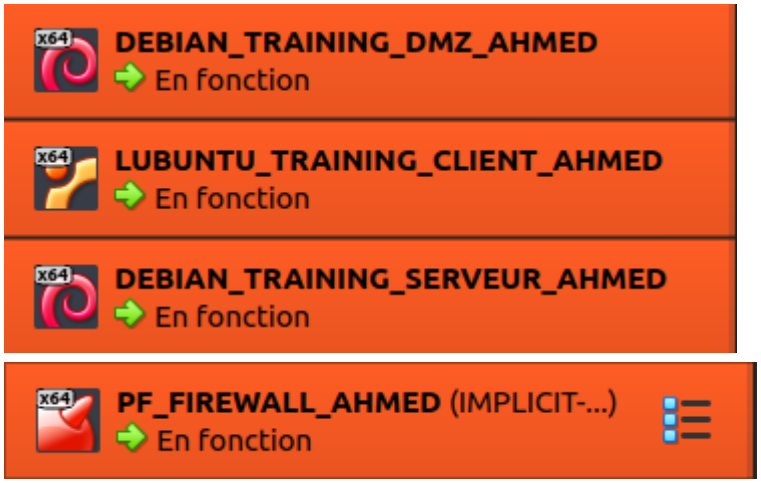
DOC - APACHE

1°) Travaux préparatoires

Je commence tout d'abords par lancer les docs nécessaire à la réalisation du contexte :



Sur la machine DEBIAN_TRAINING_DMZ :

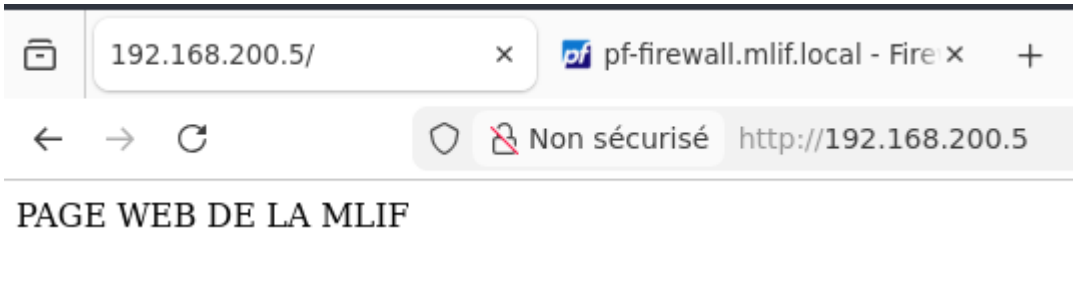
On effectue la commande "ps -ef | grep apache" pour vérifier que notre serveur web est en écoute

```
root@www:~# ps -ef | grep apache
root         662       1  0 nov.23 ?        00:00:00 /usr/sbin/apache2 -k start
www-data     955     662  0 nov.23 ?        00:00:00 /usr/sbin/apache2 -k start
www-data     956     662  0 nov.23 ?        00:00:00 /usr/sbin/apache2 -k start
www-data     957     662  0 nov.23 ?        00:00:00 /usr/sbin/apache2 -k start
www-data     958     662  0 nov.23 ?        00:00:00 /usr/sbin/apache2 -k start
www-data     959     662  0 nov.23 ?        00:00:00 /usr/sbin/apache2 -k start
www-data    1118     662  0 00:40 ?         00:00:00 /usr/sbin/apache2 -k start
root        1131     803  0 00:53 tty1      00:00:00 grep apache
```

le propriétaire des processus Apache est l'utilisateur www-data

Sur la machine DEBIAN_TRAINING_CLIENT1

En saisissant l'adresse ip je me retrouve bel et bien sur la page par défaut du serveur web



2°) Principales directives

Sur la machine DEBIAN_TRAINING_DMZ :

étape 1 :
On vas maintenant changer l'emplacement de stockage de la page web du site web par défaut.

Pour cela se rendre sur :

- cd etc/apache2/sites-available
- nano 000-default.conf

on obtient alors un document semblable :

```
  GNU nano 7.2                                                 000-default.conf
<VirtualHost *:80>
        # The ServerName directive sets the request scheme, hostname and port that
        # the server uses to identify itself. This is used when creating
        # redirection URLs. In the context of virtual hosts, the ServerName
        # specifies what hostname must appear in the request's Host: header to
        # match this virtual host. For the default virtual host (this file) this
        # value is not decisive as it is used as a last resort host regardless.
        # However, you must set it for any further virtual host explicitly.
        #ServerName www.example.com

        ServerAdmin webmaster@localhost
        DocumentRoot /var/www/html

        # Available loglevels: trace8, ..., trace1, debug, info, notice, warn,
        # error, crit, alert, emerg.
        # It is also possible to configure the loglevel for particular
        # modules, e.g.
        #LogLevel info ssl:warn

        ErrorLog ${APACHE_LOG_DIR}/error.log
        CustomLog ${APACHE_LOG_DIR}/access.log combined

        # For most configuration files from conf-available/, which are
        # enabled or disabled at a global level, it is possible to
        # include a line for only one particular virtual host. For example the
        # following line enables the CGI configuration for this host only
        # after it has been globally disabled with "a2disconf".
        #Include conf-available/serve-cgi-bin.conf
</VirtualHost>
```

On va modifier la ligne "DocumentRoot" afin de la faire pointer vers le répertoire que nous allons créer.

On obtient alors un document de ce type :

```
ServerAdmin webmaster@localhost
DocumentRoot /usr/local/httpd/html
```

étape 2 :

On vas maintenant crée le répertoire que l'on vient de renseigner dans la ligne documentroot, à l'aide de la commande mkdir -p :

- mkdir -p /usr/local/httpd/www

```
root@www:/etc/apache2/sites-available# mkdir -p /usr/local/httpd/www
root@www:/etc/apache2/sites-available# cd /usr/local/httpd/www
```

étape 3 :

À cette étape, nous devons attribuer la propriété de toute la nouvelle arborescence à l'utilisateur utilisé par Apache, c'est-à-dire *www-data*. Pour cela, nous exécutons un *chown* avec l'option *-R* afin d'appliquer la modification de façon récursive

```
root@www:/usr/local/httpd/www# chown -R www-data:www-data /usr/local/httpd/www
```

étape 4 :

