Alec Berney

SEC – 08.06.2022

Analyze and fix an application

Labo 3

# Améliorations apportées

## Base de données

* Stockage d’un hash et pas du mdp en clair dans la BD

## Login

* Comparaison des hash et pas des password lors du login
* Le hash est de toute façon généré avec au pire une valeur par défaut pour empêcher les « side channels attacks ».
* J’ai fait en sorte que les messages d’erreurs pour le login soient les mêmes si le mdp est faux ou si l’utilisateur n’existe pas pour empêcher les « Usually Bad Error Messages ».

## Inputs et outputs

* Validation des inputs via une libraire externe et des regex -> fait pour faciliter la validation d’input côté client plus tard si voulu
* Validation des outputs : On passe seulement username et phone\_number au client pour les comptes utilisateur
* Validation des inputs du côté client

## Role-Based Access Control

// A Role-Based Access Control (RBAC) system will be implemented

// Here a the roles and the actions that they can perform

// |show users|change own phone|change phone|add user|login|logout|exit|

// anonymous users: | x | | | | x | | x |

// authenticated users: | x | x | | | | x | x |

// HR users: | x | x | x | x | | x | x |

https://github.com/casbin/casbin-rs

* Gestion des droits centralisées dans une fonction et un fichier, éviter de faire la logique dans chaque fonction de handle.
* Fichier pour gérer les accès avec casbin

## Log

* Ajout des logs

Politique mise en place de Warn affiché (trace pour le debug de l’app) avec la libraire [simplelog](https://docs.rs/simplelog/latest/simplelog/).

Les logs ont été uniquement mis en place du côté serveur comme le veut la logique. Ils ont également été concentré sur les actions que l’utilisateur peut réaliser et quelques informations que le serveur fourni lors du démarrage notamment.

## Autres refactor

* Bouger userConnected dans un fichier
* Créer un fichier contenant toutes les erreurs possibles
* Création d’un fichier « .env » pour stocker les secrets du serveur -> évite les secrets dans le code (on s’en fiche du côté client)

# Améliorations possibles restantes

Multifactor auth

Challenge response

Slow down login request avec un système de comptage de fail

Redemander l’authentification pour les actions demandant des changements majeurs (changement de son numéro de téléphone, d’un numéro de téléphone ou ajout d’un utilisateur)

Les logs devraient s’enregistrer sur un volume externe mais pour le bien du labo, ils sont affichés dans la console.