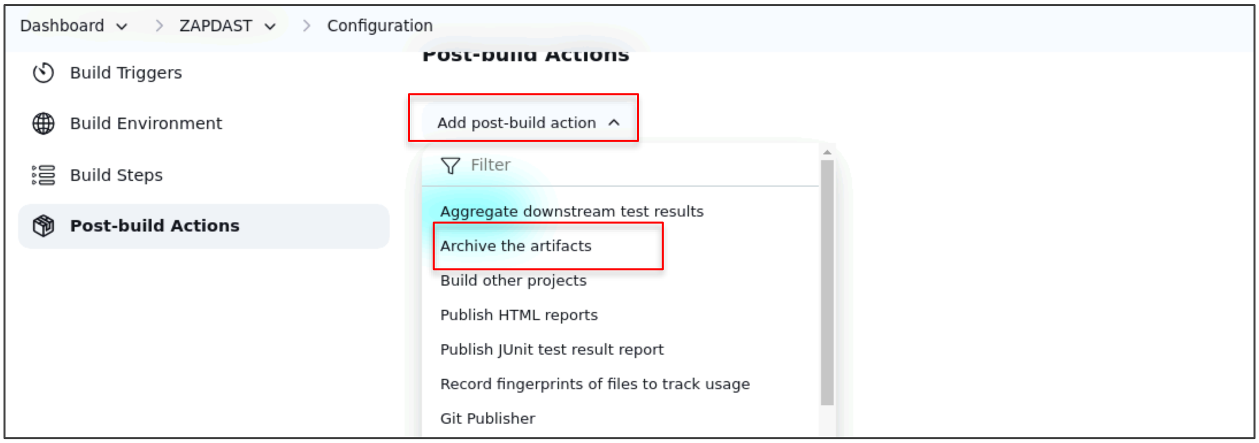
● Generate Report

Format ?

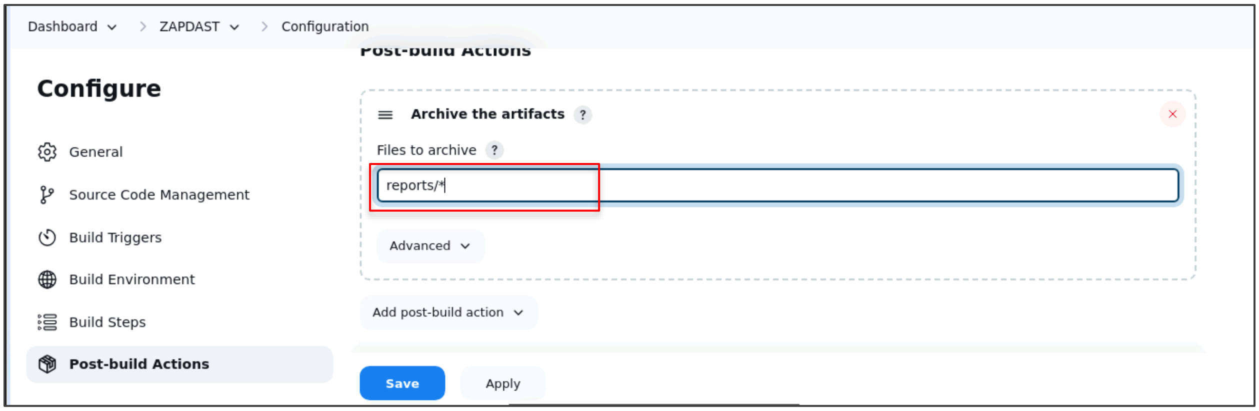
xml
html

○ Export Report

2.10 In the **Post-build-Actions,** click on **Add post-build-action** and select **Archive the artifacts** and write **reports/*** under **Files to archive**, then click on **Save**



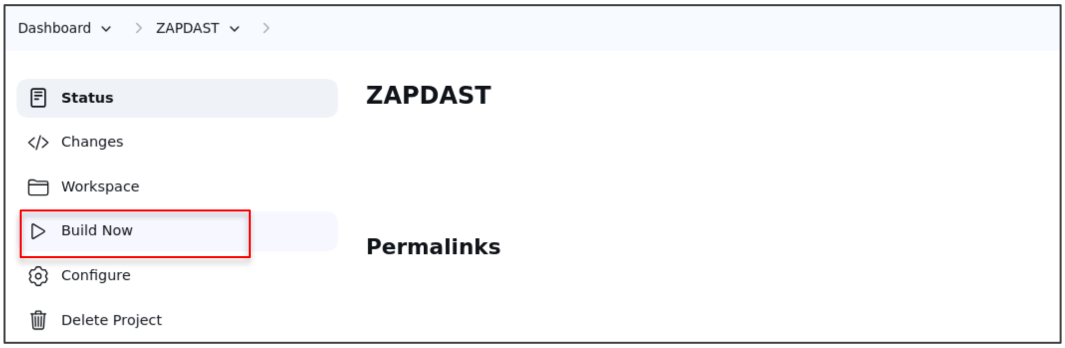
.



