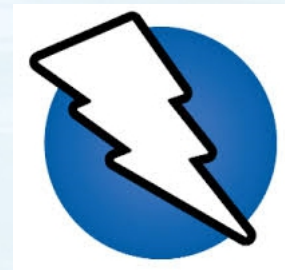


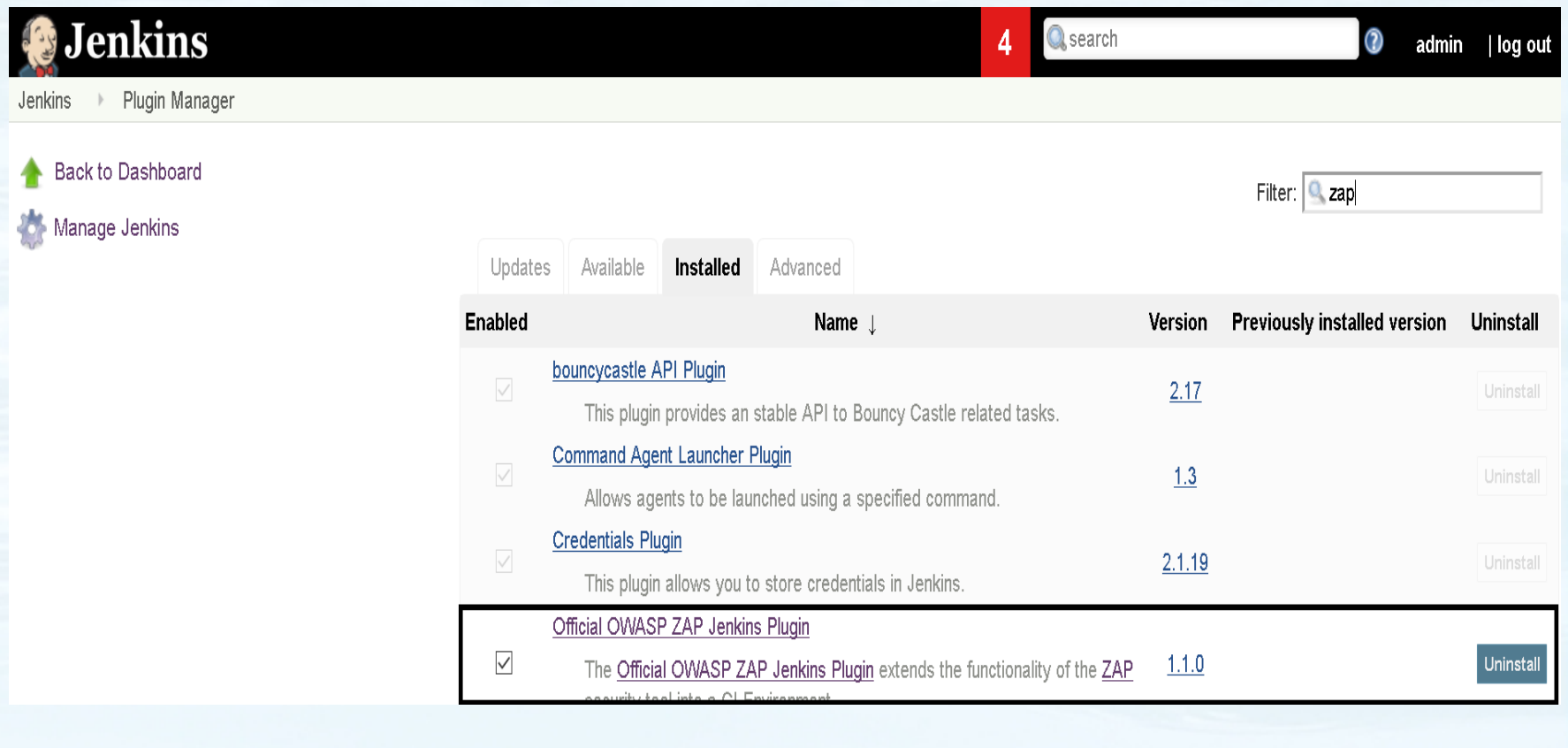
DAST SECURITY : OWASP-ZAP

- Owasp-zap is one of the world's most popular free security tool and is actively maintained by hundreds of international volunteers.
- It helps to find vulnerabilities automatically with every ci/cd build.
- One of the best free tool for experienced pen testers to be used for manual security testing.