Nous rouvrons le fichier *000-default.conf* et ajoutons un bloc *Directory* pour notre nouvelle arborescence. Ce bloc définit les autorisations d'accès. Nous le plaçons juste sous la ligne *DocumentRoot* en recopiant les lignes de la capture.

```
  GNU nano 7.2                                          000-default.conf *
<VirtualHost *:80>
        # The ServerName directive sets the request scheme, hostname and port that
        # the server uses to identify itself. This is used when creating
        # redirection URLs. In the context of virtual hosts, the ServerName
        # specifies what hostname must appear in the request's Host: header to
        # match this virtual host. For the default virtual host (this file) this
        # value is not decisive as it is used as a last resort host regardless.
        # However, you must set it for any further virtual host explicitly.
        #ServerName www.example.com

        ServerAdmin webmaster@localhost
        DocumentRoot /usr/local/httpd/html

        # Available loglevels: trace8, ..., trace1, debug, info, notice, warn,
        # error, crit, alert, emerg.
        # It is also possible to configure the loglevel for particular
        # modules, e.g.
        #LogLevel info ssl:warn

        ErrorLog ${APACHE_LOG_DIR}/error.log
        CustomLog ${APACHE_LOG_DIR}/access.log combined

        # For most configuration files from conf-available/, which are
        # enabled or disabled at a global level, it is possible to
        # include a line for only one particular virtual host. For example the
        # following line enables the CGI configuration for this host only
        # after it has been globally disabled with "a2disconf".
        #Include conf-available/serve-cgi-bin.conf

<Directory /usr/local/httpd/www>
        Options Indexes
        Require all granted
</Directory>

</VirtualHost>
```

je me suis permis une connexion ssh depuis ma machine physique afin de faciliter la saisie de texte.

étape 5 :

Se déplacer vous dans la nouvelle arborescence /usr/local/httpd/www et créer une page html de
test avec la commande suivante :

- echo "Changement de racine OK" > index.html

```
root@www:/etc/apache2/sites-available# cd /usr/local/httpd/www
root@www:/usr/local/httpd/www# ls
root@www:/usr/local/httpd/www# echo "Changement de racine OK" > index.html
root@www:/usr/local/httpd/www# ls
index.html
```

étape 6 :
Redémarrer apache et tester avec la commande wget que le changement de racine est effectif.

```
root@www:/etc/apache2/sites-available# systemctl restart apache2
root@www:/etc/apache2/sites-available# wget localhost
--2025-12-03 22:04:07--  http://localhost/
Résolution de localhost (localhost)… ::1, 127.0.0.1
Connexion à localhost (localhost)|::1|:80… connecté.
requête HTTP transmise, en attente de la réponse… 200 OK
Taille : 24 [text/html]
Sauvegarde en : « index.html »

index.html                      100%[=================================================================>]      24  --.-KB/s    ds 0s

2025-12-03 22:04:07 (620 KB/s) – « index.html » sauvegardé [24/24]

root@www:/etc/apache2/sites-available#
```

attention à bien mettre les bon chemins, je me suis trompé dans le chemin du documentRoot ca me bloque et m'affichais un message forbiden access.

Depuis la machine client : je vide le cache et je me rend sur la page.

Le changement est bien effectif.

```
2025-12-03 22:04:07 (620 KB/s) – « index.html » sauvegardé [24/24]

root@www:/etc/apache2/sites-available# ls
000-default.conf  default-ssl.conf  index.html
root@www:/etc/apache2/sites-available# cat index.html
Changement de racine OK
```

2.2°) Directive Listen

Sur la machine DEBIAN_TRAINING_DMZ

Nous devons modifier le port d'écoute d'Apache et le passer à **8001**. Pour cela, nous ouvrons d'abord ***ports.conf*** pour changer le port, puis nous faisons la même modification dans le fichier ***000-default.conf***, là où le VirtualHost utilise encore le port d'origine.

Je modifie la première ligne.

```
  GNU nano 7.2                                          /etc/apache2/ports.conf
# If you just change the port or add more ports here, you will likely also
# have to change the VirtualHost statement in
# /etc/apache2/sites-enabled/000-default.conf

Listen 8001

<IfModule ssl_module>
        Listen 443
</IfModule>

<IfModule mod_gnutls.c>
        Listen 443
</IfModule>
```

je change aussi dans le fichier **000-default.conf :**

```
  GNU nano 7.2                                          000-default.conf *
<VirtualHost *:8001>
        # The ServerName directive sets the request scheme, hostname and port that
        # the server uses to identify itself. This is used when creating
        # redirection URLs. In the context of virtual hosts, the ServerName
        # specifies what hostname must appear in the request's Host: header to
        # match this virtual host. For the default virtual host (this file) this
        # value is not decisive as it is used as a last resort host regardless.
        # However, you must set it for any further virtual host explicitly.
        #ServerName www.example.com

        ServerAdmin webmaster@localhost
        DocumentRoot /usr/local/httpd/www
        <Directory /usr/local/httpd/www>
```

Je n'oublie pas de redémarrer le service et de télécharger la nouvelle page (commande wget)

```
root@www:/etc/apache2/sites-available# systemctl restart apache2
root@www:/etc/apache2/sites-available# wget localhost:8001
--2025-12-03 22:14:10--  http://localhost:8001/
Résolution de localhost (localhost)… ::1, 127.0.0.1
Connexion à localhost (localhost)|::1|:8001… connecté.
requête HTTP transmise, en attente de la réponse… 200 OK
Taille : 24 [text/html]
Sauvegarde en : « index.html.1 »

index.html.1                    100%[=============================================================>]      24  --.-KB/s    ds 0s

2025-12-03 22:14:10 (7,63 MB/s) – « index.html.1 » sauvegardé [24/24]
```

La commande **wget localhost** échoue car elle fair référence a un port non utilisé à savoir le port 80.

```
root@www:/etc/apache2/sites-available# wget localhost
--2025-12-03 22:14:54--  http://localhost/
Résolution de localhost (localhost)… ::1, 127.0.0.1
Connexion à localhost (localhost)|::1|:80… échec : Connexion refusée.
Connexion à localhost (localhost)|127.0.0.1|:80… échec : Connexion refusée.
```

2.3°) Directive Alias

Sur la machine DEBIAN_TRAINING_DMZ :

Cette directive permet l'accès à des documents stockés en-dehors de l'arborescence définie par la directive DocumentRoot, par exemple pour l'accès à une documentation.

