Fachbereich Informatik
Prof. Dr. R. Hüttl

IT-Security

Übung 10

Aufgabe 1: OWASP Mutillidae 2 Web Pen Test

In dieser Übung arbeiten wir weiter mit der OWASP Mutillidae 2 Web Pen Test Training Environment.

Jeder Teilnehmer der Übung sucht sich als Hausaufgabe vor der Übung eine Sicherheitslücke von Mutillidae aus und führt sie den anderen in der Übung per Videokonferenz vor.

Dabei suchen wir nach den Sicherheitslücken, die wir schon in unserem Vortrag in Übung 8 behandelt haben:

- A2 Broken Authentication:
- A3 Sensitive data exposure:
- A4 XML External Entities:
- A5 : Broken Access Control:
- A6 Security Misconfiguration:
- A8 Insecure Desirialization:
- A10 : Insufficient Logging and monitoring:

Alle anderen suchen sich eine OWASP-Schwachstelle ihrer Wahl aus.

Aufgabe 2: OWASP Dependency Check

In dieser Übung verwenden wir den OWASP Dependency Check, um in einer Anwendung veraltete Komponenten bzw. Komponenten mit Verwundbarkeiten zu finden.

Dazu müssen sie zuerst des **Command Line** Tool Dependency Check von OWASP installieren:

1. Unter https://owasp.org/www-project-dependency-check/ Command Line version herunterladen
2. Installation siehe https://jereub.io/DependencyCheck/ und https://jeremylong.github.io/DependencyCheck/dependency-check-cli/index.html
3. Zip-datei herunterladen und entpacken.
   PATH Variable um das Verzeichnis *bin* von Dependency Check erweitern
4. Dann kann über cmd-Fenster der Befehl dependency-check aufgerufen werden

Wir überprüfen nun die Anwendung WebGoat. Das ist eine unsichere Anwendung von OWASP für Übungszwecke.

- Web Goat „Standalone jars“ herunterladen
  https://owasp.org/www-project-webgoat/

oder
https://github.com/WebGoat/WebGoat/releases/tag/v8.1.0

- Eine Console (cmd) öffnen und in den Ordner navigieren in dem die jar-Datei von Webgoat steht

- Nun mit dem OWASP Dependency Check die Datei webgoat-server-8.1.0.jar analysieren
  Aufruf: dependency-check –s . webgoat-server-8.1.0.jar (Windows)
  dependency-check.sh –scan . webgoat-server-8.1.0.jar (Linux, Mac)

Schaut sie den erzeugten Report an und macht sie sich mit den Begriffen CVE und CVSS vertraut. Verwenden sie eine Suchmaschine, um die Diskussionen in den Entwicklerforen zu den Sicherheitsproblemen zu finden. Suchen sie am besten nach der CVE-Nummer. Verschaffen sie sich einen Überblick, welche Sicherheitslücke ein konkretes Problem ist.