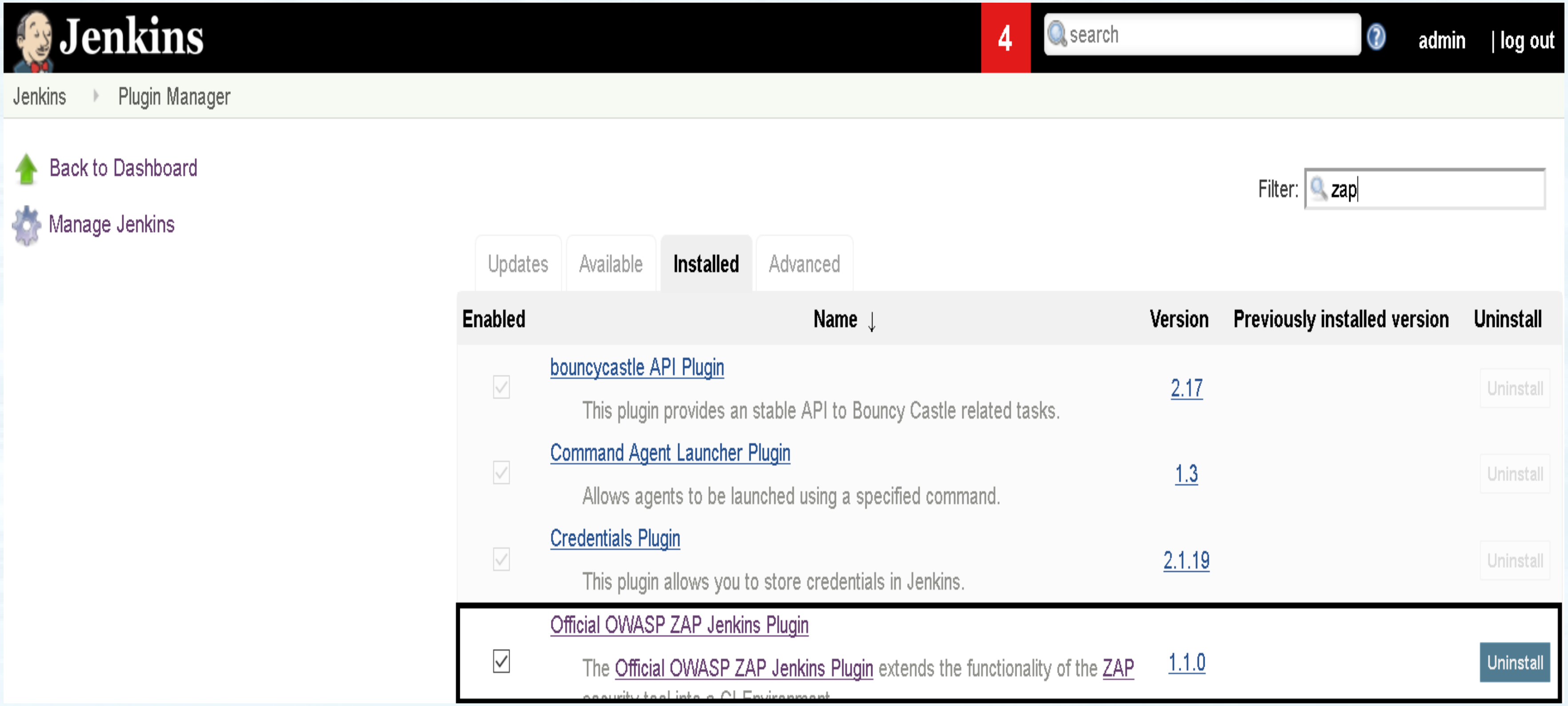
DAST SECURITY : OWASP-ZAP

- 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

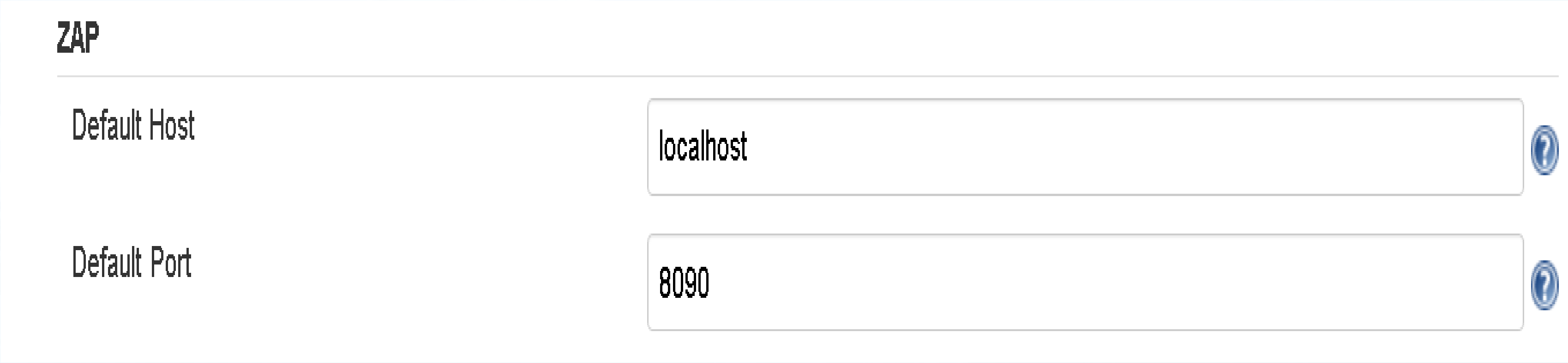


Enabled	Name ↓	Version	Previously installed version	Uninstall
☑	bouncycastle API Plugin This plugin provides an stable API to Bouncy Castle related tasks.	2.17		Uninstall
☑	Command Agent Launcher Plugin Allows agents to be launched using a specified command.	1.3		Uninstall
☑	Credentials Plugin This plugin allows you to store credentials in Jenkins.	2.1.19		Uninstall
☑	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, downlaod it to some location at app server