étape 1 : Création de l'arborescence

Nous créons l'arborescence **/usr/local/doc**, puis nous y ajoutons le fichier **ladoc.html** contenant le texte "**Voici la documentation."**

```
root@www:~# mkdir -p /usr/local/doc
```

```
root@www:/usr/local/doc# nano ladoc.html
root@www:/usr/local/doc# cat ladoc.html
ceci est ma documentation_!
```

Étape 2: Création de l'alias vers cette documentation

On vérifie d'abord que le module **alias_module** est bien chargé à l'aide de la commande :

- ls /etc/apache2/mods-enabled | grep alias

```
root@www:~# ls /etc/apache2/mods-enabled | grep alias
alias.conf
alias.load
```

On va maintenant créer un alias **docs**, pour cela dans le fichier **000-default.conf.** On rajotue la ligne **Alias /docs /usr/local/doc**

```
#ServerName www.example.com
Alias /docs /usr/local/doc
```

Étape 3: Création d'un DIRECTORY dans le VirtualHost

```
ano 7.2                                                    000-default.conf
lHost *:8001>
 # The ServerName directive sets the request scheme, hostname and port that
 # the server uses to identify itself. This is used when creating
 # redirection URLs. In the context of virtual hosts, the ServerName
 # specifies what hostname must appear in the request's Host: header to
 # match this virtual host. For the default virtual host (this file) this
 # value is not decisive as it is used as a last resort host regardless.
 # However, you must set it for any further virtual host explicitly.
 #ServerName www.example.com
 Alias /docs /usr/local/doc


 ServerAdmin webmaster@localhost
 DocumentRoot /usr/local/httpd/www
 <Directory /usr/local/httpd/www>
         Options Indexes
         Require all granted
 </Directory>
 <Directory /usr/local/doc>
         Options Indexes
         Require all granted
 </Directory>
```

Nouveaux directory ajouté.

```
root@www:/etc/apache2/sites-available# chown -R www-data:www-data /usr/local/doc
root@www:/etc/apache2/sites-available# systemctl restart apache2
```

On donne les droit et on redémarre le service web.

Étape 4: Redémarrage du serveur et test

Redémarrer votre serveur web avec tester un accès à votre documentation à l'aide de la commande suivant :

- wget localhost:8001/docs/ladoc.html

```
requête HTTP transmise, en attente de la réponse… 200 OK
Taille : 29 [text/html]
Sauvegarde en : « ladoc.html.1 »

ladoc.html.1                    100%[=================================================================>]      29  --.-KB/s    ds 0s

2025-12-03 22:47:26 (9,22 MB/s) – « ladoc.html.1 » sauvegardé [29/29]

root@www:/usr/local/doc# ls
ladoc.html  ladoc.html.1
root@www:/usr/local/doc# cat ladoc.html.1
ceci est ma documentation !
```

STOP 1 : Appelez moi pour que je puisse vérifier cette partie du travail.

4°) VirtualHost HTTP et HTTPS

4.1°) Création de deux nouveaux VirtualHost HTTP

Sur la machine DEBIAN_TRAINING_DMZ :

Étape 1: Vous devez créez un nouveau VirtualHost HTTP. Pour cela, copier le fichier 000-default.conf, présent dans /etc/apache2/sites-available, en le renommant sitea.conf. Pour cela, utiliser la commande cp.

```
root@www:/usr/local/doc# cp /etc/apache2/sites-available/000-default.conf /etc/apache2/sites-available/sitea.conf
root@www:/usr/local/doc# cd /etc/apache2/sites-available/
root@www:/etc/apache2/sites-available# ls
000-default.conf  default-ssl.conf  index.html  index.html.1  sitea.conf
```

Étape 2: Ensuite, modifier la configuration du virtualhost sitea.conf avec les paramètres suivants :

- *port d'écoute : 80 (n'oubliez pas de modifier aussi le fichier ports.conf) ;*
- *pas d'alias ;*
- *DocumentRoot : /var/www/html/sitea (n'oubliez pas de créer le répertoire sitea dans www) ;*
- *ServerName = sitea.mlif.local.*
- *Page web dans le répertoire /var/www/html/sitea de nom index.html affichant le texte suivant : "SITE A OK"*

```
  GNU nano 7.2                                                  sitea.conf *
<VirtualHost *:80>
        # The ServerName directive sets the request scheme, hostname and port that
        # the server uses to identify itself. This is used when creating
        # redirection URLs. In the context of virtual hosts, the ServerName
        # specifies what hostname must appear in the request's Host: header to
        # match this virtual host. For the default virtual host (this file) this
        # value is not decisive as it is used as a last resort host regardless.
        # However, you must set it for any further virtual host explicitly.
        ServerName sitea.mlif.local


        ServerAdmin webmaster@localhost
        DocumentRoot /var/www/html/sitea
        <Directory /var/www/html/sitea>
                Options Indexes
                Require all granted
        </Directory>

        # Available loglevels: trace8, ..., trace1, debug, info, notice, warn,
        # error, crit, alert, emerg.
        # It is also possible to configure the loglevel for particular
        # modules, e.g.
        #LogLevel info ssl:warn

        ErrorLog ${APACHE_LOG_DIR}/error.log
        CustomLog ${APACHE_LOG_DIR}/access.log combined

        # For most configuration files from conf-available/, which are
        # enabled or disabled at a global level, it is possible to
        # include a line for only one particular virtual host. For example the
        # following line enables the CGI configuration for this host only
        # after it has been globally disabled with "a2disconf".
        #Include conf-available/serve-cgi-bin.conf


</VirtualHost>
```

Voici le fichier modifé.

On oublie pas de modifier le fichier de port :

```
 GNU nano 7.2                                                /etc/apache2/ports.conf *
# If you just change the port or add more ports here, you will likely also
# have to change the VirtualHost statement in
# /etc/apache2/sites-enabled/000-default.conf

Listen 8001
Listen 80
```

Une fois cela fait, on oublie pas de créer la page web dans le bon répertoire.

```
 GNU nano 7.2                                                  sitea/index.html
§ SITE A OK §
```

On donne les droit a l'utilisateur :

```
root@www:/etc/apache2/sites-available# chown -R www-data:www-data sitea.conf
root@www:/etc/apache2/sites-available# ls -l
total 24
-rw-r--r-- 1 root     root     1566  3 déc.  22:42 000-default.conf
-rw-r--r-- 1 root     root     6195  5 avril  2024 default-ssl.conf
-rw-r--r-- 1 root     root       24  3 déc.  21:54 index.html
-rw-r--r-- 1 root     root       24  3 déc.  21:54 index.html.1
-rw-r--r-- 1 www-data www-data 1418  3 déc.  23:05 sitea.conf
```

Depuis la machine DEBIAN_TRAINING_SERVEUR :

