

*Sécurité des Technologies Internet*

**Projet 1**

*Manuel d'utilisation*

Adrien Marco  
adrien.marco@heig-vd.ch

Julien Brêchet  
julien.brechet@heig-vd.ch

## **Table des matières**

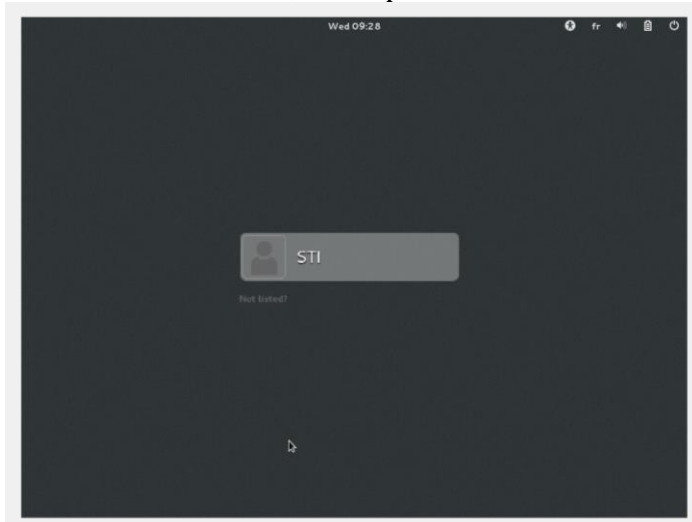
---

<b>1. Démarrage</b>	<b>3</b>
<b>2. Organisation</b>	<b>4</b>
<b>3. Utilisation et fonctionnalités du site web</b>	<b>5</b>

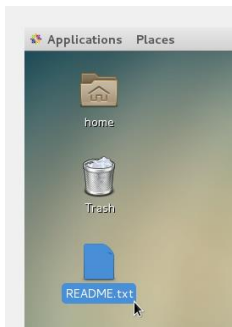
## 1. Démarrage

---

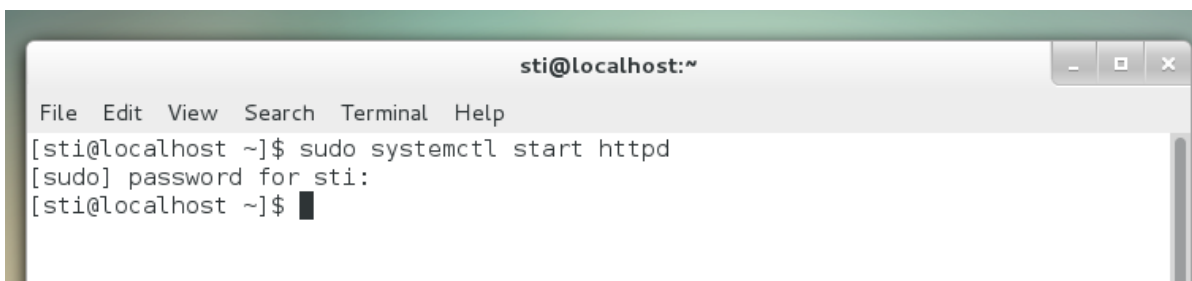
Au lancement de la VM, le compte STI doit être choisi. Le mot de passe est « sti » :



Un fichier « README.txt » se trouve sur le bureau. Il contient la ligne de commande à entrer dans le terminal pour lancer le serveur en local :



Ligne de commande :