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



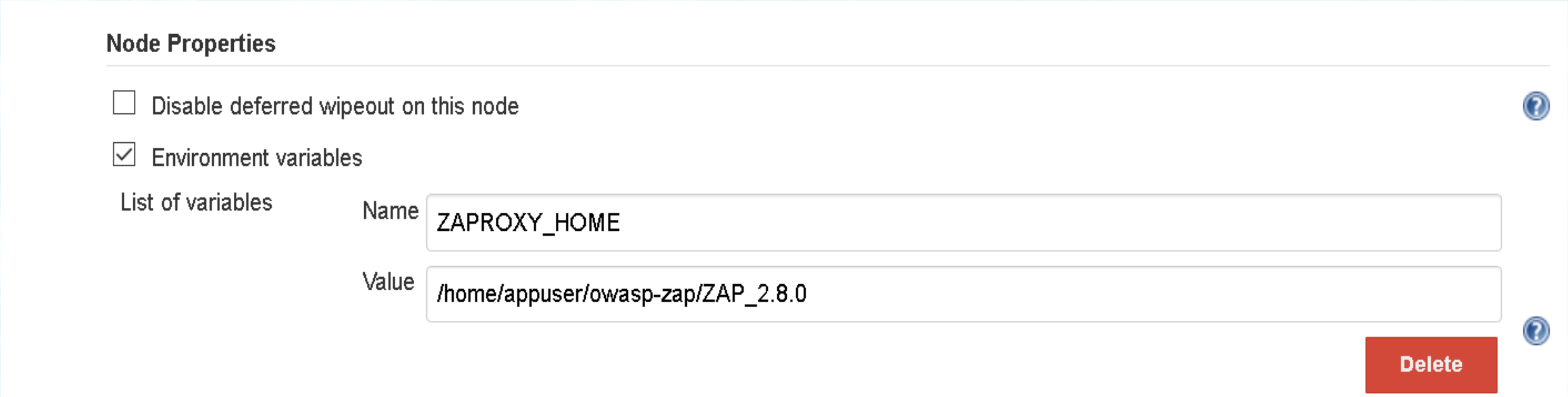
ZAP

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

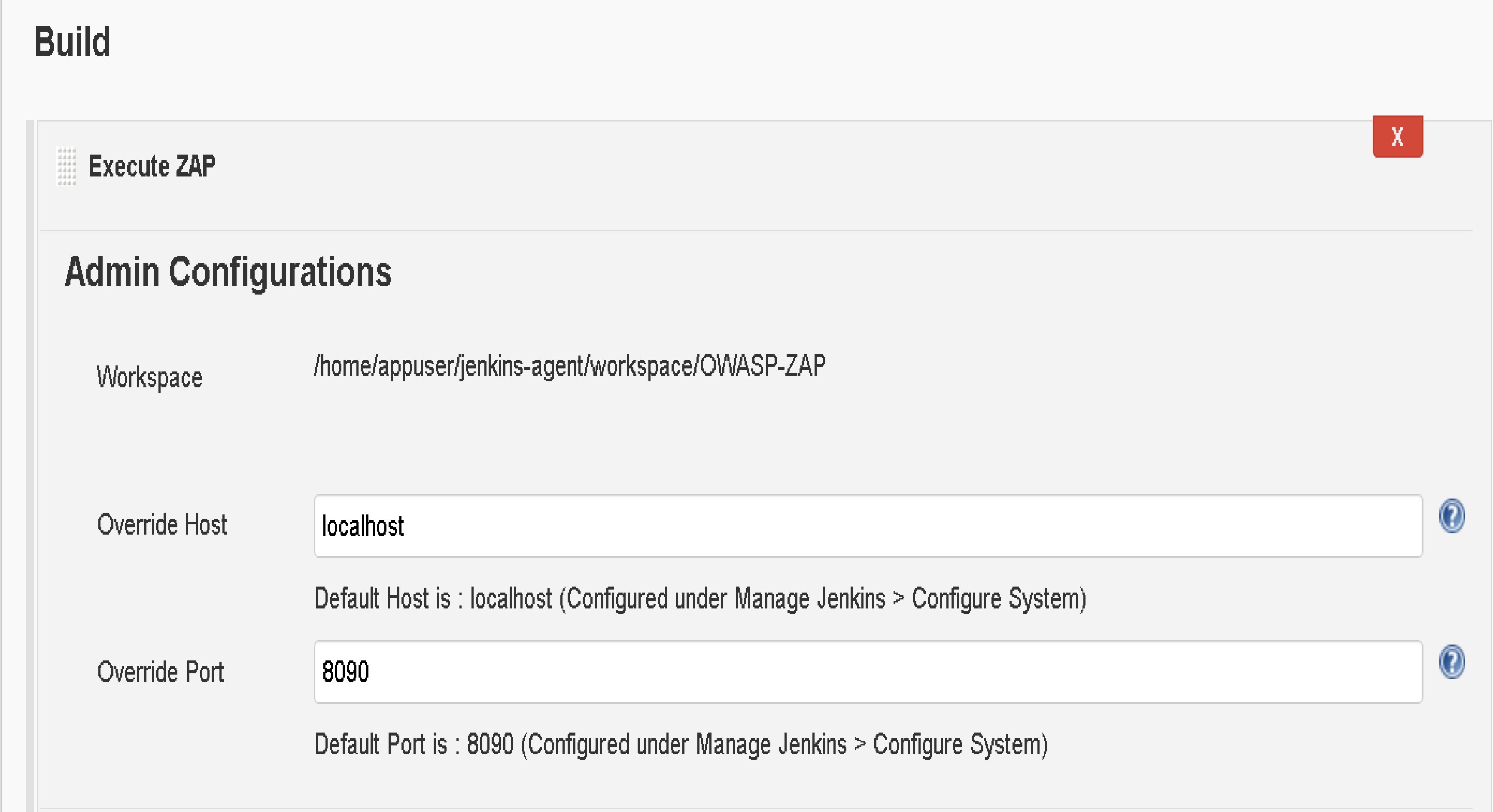
☑ Environment variables

List of variables

Name: ZAPROXY_HOME

