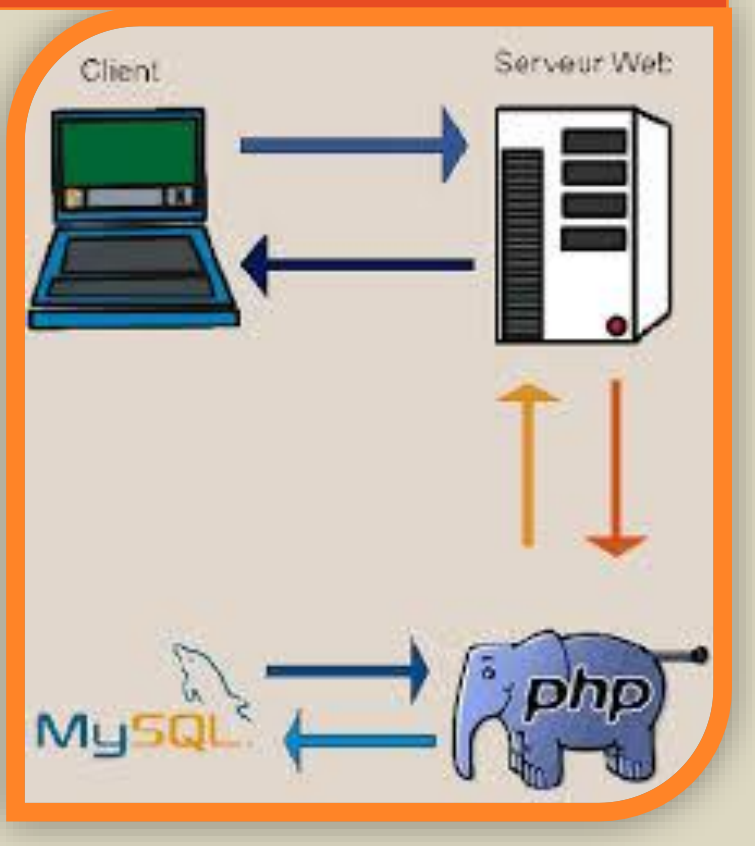
TP SERVEUR WEB



NGUELE YVES GABIN
2ème année BTS SIOR
10 Octobre 2013

CONSIGNES

Remplacez ce texte par le vôtre. Vous pouvez également remplacer les images (sur la page précédente et à droite) par les vôtres.

Rédiger un document relatif à l'installation du serveur APACHE (mode opératoire, vos choix de configuration...)

Rédiger un document qui présente les choix de sécurisation du serveur APACHE.

Pour chaque option de sécurité préciser:

- le principe de sécurisation (en quoi consiste cette sécurisation)

- son implémentation (extrait des fichiers de configuration)

- les éléments utilisés pour vérifier le bon fonctionnement de l'option de sécurité (copies d'écrans, messages, rapport de log...)

