DEISS
Thomas

LP GL
28/01/2019

Compte rendu sur la sécurisation d'un site web.

But du site web

Le site web, intitulé « Maplan », a pour but d'afficher un local sur un plan. L'utilisateur n'a qu'à rentrer le nom du local recherché sur la page **index** et si le local existe, il apparaît.
Le site comporte 3 types d'utilisateurs :

- Le visiteur : il n'a accès qu'à la recherche d'un local ainsi qu'à la connexion
- L'utilisateur : il a les mêmes droits que le visiteur (aura des droits supplémentaires dans une version future du site)
- L'administrateur : Il a les mêmes droits que l'utilisateur et peut accéder à la partie « Administration »

Certaines parties du site sont en développement ou servent de test et ne sont donc pas sécurisées, j'ai donc choisi de ne pas les inclure donc certains URL ne fonctionneront pas (notamment dans la partie administration).

Bibliothèques utilisées

Pour la connexion à la base de données, le site utilise l'extension **PDO** de PHP qui permet de se protéger des injections SQL notamment grâce à sa méthode `PDO::prepare()`.

Failles corrigées

Accès indirect non autorisé

- L'utilisateur ne peut plus accéder à la page réservée aux administrateurs (en incluant le fichier « secure_admin.php » qui vérifie le groupe de l'utilisateur dans la variable de session.

CSRF

- La méthode de connexion est en POST
- Utilisation d'un jeton de sécurité (id de la BDD stocké dans une variable de session)

Injection SQL

- Utilisation de `PDO::prepare()` au lieu de `PDO::exec()` qui, grâce à ses requêtes préparées, bloque toutes les injections SQL.

Autres

- La session est régénérée à la connexion grâce à « `session_regenerate_id(true)` »
- Le mot de passe est crypté dans la base de données grâce à la méthode « `password_verify()` »
- Dans le php.ini :
    - L'identifiant de session n'est pas utilisé dans les URL (`session.use_trans_sid = 0`)

    - « session.use_only_cookies = 1 » pour n'utiliser que les identifiants contenus dans les cookies
    - La durée d'une session est limitée à 24 minutes (« `session.gc_maxlifetime=1440` »)
- « `autocomplete="off"` » sur les champs de type password
- Taille maximum de 50 caractères pour le login et le mot de passe pour éviter le buffer overflow.
- Utilisation d'un captcha lors de 3 tentatives erronées pour éviter le brute force (retiré du site car le reCAPTCHA de Google ne fonctionne que pour un nom de domaine renseigné au préalable)
- Ajout d'un bouton de déconnexion qui détruit la session ainsi que les données de session.

Note

L'utilisation du fichier .htacess à la racine du serveur est obligatoire car tous les liens du site n'utilisent pas l'extension .PHP et ne peuvent pas fonctionner sans ce fichier.