**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

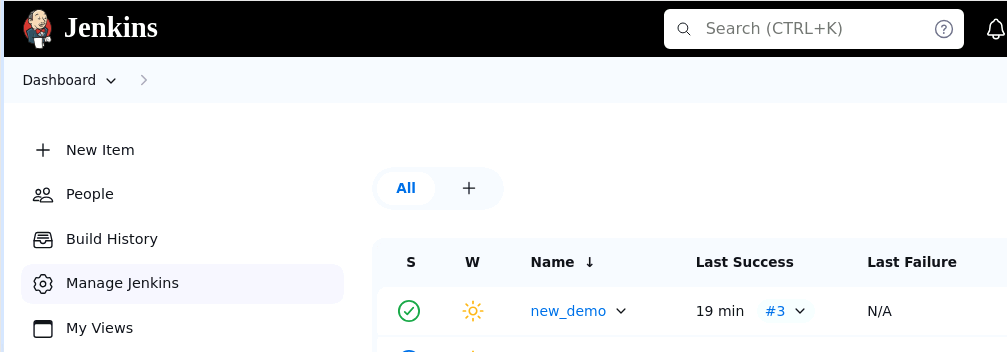
**Step 1:** **Configure OWASP ZAP tool in Jenkins**

1. Log in to **Jenkins** using your credentials



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

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



A screenshot of a computer

Description automatically generated

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

A screenshot of a computer

Description automatically generated

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

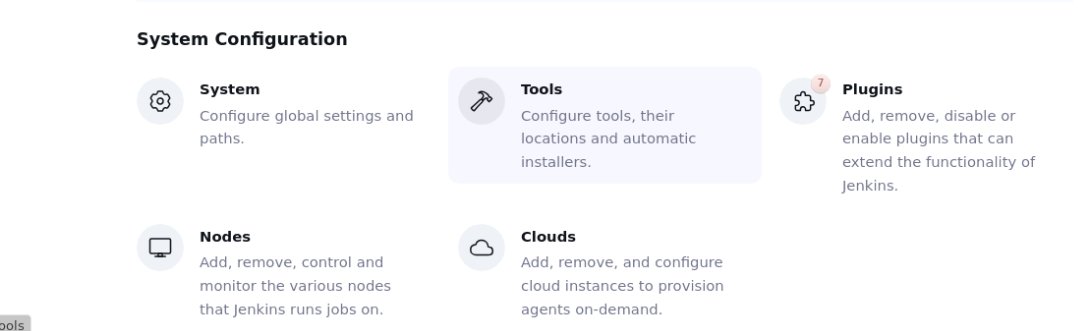
A screenshot of a computer

Description automatically generated

1. Navigate back to the **Manage Jenkins**, click on **Tools**,andunder **Custom tools installations**, click on **Add Custom tool**