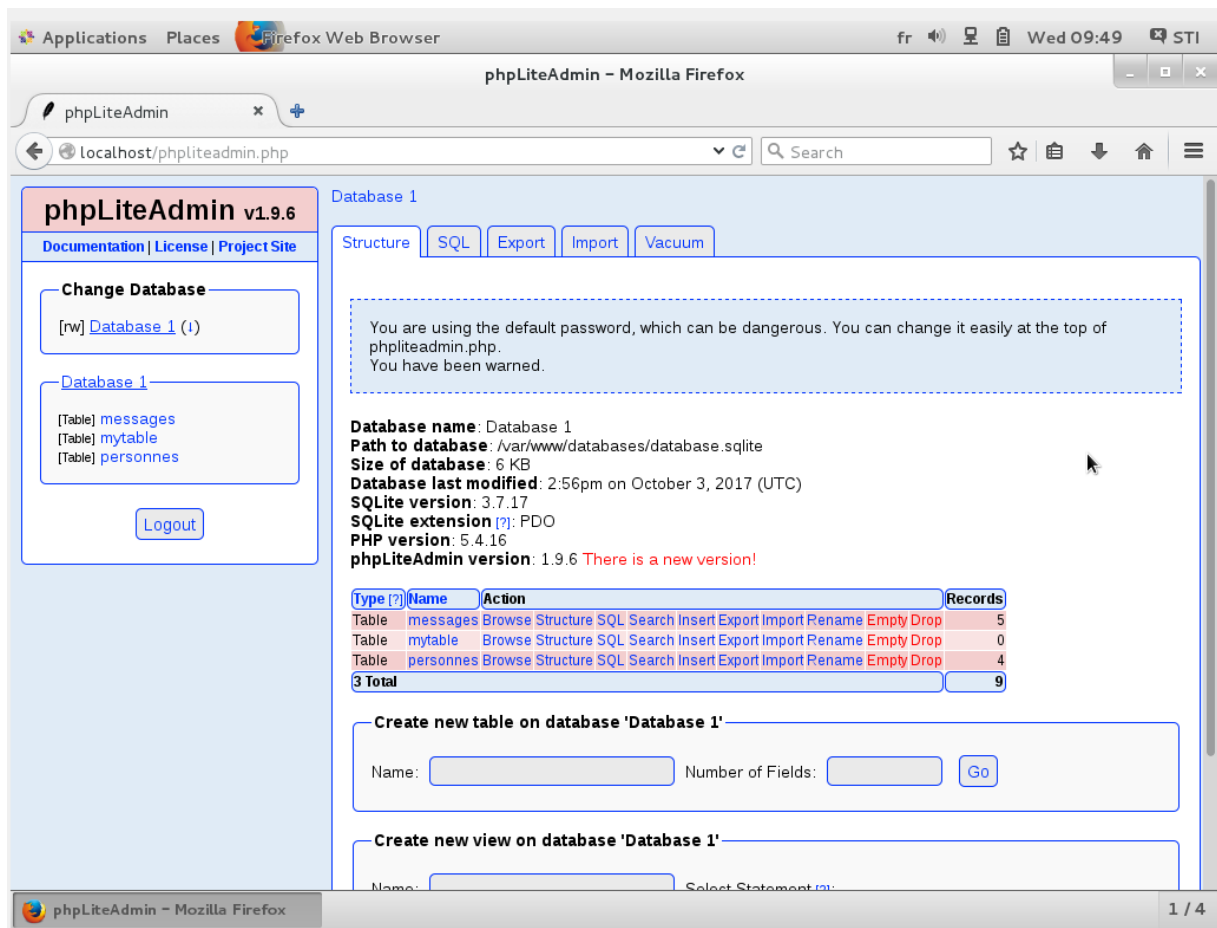
## 2. Organisation

Les fichiers concernés sont répartis entre ces deux dossiers sous `/var/www` :



Le dossier « `html` » contient toutes les fichiers « `php` » et le dossier « `databases` » possède le fichier de configuration de la base de données.

Il est cependant plus aisé de configurer la base de données en utilisant l'interface fournie via le navigateur. Pour cela, il suffit d'ouvrir le fichier « `phpliteadmin.php` » qui se trouve à la racine du serveur puisque ce dernier consulte automatiquement le contenu depuis `/var/www/html` :



Remarque : l'accès à un fichier du dossier « `html` » se fait en indiquant le chemin depuis « `localhost/nom_fichier.php` ». Par défaut, le fichier « `index.php` » est ouvert si seul le chemin « `localhost` » est mentionné. C'est d'ailleurs ce qu'il faudra faire pour lancer le site web.