Étape 3: Ajouter l'enregistrement suivant de type CNAME dans le fichier de zone directe de votre serveur DNS en faisant référence au nom sitea.

```
 GNU nano 7.2                                                /var/lib/bind/db.mlif.local
;
; BIND data file pour zone directe.
;
$TTL    604800
@       IN      SOA     messagelab.mlif.local. root.mlif.local. (
                              11         ; Serial
                          604800         ; Refresh
                           86400         ; Retry
                         2419200         ; Expire
                          604800 )       ; Negative Cache TTL
;
@       IN      NS      messagelab.mlif.local.
@       IN      MX      10      mail.mlif.local.

messagelab      IN      A       192.168.100.10
mail            IN      A       192.168.100.20
pfsense         IN      A       192.168.50.254
toip            IN      A       192.168.100.40
backup          IN      A       192.168.100.50
wpad            IN      A       192.168.50.254
cdp             IN      A       192.168.100.30
www             IN      A       192.168.200.5
www-bis         IN      A       192.168.200.52

imap    IN      CNAME   mail.mlif.local.
smtp    IN      CNAME   mail.mlif.local.
sitea   IN      CNAME   www.mlif.local.
```

Depuis les machines DEBIAN_TRAINING_DMZ et DEBIAN_TRAINING_SERVEUR:

étape 4 : Recommencer les étape 1 à 3.

- *étape 1 :*

```
  GNU nano 7.2                                                  siteb.conf
<VirtualHost *:80>
        # The ServerName directive sets the request scheme, hostname and port that
        # the server uses to identify itself. This is used when creating
        # redirection URLs. In the context of virtual hosts, the ServerName
        # specifies what hostname must appear in the request's Host: header to
        # match this virtual host. For the default virtual host (this file) this
        # value is not decisive as it is used as a last resort host regardless.
        # However, you must set it for any further virtual host explicitly.
        ServerName sitea.mlif.local


        ServerAdmin webmaster@localhost
        DocumentRoot /usr/local/httpd/siteb
        <Directory /var/www/html/siteb>
                Options Indexes
                Require all granted
        </Directory>
        <Directory /usr/local/doc>
                Options Indexes
                Require all granted
        </Directory>

        # Available loglevels: trace8, ..., trace1, debug, info, notice, warn,
        # error, crit, alert, emerg.
        # It is also possible to configure the loglevel for particular
        # modules, e.g.
        #LogLevel info ssl:warn

        ErrorLog ${APACHE_LOG_DIR}/error.log
        CustomLog ${APACHE_LOG_DIR}/access.log combined

        # For most configuration files from conf-available/, which are
        # enabled or disabled at a global level, it is possible to
        # include a line for only one particular virtual host. For example the
        # following line enables the CGI configuration for this host only
        # after it has been globally disabled with "a2disconf".
        #Include conf-available/serve-cgi-bin.conf


</VirtualHost>
```

- *étape 2 :*
-

```
root@www:/var/www/html# chown -R www-data:www-data /etc/apache2/sites-available/siteb
```

-

```
root@www:/var/www/html/siteb# ls
siteb.conf
root@www:/var/www/html/siteb# cat siteb.conf
§§ SITE B §§
```

Étape 3: Ajouter l'enregistrement suivant de type CNAME dans le fichier de zone directe de votre serveur DNS en faisant référence au nom sitea

```
 GNU nano 7.2                                                    /var/lib/bind/db.mlif
;
; BIND data file pour zone directe.
;
$TTL    604800
@       IN      SOA     messagelab.mlif.local. root.mlif.local. (
                              11         ; Serial
                          604800         ; Refresh
                           86400         ; Retry
                         2419200         ; Expire
                          604800 )       ; Negative Cache TTL
;
@       IN      NS      messagelab.mlif.local.
@       IN      MX      10      mail.mlif.local.

messagelab      IN      A       192.168.100.10
mail            IN      A       192.168.100.20
pfsense         IN      A       192.168.50.254
toip            IN      A       192.168.100.40
backup          IN      A       192.168.100.50
wpad            IN      A       192.168.50.254
cdp             IN      A       192.168.100.30
www             IN      A       192.168.200.5
www-bis         IN      A       192.168.200.52

imap    IN      CNAME   mail.mlif.local.
smtp    IN      CNAME   mail.mlif.local.
sitea   IN      CNAME   www.mlif.local.
siteb   IN      CNAME   www.mlif.local.
```

Étape 5: Désactiver le virtualhost par défaut 000-default en saisissant la commande suivante :

```
root@www:/var/www/html/siteb# a2dissite 000-default
Site 000-default disabled.
To activate the new configuration, you need to run:
  systemctl reload apache2
```

Ensuite, on active nos deux autre sites à savoir, site a et site b :

```
root@www:/var/www/html/siteb# a2ensite sitea
Enabling site sitea.
To activate the new configuration, you need to run:
  systemctl reload apache2
root@www:/var/www/html/siteb# a2ensite siteb
Enabling site siteb.
To activate the new configuration, you need to run:
  systemctl reload apache2
```

On redémarre le serveur apache2 :

```
root@www:/var/www/html/siteb# systemctl restart apache2
root@www:/var/www/html/siteb# systemctl status apache2
● apache2.service - The Apache HTTP Server
     Loaded: loaded (/lib/systemd/system/apache2.service; enabled; preset: enabled)
     Active: active (running) since Wed 2025-12-03 23:25:42 CET; 7s ago
       Docs: https://httpd.apache.org/docs/2.4/
```

Étape 6: Tester depuis le navigateur de la machine cliente :

4.2°) Activation d'un VirtualHost HTTPS

Le chiffrement est essentiel lors de certaines transactions comme l'accès à un serveur bancaire. Si la conversation n'est pas chiffrée, un attaquant peut capturer des trames et observer leurs contenus avec un logiciel comme wireshark.

