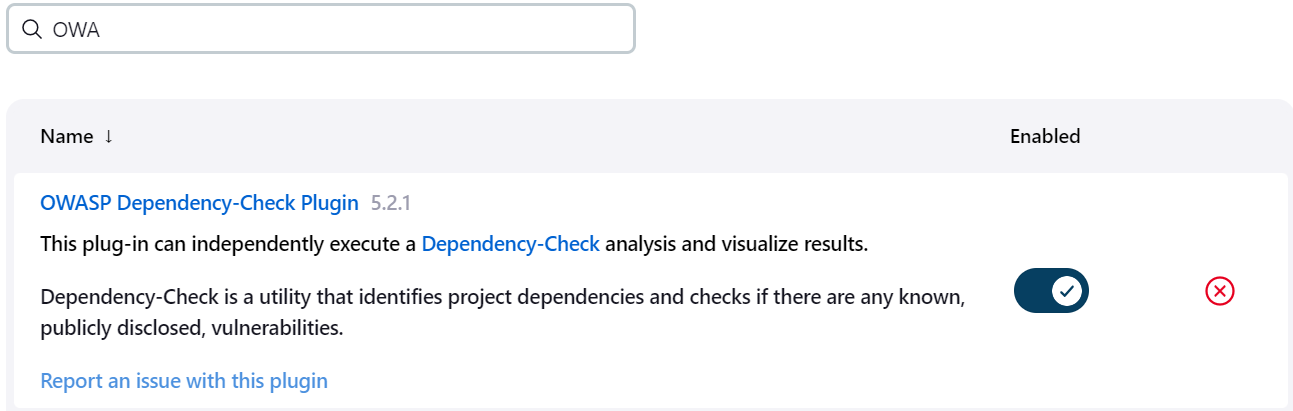
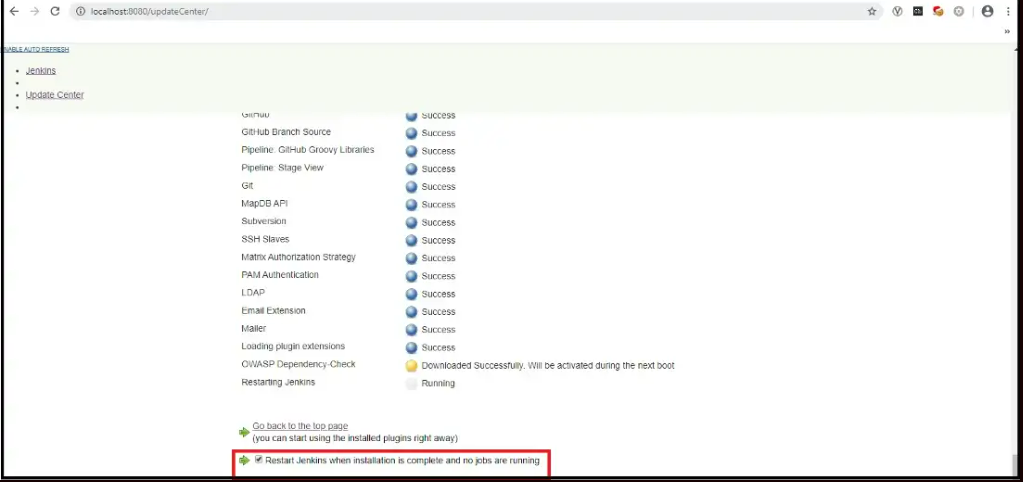
OWASP dependency-check is an open source solution the OWASP Top 10 2013 entry: A9 — Using Components with Known Vulnerabilities. Dependency-check can be used to scan Java and .NET applications to identify the known vulnerable components.

Step 1: Download the OWASP-dependency-check plugin from plugin manager (Manage Jenkins -> Manage Plugins -> Available)

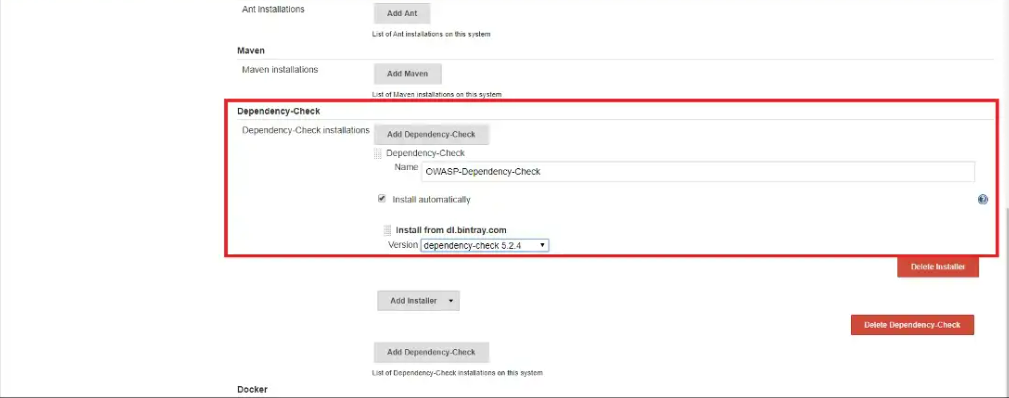


**Step 2:** Even though restart is not mandatory , it is recommended to restart. Once download is done, check on restart jenkins. If restart doesn’t start properly, then navigate to [http://localhost:8080/](http://localhost:8080/restart)restart to restart jenkins manually.