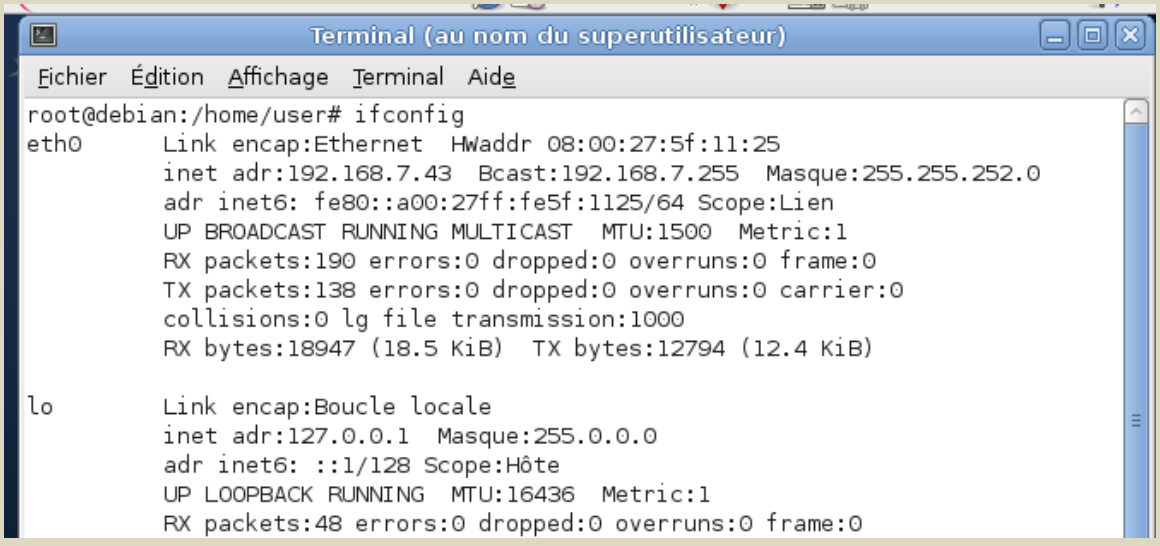
Ces deux documents seront enregistrés dans un fichier nommé TP_securisation_VotreNom.pdf.

Détaillez le plus possible vos réponses et soignez la forme.

PARTIE 1 : INSTALLATION DU SERVEUR

1- Mettre le serveur en adresse fixe 192.168.7.43 et la machine cliente 192.168.7.44

```
root@debian:/home/user# ifconfig
eth0      Link encap:Ethernet  HWaddr 08:00:27:5f:11:25
          inet adr:192.168.7.44  Bcast:192.168.7.255  Masque:255.255.252.0
          adr inet6: fe80::a00:27ff:fe5f:1125/64 Scope:Lien
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:162 errors:0 dropped:0 overruns:0 frame:0
          TX packets:169 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 lg file transmission:1000
          RX bytes:18008 (17.5 KiB)  TX bytes:14761 (14.4 KiB)

lo        Link encap:Boucle locale
          inet adr:127.0.0.1  Masque:255.0.0.0
          adr inet6: ::1/128 Scope:Hôte
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:48 errors:0 dropped:0 overruns:0 frame:0
          TX packets:48 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 lg file transmission:0
          RX bytes:3876 (3.7 KiB)  TX bytes:3876 (3.7 KiB)
```



2- Création d'une base de données pour héberger le site appelé worlds_cook avec 5 tables

```
mysql> show databases;
+--------------------+
| Database           |
+--------------------+
| information_schema |
| mysql              |
| worlds_cook        |
+--------------------+
3 rows in set (0.02 sec)

mysql>
```

```
Database changed
mysql> show tables;
+----------------------+
| Tables_in_worlds_cook |
+----------------------+
| adherent             |
| chef                 |
| cours                |
| inscription          |
| session              |
+----------------------+
5 rows in set (0.00 sec)
```

3- Création d'un utilisateur avec tous les droit sur la base de donnée worlds_cook appelé worlds_cook et son mot de passe worlds_cook