Steps to Configure

- Install the zap plugin in Jenkins



The screenshot shows the Jenkins Plugin Manager interface. The top navigation bar includes the Jenkins logo, a search bar, and user information (admin | log out). The breadcrumb trail indicates the current location is Jenkins > Plugin Manager. On the left sidebar, there are links for 'Back to Dashboard' and 'Manage Jenkins'. The main content area displays a list of installed plugins under the 'Installed' tab. The list is filtered by 'zap'. The plugins listed are:

Enabled	Name ↓	Version	Previously installed version	Uninstall
<input checked="" type="checkbox"/>	bouncycastle API Plugin This plugin provides an stable API to Bouncy Castle related tasks.	2.17		Uninstall
<input checked="" type="checkbox"/>	Command Agent Launcher Plugin Allows agents to be launched using a specified command.	1.3		Uninstall
<input checked="" type="checkbox"/>	Credentials Plugin This plugin allows you to store credentials in Jenkins.	2.1.19		Uninstall
<input checked="" type="checkbox"/>	Official OWASP ZAP Jenkins Plugin The Official OWASP ZAP Jenkins Plugin extends the functionality of the ZAP security tool into a CI Environment.	1.1.0		Uninstall

Global Config Settings

- Go to Manage Jenkins → Configure system
- Get ZAP zip from git url, download it to some location at app server

<https://github.com/trainmefordevsecops/owasp-zap.git>

ZAP

Default Host

localhost



Default Port

8090



Jenkins Agent : Env Setup

- Go to Jenkins Agent for App server
- Provide the location of downloaded zap unzip file as shown below

Node Properties

☐ Disable deferred wipeout on this node 

☒ Environment variables

List of variables

Name

Value



Delete

Follow Instructions For Jenkins Job Setup

Build

 Execute ZAP

X

Admin Configurations

Workspace `/home/appuser/jenkins-agent/workspace/OWASP-ZAP`

Override Host



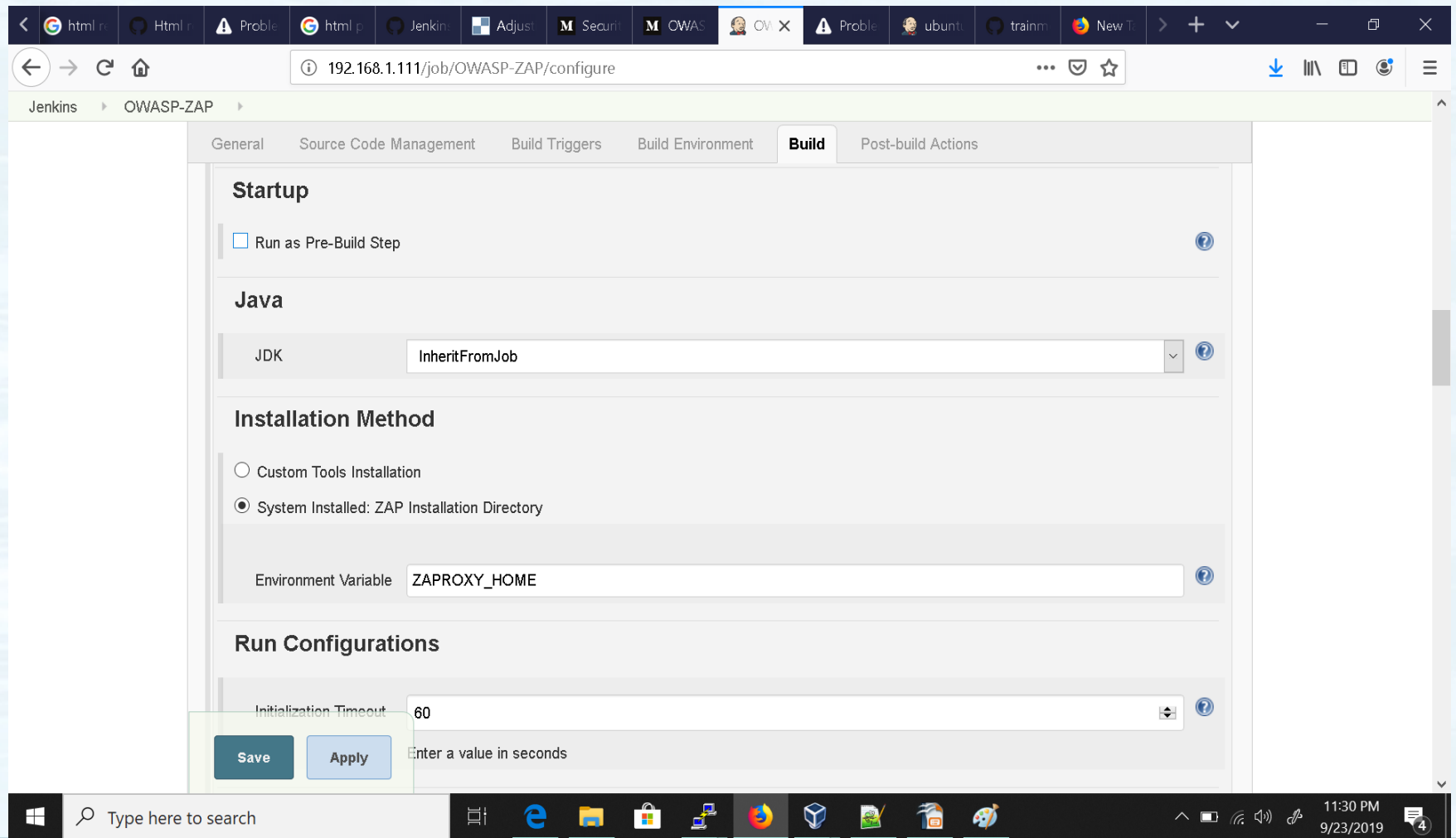
Default Host is : localhost (Configured under Manage Jenkins > Configure System)