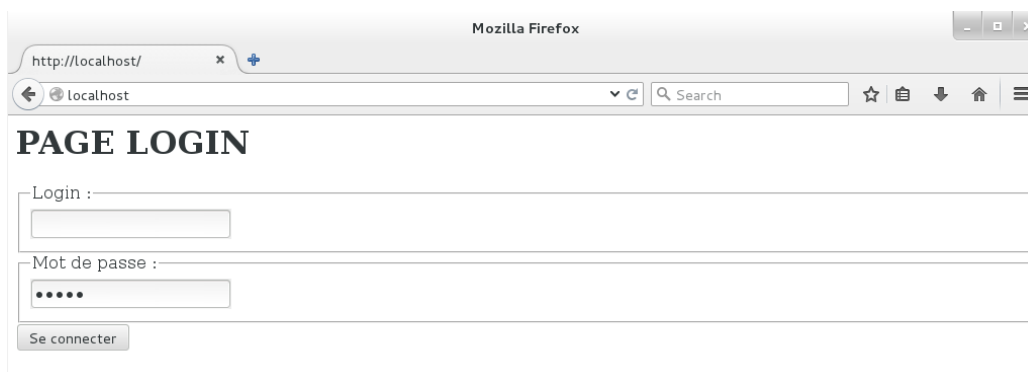
Dans la configuration de la base de données fournie, il existe déjà les deux tables nécessaires et remplies (personnes et messages). Mais il reste cependant possible d'utiliser cette interface pour modifier, supprimer, ajouter du contenu bien que le site web soit là pour ça.

Pour ceux qui souhaiteraient directement tester le site web, il suffit de récupérer les deux dossiers (html et databases) dans l'archive du projet puis de les mettre dans « /var/www » afin de remplacer la configuration de base du serveur sur la VM. Après cela, la démo peut tout de suite être lancée.

### ***3. Utilisation et fonctionnalités du site web***

---

On lance donc le site depuis le navigateur avec l'url « localhost ». Ce qui nous amène à une page de login accessible de tous (ce qui n'est pas le cas pour les autres fichiers du site) :



The screenshot shows a Mozilla Firefox browser window with the address bar set to 'http://localhost/'. The page title is 'PAGE LOGIN'. Below the title, there are two input fields: 'Login :' and 'Mot de passe :'. The 'Mot de passe :' field contains four dots. Below these fields is a button labeled 'Se connecter'.

Remarque : le mot de passe « admin » est sélectionné par défaut.

Il existe 4 comptes par défaut dans la base de données :

Login: Trudy  
Rôle: user  
Mdp: 1234  
Validité: actif

Login: Bob  
Rôle: admin  
Mdp: admin  
Validité: actif

Login: Adrien  
Rôle: user  
Mdp: adad  
Validité: inactif

Login: Julien  
Rôle: admin  
Mdp: juju  
Validité: inactif

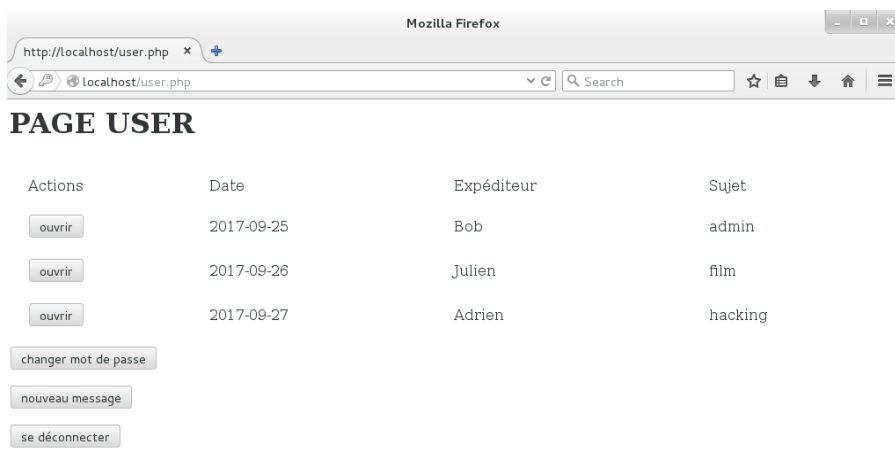
Le login devra se faire en fonction de ces informations sinon l'accès sera refusé. De plus, le compte doit être actif.

Une fois connecté, une page « user » ou « admin » va s'ouvrir selon le type de compte choisi.

