snyk Cheat Sheet: M 10 Maven Security Best Practices

www.snyk.io

1. Encrypt your Secrets

```
$ mvn --encrypt-master-password
Master password: *********
{encrypted_master_password}
```

Store this in `~/.m2/settings-security.xml`

```
<settingsSecurity>
  <master>{encrypted_master_password}</master>
</settingsSecurity>
```

Now encrypt your server password:

```
mvn --encrypt-password
Master password: *********
{encrypted_password}
```

Store this in your `settings.xml` file as follows:

```
<server>
  <id>my.server</id>
  <username>smaple</username>
  <password>{encrypted_password}</password>
</server>
```

2. Don't use passwords in the CLI

Never enter passwords in plain text on the CLI:

```
$ mvn --encrypt-master-password P@ssw0rd

$ mvn --encrypt-password P@ssw0rd
```

3. Always Use HTTPS

Use HTTPS to connect to remote Maven repositories, to avoid MITM attacks.

Ensure your `<repositories>` and `<pluginRepositories>` use https in their URLs.

4. Check Dependency Health

Verify the health of your third-party libraries by confirming they have:

- A team of committers
- Well documented security policies
- Regular updates and releases

5. Test for Known Vulnerabilities

Do not use Maven dependencies with known vulnerabilities. Use a tool like Snyk to:

- Test your app for known vulnerabilities.
- Automatically fix issues that exist.
- Continuously monitor for new vulnerabilities

6. Test your Checksums

As part of validating the authenticity of your dependencies, test their checksums using the `-C` flag on Maven commands:

```
$ mvn -C install
// fail if checksums don't match

$ mvn -c install
// warn if checksums don't match
```

7. Don't use Properties for Passwords

Never store your secrets in your pom.xml properties.

```
<properties>
    <my.property>P@ssw0rd</my.property>
  </properties>
```

8. Use Maven developers/roles

Use Maven roles to state who should be contacted for security issues.

```
<developers>
    <developer>
      <id>grander</id>
      <name>Danny Grander</name>
      <email>security@your_org.com</email>
      <roles>
        <role>security</role>
      </roles>
    <developer>
<developers>
```

9. Stay up-to-date

Try to stay on the latest releases of Maven. Check the download page for the latest version.

Avoid Maven 3.0.4 as it ignores certificates for HTTPS connections.

10. Check Security Bulletins

Monitor the security bulletins the Apache Maven team publish on the Maven site.

Authors:


@sjmaple
Java Champion and Developer Advocate at Snyk


@rfscholte
CEO of Sourcegrounds, Chairman of the Apache Maven project