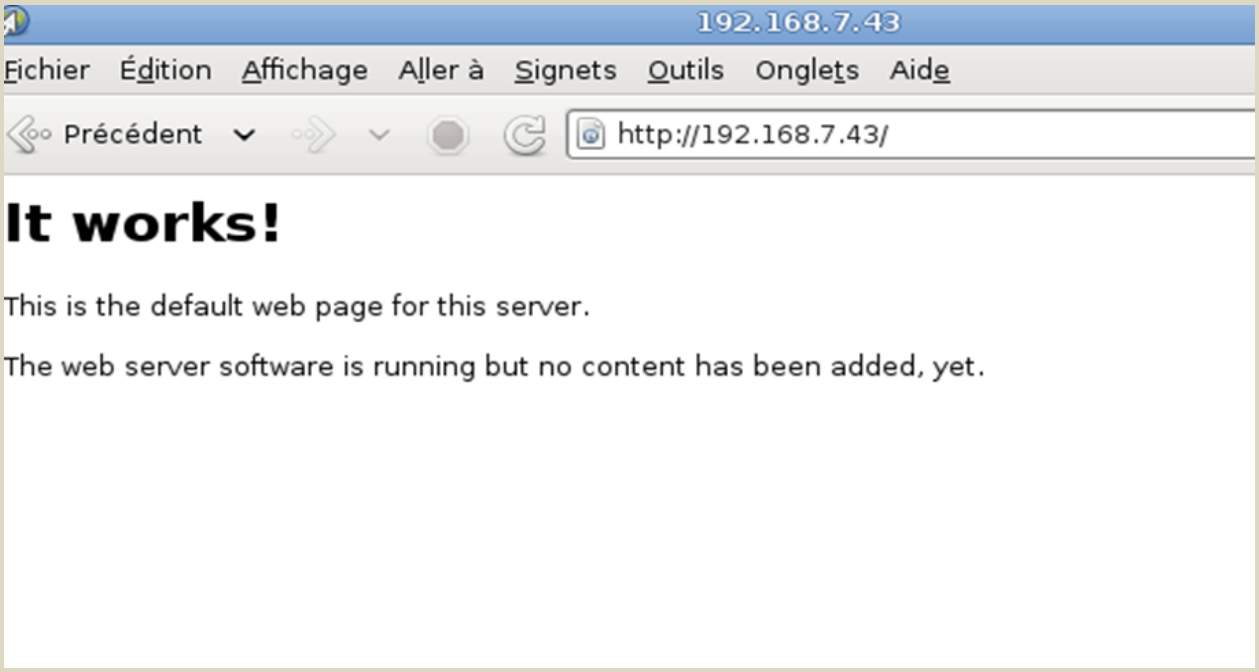
```
mysql> select user from user;
+------------------+
| user             |
+------------------+
| words_cook       |
| worlds_cook      |
| root             |
| root             |
| debian-sys-maint |
| root             |
+------------------+
6 rows in set (0.00 sec)

mysql>
```

4- Installer des paquetages apache2 (et, pour les versions d'Ubuntu avant 10.04, installer manuellement les paquetages apache2.2-common et apache2-utils) pour la version de base

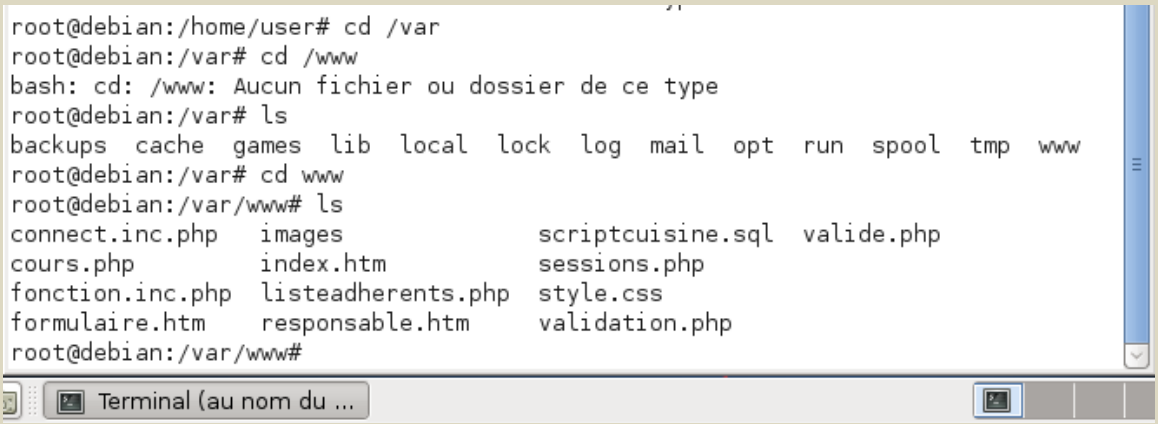
5- Pour ajouter des fonctions d'authentification, la gestion du multi-processing et la possibilité de changer le service en mode root :

