Práctica 5

Antes de comenzar con el trabajo:

- Es conveniente haber realizado previamente el resto de prácticas
- Dispones de toda la documentación sobre apache en: http://httpd.apache.org/docs/current/
- Esta práctica tiene una base teórica que se explica en la propia práctica y que será evaluada en los correspondientes controles teóricos

¿Cómo se valora quién puede conectarse al sitio o acceder a determinados recursos del mismo?

- Tradicionalmente se han usado la directivas “allow” y “deny” para permitir y denegar el acceso en función de múltiples circunstancias sobre directorios concretos del sitio web.
- Junto con la directiva ‘Order’ que indicaba el orden en que deberían aplicarse los permisos anteriores configuraban un escenario que permitía arbitrar diversas configuraciones.
- Estas directivas pertenecen al módulo ‘mod_access_compat’, pero están obsoletas y van a ser retiradas en futuras versiones por lo que es recomendable evitar su uso.

¿Cómo se usan Order, Allow y Deny? (Por si nos encontramos con algún sitio que lo mantenga configurado de esta manera)

- Order:
    - allow,deny: Primero aplicará los permisos de allow y luego los de deny. Es decir, las directivas ‘allow’ son evaluadas, al menos una debe coincidir o la petición será rechazada. Después se evalúan todas las directivas ‘deny’ y con que una se cumpla la petición será rechazada.
    - deny,allow: Primero aplicará los permisos de deny y luego los de allow. Es decir todas las directivas ‘deny’ son evaluadas y si alguna se cumple la petición es rechazada salvo que se cumplan las directivas ‘allow’. Cualquier petición que no cumpla ninguna de ‘allow’ o ‘deny’ será permitida.
- Allow
    - from all: Admite cualquier acceso al directorio
    - from IP: Admite cualquier acceso al directorio proveniente de la dirección IP indicada
    - from <dominio>: Admite cualquier acceso al directorio desde el dominio especificado
- Deny
    - from all: Deniega cualquier acceso al directorio
    - from IP: Deniega cualquier acceso al directorio proveniente de la dirección IP indicada

        - from dominio: Deniega cualquier acceso al directorio desde el dominio especificado.

Si hemos entendido bien lo anterior deberíamos saber qué hacen las siguientes directivas:

- allow from 10.0.128+X.250 127.0.0.1
- O lo que ocurriría si configuramos las directivas:
    - Order deny,allow
    - Deny from 10.0.128+X.250
- Podríamos de esta forma configurar las directivas por ejemplo:
    - Para permitir todos los accesos desde tu propio servidor solamente
    - Para permitir los accesos solamente desde tu máquina cliente.

¿Cuál es la recomendación actual y la que vamos a aplicar nosotros?

La recomendación actual es utilizar al menos una autenticación básica (mod_auth_basic)

- La protección básica se basa en el uso de la directiva “AuthUserFile” que usamos para especificar un fichero de claves, que será de texto con los usuarios y sus contraseñas: AuthUserFile “/etc/apache2/usuarios.txt”
- Se añade además con la directiva “AuthName” un texto para invitar al acceso: AuthName “Identificación”, por ejemplo
- La directiva AuthType Basic permite establecer el tipo de autenticación y la directiva Require valid-user configurarla
- El fichero lo creamos con el comando htpasswd:
    - La primera vez podría ser: htpasswd –c usuarios.txt usuario1, y se nos pediría la contraseña para el “usuario1” dos veces, que se almacena con un hash
    - Si el fichero ya existe no es necesario añadir “-c”, por ejemplo htpasswd usuarios.txt usuario2
    - Podemos editar el fichero para verlo o para borrar usuarios
- Podemos usarla para todo el sitio o para un directorio concreto al que solamente queramos que se acceda con usuario y contraseña

De este modo también es posible la autenticación básica basada en grupos

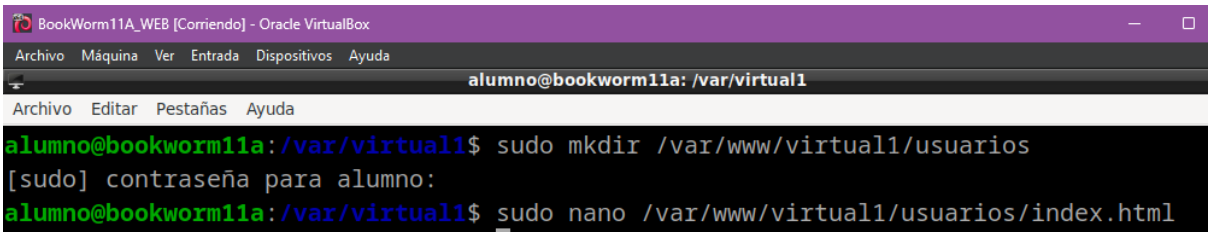
- Será necesario tener un fichero de texto con los grupos en que aparecerá una línea por grupo con el nombre seguido de “:” y de los usuarios que pertenecen a cada grupo separados por espacios. Por ejemplo /etc/apache2/groups.txt
- Será necesario tener activado el módulo “authz_groupfile” (obligado restart)
- Modificamos el sitio virtual para añadir:
    - La directiva: AuthGroupFile “/etc/apache2/groups.txt”
    - Sustituimos la directiva de 'Require' de usuario por la de grupos, por ejemplo: Require group grupo1 grupo2, lo que permitirá que aquellos usuarios que pertezcan a los grupos

1 o 2 tendrán acceso pero no otros, aunque estén en el fichero de usuarios

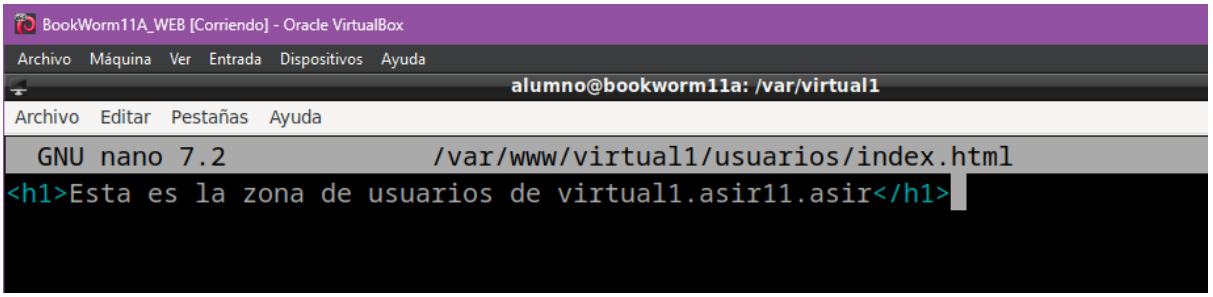
Aplicación de la autorización básica de Apache:

