

# Cours SRW3

---

Henry Nicolas

SI-T1a

## Laboratoire

LABO : SSL

### Travail pratique

0. Désactiver les sites du labo précédent.

```
# a2dissite site1 site2 site3
```

1. Créez dans le répertoire `/var/www/site_ssl/` un site web avec une partie publique `/var/www/site_ssl/` et une partie privée `/var/www/site_ssl/private`. Seul l'utilisateur pingouin avec le mot de passe banque est autorisé à accéder à la section privée.

Créer les répertoires suivants :

```
# mkdir /var/www/site_ssl
# mkdir /var/www/site_ssl/private
```

Puis une page html dans chaque répertoire :

```
# nano /var/www/site_ssl/index.html
# nano /var/www/site_ssl/private/index.html
```

Puis, créer un fichier de configuration :

```
# nano /etc/apache2/sites-available/site_ssl.conf
```

Ajoutez le code suivant :

```
<VirtualHost *:80>
    ServerName site_ssl
    ServerAdmin webmaster@site_ssl
    DocumentRoot /var/www/site_ssl
    <Directory /var/www/site_ssl>
        Options Indexes FollowSymLinks
        Order allow,deny
        Allow from all
```

```

        DirectoryIndex index.html
        Require all granted
        AllowOverride None
    </Directory>
    <Directory /var/www/site_ssl/private>
        Options Indexes FollowSymLinks
        DirectoryIndex index.html
        AllowOverride All
    </Directory>
</VirtualHost>
Listen 443
<VirtualHost *:443>
    SSLEngine on
    ServerName site_ssl
    ServerAdmin webmaster@site_ssl
    DocumentRoot /var/www/site_ssl
    <Directory /var/www/site_ssl>
        Options Indexes FollowSymLinks
        Order allow,deny
        Allow from all
        DirectoryIndex index.html
        AllowOverride None
        Require all granted
    </Directory>
    <Directory /var/www/site_ssl/private>
        Options Indexes FollowSymLinks
        DirectoryIndex index.html
        AllowOverride All
    </Directory>
</VirtualHost>

```

2. La protection du répertoire privé se fait par l'intermédiaire d'un fichier .htaccess, en mode basique.

```
# nano /var/www/site_ssl/private/.htaccess
```

Puis, ajoutez le texte suivant :

```

AuthType Basic
AuthName "Password Required"
AuthUserFile "/etc/apache2/passwd/.user"
Require user pinguin

```

Créer ensuite votre utilisateur pinguin

```
# htpasswd -c /etc/apache2/passwd/.user pinguin
```

Puis entrez son mot de passe "banquise".

3. En mode basique votre mot de passe circule en clair sur le net. Que faudrait-il faire pour sécuriser

l'authentification de la section privée ?

Pour masquer votre mot de passe dans le fichier, effectuez :

```
# htdigest -c /etc/apache2/passwd/.userdigest "@SRW3-debian.local" penguin
```

Puis, pour protéger lors de la connexion, effectuez :

```
# nano /var/www/site_ssl/private/.htaccess
```

Et ajoutez :

```
AuthName "@SRW3-debian.local"
AuthType Digest
AuthDigestDomain "/private/" "http://192.168.106.128/private/"
"https://192.168.106.128/AuthUserFile "/etc/apache2/passwd/.userdigest"
```

Ensuite, activez digest :

```
# a2enmod auth_digest
```

4. Contrôlez que tous les modules nécessaires à l'installation et la configuration d'un serveur sécurisé soient présent sur votre système.

Contrôler les modules compilés avec le core et que mod\_ssl y soit :

```
# apache2ctl -t -D DUMP_MODULES | grep mod_ssl
```

Puis les modules chargés par Apache :

```
# apache2 -l | grep mod_ssl
```

Maintenant, les modules activés par Apache :

```
# apache2ctl -M | grep mod_ssl
```

5. Générez votre propre certificat autosigné.

Créer le répertoire suivant : 

```
# mkdir /etc/apache2/ssl
```

Générer un certificat auto-signé : 

```
# make-ssl-cert /usr/share/ssl-cert/ssleay.cnf /etc/apache2/ssl/FQDN.pem
```

Ensuite, saisissez votre nom d'hôte, votre ip pour chaque ip du serveur.