La différence est que l'admin possède quelques fonctionnalités supplémentaires (gestion des comptes).

De manière générale, tout le monde peut consulter les messages reçus, ouvrir le détail des messages, répondre aux messages, les supprimer, en écrire des nouveaux et, finalement, changer son mot de passe. Sur la page principale, il est possible de se déconnecter (seul moyen de revenir à la page de login car des redirections automatiques sont faites lorsque l'on tente de « court circuiter » l'accès aux fichiers). Il est aussi, en tout temps, possible de revenir en arrière avec un bouton « retour ».

Chaque action est indiquée par un bouton. Voici la page principale pour un « user » :



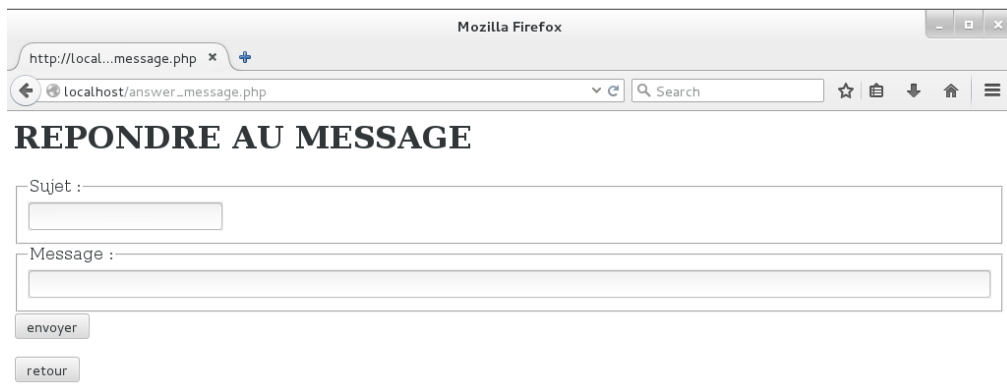
On y voit les messages reçus et les actions possibles (boutons). Le corps du message peut être affiché avec l'action « ouvrir ». De nouvelles actions sont proposées comme répondre au message ou le supprimer.

Exemple détail de message :



Remarque : « supprimer message » supprime directement et sans validation.

Exemple de réponse au message :



The screenshot shows a Mozilla Firefox browser window with the address bar displaying 'http://localhost/answer\_message.php'. The page title is 'REPONDRE AU MESSAGE'. Below the title, there are two text input fields: 'Sujet : ' and 'Message : '. Below these fields are two buttons: 'envoyer' and 'retour'.

Remarque : le destinataire est automatiquement reconnu et les champs de sujet et message sont obligatoires.

Attention : il faut s'assurer d'avoir les droits en lecture/écriture sur le fichier database.sqlite. De plus, certains caractères spéciaux comme « ' » ne sont pas supportés.

Exemple de changement de mot de passe :



The screenshot shows a Mozilla Firefox browser window with the address bar displaying 'http://localhost/change\_pwd.php'. The page title is 'CHANGEMENT MOT DE PASSE'. Below the title, there is a text input field for 'Nouveau mot de passe : ' with five dots indicating a password. Below this field are two buttons: 'appliquer changement' and 'retour'.

Remarque : le champ du mot de passe est rempli par défaut avec la valeur « admin ». Il faut appliquer le changement s'il on veut qu'il se fasse. Sinon, il y a toujours la possibilité de taper « retour » pour revenir en arrière.

Exemple d'un nouveau message :



The screenshot shows a Mozilla Firefox browser window with the address bar displaying 'http://localhost/new\_message.php'. The page title is 'NOUVEAU MESSAGE'. Below the title, there are three text input fields: 'Destinataire : ', 'Sujet : ', and 'Message : '. Below these fields are two buttons: 'envoyer' and 'retour'.

Remarque : les champs sont obligatoires et le message ne peut s'envoyer avant que quelque chose n'ait été saisi. Cependant, on ne vérifie pas si le login destinataire existe ou pas.