Configura tu sitio 'virtual1.asirXX.asir' para que solamente se pueda acceder al directorio del sitio ./usuarios previa introducción de un usuario y una contraseña. Para ello:

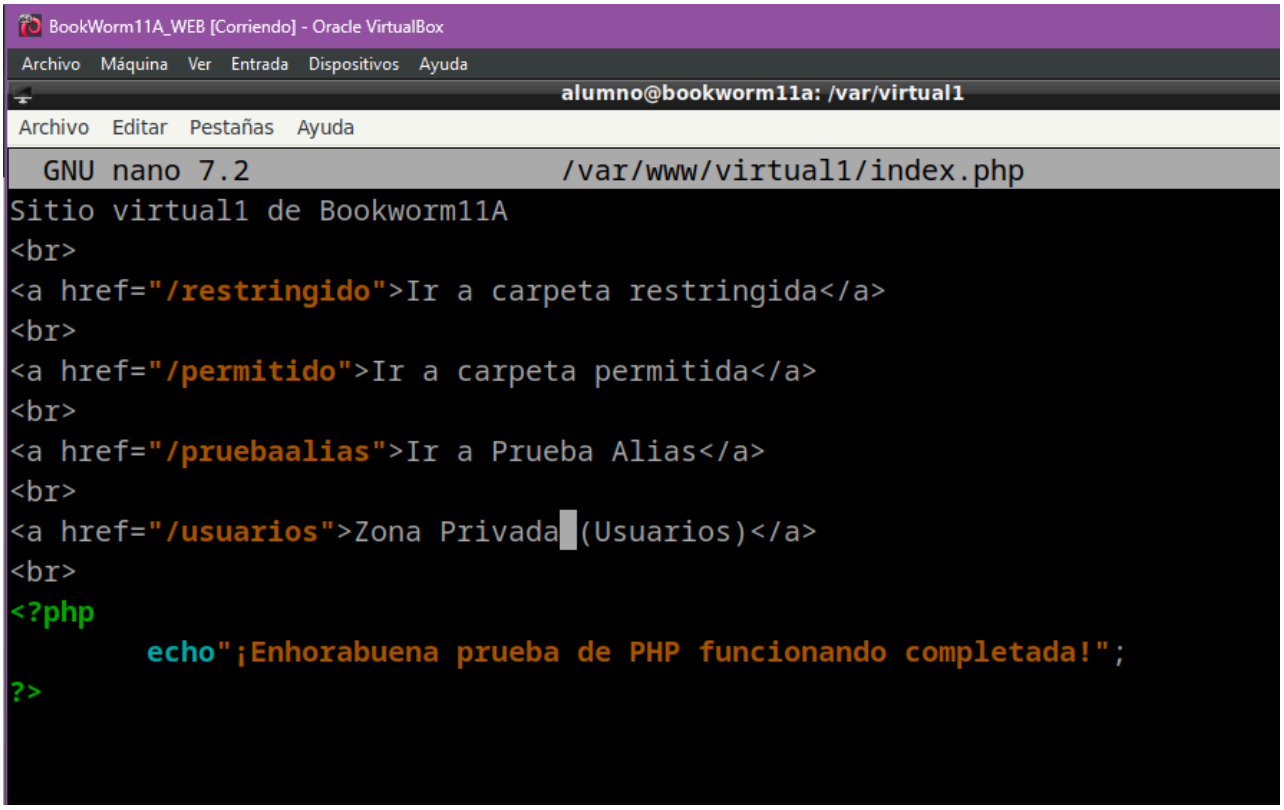
1. Crea el directorio correspondiente



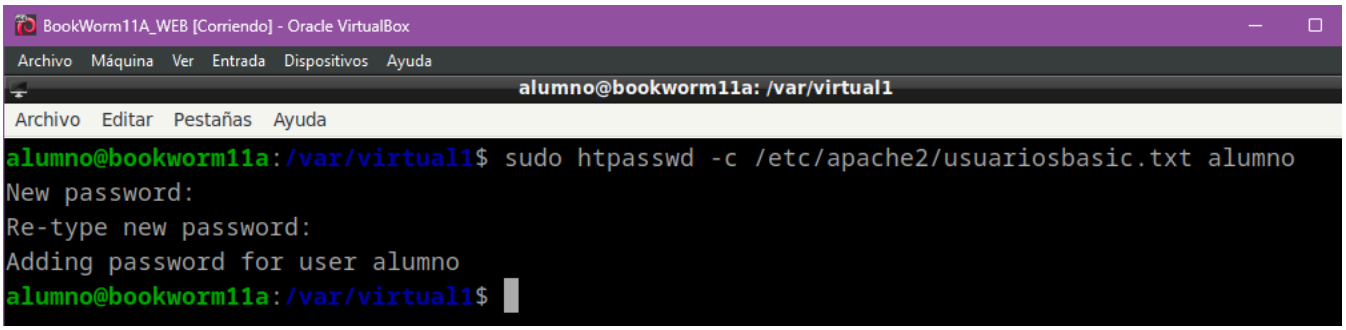
2. Añade un fichero html en dicho directorio en que ponga 'Este es la zona de usuarios de virtual1.asirXX.asir'



