Règles de base

* Le développeur ne doit jamais connaitre les passwords de nos utilisateurs
* Ne pas envoyer de passwords par mail
* On doit **hasher** les passwords, pas les **encrypter**. Un password encrypté peut être décrypté. Le hashing est une fonction qui modifie le password et qui n’est pas réversible
* On enregistre les passwords hashés dans notre BD. Un hacker verra uniquement un ensemble de mots qui ne font aucun sens
* Actuellement on utilise bcrypt pour hasher
* Il y a deux possibles scenarios concernant le password : le login et l’inscription au site
* On doit filtrer (en utilisant les fonctions **filter** de PHP ou n'importe quel autre outil) l'entrée d'un formulaire d'inscription ou de login