Puis, configurez votre module ssl : 

```
# nano /etc/apache2/site-available/site_ssl.conf
```

Et rajoutez la directive VirtualHost \* :443

```
SSLCertificateFile /etc/apache2/ssl/FQDN.pem
```

Et pour finir, redémarrez votre serveur apache.

```
# service apache2 restart
```

6. Modifiez la configuration de votre serveur afin que votre serveur apache puisse être exécuté en mode sécurisé.

Pour l'exécuter en mode sécurisé, il faut activer le module mod\_ssl

```
# a2enmod ssl
```

Puis redémarrer votre serveur :

```
# service apache2 restart
```

7. Démarrez et contrôlez le bon fonctionnement de votre serveur sécurisé.

Pour démarrer le site\_ssl, activez le :

```
# a2ensite site_ssl
```

Redémarrez votre serveur :

```
# service apache2 restart
```

Testez le :

```
# lynx http://127.0.0.1
```

Puis en https :

```
# lynx https://127.0.0.1
```

Puis la section privée :

```
# lynx http://127.0.0.1/private
```

Et enfin, en https :

```
# lynx https://127.0.0.1/private
```

8. Contrôlez que votre site ne puisse pas être accessible par une connexion non sécurisée.

Rediriger http vers https :

```
# nano /etc/apache2/sites-available/site_ssl.conf
```

Puis dans le VirtualHost :80 :

```
Redirect / https://192.168.106.128
```

Redémarrez apache :

```
# service apache2 restart
```

Testez les redirections :

```
\# lynx http://127.0.0.1
\# lynx http://127.0.0.1/private
```

9. Faites en sorte que seule la section privée soit sécurisée par le protocole SSL.

Pour mettre la partie "private" en https, modifiez le fichier site\_ssl.conf

```
# nano /etc/apache2/sites-available/site_ssl.conf
```

Et mettez y le code suivant

```
<VirtualHost *:80>
    ServerName 192.168.106.128
    ServerAdmin webmaster@site_ssl
    DocumentRoot /var/www/site_ssl
    <Directory /var/www/site_ssl>
        Options Indexes FollowSymLinks
        Order allow,deny
        Allow from all
        DirectoryIndex index.html
        AllowOverride None
        Require all granted
    </Directory>
    <Directory /var/www/site_ssl/private>
        Options Indexes FollowSymLinks
        DirectoryIndex index.html
        AllowOverride All
        RewriteEngine on
        RewriteCond %{HTTPS} off
        RewriteRule ^(.*)$ https://%{SERVER_NAME}%{REQUEST_URI} [R=301]
    </Directory>
</VirtualHost>
Listen 443
<VirtualHost *:443>
    SSLEngine on
    SSLCertificateFile /etc/apache2/ssl/FQDN.pem
    ServerName 192.168.106.128
    ServerAdmin webmaster@site_ssl
    DocumentRoot /var/www/site_ssl
    <Directory /var/www/site_ssl>
        Options Indexes FollowSymLinks
        Order allow,deny
        Allow from all
        DirectoryIndex index.html
        AllowOverride None
        Require all granted
    </Directory>
    <Directory /var/www/site_ssl/private>
        Options Indexes FollowSymLinks
```

```
        DirectoryIndex index.html
        AllowOverride All
    </Directory>
</VirtualHost>
```

Pour rediriger le http vers https en réécrivant l'URL :

```
# a2enmod rewrite
```

Redemarrez apache :

```
# service apache2 restart
```

Testez les différents sites en http et https :

```
# lynx http://127.0.0.1
# lynx https://127.0.0.1
# lynx http://127.0.0.1/private
# lynx https://127.0.0.1/private
```