3. Añade un enlace a dicho directorio en la página principal del sitio



4. Crea un fichero denominado '/etc/apache2/usuariosbasic.txt' con el usuario 'alumno' y la contraseña '232425'.



BookWorm11A_WEB [Corriendo] - Oracle VirtualBox

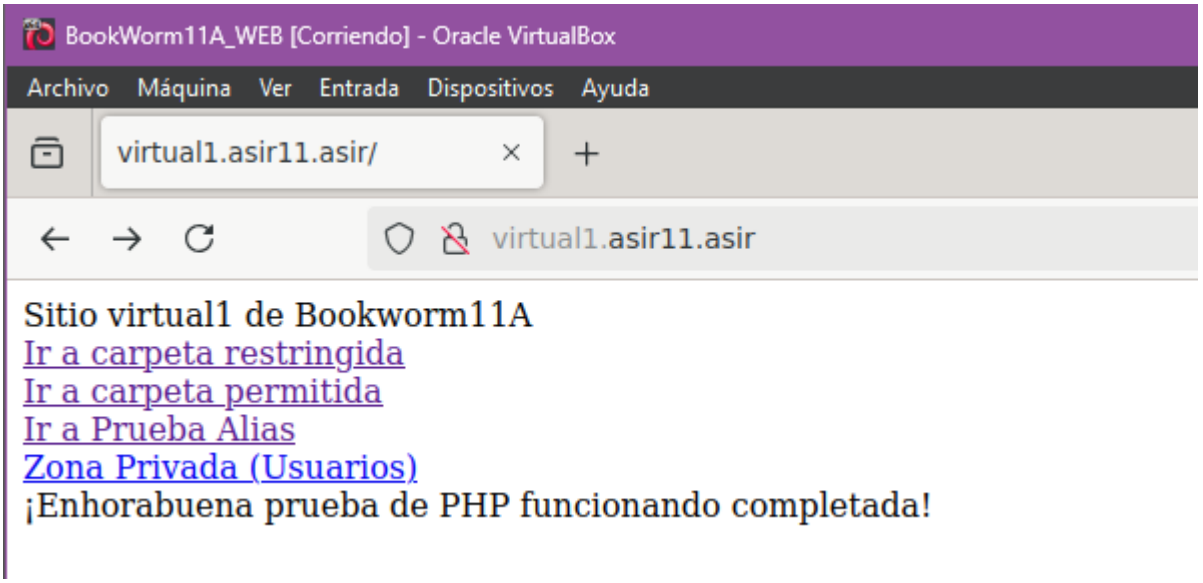
Archivo Máquina Ver Entrada Dispositivos Ayuda

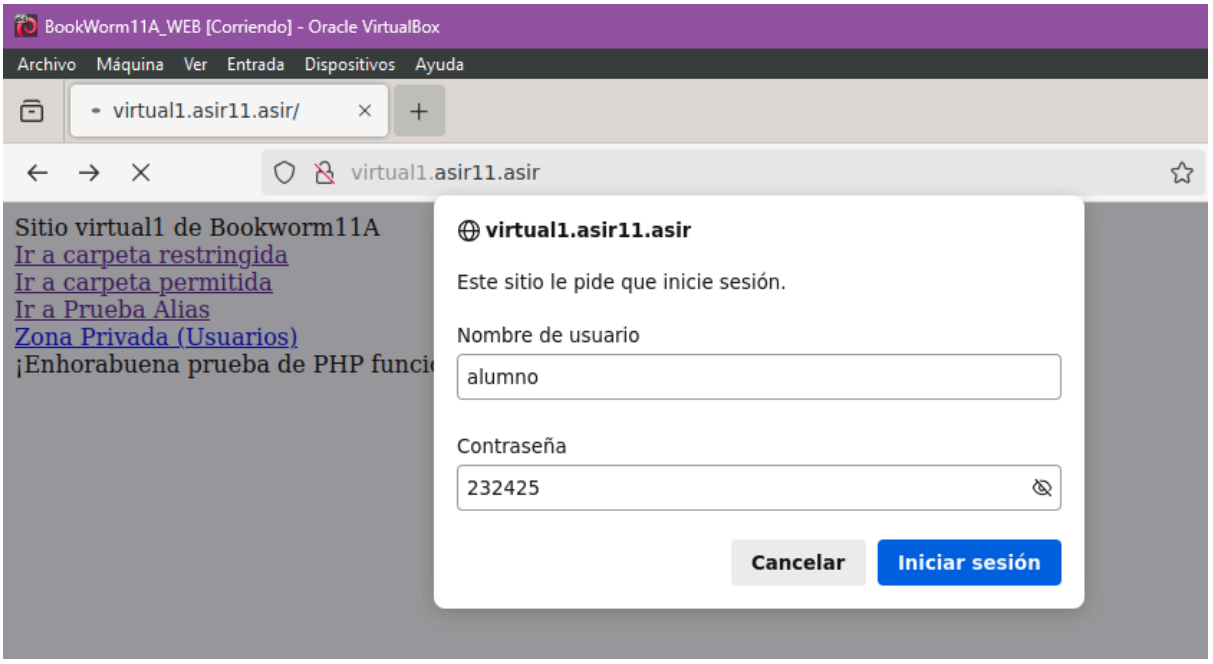
alumno@bookworm11a: /var/virtual1

Archivo Editar Pestañas Ayuda

```
 GNU nano 7.2                /etc/apache2/sites-available/virtual1.conf *
<VirtualHost 10.0.139.1:80>

        ServerName virtual1.asir11.asir
        ServerAdmin webmaster@localhost
        DocumentRoot /var/www/virtual1
        Alias /pruebaalias /var/www/virtual1/permitido
        #Redirect / https://virtual1.asir11.asir/
        ErrorDocument 403 /errors/forbidden.html

        ErrorLog ${APACHE_LOG_DIR}/error.log
        CustomLog ${APACHE_LOG_DIR}/access.log combined

        <Directory /var/www/virtual1/restringido>
                Require all denied
        </Directory>
        <Directory /var/www/virtual1/permitido>
                #Options -Indexes
                DirectoryIndex permitido.html
        </Directory>
        <Directory /var/www/virtual1/usuarios>
                AuthType Basic
                AuthName "Identificacion"
                AuthUserFile "/etc/apache2/usuariosbasic.txt"
                Require valid-user
        </Directory>
</VirtualHost>
```

