Pràctica 4c: 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 texte 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 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 facilment **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 texte 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**.

b) Crea un directori de nom **news** dins del directori **/var/www/html**. Descarrega dins del directori **/var/www/html/news** el fixer **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**).

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.

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 auorització 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'ennunciat, has d'executar:

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

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

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.

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**.

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- Tips de proveïdor d'autenticació: **file**
5- Fitxer proveïdor d'utenticació: **etc/apache2/passwd/passwords2**
6- Per accedir al realm, s'ha de ser l'usuari **reader**.

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

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**.

Comprovació
a) Data de comprovació de la pràctica: **7/2/18**.