



Pràctica 2d: Mecanismes d'autenticació i autorització. Realms.

1- Introducció

L'objectiu de la pràctica és fer un breu estudi dels mecanismes [d'autenticació i autorització](#) del servidor de pàgines web Apache2.

El mecanisme d'**autenticació** permet demanar a un usuari que vol accedir a un recurs del servidor un **nom d'usuari i una contrasenya** i d'aquesta manera es pot confirmar l'identitat de l'usuari, o en altres paraules, verificar que un usuari és realment qui afirma ser. La llista d'usuaris i les seves contrasenyes es desen en un **proveïdor d'autenticació**, que és un fitxer de text o una base de dades SQL o LDAP.

El mecanisme d'**autorització** és un procés pel qual es dona a un usuari els permisos necessaris per accedir als recursos disponibles en el servidor. Per donar permisos, s'utilitza un sistema de [llistes de control d'accés ACL](#) als diferents recursos del servidor, com per exemple un directori, un fitxer o una base de dades.

Un conjunt de recursos els quals es troben sota el control dels mateixos mecanismes d'autenticació i autorització, i que fa servir el mateix proveïdor d'autenticació conformen un **realm**. Un **realm** necessita un **nom de realm** per ser identificat.

Per poder implementar aquests mecanismes d'autenticació i autorització cal que el servidor Apache2 tingui habilitats una sèrie de mòduls. Els tres tipus de mòduls necessaris són els següents:

a) S'ha d'habilitar com a mínim un **mòdul d'autenticació**, que indica el tipus d'autenticació utilitzada. Existeixen dos mètodes d'autenticació. Primer hi ha el [mètode bàsic](#), a on els noms d'usuaris i contrasenyes son enviats dins d'una capçalera HTTP sense encriptar les dades (tot i que estiguin codificades amb el sistema [base64](#), que és fàcilment [reversible](#)). Per activar-lo cal tenir habilitat el mòdul **mod_auth_basic**. El segon, és el [mètode digest](#) que proporciona confidencialitat aplicant al nom d'usuari i contrasenya l'algorisme **MD5**, que és una [funció hash criptogràfica](#), que produeix un valor **hash** de 128 bits. Per activar-lo cal tenir habilitat el mòdul **mod_auth_digest**.

b) S'ha d'habilitar com a mínim un mòdul per indicar el **proveïdor d'autenticació**. Per defecte està habilitat el mòdul **mod_authn_file** que permet desar la llista d'usuaris i contrasenyes dins d'un fitxer de text pla. Altres mòduls són per exemple **mod_authn_dbd** per desar la llista en una base de dades SQL o **mod_authn_ldap** per desar la llista en una base de dades LDAP.

c) S'ha d'habilitar com a mínim un mòdul d'**autorització** que proporciona el mecanisme per permetre que els usuaris autenticats se'ls doni o denegui el permís per accedir als diversos recursos del servidor per mitjà de **llistes de control d'accés**. Alguns d'aquests mòduls són per exemple: **mod_authz_user**, **mod_authz_host**, **mod_authz_dbm** o **mod_authz_ldap**.



2- Configurant Apache2 per accedir a un realm amb el mecanisme d'autenticació digest, proveïdor d'autorització de tipus file i autorització de tipus user

a) Amb l'ordre **apachectl -M**, verifica que els mòduls **auth_digest_module**, **authn_file_module** i **authz_user_module** estan instal·lats i habilitats. En cas negatiu, comprova si tens aquest mòdul disponible a **/etc/apache2/mods-available**, i habilita'l amb l'ordre **a2enmod**.

```
root@debianDaw:/etc/apache2/mods-available# a2enmod auth_digest.load
Considering dependency authn_core for auth_digest:
Module authn_core already enabled
Enabling module auth_digest.
To activate the new configuration, you need to run:
  systemctl restart apache2
root@debianDaw:/etc/apache2/mods-available# a2enmod authn_file.load
Module authn_file already enabled
root@debianDaw:/etc/apache2/mods-available# a2enmod authz_user.load
Considering dependency authz_core for authz_user:
Module authz_core already enabled
Module authz_user already enabled
root@debianDaw:/etc/apache2/mods-available# _
```

```
root@debianDaw:/etc/apache2/mods-available# systemctl restart apache2
root@debianDaw:/etc/apache2/mods-available# apachectl -M
Loaded Modules:
  core_module (static)
  so_module (static)
  watchdog_module (static)
  http_module (static)
  log_config_module (static)
  logio_module (static)
  version_module (static)
  unixd_module (static)
  access_compat_module (shared)
  alias_module (shared)
  auth_basic_module (shared)
  auth_digest_module (shared)
  authn_core_module (shared)
  authn_file_module (shared)
  authz_core_module (shared)
  authz_host_module (shared)
  authz_user_module (shared)
  autoindex_module (shared)
```

b) Crea un directori de nom **news** dins del directori **/var/www/html**. Descarrega dins del directori **/var/www/html/news** el fitxer **news.tar.gz** que trobaràs a [aquest enllaç](#). Extreu el seu contingut. Comprova que has obtingut els següents fitxers: **index.html**, **sportsnews.html** i **nationalnews.html**. Esborra el fitxer descarregat (només has de tenir els fitxers **.html**).

```
root@debianDaw:/etc/apache2/mods-available# mkdir /var/www/html/news
root@debianDaw:/etc/apache2/mods-available# _
```

```
root@debianDaw:/etc/apache2/mods-available# cat /var/www/html/news/nationalnews.html
<html>

<h1>NATIONAL NEWS </h1>

National news contents...

</html>
root@debianDaw:/etc/apache2/mods-available# cat /var/www/html/news/sportsnews.html
<html>

<h1> SPORTS NEWS </h1>

Sports news contents...

</html>
root@debianDaw:/etc/apache2/mods-available# cat /var/www/html/news/index.html
<html>
<h1> NEWS OF THE WORLD HOME PAGE </h1>

<ul>
  <li><a href="nationalnews.html">National News</a></li>
  <li><a href="sportsnews.html">Sports News</a></li>
</ul>
</html>
root@debianDaw:/etc/apache2/mods-available#
```



