Fakultät für Informatik
Prof. Dr. R. Hüttl

IT-Security

Exercise 10

Task 1: OWASP Dependency Check

In this exercise, we use the OWASP Dependency Check to find outdated components or components with vulnerabilities in an application.

To do this, you must first install the **Command Line** Tool Dependency Check from OWASP:

1. Download https://owasp.org/www-project-dependency-check/ Command Line version
2. For installation, see https://jereub.io/DependencyCheck/ and https://jeremylong.github.io/DependencyCheck/dependency-check-cli/index.html
3. Download the zip file and unzip it
   Extend the PATH variable with the bin directory of Dependency Check
4. Then the dependency-check commands can be called via cmd window

We are now reviewing the WebGoat application. This is an unsafe application of OWASP for training purposes.

- Download Web Goat „Standalone jars“
  https://owasp.org/www-project-webgoat/
  or
  https://github.com/WebGoat/WebGoat/releases/tag/v8.2.2

- Open a console (cmd) and navigate to the folder where Webgoat's jar file is located

- Now use the OWASP Dependency Check to analyze the webgoat-server-8.2.2.jar file
  Command: dependency-check –s . webgoat-server-8.2.2.jar (Windows)
  dependency-check.sh –scan . webgoat-server-8.2.2.jar (Linux, Mac)

Look at the generated report and familiarize yourself with the terms CVE and CVSS. Use a search engine to find the discussions in the developer forums about the security issues. It is best to search for the CVE number. Get an overview of which vulnerability is a specific problem.

Task 2: Dependency check of one of your current projects

Perform a dependency check of a project in which you are/were involved, e.g. your SEP project.

In addition to Java, other technologies are also supported:
https://jeremylong.github.io/DependencyCheck/analyzers/index.html

Take a look at the report and consider whether you need to become active in your project.

Task 3: Awareness Training Part 2

https://training.is-fox.de/fh-rosenheim-informatik

We complete the modules from out awareness Training in Exercise 1.

We start with the modules which are related to our chapter Authentication&Autorization

- Secure Passwords
- Password management
- Multi-factor authencation

Then we finish the training with the modules

- E-mail & phishing
- Sensitive information
- Social engineering