**A screenshot of a computer

Description automatically generated**



A screenshot of a computer

Description automatically generated

1. Under **Custom tool**, provide **ZAP** asthe **Name**

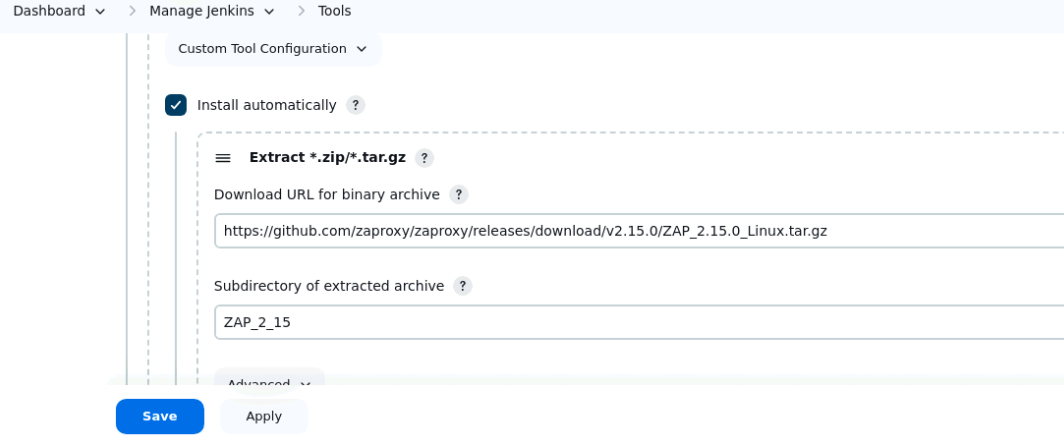
A screenshot of a computer

Description automatically generated

* 1. 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**

A screenshot of a computer

Description automatically generated



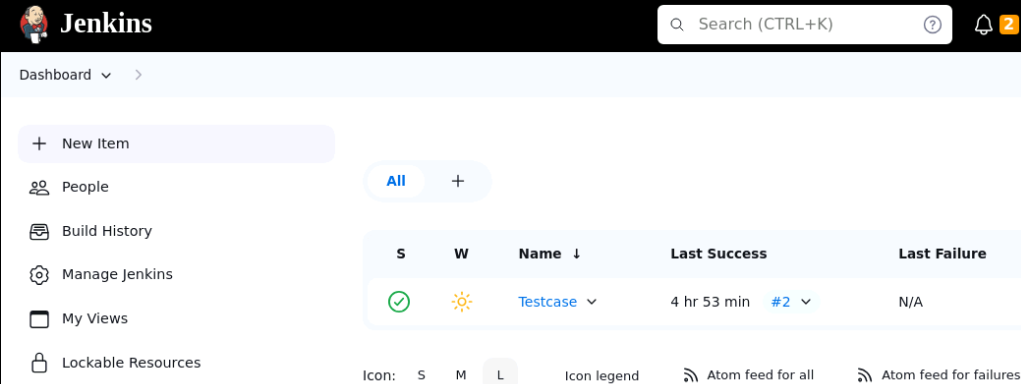
* 1. Navigate back to the **Manage Jenkins** and select **Configure System**, scroll down to **ZAP**, and fill the **Default Host** as **localhost** and **Default Port** as **8090**

A white background with black lines

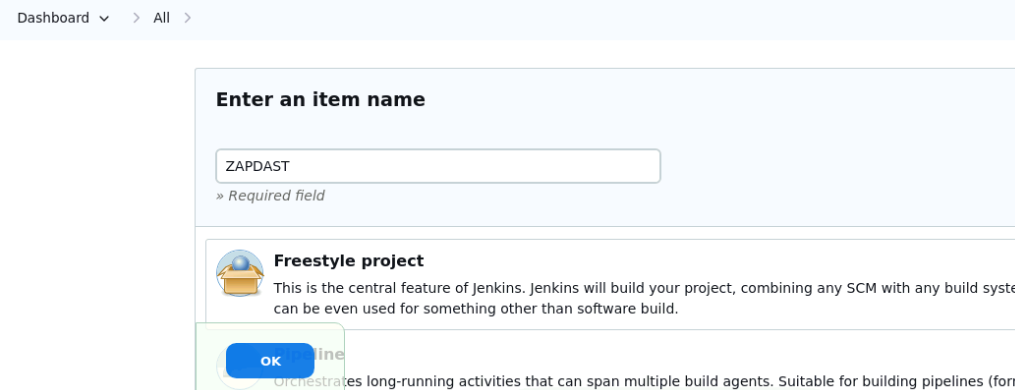
Description automatically generated

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

* 1. Navigate the **Jenkins Dashboard** and click on **New Item**



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



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

A screenshot of a computer

Description automatically generated

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

A screenshot of a computer

Description automatically generated

* 1. Scroll down to the **ZAP** **Home Directory** and provide the path **/var/lib/jenkins/za\_proxy**

A screenshot of a computer

Description automatically generated

* 1. In the **Session Management** section, select **Persist Session** and write **Filename** as

