ACTIVIDAD 6.4 - AUTORIZACIÓN DE ACCESO A PÁGINAS PRIVADAS

1. DIRECTIVAS

A continuación, veremos una serie de directivas que utilizaremos combinadas para autorizar el acceso a determinadas partes de una web.

1.1 AuthType

Esta directiva selecciona el tipo de autenticación de usuario para acceder a un directorio. Tiene un argumento, que puede tomar cuatro valore, atendiendo a **cuatro tipos de autenticación**:

- **None**: sin autenticación de usuario.
- **Basic**: la más sencilla el nombre de usuario y la contraseña se envían al servidor **sin encriptar**, tan solo usando codificación textual **base64**. Sólo debe usarse con **HTTPs**, ya que la contraseña puede ser fácilmente capturada. Implementada por el módulo *auth_basic*
- **Digest**: la información de autenticación va **encriptada** en base a un timestamp generado por el servidor en el momento de la petición, aumentando por tanto la **seguridad**. Implementada por el módulo *auth_digest*
- **Form**: permite la **autenticación desde un formulario.** Implementada por el módulo *auth_form*.

1.2 AuthName

Esta directiva establece un nombre al ámbito de la autorización. Este nombre se le da al cliente para que el usuario sepa qué credenciales debe enviar. Si el nombre del ámbito tiene espacios, se puede poner entre comillas dobles. Por ejemplo:

```
AuthName “Zona Intranet”
```

1.3 AuthUserFile

Establece la ruta y el nombre del fichero de texto que contiene un listado de nombres de usuarios y contraseñas para autenticación. Si la ruta no es absoluta se considera relativa a ***ServerRoot***. Para evitar que este fichero pueda ser consultado por intrusos en el servidor se recomienda que se almacene fuera del árbol de directorios servidos por nuestro Apache2.

Cuando usamos ***AuthType Basic***, la creación del fichero de usuarios se hace con el comando ***htpasswd***. Cuando usamos ***AuthType Digest***, el comando para crear el fichero de usuarios es ***htdigest***.

1.3.1 Uso con AuthType Basic

Para **crear el fichero con el primer nombre de usuario** se emplea el siguiente comando:

```
htpasswd -c Filename username
```

Si el fichero Filename existe se reescribirá. Al ejecutar el comando se pedirá la contraseña.

Para añadir más usuarios:

```
htpasswd Filename username2
```

Cada línea del fichero contiene un nombre de usuario, seguido de dos puntos y la contraseña encriptada.

1.3.2 Uso con AuthType Digest

Cuando usamos autenticación Digest, en lugar del comando ***htpasswd*** usamos el comando ***htdigest***, cuyo funcionamiento es muy similar, pero añade al

Para **crear el fichero con el primer nombre de usuario** se emplea el siguiente comando:

```
htdigest -c Filename auth_name username
```

Si el fichero Filename existe se reescribirá. Al ejecutar el comando se pedirá la contraseña.

Para añadir más usuarios:

```
htdigest Filename auth_name username2
```

Cada línea del fichero contiene un nombre de usuario, seguido de dos puntos, el nombre del ámbito, otros dos puntos y la contraseña encriptada.

1.4 AuthGroupFile

Esta directiva permite establecer la ruta y el nombre del fichero de texto que contiene la lista de usuarios que componen los grupos para autenticación. Igual que antes, si la ruta no es absoluta se considera relativa a ***ServerRoot***.

Cada línea contiene un nombre de grupo seguido de dos puntos y a continuación una lista de nombres de usuario separados por espacio. Por ejemplo:

```
mygroup: bob joe anne
```

1.5 Require

Esta directiva, que ya vemos en la práctica anterior, se utiliza para permitir el acceso bien a un listado de usuarios:

```
Require user bob joe
```

O bien a un listado de grupos de usuarios:

```
Require group mygroup
```

1.6 Ejemplo

A continuación, vemos un ejemplo en el que sólo se permite el acceso al directorio **/var/www/docs/** a los usuarios del grupo **admin**. Los grupos se definen en el fichero **web/groups** y los usuarios en el fichero **web/users**:

```
<Directory "/www/docs">
      AuthType Basic
      AuthName "Authorized personal only"
      AuthUserFile web/users
      AuthGroupFile web/groups
      Require group admin
</Directory>
```

2. EJERCICIOS

Para hacer este ejercicio primero crearemos el directorio **/var/www/html/restricted/** y en su interior una página llamada **intranet.html** con el contenido que consideres. Para facilitarte el acceso a esta página, puedes crear un hipervínculo en la página por defecto del servidor **index.html**.

2.1 Autorización básica de usuarios

1. Comprueba que puedes acceder a la página **intranet.html**.
2. Crea un archivo de usuarios **usando *htpasswd*** que incluya a los **usuarios usu1 y usu2**. Usa su mismo nombre como contraseña para recordarlo.
3. En el fichero **000-default.conf**, añade las directivas **AuthType, AuthName, AuthUserFile y Require user** para controlar acceso a directorio **/var/www/html/restricted/**, de manera que **sólo el usuario usu1** pueda acceder.
4. Reinicia el servidor y comprueba que sólo puedes acceder con el usuario **usu1**.

Si el archivo **000-default.conf** tiene algún error el servidor no podrá reiniciarse y dará un mensaje de error. Puedes consultar el mensaje de error en **/var/log/apache2/**

2.2 Autorización básica de grupos

Para poder autorizar a grupos y usar, por tanto, la directiva ***AuthGroupFile***, debemos activar el módulo ***auth_groupfile***. Para activar módulos de Apache se usa el comando ***a2enmod***:

```
sudo a2enmod authz_groupfile
```

1. Crea un archivo llamado **webgroup** en el que se defina que el grupo **intranet** está formado por usu1 y usu2.
2. Añade la directiva ***AuthGroupFile*** y modifica la directiva ***Require*** para que sólo puedan acceder al directorio **restricted** los usuarios del grupo **intranet**.
3. Reinicia el servidor y comprueba que sólo puedes acceder tanto **con el usuario usu1 como con el usuario usu2**.

2.3 Autorización digest

1. Comprueba que el módulo ***auth_digest*** esté activado.
2. Crea fichero de usuarios llamado **d_users**. Incluye los usuarios **d_usu1** y **d_usu2** bajo el ámbito **daw**
3. Cambia las directivas:
   - ***AuthType*** para usar autenticación **Digest**
   - ***AuthName*** para que se refiera al ámbito **daw**
   - ***AuthUserFile*** para referirse al fichero **d_users**
   - ***Require*** para que sólo se permita conectarse al usuario **d_usu1**.
4. Reinicia el servidor y comprueba que sólo puedes acceder con el usuario **d_usu1**.