Maintenant, nous désirons quitter le mode « user » pour passer en « admin ». Il faut se déconnecter depuis la page principale du « user » :

### PAGE USER

Actions	Dat
<a href="#">ouvrir</a>	201
<a href="#">ouvrir</a>	201
<a href="#">ouvrir</a>	201
<a href="#">changer mot de passe</a>	
<a href="#">nouveau message</a>	
<a href="#">se déconnecter</a>	

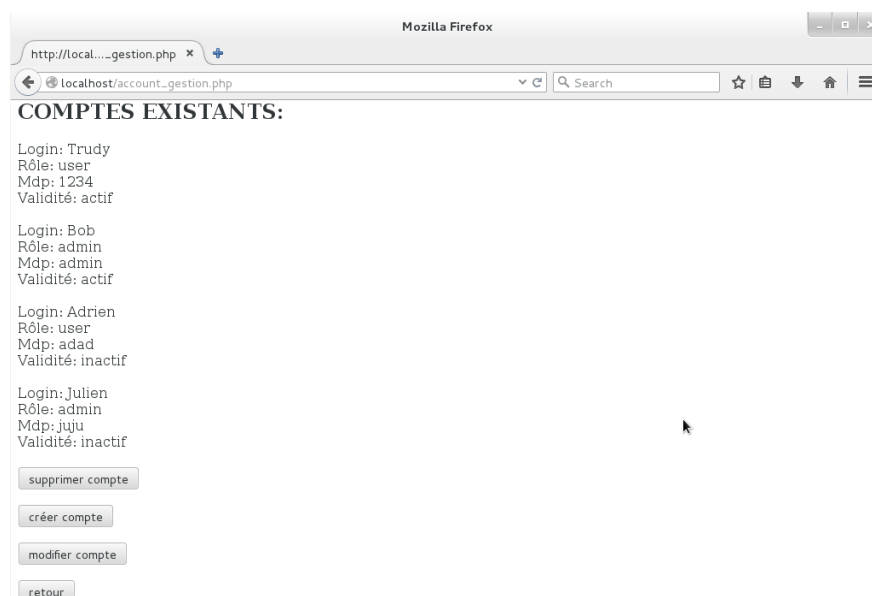
Ce qui nous amène à nouveau à la page de login où il faudra se connecter avec un compte administrateur actif afin d'arriver à la page principal de l'admin :



### PAGE ADMIN

Actions	Date	Expéditeur	Sujet
<a href="#">ouvrir</a>	2017-09-25	Trudy	test
<a href="#">ouvrir</a>	2017-09-26	Julien	ajout user
<a href="#">changer mot de passe</a>			
<a href="#">se déconnecter</a>			
<a href="#">nouveau message</a>			
<a href="#">gérer les comptes</a>			

Remarque : les actions sont les mêmes que pour le « user » mais on peut aussi gérer les comptes :



Remarque : les comptes existants sont affichés pouvoir connaître en tout moment l'état de la BD.



Exemple de suppression de compte en indiquant le login à supprimer:



login à supprimer:

supprimer

retour

Remarque : la saisie est obligatoire sinon impossible de supprimer. Il n'y a pas de message de confirmation de suppression et la redirection est faite vers la page principale de l'admin. Si le login n'existe pas, rien ne va être supprimer et la redirection sera faites quand même.

Exemple de création de compte :



login :

Mot de passe :

Validité : ☒ active ☐ inactive

Rôle : ☐ admin ☒ user

créer

retour

Remarque : tous les champs sont obligatoires. Il n'y a pas de message de confirmation et la redirection est faite vers la page principale de l'admin.

Exemple de modification d'un compte (première étape):



login à modifier:

modifier

retour

Remarque : cette étape consiste juste à saisir le login du compte à modifier. Le champ est donc obligatoire.

Si le login n'existe pas, un message d'erreur va l'indiquer et il sera possible de recommencer :



Remarque : la suite de l'étape deux ne se fera donc pas.

Exemple de l'étape deux quand le login est bon :



Remarque : le login « Trudy » a été sélectionné et le formulaire est déjà pré-rempli avec les information de base. Il est possible de les modifier (sauf le login) avant de confirmer la modification. Il n'y a aussi pas de message de confirmation pour cette étape et la redirection se fait vers la page principale de l'admin.