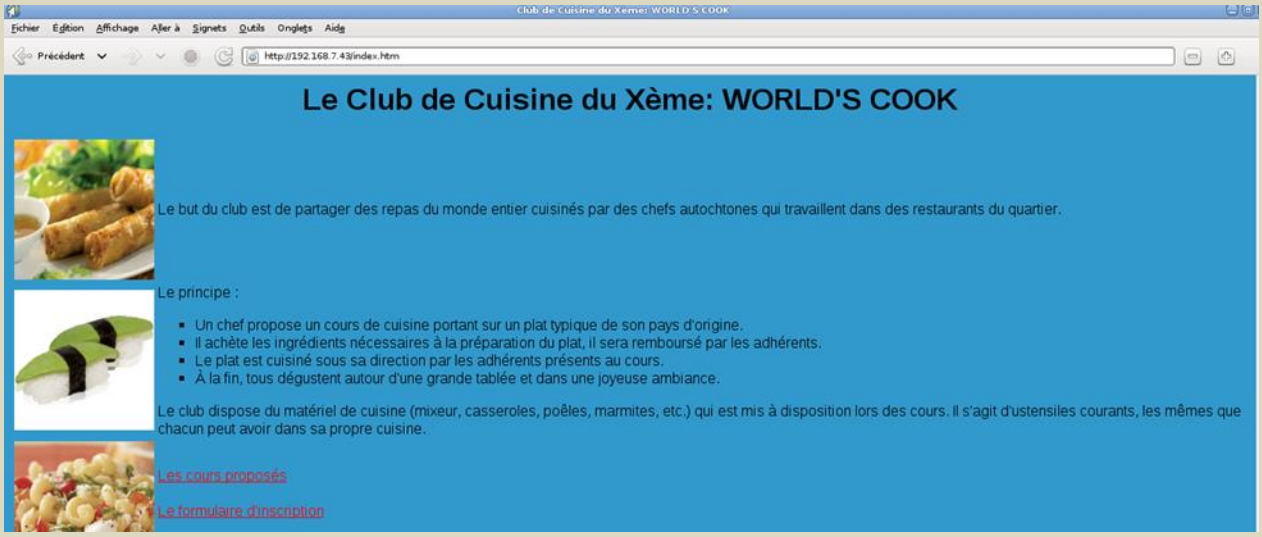
installer les paquetages apache2-mpm-prefork, libapache2-mod-chroot, libapache2-mod-auth-pam, libapache2-mod-auth-sys-group

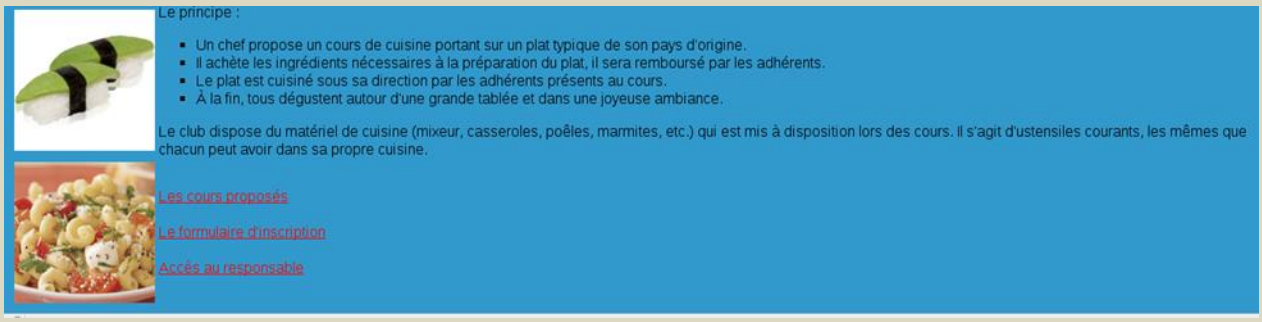
6- Test du bon fonctionnement du serveur web à partir du client