Activer votre VirtualHost HTTPS à l'aide de la commande suivante

```
root@www:/etc/apache2/sites-available# a2ensite default-ssl.conf
Site default-ssl already enabled
```

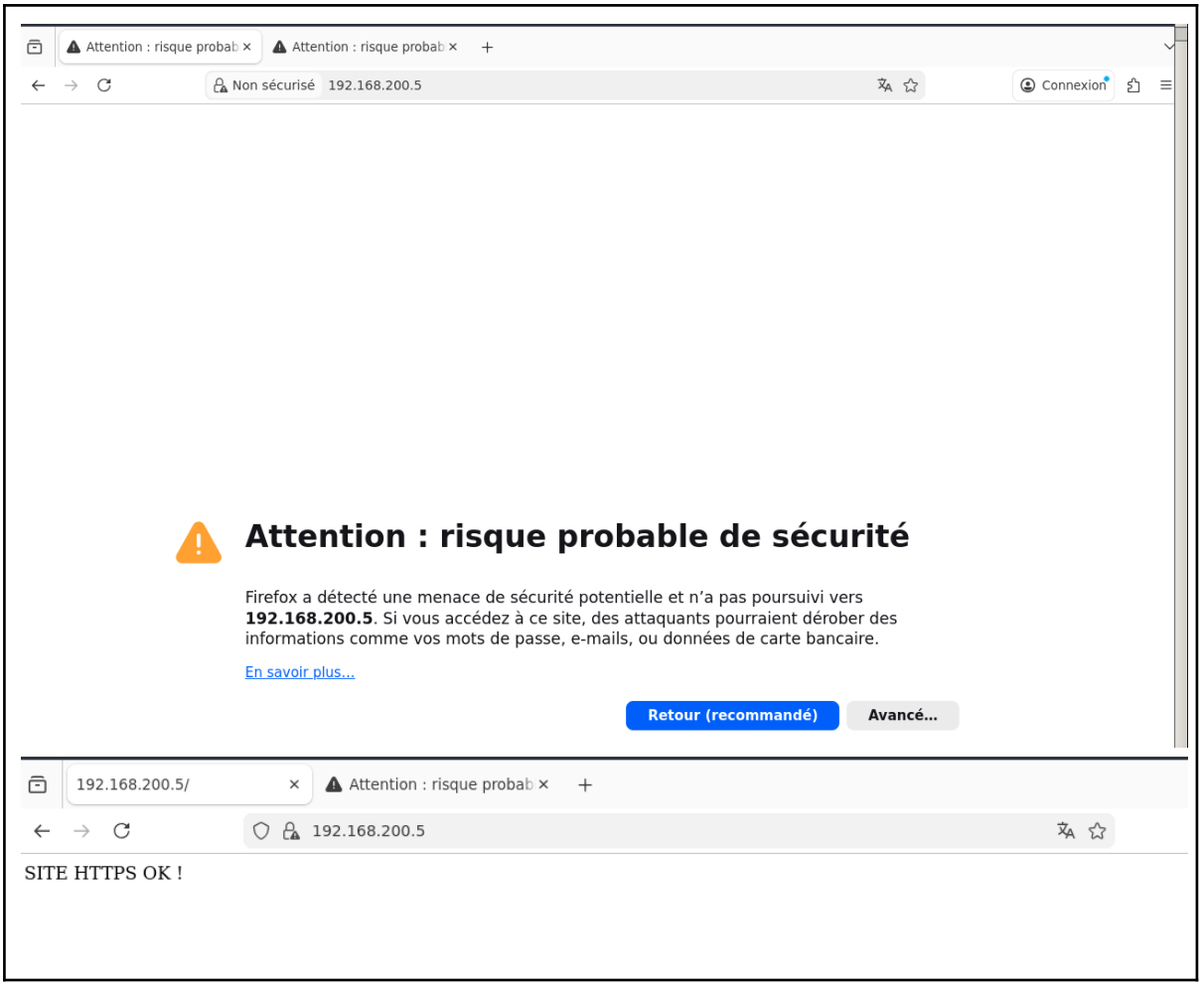
Ensuite, activer le module ssl à l'aide de la commande suivante :

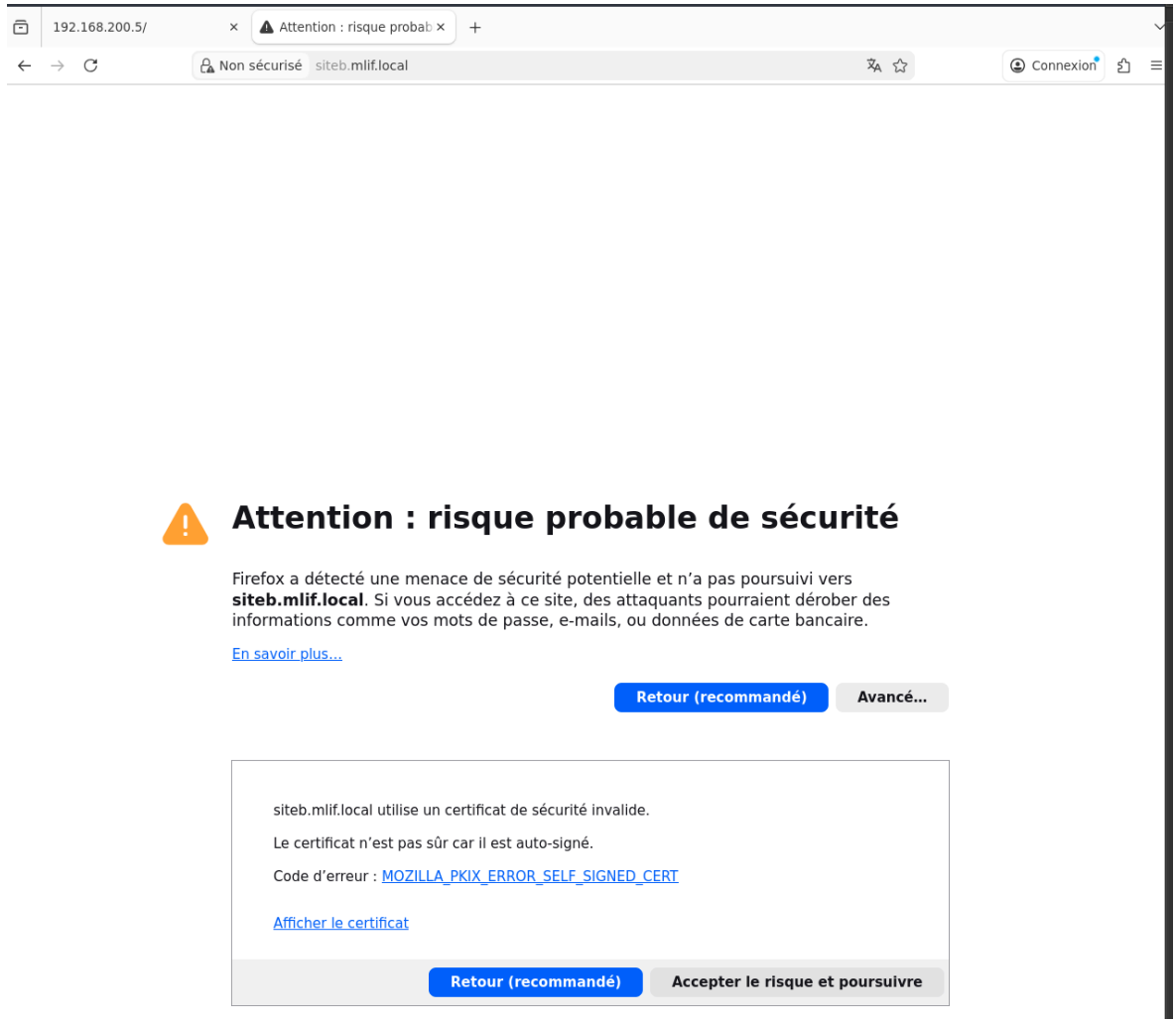
```
root@www:/etc/apache2/sites-available# a2enmod ssl
Considering dependency setenvif for ssl:
Module setenvif already enabled
Considering dependency mime for ssl:
Module mime already enabled
Considering dependency socache_shmcb for ssl:
Enabling module socache_shmcb.
Enabling module ssl.
See /usr/share/doc/apache2/README.Debian.gz on how to configure SSL and create self-signed certificates.
To activate the new configuration, you need to run:
  systemctl restart apache2
```

