STI

Sécurité des Technologies Internet

Projet 2. Messagerie électronique sécurisée

Professeur

Abraham Rubinstein

abraham.rubinstein@heig-vd.ch

Assistant

Stéphane Teixeira Carvalho

stephane.teixeiracarvalho@heig-vd.ch

septembre 2021 – février 2022

heig-vd
HAUTE ÉCOLE D'INGÉNIERIE ET DE GESTION DU CANTON DE VAUD
www.heig-vd.ch

Projet n°2

- Objectifs
  - Identifier les failles de sécurité (applicatif uniquement !)
  - Analyse de menaces
  - Sécuriser l'application
- Application de messagerie
  - Même cahier des charges que le projet 1
- Par groupe de 2 étudiants
  - Groupes différents du projet 1 (merci
- Utiliser une image Docker
- Utiliser PHP et SQLite (ou même technologie que P1)
- Si des librairies sont nécessaires,
  les faire valider par le professeur

Projet n°2

- Attentes
  - Respect du cahier des charges
  - Code propre et commenté
  - Analyse de menaces complète
  - Sécurisation de l'application
- Critères de notation
  - Qualité du rendu
  - Rapport de l'analyse de menaces
  - Aspects fonctionnels de l'application
  - Implémentation de la sécurité
  - Manuel (README)

Projet n°2

- Travail encadré
  - Du 20 octobre 2021 au 20 janvier 2022
- Rendu
  - **Vendredi 20 janvier 2021 à 23h59**
  - Docker
  - Rapport de l'analyse de menaces
  - Code de l'application sur GitHub (prof + assistants)
  - Eventuellement base de données
  - Manuel d'installation/utilisation (README)

Projet n°2 - Rapport étude de menaces

- Introduction
- Décrire le système
  - DFD
  - Identifier ses biens
  - Définir le périmètre de sécurisation
- Identifier les sources de menaces
- Identifier les scénarios d'attaques
  - Eléments du système attaqué
  - Motivation(s)
  - Scénario(s) d'attaque
  - STRIDE
- Identifier les contre-mesures
  - En fonction des scénarios d'attaques
- Conclusion