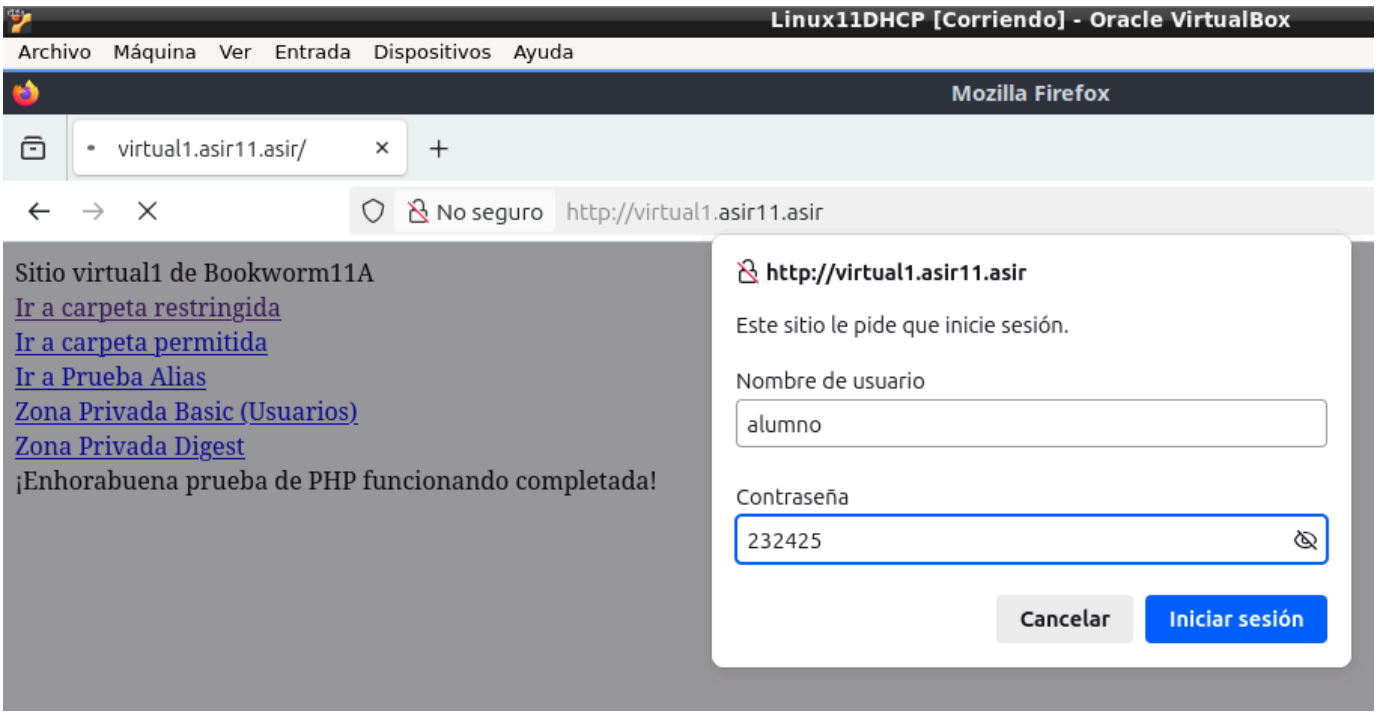
5. Prueba el funcionamiento



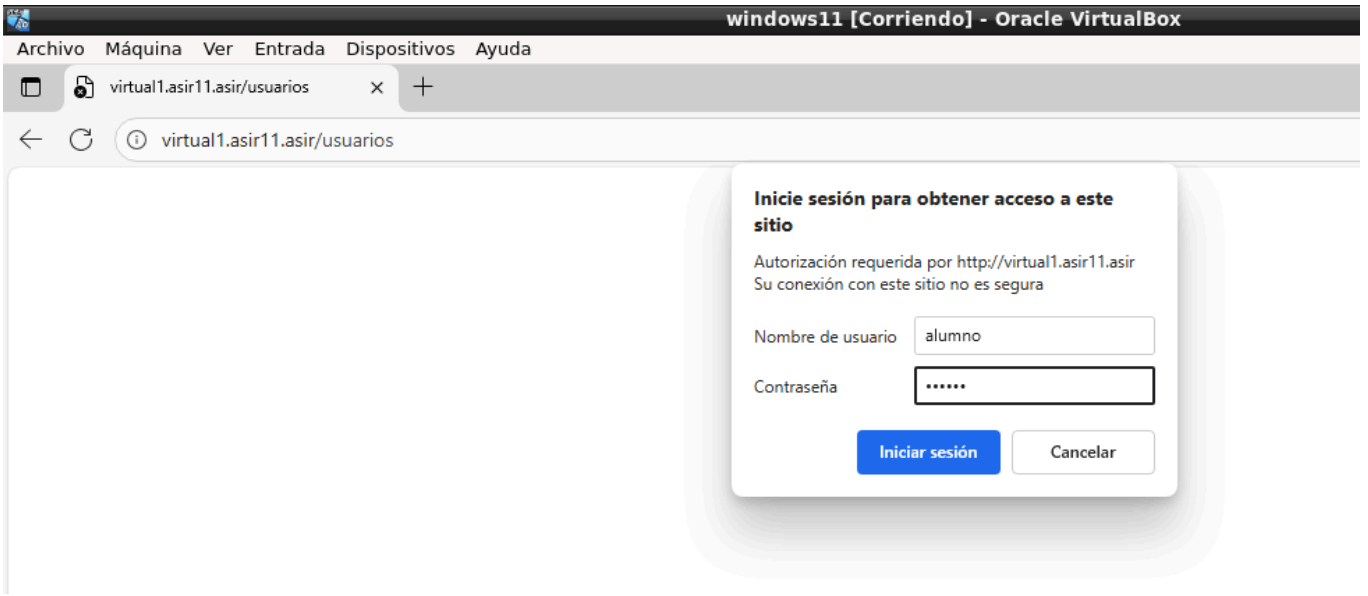

BookWorm11A_WEB [Corriendo] - Oracle VirtualBox
Archivo Máquina Ver Entrada Dispositivos Ayuda
virtual1.asir11.asir/
virtual1.asir11.asir
Sitio virtual1 de Bookworm11A
Ir a carpeta restringida
Ir a carpeta permitida
Ir a Prueba Alias
Zona Privada (Usuarios)
¡Enhorabuena prueba de PHP funci
virtual1.asir11.asir
Este sitio le pide que inicie sesión.
Nombre de usuario
alumno
Contraseña
232425
Cancelar
Iniciar sesión