Value: /home/appuser/owasp-zap/ZAP_2.8.0

Follow Instructions For Jenkins Job Setup



Admin Configurations

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

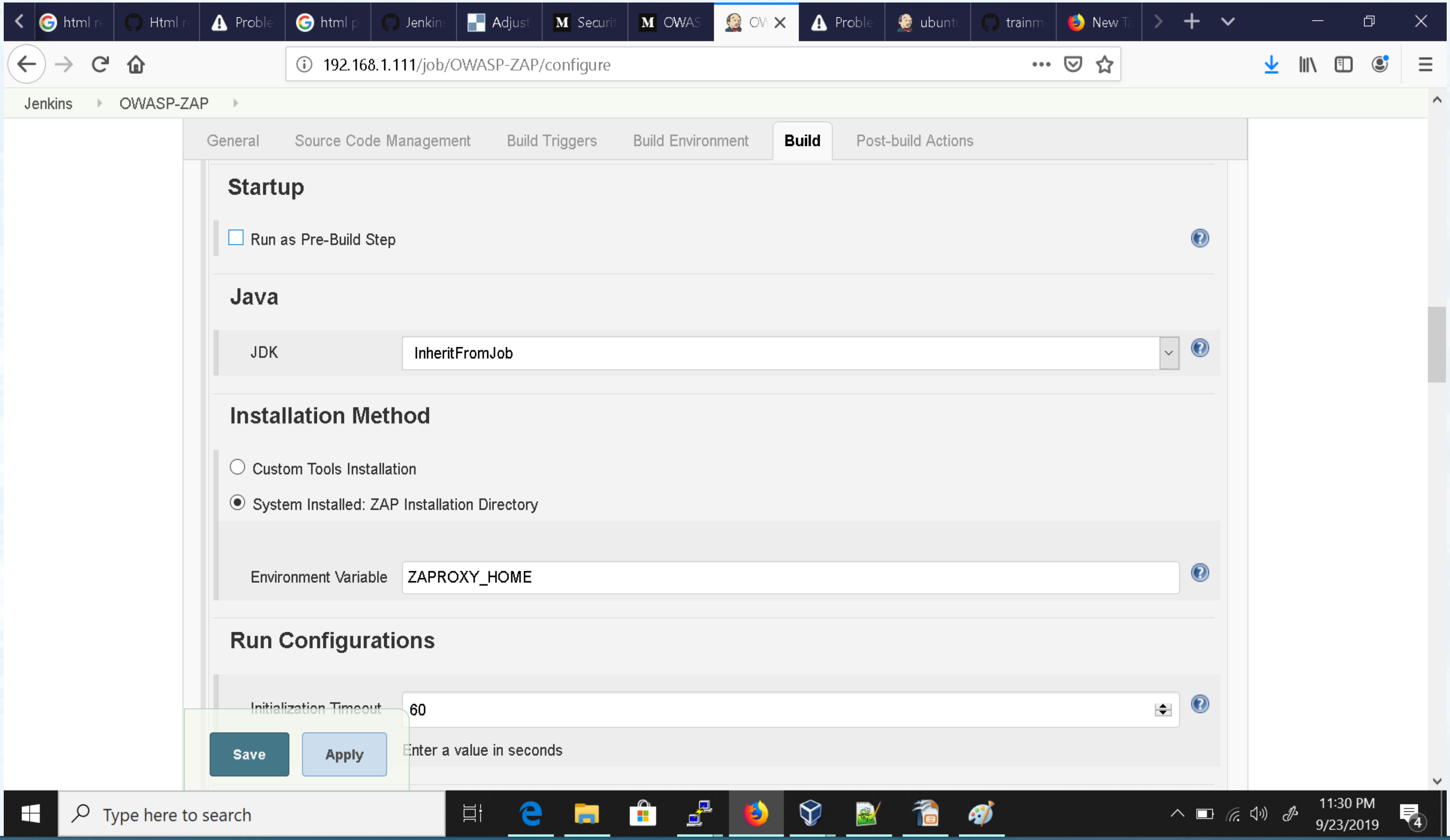
Override Host: localhost