Override Port



Default Port is : 8090 (Configured under Manage Jenkins > Configure System)

Jenkins Job Setup



The screenshot displays the Jenkins web interface for configuring a job named 'OWASP-ZAP'. The browser's address bar shows the URL '192.168.1.111/job/OWASP-ZAP/configure'. The configuration page has several tabs: 'General', 'Source Code Management', 'Build Triggers', 'Build Environment', 'Build' (which is currently selected), and 'Post-build Actions'. The 'Build' tab contains three main sections: 'Startup', 'Java', and 'Installation Method'. In the 'Startup' section, the checkbox 'Run as Pre-Build Step' is unchecked. The 'Java' section shows 'JDK' set to 'InheritFromJob'. The 'Installation Method' section has two radio buttons: 'Custom Tools Installation' (unselected) and 'System Installed: ZAP Installation Directory' (selected). Below these, an 'Environment Variable' is set to 'ZAPROXY_HOME'. The 'Run Configurations' section at the bottom shows 'Initialization Timeout' set to '60' seconds. At the bottom of the configuration area, there are 'Save' and 'Apply' buttons. The Windows taskbar at the bottom of the screen shows the time as 11:30 PM on 9/23/2019.

192.168.1.111/job/OWASP-ZAP/configure

Jenkins > OWASP-ZAP >

General Source Code Management Build Triggers Build Environment **Build** Post-build Actions

Startup

☐ Run as Pre-Build Step

Java

JDK InheritFromJob

Installation Method

☐ Custom Tools Installation

☒ System Installed: ZAP Installation Directory

Environment Variable ZAPROXY_HOME

Run Configurations

Initialization Timeout 60

Save Apply Enter a value in seconds

Type here to search

11:30 PM 9/23/2019

Jenkins Job Setup

ZAP Home Directory

Path

`${WORKSPACE}/OWASP-ZAP`



Session Management

- ☐ Load Session
- ☒ Persist Session

Filename

`Session_${BUILD_ID}`



☐ Remove External Sites



Session Properties

Context Name

default



Include in Context

`http://multiplayer-snake.tk/*`



Jenkins Job Setup

Attack Mode

Starting Point



☒ Spider Scan



☒ Recurse



☐ Subtree Only



Max Children to Crawl



☐ AJAX Spider



☒ Active Scan



Policy



☒ Recurse





Save

Apply

Jenkins Job Setup

Finalize Run

☒ Generate Reports 

☒ Clean Workspace Reports 

Filename

JENKINS_ZAP_VULNERABILITY_REPORT 

☐ Generate Report

Format

xml
html 

HTTP ERROR 404

Problem accessing /job/OWASP-ZAP/null. Reason:

Not Found

Powered by [Jetty:// 9.4.z-SNAPSHOT](#)

Jenkins Job

Publish HTML reports

Reports

HTML directory to archive



Index page[s]

*.html



Index page title[s] (Optional)



Report title

OWASP-ZAP-REPORT



Keep past HTML reports

☐

Always link to last build

☒

Allow missing report

☐

Include files

reports/*.html

Follows the Ant glob syntax, such as `**/*.html,**/*.css`

Escape underscores in Report Title ☒

