Procédure : Authentification Apache & HTTPS

Moi je vais juste vous montrer comment aller plus loin en sécurisant votre site avec l'authentification de type *BASIC*, de type *DIGEST*, et HTTPS qui est sécurisé par un certificat. Bien sur, on peut combiner une authentification et HTTPS.

Il faut juste savoir que l'authentification est cryptée (et donc peut-être décrypter avec un peu de connaissances) tandis que HTTPS est chiffrée (par des algorithmes de hashage) et donc plus sécurisée.

⇒ Mise en place de l'authentification de type *BASIC*

1. Pour commencer nous allons d'abord créer un utilisateur qui aura le droit de se connecter au site avec la commande suivante : `htpasswd –c /etc/apache2/users toto`
   Le fichier **users** n'existe pas mais il sera créé en même que l'utilisateur. Si par la suite vous décider de voir ce fichier, vous verrez que le mot de passe à été crypté en Base64.

```
root@lub-web:/# htpasswd -c /etc/apache2/users toto
New password:
Re-type new password:
Adding password for user toto
root@lub-web:/#
```

2. Nous allons activer le mode d'authentification avec la commande :
   `a2enmod auth_basic.load` (activer par défaut)

3. Ensuite nous allons modifier le fichier de configuration de notre site, qui se trouve dans /etc/apache2/sites-available/

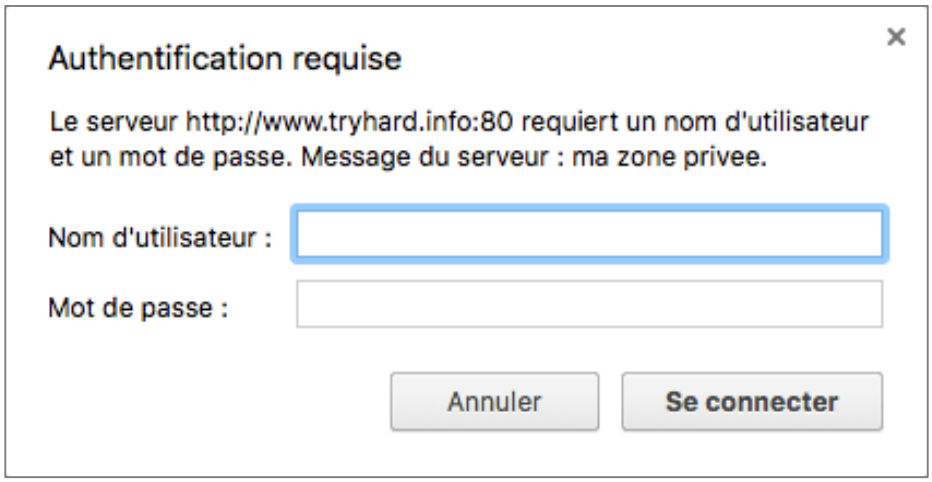
```
root@lub-web:/# cd /etc/apache2/sites-available/
root@lub-web:/etc/apache2/sites-available# nano tryhard.conf
```

Et ajouter les lignes suivantes :

```
<Directory /var/www/tryhard>                  → donne le chemin du site
   AuthType Basic                             → Type de l'authentification
   AuthName "ma zone privee"                  → Nom de l'authentification
   AuthBasicProvider file
   AuthUserFile /etc/apache2/users            → Fichier où sont situés les utilisateur
   Require valid-user                         → Requiert utilisateurs valide
</Directory>                                  → fermeture de la balise
```

```
<VirtualHost 192.168.182.139:80>
        # 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
        ServerName www.tryhard.info
        DocumentRoot /var/www/tryhard

        <Directory /var/www/tryhard>
                AuthType Basic
                AuthName "ma zone privee"
                AuthBasicProvider file
                AuthUserFile /etc/apache2/users
                Require valid-user
        </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>
```

4. Pour tester, entrez la commande `service apache2 reload` puis rendez vous l'adresse de votre site depuis un navigateur. Normalement vous obtenez ça :



Ainsi vous pouvez vous connecter avec l'utilisateur toto !

⇒ Mise en place de l'authentification de type *DIGEST*

1. Pour commencer nous allons d'abord créer un utilisateur qui aura le droit de se connecter au site avec la commande suivante :
   `htdigest /etc/apache2/users "ma zone privee" tata`

   Note : "ma zone privee" est la valeur que nous mettons dans AuthName.

```
root@lub-web:/# htdigest /etc/apache2/users "ma zone privee" tata
Adding user tata in realm ma zone privee
New password:
Re-type new password:
root@lub-web:/#
```

