

STI

Sécurité des Technologies Internet

Projet 2. Messagerie électronique sécurisée

Professeur

Abraham Rubinstein

abraham.rubinstein@heig-vd.ch

Assistant

Yann Lederrey

yann.lederrey@heig-vd.ch

Assistante

Lucie Steiner

lucie.steiner@heig-vd.ch

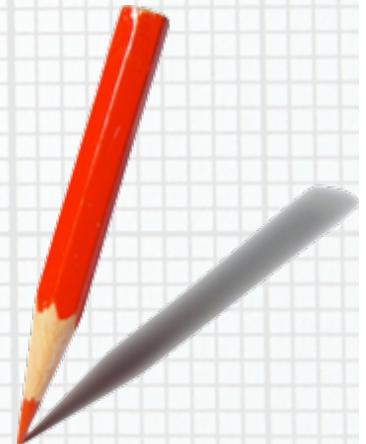
heig-vd

Haute Ecole d'Ingénierie et de Gestion
du Canton de Vaud

septembre 2019 – février 2020

Projet n°2

- Objectifs
 - Identifier les failles de sécurité (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
- Utiliser une image Docker
- Utiliser PHP et SQLite
- Si des librairies sont nécessaires,
les faire valider par le professeur



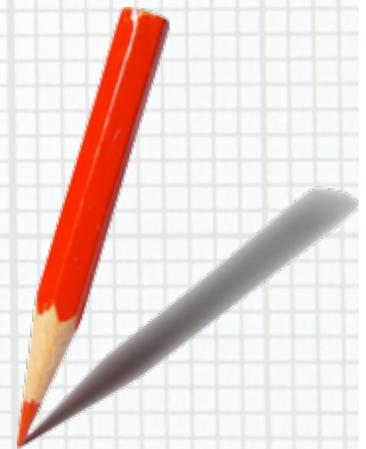
Projet n°2

- 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)
 - Présentation



Projet n°2

- Travail encadré
 - Du 30 octobre 2019 au 15 janvier 2020
- Rendu
 - **Mercredi 15 janvier 2020 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)~~
- Présentations
 - **Du 17 au 24 janvier 2020**
 - Environ 15 minutes de présentation par projet



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