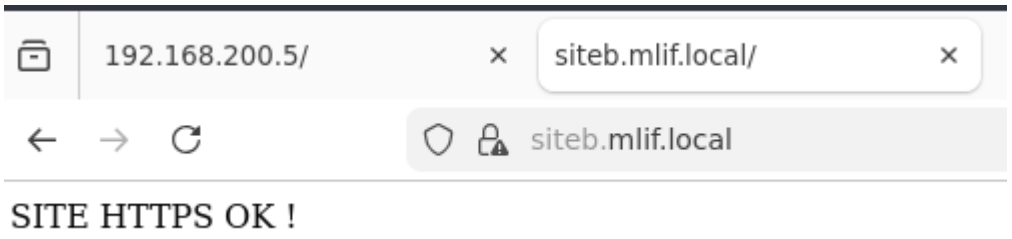
Modifier la page HTML située dans /var/www/html pour qu'elle affiche le texte suivante : "SITE HTTPS OK."

```
  GNU nano 7.2                                                index.html
SITE HTTPS OK !
```

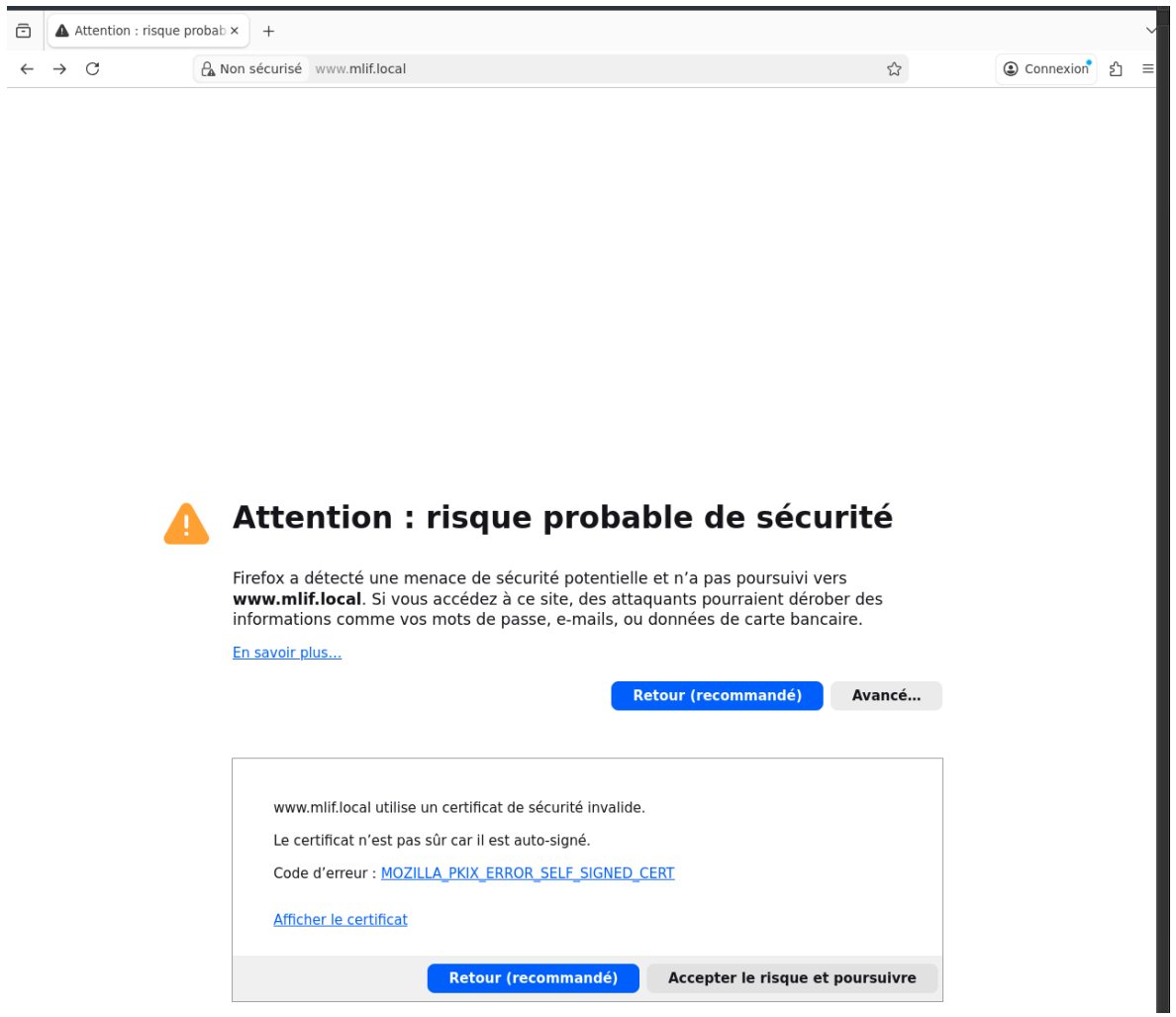
Ne pas oublier de redémarrer apache.

