

Sécurité des Technologies Internet

Projet 1

Abraham Rubinstein

abraham.rubinstein@heig-vd.ch

Septembre 2020 - Février 2021

Objectifs du projet

- Développer une application Web **très simple**
- Application Web permettant d'envoyer des messages de texte entre les collaborateurs d'une entreprise
 - Aucun protocole de communication devra être implémenté
 - Les messages sont tout simplement échangés utilisant une base de données SQLite
- Travail sera réalisé par groupes de **2 étudiants**

Technologies

- Docker
- PHP ou le langage de votre choix
 - PHP hautement conseillé
- SQLite (éventuellement MySQL ou autre)
- Libs/frameworks/etc. à éviter (Bootstrap autorisé pour “embellir” l’application)

Rendu

- Rendu sur un repo GitHub
- Code complet de l'application
- Base de données (si nécessaire)
- Scripts pour déploiement automatique
- Mode d'emploi

Échéance : Mercredi 16 octobre 2020 à 23h59

Cahier des charges

- Définition globale
 - Mise en oeuvre d'une messagerie électronique basée uniquement sur bases de données (pas de SMTP ou autre)
 - Budget limité : aucun budget accordé à la sécurité
 - Une deuxième équipe viendra compléter la sécurité plus tard (P2)
 - Même l'environnement dans lequel l'application tourne pourrait être mal sécurisé
- Authentification
 - Authentification simple - “fait maison”
 - Vous ne pouvez en aucun cas utiliser des modules/paquets/frameworks/etc. vous permettant de simplifier la gestion d'accès et l'authentification
 - Seule la page de login sera accessible sans être authentifié

Cahier des charges

- Rôles et authentification
 - Deux rôles proposés
 - Collaborateur
 - Administrateur
 - Mécanisme d'authentification simple
 - Username
 - Mot de passe
 - Possibilité de rendre un utilisateur “inactif”
- Navigation
 - Navigation aisée d'une page à l'autre, via des liens ou boutons
 - Vous ne pouvez en aucun cas utiliser des modules/paquets/frameworks/etc vous permettant de simplifier la navigation

Fonctionnalités

Collaborateur

- Liste de messages reçus, triée par date de réception affichant
 - Date de réception
 - Expéditeur
 - Sujet
 - Bouton ou lien permettant la réponse au message
 - Bouton ou lien permettant la suppression du message
 - Bouton ou lien permettant d'ouvrir les détails du message

Date	Expéditeur	Sujet	
14.09.20	Donald Trump	Blah blah blah	Répondre Supprimer Lire
15.09.20	Bill Gates	Vaccin Covid	Répondre Supprimer Lire

Fonctionnalités

Collaborateur

- Rédaction d'un nouveau message
 - Destinataire (unique)
 - Sujet
 - Corps du message
- Changement du mot de passe

Fonctionnalités

Administrateur

- Mêmes fonctionnalités qu'un Collaborateur
- En plus :
 - Ajout d'un utilisateur
 - Modification d'un utilisateur
 - Suppression d'un utilisateur
- Un utilisateur est représenté par :
 - Un login ou username (non modifiable)
 - Un mot de passe (modifiable)
 - Une validité (état actif ou inactif, modifiable)
 - Un rôle (modifiable)

Image Docker

- Une image Docker est fournie
- Elle utilise de vieilles versions de
 - Nginx
 - PHP
 - SQLite
- Volontairement vulnérable
- Vous pouvez préparer vos propres images Docker

Evaluation

- Qualité du rendu
 - Respect des consignes (délai, archives, noms des fichiers, etc)
 - Présence de tous les éléments,
 - Installation/utilisation aisée,
 - etc.
- Mode d'emploi
- Aspects fonctionnels de l'application
 - Fonctionnalités du cahier des charges,
 - Appréciation du code (lisible, commentaires, etc.)

Ces critères sont donnés à titre indicatif