Réinitialisation du mot de passe

Jusqu'à présent vous avez réalisé une page permettant de créer un compte utilisateur et une page permettant à l'utilisateur de se connecter de manière sécurisée.

L'étape suivante est de proposer à l'utilisateur ayant perdu son mot de passe d'en redéfinir un.

Travail à faire :

Cette réinitialisation du mot de passe s'effectuera par l'envoi d'un mot de passe.

1. Vous devez rajouter un lien « **Mot de passe oublié** » sur votre formulaire de connexion **login.php**
2. Ce lien vous amène sur une nouvelle page **resetpassword.php** contenant un unique champ de saisi demandant à l'utilisateur de saisir son email
3. Après validation du formulaire, si l'email existe bien en base de données alors un email est envoyé à l'utilisateur (*voir annexes*). Cet email doit contenir un lien envoyant vers la page **newpassword.php**. Vous demanderez alors à l'utilisateur de retaper deux fois son nouveau mot de passe et vous l'enregistrerez en base de données.
4. Vérifiez que le nouveau mot de passe fonctionne en essayant de vous connecter avec le compte modifié
5. Si l'email saisi dans la page **resetpassword.php** n'existe pas, on l'indique à l'utilisateur

Contraintes :

Le reset d'un password doit être fait correctement. Pour commencer, l'email que vous enverrez à l'utilisateur doit contenir un lien personnel, unique et suffisamment sécurisé pour ne pas qu'un autre utilisateur puisse le « deviner » et modifier le mot de passe d'un autre utilisateur à son insu. On génèrera donc un lien de la forme *: newpassword.php ?id=14&token=fkzhxEqkOpeLd2Nvs54ec7*

Id sera l'id de l'utilisateur qui veut réinitialiser son mot de passe.

A quoi sert **token** ? Comment générer ce genre de token ? Comment s'assurer que le lien que l'utilisateur aura ouvert dans son navigateur sera bien celui que vous aurez généré vous préalablement (avec le bon token) ? Faîtes les modifications en base de données nécessaires ☺

Bonus :

- Pour plus de sécurité un lien de réinitialisation du mot de passe ne doit pas être valide plus d'un certain temps (3h, 12h, 1 jour …). En effet quelqu'un qui se ferait pirater son adresse mail ne doit pas dans la foulée se faire pirater tous ses comptes à cause des liens de réinitialisation des mots de passes passés retrouvés dans de vieux emails. Faîtes en sorte que les liens ne soient pas valides plus de 15 minutes ! Si l'utilisateur clique sur un lien déjà expiré, indiquez-le-lui et proposez-lui de réinitialiser à nouveau son mot de passe.
- De même, si l'utilisateur a déjà réinitialisé son mot de passe avec un lien généré, il est conseillé d'invalider le lien qui a déjà servi (afin qu'il ne serve plus à nouveau). L'utilisateur ne

doit donc plus pouvoir réutiliser un lien qui a déjà servi. Faîtes en sorte que ce soit impossible et indiquez lui l'erreur s'il réutilise un lien déjà consommé.

Annexe :

Pour l'envoi d'email depuis **Laragon**, vous utiliserez le fichier **sendemail.php** fourni dans l'archive. A vous de l'importer et d'appeler sa fonction avec les bons paramètres pour expérimenter l'envoi d'emails.