2. Nous allons activer le mode d'authentification avec la commande :
   `a2enmod auth_digest.load`

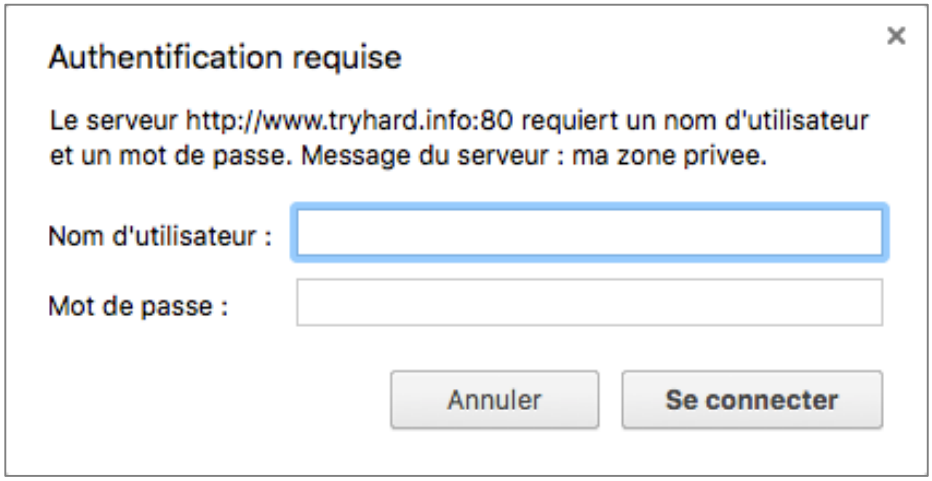
3. Ensuite nous allons modifier le fichier de configuration de notre site, qui se trouve dans /etc/apache2/sites-available/

```
root@lub-web:/# cd /etc/apache2/sites-available/
root@lub-web:/etc/apache2/sites-available# nano tryhard.conf
```

   Et ajouter les lignes suivantes :

```
<Directory /var/www/tryhard>          → donne le chemin du site
   AuthType Digest                    → Type de l'authentification
   AuthName "ma zone privee"          → Nom de l'authentification
   AuthDigestProvider file
   AuthUserFile /etc/apache2/users    → Fichier où sont situés les utilisateur
   Require valid-user                 → Requiert utilisateurs valide
</Directory>                          → fermeture de la balise
```

```
<VirtualHost 192.168.182.139:80>
        # 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
        ServerName www.tryhard.info
        DocumentRoot /var/www/tryhard

        <Directory /var/www/html/site3>
                AuthType Digest
                AuthName "ma zone privee"
                AuthDigestProvider file
                AuthUserFile /etc/apache2/users
                Require valid-user
        </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>
```

4. Pour tester, entrez la commande `service apache2 reload` puis rendez vous l'adresse de votre site depuis un navigateur. Normalement vous obtenez ça :
5. 

Ainsi vous pouvez vous connecter avec l'utilisateur toto !

⇒ Mise en place de HTTPS

I. Générations des certificats

1. Installer OpenSSL avec la commande `apt-get install openssl` si celui n'est pas déjà installé. Et activer le mode ssl avec la commande : `a2enmod ssl.load`

2. Générer le certificat avec la commande suivante :

   ```
   openssl req -x509 -nodes -days 700 -newkey rsa:2048 -sha256 -
   out /etc/apache2/server.crt -keyout /etc/apache2/server.key
   ```

   Et remplissez les informations nécessaire…

```
root@lub-web:/# openssl req -x509 -nodes -days 700 -newkey rsa:2048 -sha256 -out /etc/apache2
/server.crt -keyout /etc/apache2/server.key
Generating a 2048 bit RSA private key
.....................................................+++
.............................+++
writing new private key to '/etc/apache2/server.key'
-----
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [AU]:FR
State or Province Name (full name) [Some-State]:
Locality Name (eg, city) []:
Organization Name (eg, company) [Internet Widgits Pty Ltd]:LPJP
Organizational Unit Name (eg, section) []:IT
Common Name (e.g. server FQDN or YOUR name) []:
Email Address []:exemple@mail.com
root@lub-web:/#
```

3. Pour finir on modifie les permissions sur la clé afin de ne pas autoriser la lecture par les « autres » mais uniquement par le propriétaire et le groupe propriétaire.

   ```
   chmod 440 /chemin/server.crt
   ```

II. Configuration d'Apache

4. Dans /etc/apache2/sites-available faite une copie de **default-ssl.conf** en **tryhard-ssl.conf**

```
root@lub-web:/etc/apache2/sites-available# cp default-ssl.conf tryhard-ssl.conf
root@lub-web:/etc/apache2/sites-available# nano tryhard-ssl.conf
```

Puis éditer tryhard-ssl.conf :

- Modifier l'adresse IP dans la balise <*VirtualHost*>
- Modifier le **DocumentRoot**
- Et modifier le chemin **SSLCertificateFile** & **SSLCertificateKeyFile**

```
<IfModule mod_ssl.c>
        <VirtualHost 192.168.182.139:443>
                ServerAdmin webmaster@localhost

                DocumentRoot /var/www/tryhard

                # 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

                #   SSL Engine Switch:
                #   Enable/Disable SSL for this virtual host.
                SSLEngine on

                #   A self-signed (snakeoil) certificate can be created by installing
                #   the ssl-cert package. See
                #   /usr/share/doc/apache2/README.Debian.gz for more info.
                #   If both key and certificate are stored in the same file, only the
                #   SSLCertificateFile directive is needed.
                SSLCertificateFile /etc/apache2/server.crt
                SSLCertificateKeyFile /etc/apache2/server.key
```

5. Enfin, tapez : `a2ensite tryhard-ssl.conf` PUIS `service apache2 reload`

6. Pour tester, ouvrez un navigateur et tapez : https://www.tryhard.info