7- Copie des fichiers du site web que j'ai fait expressément pour le TP dans le WWW





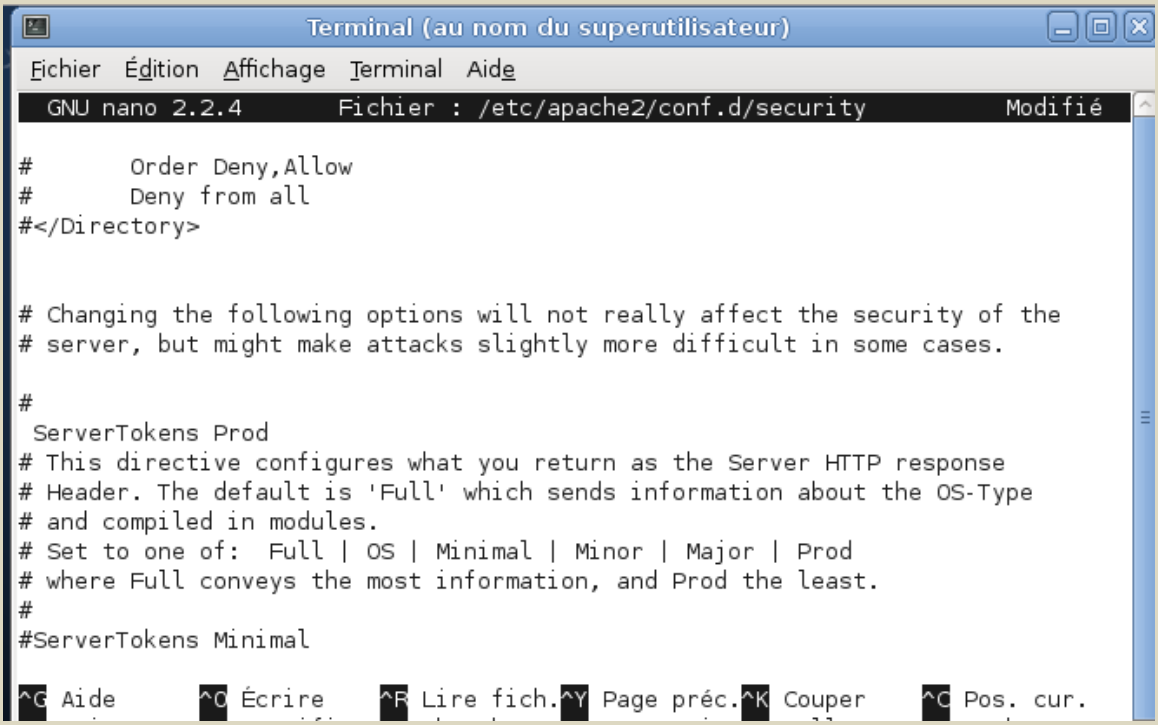


PARTIE II : SÉCURISATION DU SERVEUR WEB

1- Pour améliorer la sécurité du site, j'ai fait un mot de passe pour avoir accès à l'administration du site dans la rubrique accès au responsable.
Ca va permettre déjà de mettre une première sécurité pour que n'importe qui n'accède à cette partie-là.