**Step 3:**Post successful installation and jenkins service restart, navigate to Global tools configuration (Manage Jenkins -> Global Tools Configuration) to configure dependency check.

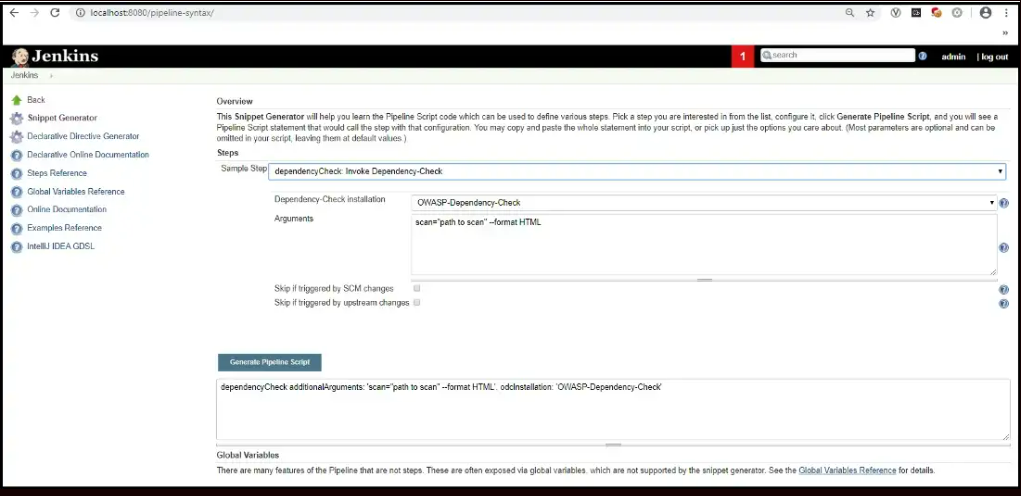
Click on ‘Add Dependency Check’ and provide name to convenience. The version by default will point to the latest release.



Step 4: dependency check can be invoked using a pipeline script. The pipeline script functionality can be accessed from the URL : <http://localhost:8080/pipeline-syntax/>

Select ‘dependecycheck: Invoke dependency check’ from sample step. Provide the scan arguments and click on ‘Generate pipeline script’ to generate the script.

**stage('OWASP-Dependency-Check'){  
            steps{  
              //Checking the 3rd-Party labarary that are be used in the code to build Application .//  
              //Means check they are having any variability  or not //  
                dependencyCheck additionalArguments: '--scan /var/lib/jenkins/workspace/${JOB\_NAME} --format ALL --disableYarnAudit', odcInstallation: 'OWASP-Dependency-Check'   
  
            }  
        }**



**Step 5:**Provide the arguments to perform the dependency checker. For demo purpose i have configured the scan to be basic. More options can be explored at: <https://jeremylong.github.io/DependencyCheck/dependency-check-cli/arguments.html>

**Step 6:**Build the project now and if it’s the first time, then Dependency checker will reach out to NVD CVE data hosted by NIST and Retire JS repo to fetch updated data. Once the database is build locally with the downloaded data, dependency analysis will be performed.

**Step 7:** Post analysis, navigate to workspace folder to access the scan report from UI.



**ISSUE FACING: -**

**[WARN] The Yarn Audit Analyzer has been disabled. Yarn executable was not found.**

**[ERROR] Exception occurred initializing Yarn Audit Analyzer.**

**Debugging: -**

**ADD --disableYarnAudit' in Jenkins Stage:-**

**stage('OWASP-Dependency-Check'){  
            steps{  
              //Checking the 3rd-Party labarary that are be used in the code to build Application .//  
              //Means check they are having any variability  or not //  
                dependencyCheck additionalArguments: '--scan /var/lib/jenkins/workspace/${JOB\_NAME} --format ALL --disableYarnAudit', odcInstallation: 'OWASP-Dependency-Check'   
  
            }  
        }**

**OWASP DEPENDENCY CHECK RESULT SHOW ON JENKINS.**

**stage('OWASP-Dependency-Check'){**

**steps{**

**dependencyCheck additionalArguments: '--scan /var/lib/jenkins/workspace/${JOB\_NAME} --format ALL --disableYarnAudit', odcInstallation: 'OWASP-Dependency-Check'**

**dependencyCheckPublisher pattern: '\*\*/dependency-check-report.xml', unstableNewCritical: 1, unstableNewHigh: 2, unstableTotalCritical: 1, unstableTotalHigh: 2**

**//\*\*/dependency-check-report.xml**

**}**

**}**