BookWorm11A_WEB [Corriendo] - Oracle VirtualBox
Archivo Máquina Ver Entrada Dispositivos Ayuda
virtual1.asir11.asir/usuarios/
virtual1.asir11.asir/usuarios/
Esta es la zona de usuarios de virtual1.asir11.asir

LINUX11:

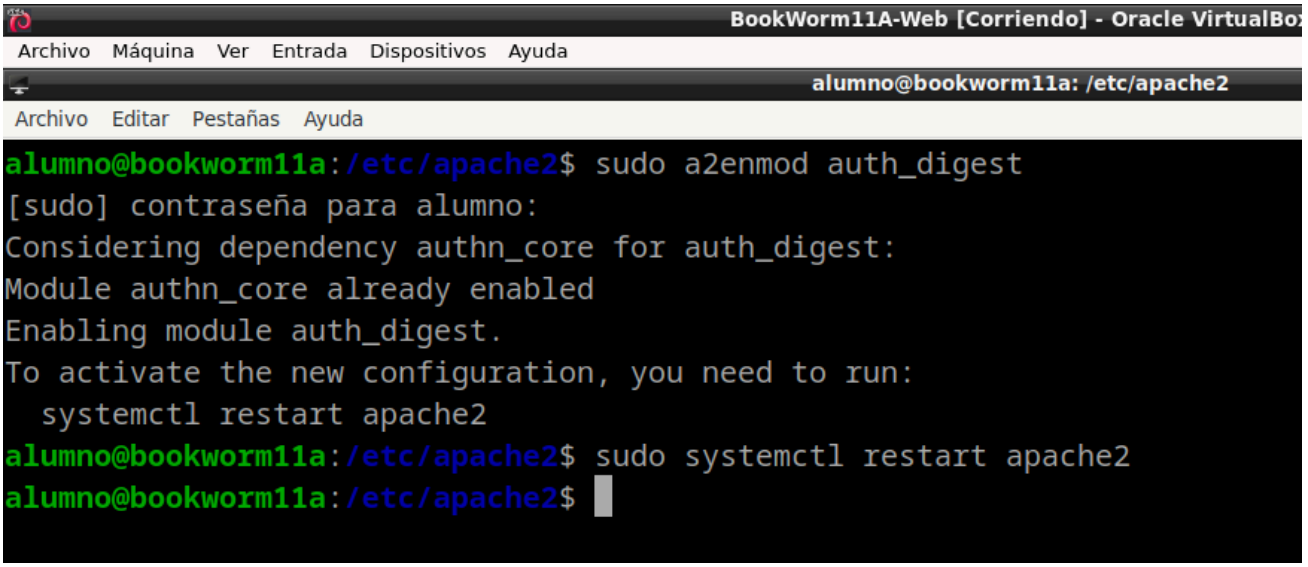

Linux11DHCP [Corriendo] - Oracle VirtualBox
Archivo Máquina Ver Entrada Dispositivos Ayuda
Mozilla Firefox
virtual1.asir11.asir/
No seguro
http://virtual1.asir11.asir
Sitio virtual1 de Bookworm11A
Ir a carpeta restringida
Ir a carpeta permitida
Ir a Prueba Alias
Zona Privada Basic (Usuarios)
Zona Privada Digest
¡Enhorabuena prueba de PHP funcionando completada!
http://virtual1.asir11.asir
Este sitio le pide que inicie sesión.
Nombre de usuario
alumno
Contraseña
232425
Cancelar
Iniciar sesión

WINDOWS11:

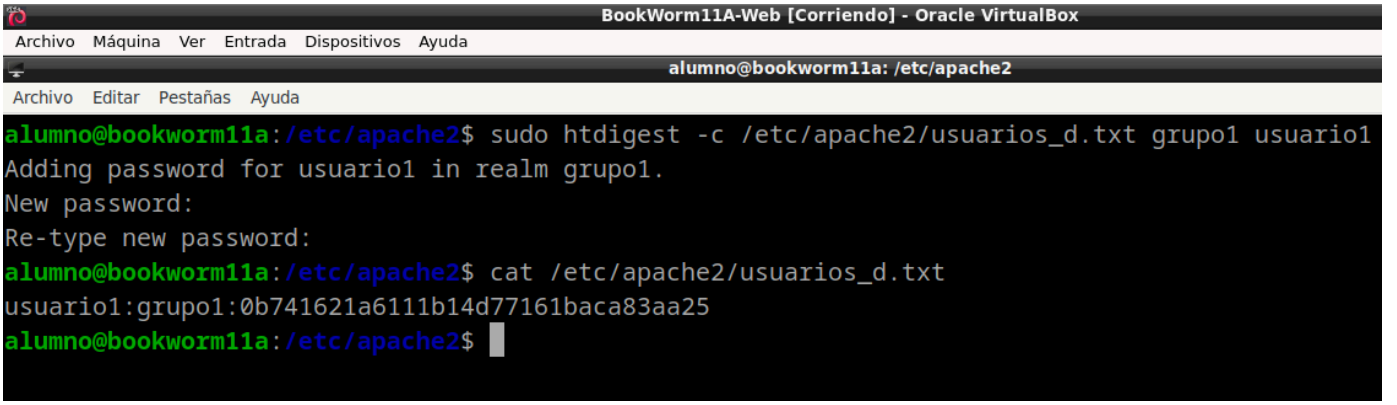


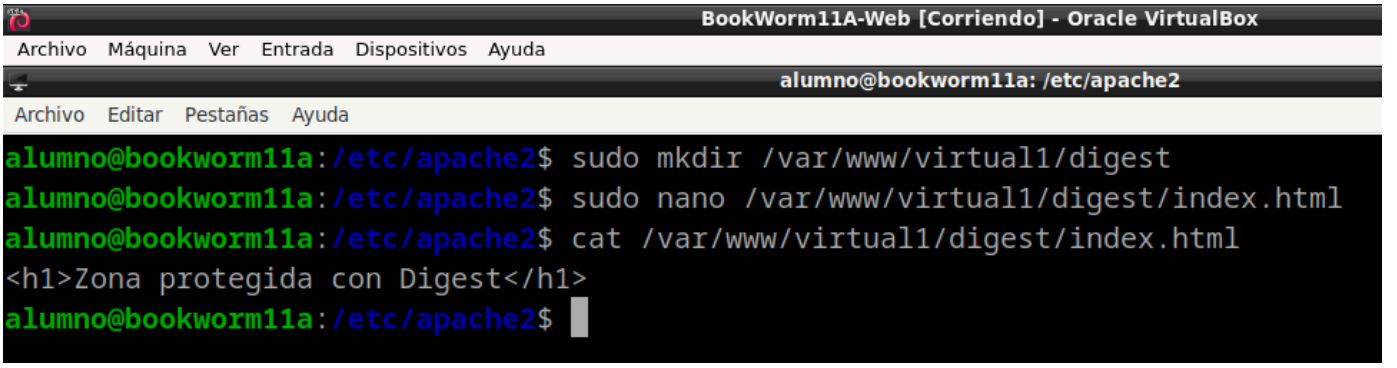
Un segundo método de autenticación es 'Digest0 (mod_auth_digest):

- Es el segundo método nativo de autenticación de Apache
- Es necesario activar el módulo de apache “auth_digest”

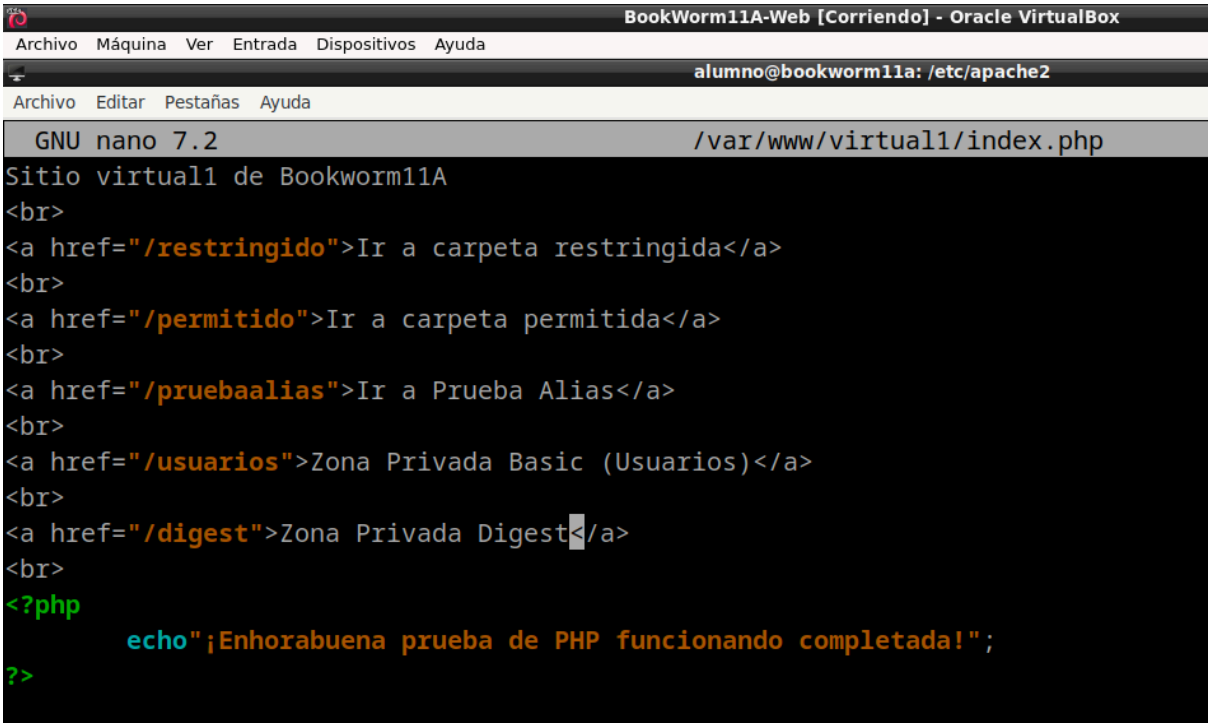


- El fichero que se crea es único en vez de los dos del caso “basic”
- Se crea con el comando “htdigest –c usuarios_d.txt grupo1 usuario1”, que permite crear el “grupo1” y añadirle el “usuario1” (“-c” solo para la creación del fichero, después no hay que ponerlo). Podemos añadir diferentes usuarios y asignarlos a diferentes grupos con la repetición del comando con distintos usuarios y grupos

