

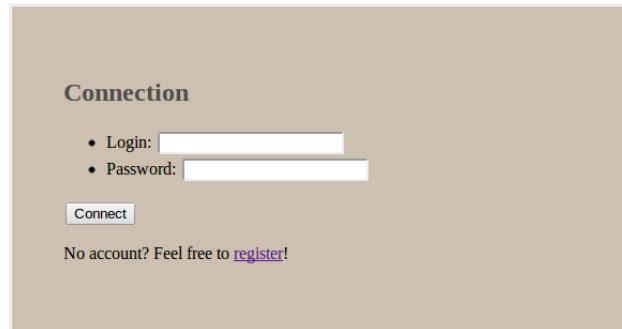
Mathieu BIVERT, Sophie VALENTIN

Projet WASP
FUGU : Find Your Guest Unisonously
Site de covoiturage

Professeur : Tamara REZK

1 Fonctionnalités de l'application web

L'utilisateur souhaitant faire du covoiturage doit tout d'abord s'authentifier. En effet, les utilisateurs possèdent leurs propres données. L'utilisateur s'authentifie via un formulaire de connexion, illustré dans la figure 1. Il doit renseigner son login et son mot de passe. S'il n'en possède pas, il peut s'enregistrer sur la page d'inscription. Pour cela, il doit cliquer sur le lien "register".



Connection

- Login:
- Password:

No account? Feel free to [register!](#)

FIGURE 1 – Formulaire de connexion

1.1 Tableau de bord de gestion

Une fois authentifié, l'utilisateur accède à son tableau de bord, représenté en figure 2. Cet écran répertorie tous ses trajets, c'est-à-dire :

- les trajets dont il est le conducteur dans la partie haute de la page ;
- les trajets dont il est le passager dans la partie basse de la page.

Manage

Propose

Search

Disconnect

Dashboard

Driver for

From	To	Duration	Distance	Description	Actions
43-57 Rue Berlioz Nice	220-250 Avenue du Golf Mougins	31.58	28	Je pars à 7h	<div>delete</div>
3 Rue Arthur Malaussena Levens	423 Route des Lucioles Valbonne	52.14	51	Trajet fait le dimanche soir	<div>delete</div>
Domaine du Loup Cagnes-sur-Mer	Route du Parc Valbonne	12.54	13	Je ne prends pas l'autoroute.	<div>delete</div>

Passenger for

Driver	From	To	Duration	Distance	Description	Actions
mathieu	43-57 Rue Berlioz Nice	220-250 Avenue du Golf Mougins	31.58	28		<div>delete</div>

FIGURE 2 – Tableau de bord

L'utilisateur a accès à tout moment à ce tableau de bord en cliquant sur "Manage" sur le menu de navigation. Et il peut se déconnecter en cliquant sur "Disconnect".

Pour chaque trajet, les adresses de départ et d'arrivée sont affichées. Le temps (en minutes) et la distance (en kilomètres), qui ont été calculés, sont également affichés. L'utilisateur peut voir la description qui a été donnée au trajet. Généralement, ce sont des informations pratiques sur le rendez-vous.

L'utilisateur peut supprimer un trajet de son tableau de bord : pour cela, il clique sur le bouton "delete" du trajet qu'il souhaite supprimer. Son tableau de bord est alors mis à jour. S'il était conducteur



FIGURE 3 – Menu de navigation

pour ce trajet, alors le trajet n'apparaîtra plus dans le tableau de bord des autres passagers.

1.2 Proposition de trajet

En cliquant sur "Propose" sur le menu de navigation, l'utilisateur peut proposer un trajet comme dans la figure 4. Au chargement, une carte apparaît avec une adresse de départ et une adresse d'arrivée par défaut. Pour indiquer son trajet, l'utilisateur a deux solutions :

- il peut entrer les adresses de départ et destination dans les champs
- il peut déplacer les marqueurs sur la carte

Dans le premier cas, les marqueurs sur la carte sont immédiatement mis à jour. Dans le second cas, les champs d'adresses sont immédiatement mis à jour. Et quelque soit la méthode pour indiquer le trajet, le temps de trajet et la distance sont calculés. L'utilisateur a ensuite la possibilité de laisser une description en remplissant le champ de texte. Pour terminer, il enregistre son trajet en cliquant sur le bouton "Propose", en-dessous de la description.

