# Failles de sécurité de sec17

## Base de données

yoga.sql, functions.php

- Elle ne contient pas un user dédié. Il n'y a que le user root par "défaut".
- Un fichier connexion.csv est accessible depuis le web. Il contient le user MySQL
- les user,password et base MySQL sont lus dans le fichier csv. On pourrait éventuellement les changer en modifiant le fichier csv

## Page de connexion de l'utilisateur

connexion.php

- La page n'est pas protégée contre les injections SQL
- Le mot de passe n'est pas haché
- Le mot de passe est visible dans le formulaire (pas de puce)
- Les champs ne sont pas filtrés

## Page d'inscription de l'utilisateur

inscription.php

- La page n'est pas protégée contre les injections SQL
- Le mot de passe n'est pas haché
- Le mot de passe est visible dans le formulaire (pas de puce)
- Le mot de passe n'est pas saisi deux fois pour confirmation
- Les champs ne sont pas filtrés
- Les champs ne sont pas vérifiés en HTML (pas de type "email" par exemple)
- On peut s'incrire sans renseigner le mot de passe ou avec un mot de passe facile à deviner

## Menu

menu.php

- L'id de l'utilisateur n'est pas vérifié. Le lien est toujours visible même si on n'est pas connecté

## Profil

profil.php

- La page n'est pas protégée contre les injections SQL
- On peut voir tous les profils même si on n'est pas connecté (présence d'une query string)
- Si l'id_user n'existe pas, ça provoque une erreur PHP
- On voit le mot de passe en clair