Cheat sheet: 10 Java security best practices

snyk

1. Use query parameterization

Use prepared statements in Java to parameterize your SQL statements.

❌
```
String query = "SELECT * FROM USERS WHERE
lastname = " + parameter;
```

✅
```
String query = "SELECT * FROM USERS WHERE
lastname = ?";
   PreparedStatement statement =
connection.prepareStatement(query);
   statement.setString(1, parameter);
```

2. Use OpenID Connect with 2FA

OpenID Connect (OIDC) provides user information via an ID token in addition to an access token. Query the /userinfo endpoint for additional user information.

3. Scan your dependencies for known vulnerabilities

Ensure your application does not use dependencies with known vulnerabilities. Use a tool like Snyk to:

- Test your app dependencies for known vulnerabilities
- Automatically fix any existing issues
- Continuously monitor your projects for new vulnerabilities over time

4. Handle sensitive data with care

Sanitize the toString() methods of your domain entities.

If using Lombok, annotate sensitive classes. `@ToString.Exclude`

Use `@JsonIgnore and @JsonIgnoreProperties` to prevent sensitive properties from being serialized or deserialized.

5. Sanitize all input

Consider using the OWASP Java encoding library to sanitize input.

Assume all input is potentially malicious, and check for inappropriate characters (whitelist preferable).

6. Configure your XML parsers to prevent XXE

Disable features that allow XXE on your SAXParserFactory and SAXParser, or equivalent.

```
SAXParserFactory factory = SAXParserFactory.
newInstance();
SAXParser saxParser = factory.newSAXParser();

factory.setFeature("http://xml.org/sax/features/
external-general-entities", false);
saxParser.getXMLReader().setFea-
ture("http://xml.org/sax/fea-
tures/external-general-entities", false);
factory.setFeature("http://apache.org/xml/
features/disallow-doctype-decl", true);
```

7. Avoid Java serialization

If you must implement the serialization interface, override the readObject method to throw an exception.

```
private final void readObject(ObjectInputStream in)
throws java.io.IOException {
   throw new java.io.IOException("Not allowed");
}
```

If you have to deserialize, use the ValidatingObjectInputStream from Apache Commons IO to add some safety checks.

```
FileInputStream fileInput = new FileInputStream
(fileName);
ValidatingObjectInputStream in = new Validatin
gObjectInputStream(fileInput);
in.accept(Foo.class);

Foo foo_ = (Foo) in.readObject();
```

8. Use strong encryption and hashing algorithms

Always use existing encryption libraries, such as Google Tink, rather than doing it yourself.

For password hashing, consider using BCrypt or SCrypt. If using Spring, you can use it's built-in BCryptPasswordEncoder and SCryptPasswordEncoder for your hashing needs.

9. Enable the Java security manager

Enable via JVM properties on startup:

```
-Djava.security.manager
```

Create a policy that you use for your applications:

```
-Djava.security.policy==/my/custom.policy
```

10. Centralize logging and monitoring

Log auditable events, such as exceptions, logins and failed logins with useful information including their origin.

Centralize logs from multiple servers with tools like Kibana.

Monitor key system resources that indicate attack spikes or load from specific IP addresses.

Authors

@BrianVerm
Developer Advocate at Snyk

@manicode
Java Champion & Manicode Security founder