Propose a route

Departure

Coordinates : (43.703010001 , 7.259760001)

Address : 43-57 Rue Berlioz Nice

Arrival

Coordinates : (43.61874 , 7.052480001)

Address : 767-777 Route des Lucioles Valbonne

Total distance : 24.07 km

Duration : 26 min

Je pars à 8h

Description

Propose

FIGURE 4 – Proposition de trajet

Après enregistrement, l'utilisateur est redirigé sur le tableau de bord où figure le nouveau trajet créé.

1.3 Recherche de trajet

En cliquant sur "Search" sur le menu de navigation, l'utilisateur peut chercher un trajet existant. Le principe est le même que pour la création de trajet à l'exception que l'utilisateur ne renseigne aucun champ de description. Après un clic sur le bouton "Search", une liste de trajets est affichée.

Pour chaque trajet, on peut s'inscrire en tant que passager. Il faut noter que les trajets sur lesquels on s'est déjà inscrit ne figurent pas dans la recherche. Pour s'inscrire, on clique sur le bouton "join" en face du trajet. On est alors redirigé vers le tableau de bord où apparaît maintenant le trajet que l'on a rejoint.

Research results

Results						
Driver	From	To	Duration	Distance	Description	Actions
toto	43-57 Rue Berlioz Nice	220-250 Avenue du Golf Mougins	31.58	28	popo	<input type="button" value="join"/>
toto	43-57 Rue Berlioz Nice	220-250 Avenue du Golf Mougins	31.58	28	oifaoifa	<input type="button" value="join"/>
toto	43-57 Rue Berlioz Nice	220-250 Avenue du Golf Mougins	31.58	28	iuiua	<input type="button" value="join"/>
toto	43-57 Rue Berlioz Nice	220-250 Avenue du Golf Mougins	31.58	28	popo	<input type="button" value="join"/>
foo	43-57 Rue Berlioz Nice	220-250 Avenue du Golf Mougins	31.58	28		<input type="button" value="join"/>

FIGURE 5 – Recherche de trajet

2 Serveur

2.1 Services

index.php
 register.php
 user.php
 proposer_trajet.php
 chercher_trajet.php
 lister_trajets.php
 disconnecte.php

2.2 Sécurité

2.2.1 Prévention de l'attaque XSRF

Une telle attaque envoie des requêtes à l'insu de l'utilisateur depuis son propre navigateur. Pour la contrer, on génère sur chaque page un jeton (ou token), qui est stocké côté serveur, avec la fonction PHP `openssl_random_pseudo_bytes()`, qui est un générateur pseudo-aléatoire d'octets. Pour obtenir un service habituel, il faut préciser en mode GET ou POST le token obtenu. Le serveur vérifie que le paramètre (GET ou POST) est bien égal au token stocké côté serveur. Ainsi, si l'attaquant tente d'envoyer une requête sans connaître le token, il n'obtiendra pas le service.

Par exemple, pour le service de proposition de trajet, la comparaison entre le token mis en mémoire sur le serveur et celui passé en paramètre se fait dans le fichier `proposer_trajet.php` à la ligne 54. Sur cette ligne, on appelle en fait la fonction `compare_token` définie dans le fichier `inc/xsrf.php`. Quant à la génération du nouveau token, elle se fait dans le fichier à la ligne 57. Sur cette ligne, on appelle la fonction `generate_token` définie dans le fichier `inc/xsrf.php`.

2.2.2 Prévention des attaques contre l'intégrité de la session

On souhaite éviter que l'utilisateur ou un attaquant puisse éditer les cookies de session. Ainsi, on stocke côté serveur une empreinte HMAC des données sensibles envoyées à l'utilisateur. Cette empreinte est calculée grâce à deux entrées :

- la donnée que l'on souhaite passer à l'utilisateur ;
- la clé privée connue seulement du serveur.