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

Override Port: 8090

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

Jenkins Job Setup



192.168.1.111/job/OWASP-ZAP/configure

Startup

□ Run as Pre-Build Step

Java

JDK: InheritFromJob

Installation Method

○ Custom Tools Installation

● System Installed: ZAP Installation Directory

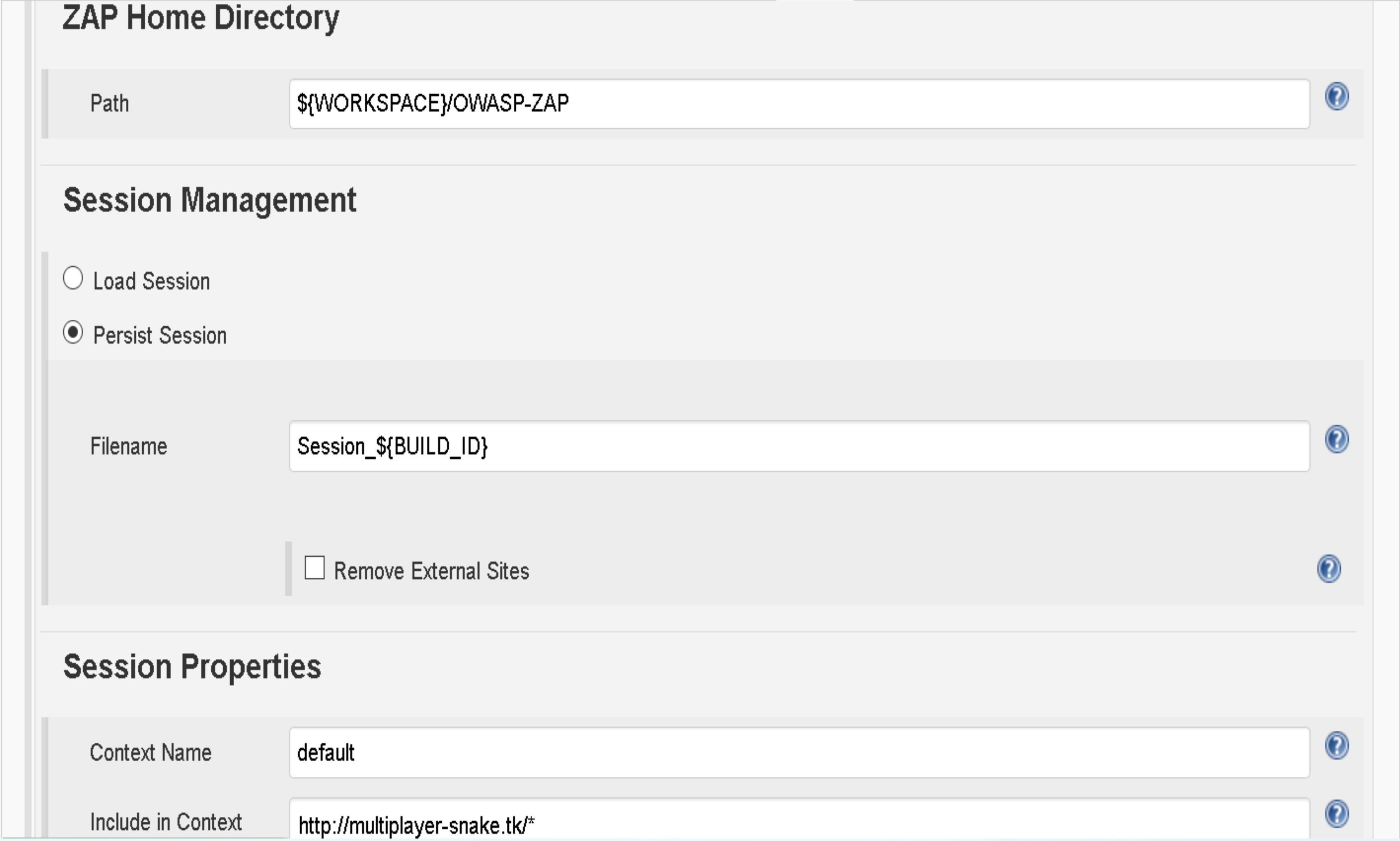
Environment Variable: ZAPROXY_HOME

Run Configurations

Initialization Timeout: 60

Enter a value in seconds

Jenkins Job Setup



