TP3 : Méthodes d'authentification

Authentification

- Par défaut le protocole http n'exige pas d'authentification. Une ressource correctement demandée et existante est fournie à un utilisateur pourvu que la machine cliente soit autorisée (directive Allow from ..).
  Il s'agit maintenant de voir comment réglementer l'accès à un espace considéré comme réservé à un ensemble d'utilisateurs autorisés. Ceux-ci devront alors satisfaire une procédure d'authentification par login et mot de passe pour pouvoir y accéder.

- Méthodes : On peut implémenter diverses méthodes :

  - Basic et digest : l'utilisateur doit posséder un compte (login/mdp) pour s'authentifier auprès d'APACHE. Dans la méthode *Basic* le mot de passe circule en clair entre le client et le serveur.
  - Https
  - base de données
  - authentification gérée par l'application, ce qui requière du code, actuellement principalement écrit en java, perl ou php

La méthode Basic

- Directives Voici les directives usuelles et leur signification

Directive	Action
AuthType basic	type d'authentification communément adopté (fait circuler les mots de passe en clair)
AuthName texte	affichera ce texte comme invite dans une boite de dialogue
AuthUserFile chemin/fichier	précise le fichier qui contient les comptes et mots de passe des utilisateurs ayant droit

	d'accès
Require valid-user Require liste-noms	l'accès s'applique à tous les comptes du fichier, ou seulement aux comptes énumérés dans la liste

- Exemple de procédure :
    1. Supposons que l'espace privé soit situé dans le répertoire /var/www/html/prive et son accès réservé à un ensemble d'utilisateurs : admin, webmaster et toto
    2. Directives à placer dans le fichier de configuration du site (par ex *default)*

```
<Directory "/var/www/html/prive">
AuthType Basic
AuthUserFile /etc/apache2/users
AuthName "Accès privé"
require valid-user
</Directory>
```

    3. Faire relire la configuration au serveur.
       Testez l'accessibilité au répertoire privé avec un navigateur
    4. Création des comptes
        - Ils doivent être placés dans le fichier spécifié par la clause *AuthUserFile*, et sont créés avec la commande **htpasswd**.

```
cd /etc/apache2
htpasswd -c users admin      (création du fichier et ajout de l'utilisateur admin)
--> mot de passe demandé, puis confirmé
htpasswd  users toto  (ajout d'un utilisateur toto)
```

       Le fichier */etc/apache2/users* contiendra alors une ligne par compte Apache créé.

    5. Testez l'accessibilité au répertoire privé : le serveur WEB affiche une boite de dialogue pour réclamer un couple login/mot de passe :

- On demande ici de protéger l'accès au sous-site privé de votre serveur, supposé situé dans le sous-répertoire **/var/www/prive/**
- Il ne devra être accessible qu'à un ensemble limité de comptes Apache (et non Linux) à créer
  La première requête adressée à ce répertoire protégé provoquera

l'affichage d'une boite de dialogue par laquelle l'utilisateur devra s'authentifier (nom et mot de passe).

- Etapes
    1. Créer le répertoire /var/www/prive, y placer quelques pages HTML. Tester leur accessibilité pour tous.

    2. Créer dans le fichier de configuration de votre site un bloc de directives concernant ce répertoire, y inclure les clauses suivante : :

       AuthType Basic
       AuthUserFile /etc/apache2/users
       AuthName "Acces prive"
       require valid-user

    3. Tests
       - Créer quelques comptes Apache, puis examiner le fichier contenant les comptes ainsi créés
       - Tester la protection par mot de passe