About OWASP Dependency Check

> **History**
>
> Please refer to history for information on released and older trunk versions. The links might fail though, since the OFBiz svn repo structure has changed while splitting frameworks from plugins.

OWASP Dependency Check is a tool for checking the Java libraries you use have no security issues. We use it through a Gradle plugin.
Once the CVEs references the Gradle dependencies are up to date, as of 2016/09/05, it takes 3,5 minutes on a standard machine to check the dependencies (it was 2+ minutes before Gradle)

Here is the Gradle command line to use to start the check:

```
gradlew -PenableDependencyUpdates dependencyUpdates -Drevision=release
```

Trunk reports

It's best to first update the dependencies before generating a report. We use
OFBIZ-10213 - Update build.gradle to the latest dependencies IN PROGRESS for that.

Here is the last report file for the trunk (2019-10-09).
There is also the tools\security folder with some information.

Since OFBiz uses Gradle, all dependent libraries (ie also dependencies from the libraries OFBiz uses and recursively) are loaded by Gradle and analysed by the OWASP Dependency Check plugin. So it's materially impossible to check all the possible vulnerabilities.

By crossing information from dependency updates and dependency check we can know if we have real dependency security issues.

You can also check in the main build.gradle, that the libs are not directly used by OFBiz but by libs used by plugins. As of 2019-10-09, there are no libs directly used by OFBiz with security issues.

Libs that can't be updated in their last version

So we keep the current version in OFBiz trunk. You may try newer version thatn below but most of the time it does not work either.

- at.bxm.svntools:at.bxm.svntools.gradle.plugin [2.2.1 -> 3.0]
- com.lowagie:itext [2.1.7 -> 4.2.2]
- org.apache.derby:derby [10.14.2.0 -> 10.15.2.0]
- org.apache.sshd:sshd-core [1.7.0 -> 2.4.0]
- org.apache.tomcat:tomcat-catalina-ha [9.0.34 -> 10.0.0-M3]
- org.apache.tomcat:tomcat-jasper [9.0.34 -> 10.0.0-M3]
- org.apache.tomcat.embed:tomcat-embed-websocket [9.0.34 -> 10.0.0-M3]
- org.apache.xmlgraphics:fop [2.3 -> 2.4]
- org.codehaus.groovy:groovy-all [2.5.8 -> 3.0.3]
- org.jasig.cas:cas-server-core [3.3.5 -> 4.2.7]
- org.apache.shiro:shiro-core [1.4.1 -> 1.5.3]
- I tried to update Solr and Lucene to 8.7.0 but crossed issues (compilation and Eclipse classpath)
- Same for Jersey with 3.0.0 version

Also be sure to check the main build.gradle. Some Java classes need internal versions update too:

- SearchWorker
- FreeMarkerWorker

Also Solr et Lucene should use the same version, luceneMatchVersion should be updated in solrconfig.xml