LU02e - LB2 - Projektauftrag

1. Projektauftrag

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 dem Sie die definierten Sicherheitsmassnahmen programmiertechnisch umsetzen.

2. 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 Notenpunkten

3. Themen

Die nachfolgenden Themen stehen zur Verfügung:

1. SQLi
2. BruteForce
3. DDoS

4. Lieferumfang

1. Zielsetzung: UseCases
2. Konzept: ERD oder Ablaufdiagramm
3. konzept: Architecktur (UML oder ähnliches)
   - 1. Schicht: Frontend oder Simulation
   - 2. Schicht: Server
   - 3. Schicht: Datenbank-Instanz, Wörderbücher, etc
4. Unsichere Version der Software

5. Sichere Version mit entsprechend umgesetzten Programmiermassnahmen

4. Erlaubte Technologien

Die nachfolgenden Technologien stehen Ihnen zur Verfügung.

- HTML-CSS
- JavaScript oder Python
- Node.js Laufzeitumgebung (Analog Python)
- CodeEditor Visual Studio Code, Webstorm oder Pycharm
- Postman Frontend-Simulation