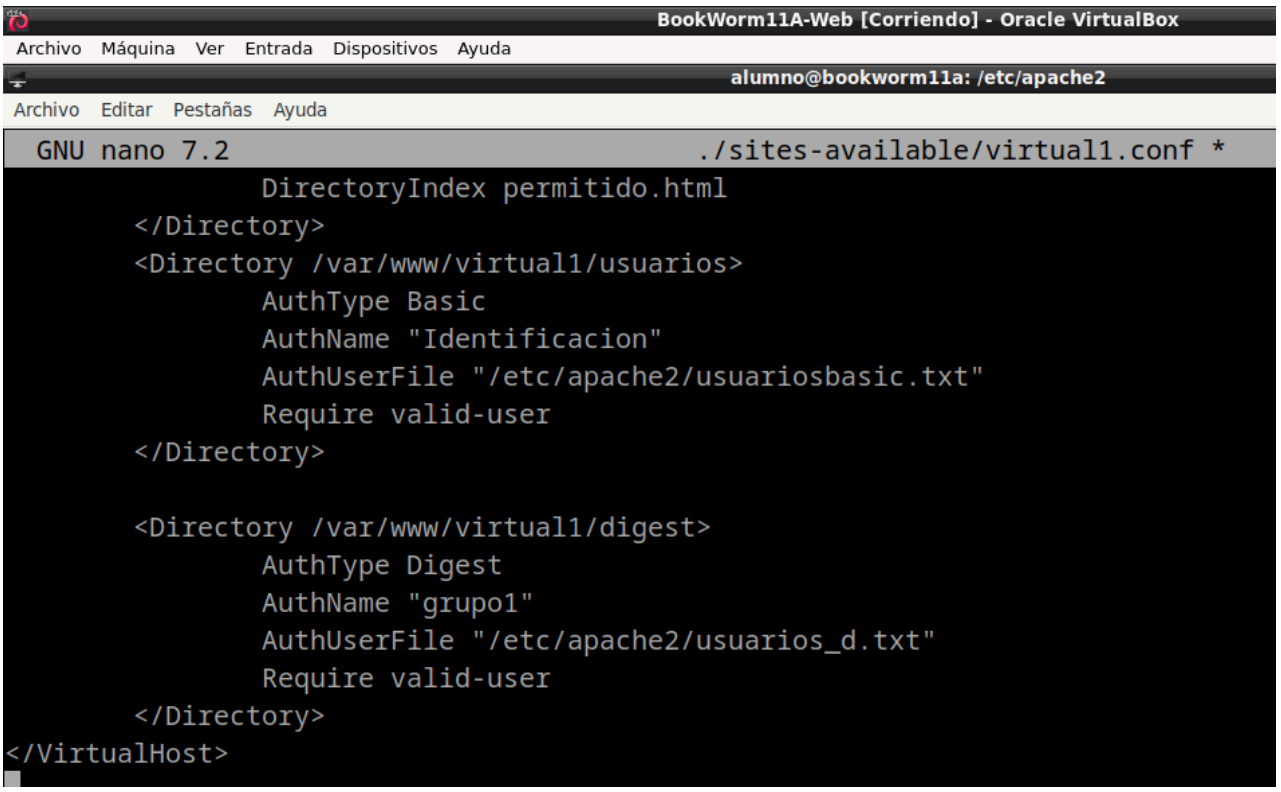




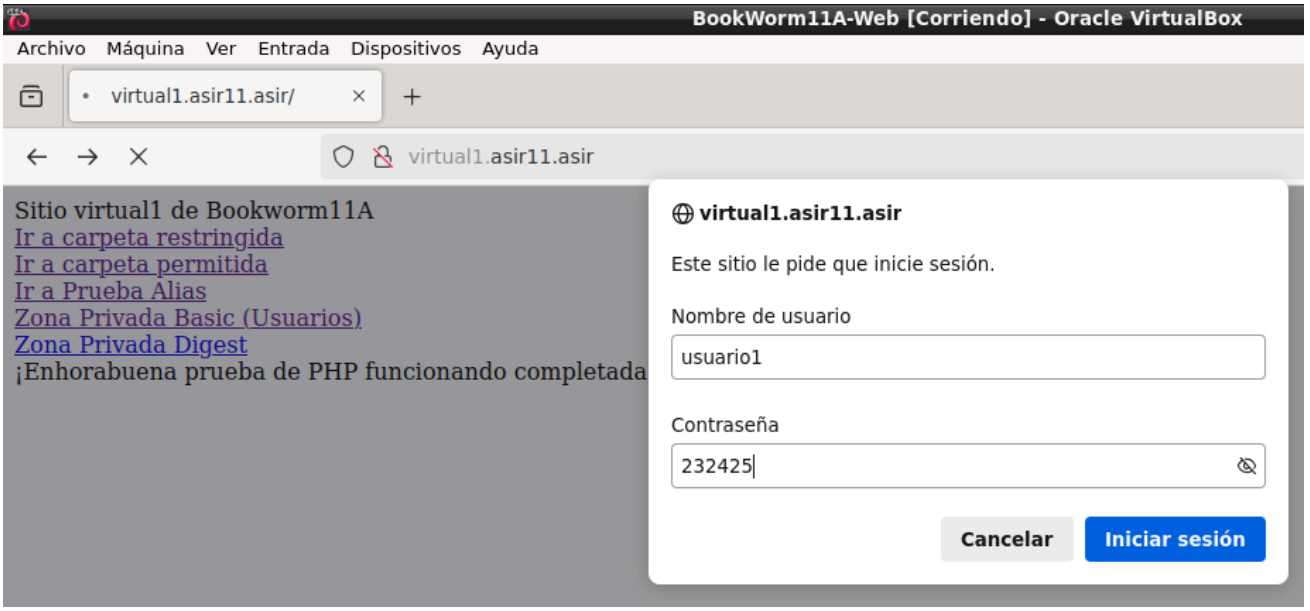
- Configuración de Apache

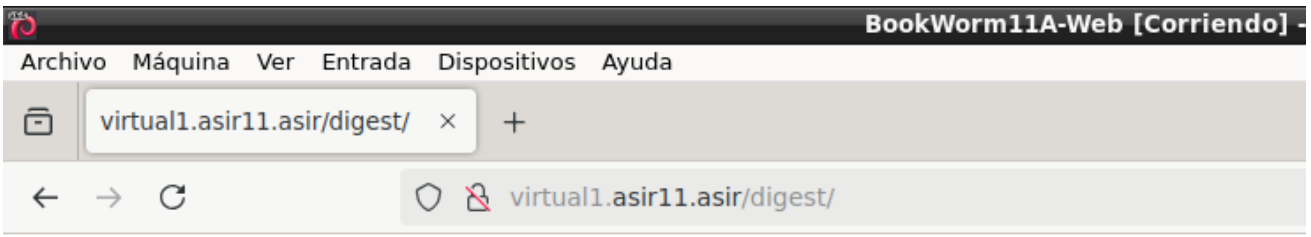


- Habría que añadir en la configuración del sitio virtual las directivas:
    - AuthType Digest (en lugar de basic)
    - AuthName “grupo1” para permitir acceso de los usuarios pertenecientes al grupo1
    - AuthUserFile “/etc/apache2/usuarios_d,txt” …archivo de usuarios y claves Digest
    - Require valid-user