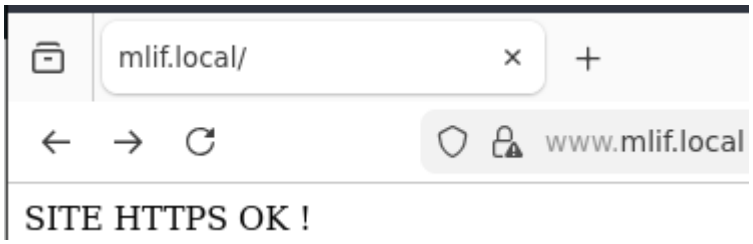

Attention : risque probab
Attention : risque probab
Non sécurisé
192.168.200.5
Connexion
Attention : risque probable de sécurité
Firefox a détecté une menace de sécurité potentielle et n'a pas poursuivi vers 192.168.200.5. Si vous accédez à ce site, des attaquants pourraient dérober des informations comme vos mots de passe, e-mails, ou données de carte bancaire.
En savoir plus...
Retour (recommandé)
Avancé...
192.168.200.5/
Attention : risque probab
192.168.200.5
SITE HTTPS OK !





ENFIN, voici la page de la mlif :





Le stop est donc validé

STOP 2 : Appelez moi pour que je puisse vérifier cette partie du travail.

5°) Authentification HTACCESS

*L'objectif est de fournir **un service d'authentification** lors de l'accès à un VirtualHost. Dans ce TP, **une authentification sera mise en place lors de l'accès à la page d'accueil index.html du VirtualHost sitea.conf**.*

Étape 1: Directive AllowOverride:

Pour ce faire :

- Se rendre de le fichier **“sitea.conf”** dans **/etc/apache2/sites-available**
- **Ajouter** la directive “ **AllowOverride AuthConfig** ” dans le bloc Directory associé au sitea

```
  GNU nano 7.2                                                  sitea.conf *
<VirtualHost *:80>
    # The ServerName directive sets the request scheme, hostname and port that
    # the server uses to identify itself. This is used when creating
    # redirection URLs. In the context of virtual hosts, the ServerName
    # specifies what hostname must appear in the request's Host: header to
    # match this virtual host. For the default virtual host (this file) this
    # value is not decisive as it is used as a last resort host regardless.
    # However, you must set it for any further virtual host explicitly.
    ServerName sitea.mlif.local

    ServerAdmin webmaster@localhost
    DocumentRoot /var/www/html/sitea

    <Directory /var/www/html/sitea>
        Options Indexes
        Require all granted
        AllowOverride AuthConfig
    </Directory>

    # Available loglevels: trace8, ..., trace1, debug, info, notice, warn,
    # error, crit, alert, emerg.
    # It is also possible to configure the loglevel for particular
    # modules, e.g.
    #LogLevel info ssl:warn

    ErrorLog ${APACHE_LOG_DIR}/error.log
    CustomLog ${APACHE_LOG_DIR}/access.log combined

    # For most configuration files from conf-available/, which are
    # enabled or disabled at a global level, it is possible to
    # include a line for only one particular virtual host. For example the
    # following line enables the CGI configuration for this host only
    # after it has been globally disabled with "a2disconf".
    #Include conf-available/serve-cgi-bin.conf
</VirtualHost>
```

Étape 2 : Création du fichier de mot de passe

A. Création du fichier des mots de passe :

- Se déplacer dans le répertoire /etc/apache2
-

Puis saisir la commande :

- **htpasswd -bc .htpasswd usertest usertest**

```
root@www:/etc/apache2# htpasswd -bc .htpasswd usertest usertest
Adding password for user usertest
```

Cette commande vas donc créé le fichier en question en associant le mot de passe usertest a l’utilisateur usertest

Le fichier est crée est caché, il sera visible avec la commande “ ls -la”

```
root@www:/etc/apache2# ls -la
total 96
drwxr-xr-x  8 root root  4096  4 déc.  21:31 .
drwxr-xr-x 78 root root  4096  4 déc.  21:28 ..
-rw-r--r--  1 root root  7177 24 avril  2025 apache2.conf
drwxr-xr-x  2 root root  4096 24 avril  2025 conf-available
drwxr-xr-x  2 root root  4096  9 juin   2024 conf-enabled
-rw-r--r--  1 root root  1782 11 oct.   2023 envvars
-rw-r--r--  1 root root    47  4 déc.  21:31 .htpasswd
-rw-r--r--  1 root root 31063 11 oct.   2023 magic
drwxr-xr-x  2 root root 16384 24 avril  2025 mods-available
drwxr-xr-x  2 root root  4096  3 déc.  23:43 mods-enabled
-rw-r--r--  1 root root   286  3 déc.  23:02 ports.conf
drwxr-xr-x  2 root root  4096  4 déc.  21:29 sites-available
drwxr-xr-x  2 root root  4096  3 déc.  23:42 sites-enabled
root@www:/etc/apache2#
```

Le contenu du fichier est chiffré et l'affichage du fichier ne permet pas de voir le mot de passe :

```
root@www:/etc/apache2# cat .htpasswd
usertest:$apr1$iW/BHTYt$0Zh1qoKDXXtHtA2Rt61ct0
```

Étape 3: Application de la politique de sécurité à notre VirtualHost avec htaccess

Se déplacer dans le répertoire **/var/www/html/sitea** afin d'y créer un fichier **.htaccess** à l'aide d'un éditeur de texte. Remplir le fichier comme demandé !

En voici le résultat :

```
root@www:/etc/apache2# cd /var/www/html/sit
root@www:/var/www/html/sitea# ls
index.html
root@www:/var/www/html/sitea# nano .htacces
root@www:/var/www/html/sitea# cat .htaccess
Authname "ESSAI"
AuthUserFile /etc/apache2/.htpasswd
AuthType Basic
require valid-user
root@www:/var/www/html/sitea#
```