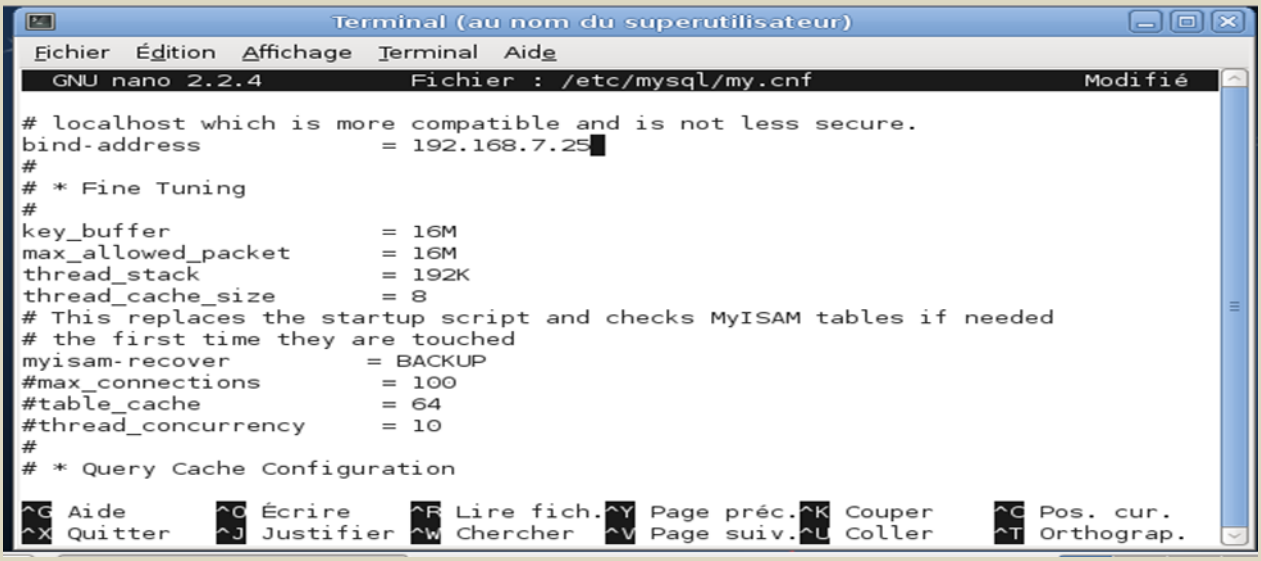
2- Cacher la version d'Apache et autres informations sensibles

Par défaut, Apache affiche la version du système d'exploitation j'utilise, ainsi que d'autres informations. Une personne malveillante peut utiliser ces informations pour mieux cibler son attaque mon serveur, je vais donc le cacher.



Pour ce faire je devais modifier les lignes ServerSignature et mettre ServerSignature Off et aussi ServerTokens par ServerTokens Prod

3- Rendre accessible ma base de donnée uniquement par mon serveur avec l'IP 192.168.7.43 en changeant le fichier /etc/mysql/my.cnf



4- Empêcher de faire le parcours du répertoire

Pour ce faire j'Ai modifié le fichier /etc/apache2/sites-available/default et j'Ai inséré

```
<Directory />
  Order Deny,Allow
  Deny from all
  Options None
  AllowOverride None
</Directory>
<Directory /web>
  Order Allow,Deny
  Allow from all
</Directory>
```

5- Installation de ModSecurity

C'est un module d'Apache spécialisé dans la sécurité. Il permet donc de sécuriser la couche applicative avant l'arrivée des requêtes sur le site hébergé sur l'Apache en question. Même s'il s'agit d'un module, ses fonctionnalités sont vastes et permettent de toucher à tous les points de sécurité nécessaire. Comme utilisations possible, citons la détection de tentatives d'inclusions, la lutte anti-spam, l'utilisation d'exploits (il permet de cacher les numéros de versions utilisées sur les pages d'erreur renvoyées par le serveur Web), l'application d'une liste noire (ou blanche), etc…

6- Installation et Configuration de Brutelock

Brutelock est un programme qui surveille les divers journaux de logs d'un système et bloque immédiatement les IP malveillante visant à attaquer votre serveur.

Brutelock ne protège pas seulement contre les attaques ssh, mais aussi d'autres services communs, comme FTP, POP et IMAP etc...