Lors de l'envoi d'un cookie modifié par le client ou un attaquant, le serveur détectera que l'empreinte de la donnée envoyée par le client n'est pas la même que celle stockée côté serveur. Ainsi on prévient les attaques visant à altérer les données de session.

2.2.3 Prévention des attaques de fixation

Pour une telle attaque, l'attaquant fixe le Session ID dans l'URL pour un autre utilisateur. Il envoie ensuite cette URL à l'utilisateur. Ce dernier s'authentifie et l'attaquant peut alors utiliser la session de l'utilisateur car il connaît le SID. Pour prévenir cette attaque, il faut modifier le fichier `php.ini` :

- en activant l'option `session.use_only_cookies` afin que le SID soit transmis exclusivement par cookie ;
- en s'assurant que l'option `session.use_trans_sid` est désactivée.

2.2.4 Prévention des attaques Man in the Middle

Afin qu'une attaque du type Man in the Middle n'opère pas, on utilise un flux chiffré tel que HTTPS. Cela nous assure les propriétés de confidentialité et d'intégrité des paquets transmis.

2.2.5 Prévention des "Replay Attacks"

Replay attack Wiki Possible même avec HTTPS...

2.2.6 Prévention des attaques XSS

Cette attaque injecte du code qui sera interprété sur le navigateur du client : il peut s'agir d'une redirection forcée pour faire du phishing ou d'un vol de cookie avec du Javascript. Pour protéger le vol de cookie, on active l'option `session.cookie_httponly` dans le fichier `php.ini`. Cela permet de rendre les cookies `HttpOnly`, c'est-à-dire qu'ils ne seront pas accessibles par des langages de script tels que Javascript. Il faut également vérifier les données utilisateur comme dans le cas des attaques d'injections de code en retraitant le code HTML produit. Pour ce faire, on appelle la fonction `htmlspecialchars`.

2.2.7 Prévention des attaques d'injection de code

La prévention des attaques d'injection de code passe par :

- une identification précise des entrées qui ne sont pas de confiance pour ensuite s'assurer que ces données ne sont pas considérées avec un niveau de sécurité plus haut dans le code (taint analysis)
- un assainissement des entrées

Injections SQL

Il faut vérifier les données de l'utilisateur et échapper les caractères spéciaux. Dans notre cas, nous utilisons des requêtes préparées en PHP. Tout d'abord, on écrit une requête à trous sans les paramètres. Ensuite, la requête est analysée et compilée. Enfin, les paramètres sont donnés et le driver MySQL pour PHP gère automatiquement l'échappement des caractères spéciaux. Concernant la vérification, elle est faite en utilisant des expressions régulières.

Injections Javascript

On veut éviter qu'un utilisateur insère un script Javascript dans un champ. Pour pallier ce problème, on transforme les caractères spéciaux du texte entré afin qu'un éventuel script Javascript deviennent du texte non interprété. Pour cela, on utilise la fonction `htmlspecialchars` du fichier `utils.php`. Cette fonction appelle la fonction PHP `htmlspecialchars`.

2.2.8 Prévention des attaques RFI / LFI

RFI

On ne fait pas de `include` en PHP en utilisant les données utilisateur. L'utilisateur ne peut pas nous forcer à inclure un fichier important du serveur. Cela nous protège des attaques LFI.

LFI

On n'inclut pas d'URL externe dans le code PHP. Par sécurité dans le fichier php.ini, on désactive l'option `allow_url_include` Cela nous protège des attaques RFI.

2.2.9 D'autres éléments de prévention

Pour limiter les vols de cookies, lors d'une déconnexion, les cookies sont effacés de la machine cliente. Cela permet, par exemple, de limiter des vols causés par une intrusion sur le disque dur de l'utilisateur.

3 Client

3.1 Google Maps

3.2 Javascript

3.2.1 Utilisation de la Prototype Chain

3.2.2 Utilisation de la Scope Chain

3.2.3 Utilisation du mot-clé `this`

3.2.4 Utilisation de la récursion

3.2.5 Manipulation du DOM

3.3 Sécurité

3.3.1 Prévention des failles Javascript