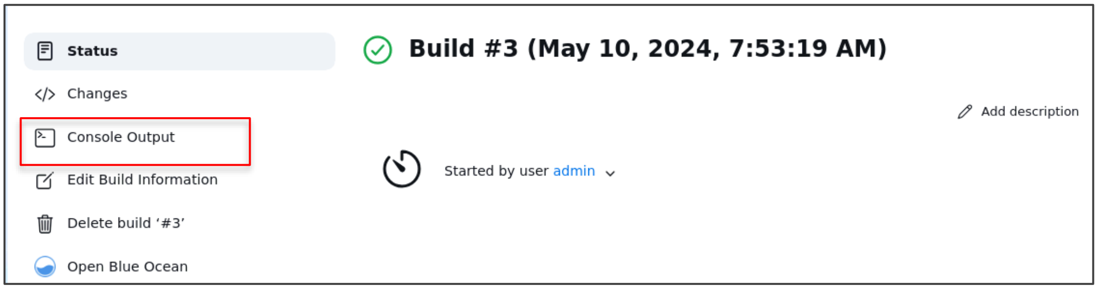
Files to archive ?

reports/*

2.11 Now, click on **Build Now** to execute the build



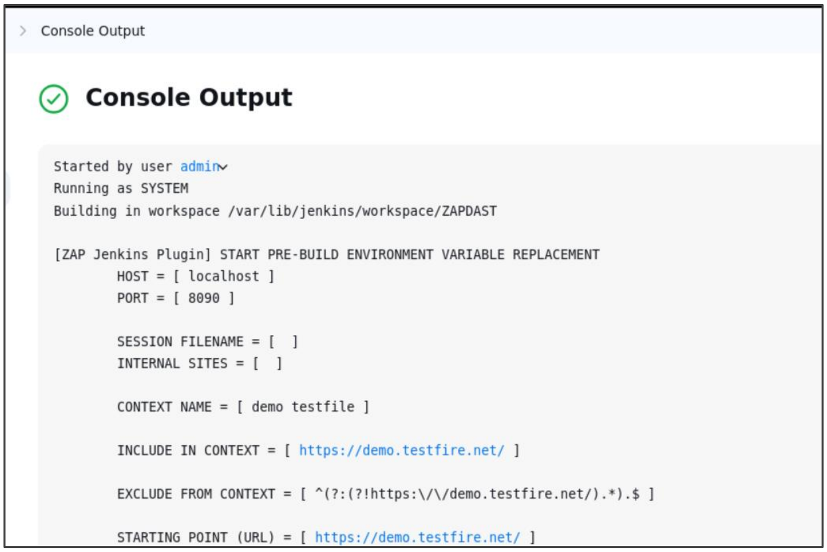
2.12 Click on **Console Output** to see the output



Build #3 (May 10, 2024, 7:53:19 AM)

Started by user admin

.



Console Output

```
Started by user admin
Running as SYSTEM
Building in workspace /var/lib/jenkins/workspace/ZAPDAST

[ZAP Jenkins Plugin] START PRE-BUILD ENVIRONMENT VARIABLE REPLACEMENT
        HOST = [ localhost ]
        PORT = [ 8090 ]

        SESSION FILENAME = [  ]
        INTERNAL SITES = [  ]

        CONTEXT NAME = [ demo testfile ]

        INCLUDE IN CONTEXT = [ https://demo.testfire.net/ ]

        EXCLUDE FROM CONTEXT = [ ^(?:(?!https:\/\/demo.testfire.net/).*).$ ]

        STARTING POINT (URL) = [ https://demo.testfire.net/ ]
```

You can see that the build is configured successfully.

By following these steps, you have successfully installed and configured the OWASP ZAP plugin on Jenkins to automate the security testing of web applications during the build process.