ZAP Home Directory

Path: ${WORKSPACE}/OWASP-ZAP

Session Management

○ Load Session

● Persist Session

Filename: Session_${BUILD_ID}

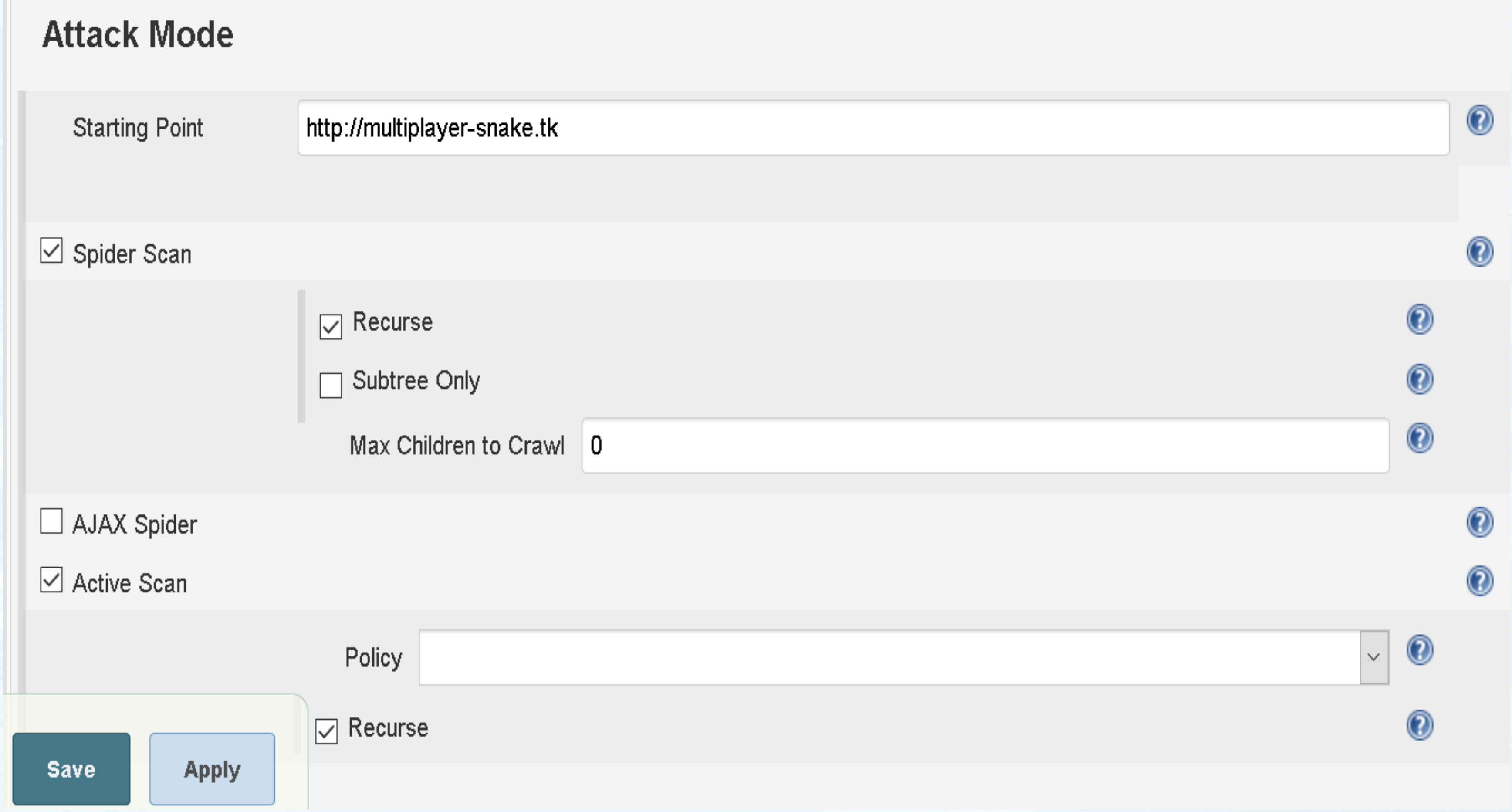
□ Remove External Sites

Session Properties

Context Name: default