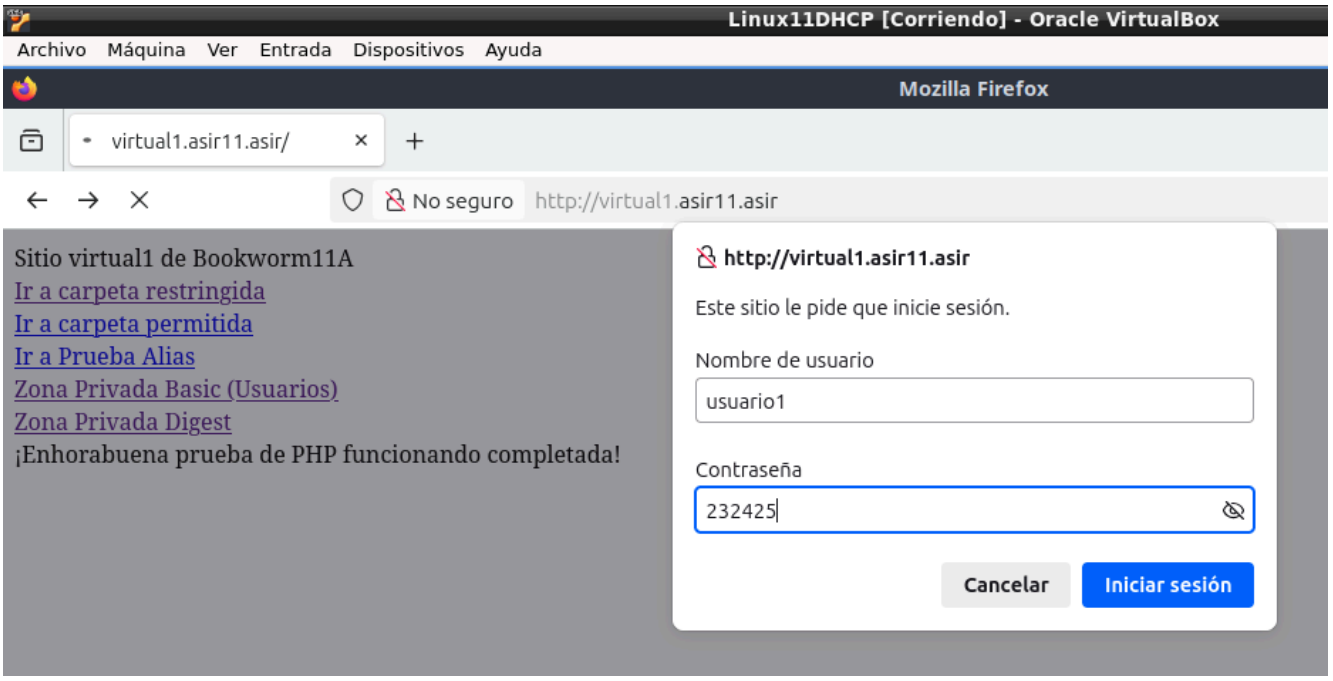
Recuerda hacer todas las capturas que consideres necesarias





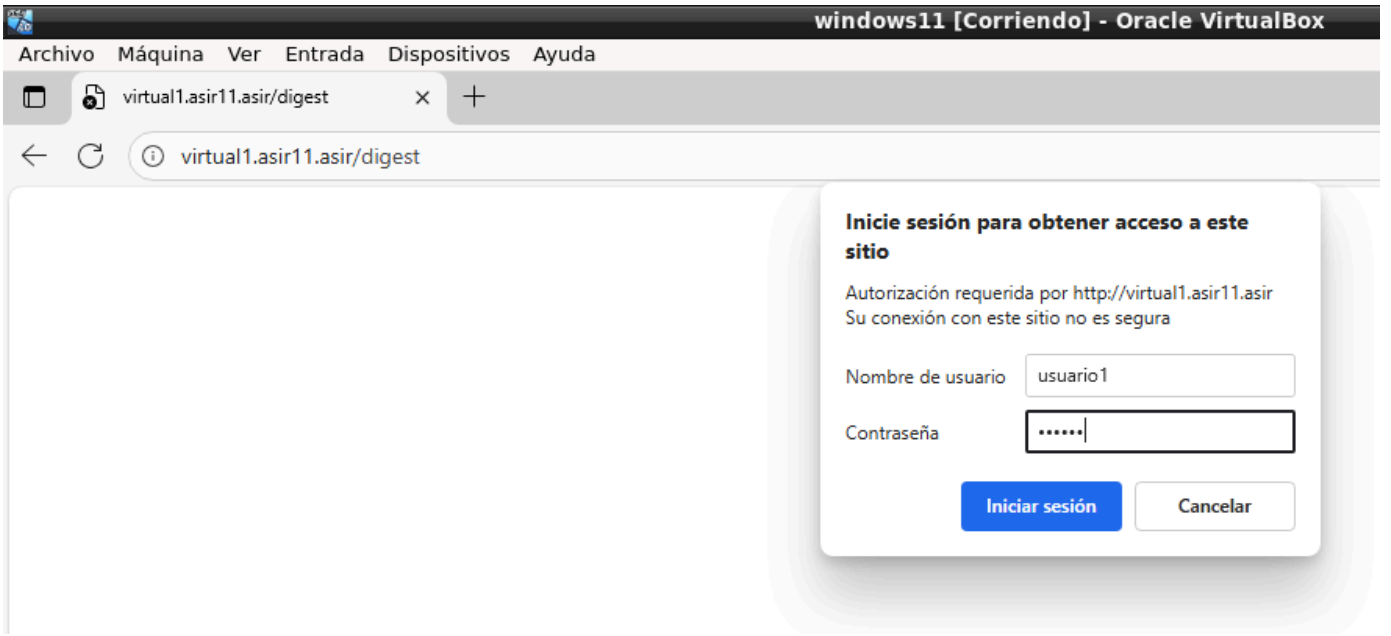
Zona protegida con Digest

LINUX11:



Zona protegida con Digest

WINDOWS11:


windows11 [Corriendo] - Oracle VirtualBox
Archivo Máquina Ver Entrada Dispositivos Ayuda
virtual1.asir11.asir/digest
virtual1.asir11.asir/digest
Inicie sesión para obtener acceso a este sitio
Autorización requerida por http://virtual1.asir11.asir
Su conexión con este sitio no es segura
Nombre de usuario
usuario1
Contraseña
Iniciar sesión
Cancelar


windows11 [Corriendo] - Oracle VirtualBox
Archivo Máquina Ver Entrada Dispositivos Ayuda
virtual1.asir11.asir/digest/
No seguro
virtual1.asir11.asir/digest/
Zona protegida con Digest