**zap\_demo**

A screenshot of a computer

Description automatically generated

* 1. 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

A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

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

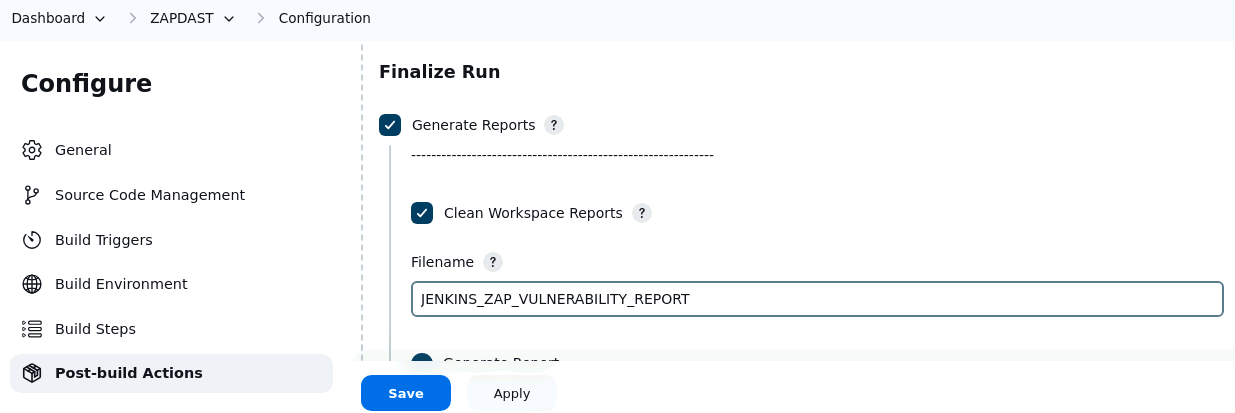
A screenshot of a computer

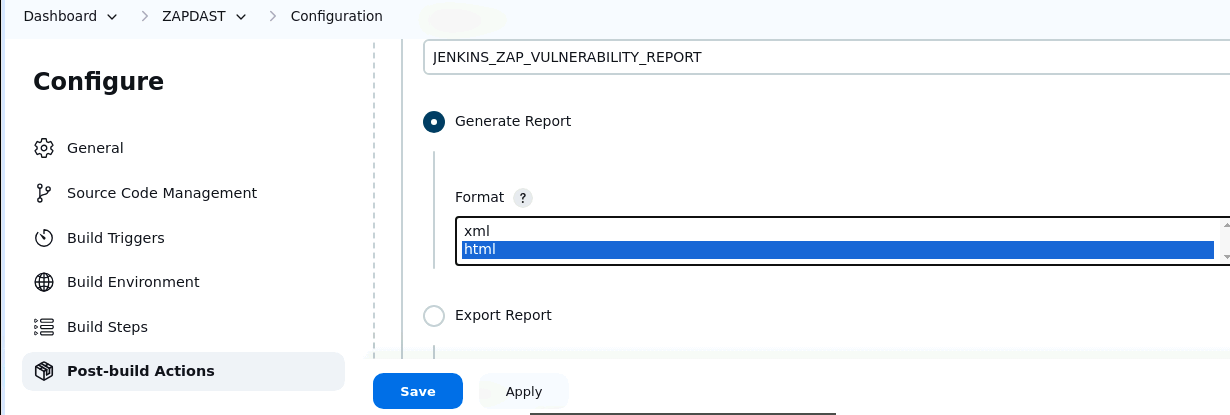
Description automatically generated

A screenshot of a computer

Description automatically generated

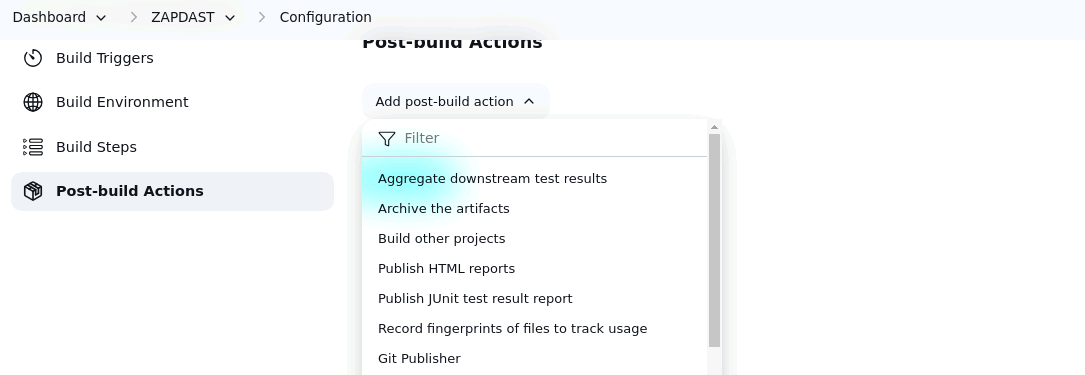
* 1. Under **Finalize Run**, select **Generate Reports**, **Clean Workspace Reports**, **Generate Reports** and select **HTML** as **format**





* 1. 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**



A screenshot of a chat box

Description automatically generated

* 1. Now, click on **Build Now** to execute the build

A white background with black text

Description automatically generated

* 1. Click on **Console Output** to see the output

A screenshot of a computer

Description automatically generated

A screenshot of a computer program

Description automatically generated

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.