- c) Crea un directori de nom **passwd** dins del directori **/etc/apache2**. Fes que el propietari del directori **/etc/apache2/passwd/** (i tots els fitxers inclosos) sigui **root** i que el grup amb permisos especials sigui **www-data**. Dóna permisos **rwX** a root, **r-x** a **www-data** i **- - -** a la resta d'usuaris.

```
root@debianDaw:/etc/apache2/mods-available# mkdir /etc/apache2/passwd
root@debianDaw:/etc/apache2/mods-available# chown -R root:root /etc/apache2/passwd/
root@debianDaw:/etc/apache2/mods-available# chown -R root:www-data /etc/apache2/passwd/
root@debianDaw:/etc/apache2/mods-available# chmod -R 750 /etc/apache2/passwd/
root@debianDaw:/etc/apache2/mods-available#
```

- d) Crea un fitxer **proveïdor d'autenticació** de nom **passwords2** dins del directori **/etc/apache2/passwd** i que tingui definit a l'usuari **reader** amb contrasenya **fjeclot00** i autorització d'accés al realm **news**.

Per dur a terme aquesta tasca, s'ha d'utilitzar l'eina **htpdigest**. Per crear l'usuari **reader** i generar el fitxer **passwords2** d'acord amb l'enunciat, has d'executar:

```
htdigest -c /etc/apache2/passwd/passwords2 news reader
```

NOTA: Si vols afegir un nou usuari a un fitxer proveïdor d'autenticació que ja existeix, **NO** s'ha de posar l'opció **-c**.

```
root@debianDaw:/etc/apache2/mods-available# htdigest -c /etc/apache2/passwd/passwords2 news reader
Adding password for reader in realm news.
New password:
Re-type new password:
root@debianDaw:/etc/apache2/mods-available#
```

```
GNU nano 5.4 /etc/apache2/passwd/passwords2
reader:$apr1$y6hChjL7$ykH9pYc7xKu8zTON9G62..
test:$apr1$DdLIPoqQ$maDFwAkx2x157Y2KXrwpr1
```

- e) Fes que el propietari del fitxer **/etc/apache2/passwd/passwords2** sigui **root** i que el grup amb permisos especials sigui **www-data**. Dóna permisos **rwX** a root, **r-x** a **www-data** i **- - -** a la resta d'usuaris.

```
root@debianDaw:/etc/apache2/mods-available# chown -R root:www-data /etc/apache2/passwd/passwords2
root@debianDaw:/etc/apache2/mods-available# chmod -R 750 /etc/apache2/passwd/passwords2
root@debianDaw:/etc/apache2/mods-available# _
```

```
chown root
chgrp www-data
chmod 750
```

- f) Fes una còpia de seguretat de **000-default.conf** que es troba dins de **/etc/apache2/sites-available** amb el nom **000-default.conf.original**.

```
root@debianDaw:/etc/apache2/sites-available# cp 000-default.conf 000-default.conf.original
root@debianDaw:/etc/apache2/sites-available#
```



g) Descarrega dins de **/etc/apache2/sites-available** una nova versió de **000-default.conf** que trobaràs en [aquest enllaç](#). Fes els canvis necessaris dins de l'arxiu perquè la configuració final sigui:

- 1- Directori del realm: **/var/www/html/news**
- 2- Autenticació: **Digest**
- 3- Nom del realm: **"news"**
- 4- Tipus de proveïdor d'autenticació: **file**
- 5- Fitxer proveïdor d'autenticació: **etc/apache2/passwd/passwords2**
- 6- Per accedir al realm, s'ha de ser l'usuari **reader**.

```
GNU nano 5.4                                000-default.conf
<VirtualHost *:80>
    ServerAdmin webmaster@localhost
    DocumentRoot /var/www/html
    <Directory "/var/www/html/news">
        Options Indexes FollowSymLinks Multiviews
        AllowOverride None
        Order Allow,Deny
        Allow from all
        AuthType Digest
        AuthName "news"
        AuthBasicProvider file
        AuthUserFile "/etc/apache2/passwd/passwords2"
        Require user reader
    </Directory>
    ErrorLog ${APACHE_LOG_DIR}/error.log
    CustomLog ${APACHE_LOG_DIR}/access.log combined
</VirtualHost>
```

h) Reinicia el servidor **apache2** executant **systemctl restart apache2**.

```
root@debianDaw:/etc/apache2/sites-available# systemctl restart apache2
root@debianDaw:/etc/apache2/sites-available# _
```

i) Intenta accedir als recursos que es troben a **/var/www/html/news** i comprova que **reader** pot accedir al realm **news**. amb la contrasenya correcta. Comprova que qualsevol altre nom d'usuari o l'usuari **reader** amb la contrasenya incorrecta no pot accedir al realm **news.fje**

Si s'insereixes un altre usuari o un altre contrasenya, la pagina tornara a pedir iniciar sessió. Si no mostrara la pagina: