SLH 2024-2025

Exercices 8 - Authentification

Nous allons implémenter dans l'application `miniauth` un mécanisme d'authentification à deux facteurs (mot de passe + TOTP), avec hachage des mots de passe, dans une application en mode texte.

L'application supporte deux processus :

- l'**enregistrement**, pendant lequel l'utilisateur fournira un nom d'utilisateur et un nouveau mot de passe, et recevra un code QR lui permettant d'utiliser une application mobile TOTP comme 2e facteur
- l'**authentification**, pendant laquelle l'utilisateur doit fournir son nom d'utilisateur, son mot de passe, et le code temporaire TOTP.

Il existe plusieurs applications mobiles gratuites pour procéder a la génération des codes TOTP (Par exemple: Aegis Authenticator, Twilio Authy, Bitwarden Authenticator, Google Authenticator). Vous pouvez aussi utiliser un outil comme `oathtool`.

1. Choisissez une politique définissant les noms d'utilisateurs valides, et implémentez une fonction de validation pour imposer cette politique.
2. Implémentez le hachage et la validation du mot de passe en utilisant **Argon2id**. Utilisez un **poivre**.
3. Implémentez la génération d'un nouveau secret TOTP et sa conversion en URL otpauth. La lib `qr2term` est utilisée pour traduire cette URL en code QR
4. Testez le fonctionnement interactivement.