Include in Context: http://multiplayer-snake.tk/*

Jenkins Job Setup



Attack Mode

Starting Point: http://multiplayer-snake.tk

☑ Spider Scan

☑ Recurse

□ Subtree Only

Max Children to Crawl: 0

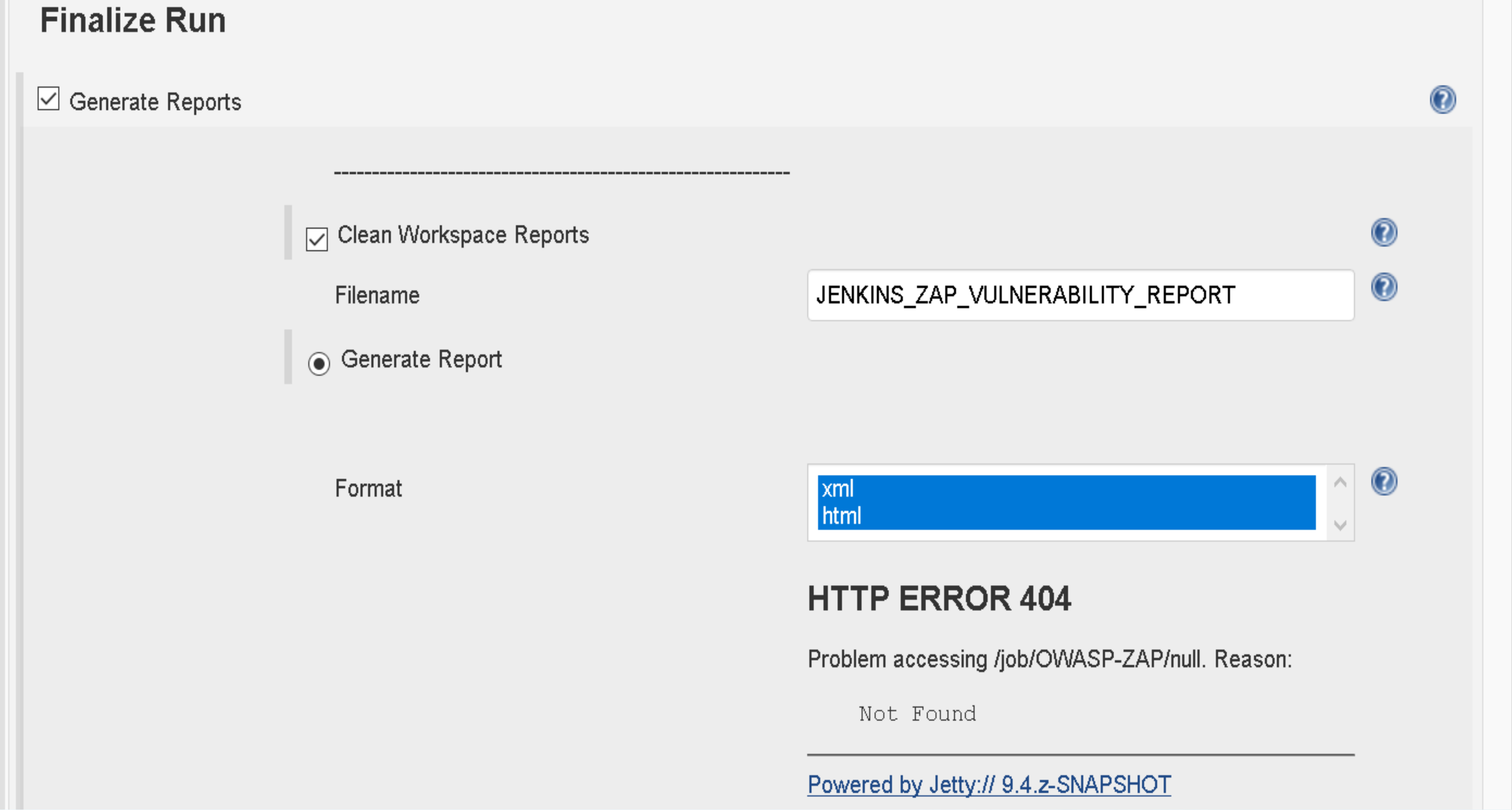
□ AJAX Spider

☑ Active Scan

Policy:

☑ Recurse

Jenkins Job Setup



Finalize Run

☑ Generate Reports

☑ Clean Workspace Reports

Filename: JENKINS_ZAP_VULNERABILITY_REPORT

● Generate Report

Format: xml, html

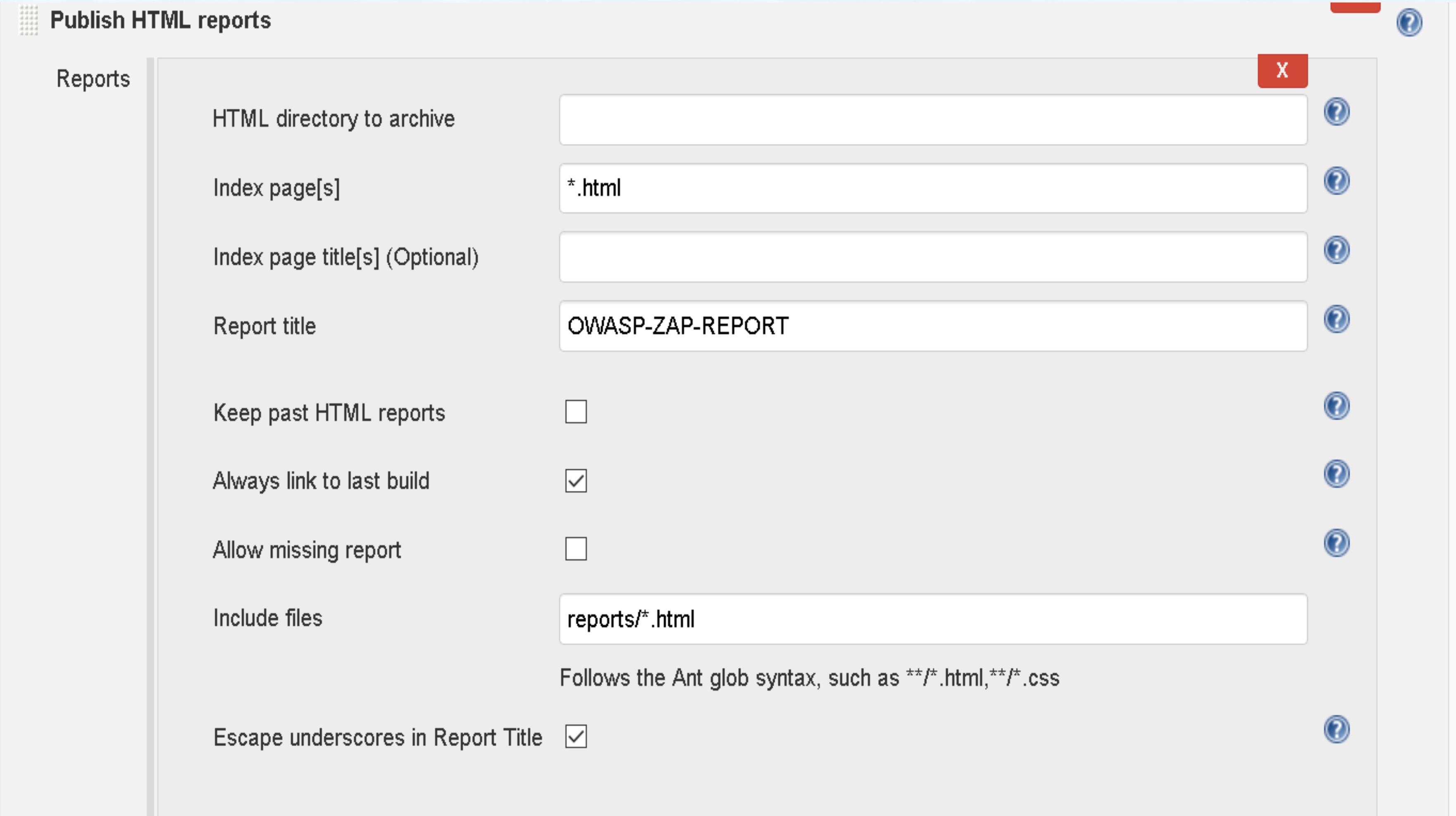
HTTP ERROR 404

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

```
    Not Found
```

Powered by Jetty:// 9.4.z-SNAPSHOT

Jenkins Job



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 ☑