

Sécurité des Technologies Internet

Projet 2. Messagerie électronique sécurisée

Professeur

Abraham Rubinstein

abraham.rubinstein@heig-vd.ch

Assistant

Yohan Martini

yohan.martini@heig-vd.ch

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 la machine virtuelle CentOS
- 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 PHP 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
 - Présentation



Projet n°2

- Travail encadré
 - Du mercredi 1 novembre au 10 janvier
- Rendu
 - **Lundi 14 janvier 2019 à 12h**
 - Machine virtuelle CentOS ou Docker (si possible) ✓
 - Rapport de l'analyse de menaces
 - Code de l'application par email (prof + assistant)
 - Eventuellement base de données ✓
 - Manuel d'installation/utilisation ✓
- Présentations
 - **Lundi 14 et Lundi 21 2019** ✓
 - Environ 15-20 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

