LU02d - LB2 - Projektauftrag

1. Projektauftrag

Ihr Auftrag besteht darin eine vulnerable Applikation zu programmieren und diese anschliessend mit geeigneten pogrammiertechnischen Massnahmen zu schützen.

Teil 1

Programmieren Sie eine Applikation, die mit den nachfolgenden Techniken angreifbar ist (vulnerable). Der Angriffsvektor kann entweder über eine Front-End-Schnittstelle oder über ein Backend-Script/File erfolgen.

Teil 2

Programmieren Sie die gleiche Applikation als sichere Version (secured), in der Sie die definierten Sicherheitsmassnahmen programmiertechnisch umsetzen.

2. Metaziele

Die Arbeit ist, gmäss Unterrichts-Input, bezüglich der CIA-Triad auszurichten. Idealerweise können Sie gegen alle 3 Meta-Ziele (Verfügbarkeit, Vertraulichkeit, Integrität) angreifen.

Selbstverständlich erstellen Sie die Sicherheitsmassnahmen so aus, dass diese Angriffe im 2. Teilauftrag nicht mehr möglich sind.

3. Ablauf

- Es werden zufällig Teams zu je 2 Personen gebildet
- Die Lehrersperson kommuniziert:
  - den Auftrag und den Umfang (Was ist zu liefern)
  - die Themen
  - die Zuteilung der Team zu den Themen
- Die Arbeitsaufteilung muss klar ersichtlich sein: Sie arbeiten am gleichen Projekt, jedoch an unterschiedlichen Teilen: Angriff VS. Verteidigung
- Die Leistungsüberprüfung geschieht durch ein Video-aufgezeichnetes Fachgespräch.
- Jedes Mitglied kann Auskunft über alle Codeteile geben, d.h. Wissenstransfer liegt in der Verantwortung der Lernenden
- Bewertet wird nach einem vorher definierten Bewertungsraster
- Je 2 Teams erhalten den gleichen Auftrag, das Team mit der besten Leistung erhält einen Bonus von 0.25 Notenpunkte

4. Themen

Die nachfolgenden Themen stehen zur Verfügung:

1. SQLi
2. BruteForce

5. Lieferumfang

- 1. Präsentionsschicht: Frontend oder Simulation
  - Script für den Angriff
  - Kann auch mit Postman o.ä. simuliert werden
- 2. Logikschicht: Businesslokig/Server
  - Script mit der unsicheren Variante
  - Script mit der sicheren Variante (ungesetzte Sicherheitsmassnahmen)
- 3. Datenschicht: Persistente Datenhaltung
  - Datenbank-Instanz
  - Wörderbücher
  - etc

6. Erlaubte Technologien

Die nachfolgenden Technologien stehen Ihnen zur Verfügung.

- HTML-CSS
- Programmiersprachen:
  - JavaScript
  - Python
  - Shell/BASH
- Node.js Laufzeitumgebung (Analog andere Programmiersprachen)
- CodeEditor Visual Studio Code, Webstorm oder Pycharm
- Postman Frontend-Simulation