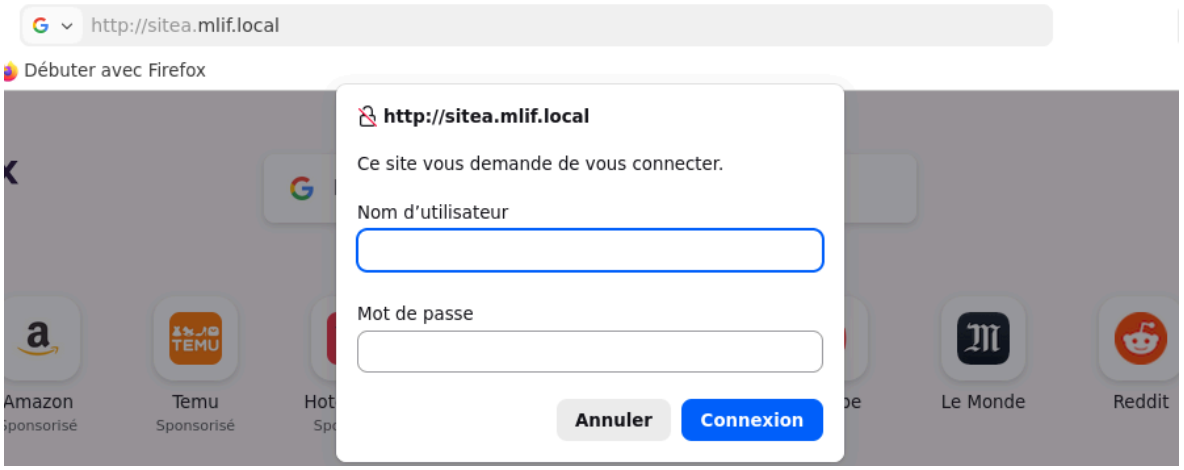
étape 4 : TEST

On passe maintenant a l'étape du test :

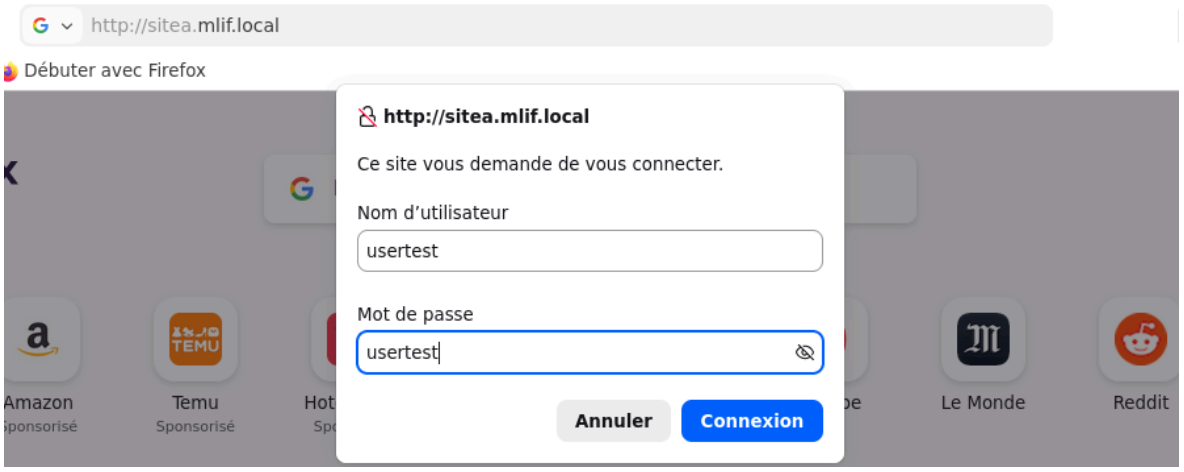
Ne pas oublier de rédémarer le service web de l'instance apache2 :

```
root@www:/var/www/html/sitea# systemctl restart apache2
root@www:/var/www/html/sitea# systemctl status apache2
● apache2.service - The Apache HTTP Server
     Loaded: loaded (/lib/systemd/system/apache2.service; enabled; preset: enabled)
     Active: active (running) since Thu 2025-12-04 21:37:10 CET; 5s ago
       Docs: https://httpd.apache.org/docs/2.4/
    Process: 980 ExecStart=/usr/sbin/apachectl start (code=exited, status=0/SUCCESS)
   Main PID: 986 (apache2)
      Tasks: 6 (limit: 1097)
```

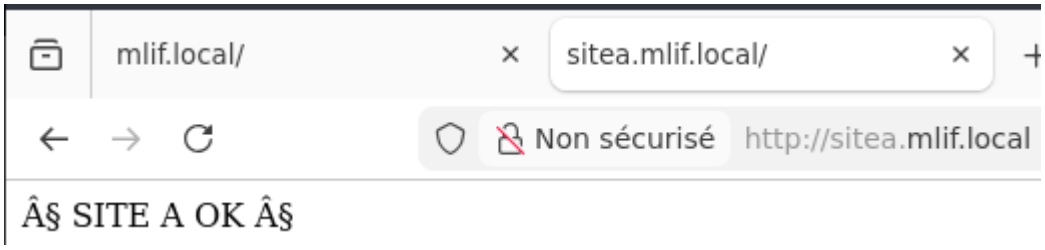
Depuis le client on réessaie l'accès à notre page web sitea.mlif.local, on obtient alors ceci :



En entrant les identifiants renseigné plus tôt dans le fichier **".htaccess"** on peut avoir accès au site web :



On appuie sur connexion :



TADAAAMM, on obtient bien l'accès à notre site.

Étape final : Sécurisation du serveur web

Il est essentiel de masquer la version du serveur web pour limiter sa "bavardise". Cette précaution empêche de fournir aux attaquants des informations clés pouvant être utilisées pour exploiter des vulnérabilités connues.

Pour ce faire :

- On Désactiver la signature de notre serveur web en utilisant la directive **ServerSignature**
- Se rendre dans le dossier " **etc/apache2/conf-enabled "**
- Dans le fichier " **security.conf"** mettre en commentaire la directive **ServerSignature ON** et activer la directive " **ServerSignature OFF "**

On as alors :

```
root@www:/etc/apache2/conf-enabled# ls
charset.conf  localized-error-pages.conf  other-vhosts-access-log.conf  security.conf  serve-cgi-bin.conf
root@www:/etc/apache2/conf-enabled# nano security.conf
```

```
  GNU nano 7.2                                                  security.conf *
# Changing the following options will not really affect the security of the
# server, but might make attacks slightly more difficult in some cases.

#
# ServerTokens
# This directive configures what you return as the Server HTTP response
# Header. The default is 'Full' which sends information about the OS-Type
# and compiled in modules.
# Set to one of:  Full | OS | Minimal | Minor | Major | Prod
# where Full conveys the most information, and Prod the least.
#ServerTokens Minimal
ServerTokens OS
#ServerTokens Full

#
# Optionally add a line containing the server version and virtual host
# name to server-generated pages (internal error documents, FTP directory
# listings, mod_status and mod_info output etc., but not CGI generated
# documents or custom error documents).
# Set to "EMail" to also include a mailto: link to the ServerAdmin.
# Set to one of:  On | Off | EMail
ServerSignature Off
#ServerSignature On
```

STOP 3 : Appelez moi pour que je puisse vérifier cette partie du travail.

FIN DE TP | FIN DE DOC