

Seguridad

Actividad 1

1.1 Funcionalidad del fichero .htaccess:

‘Se utilizan para realizar fácilmente cambios en la configuración en un directorio concreto y en sus subdirectorios.

1.2 Cuando usar ficheros .htaccess y cuando no:

- No hay que usarlos cuando tienen acceso al fichero principal de la configuración del servidor.
- Se deben usar cuando el proveedor te permite cambios de configuración, pero no se tiene acceso al root en el servidor
- En el resto de caso, se debe evitar su uso en la medida de lo posible, ya que generalmente hay otros sistemas de modificar la configuración que consumen menos recursos. Además, se está permitiendo que usuarios modifique configuración del servidor, lo cual conlleva problemas de seguridad.

1.3 Para que sirve la directiva de configuración AllowOverride relacionada con los ficheros .htaccess:

- Es una directiva que permite o bloquea los diferentes tipos de directivas que se encuentran en el fichero .htaccess también se puede establecer en All, donde

1.4 Opciones disponibles para la directiva:

- None: El archivo .htaccess es ignorado.
- All: Todas las directivas contenidas en el archivo son aplicadas.
- AuthConfig: Se aplican las directivas de autorización.
- FileInfo: Permite las directivas de control y modificación de archivos.
- Indexes: Se permiten las directivas de control de indexación de directorios.
- Limit: Se utiliza para permitir el uso de directivas que controlan el acceso al host.
- Options[=Option,...]: Permite opciones o listas de opciones más específicas.

Actividad 2

-Se crea el directorio:

```
sudo mkdir /var/www/news  
cd /var/www/news  
sudo mkdir html
```

- Se le asigna propietario:

```
sudo chown -R $USER:$USER /var/www/news/html
```

- Se le asignan permisos:

```
sudo chmod -R 755 /var/www/news/html
```

- Se crean los archivos necesarios:

```
cd html/
```

```
sudo nano index.html
```

```
<html>  
<head>  
<title>Bienvenido a tu nuevo Virtual Host!</title>  
</head>  
<body>  
<h1>Hecho! El dominio 'news.ddaw.es/index.html' funciona correctamente!</h1>  
</body>  
</html>
```

```
sudo nano sportsnews.html
```

```
<html>  
<head>  
<title>Bienvenido a tu nuevo Virtual Host!</title>  
</head>  
<body>  
<h1>Hecho! El dominio 'news.ddaw.es/sportsnews.html' funciona correctamente!</h1>  
</body>  
</html>
```

```
sudo nano nationalnews.html
```

```
<html>  
<head>  
<title>Bienvenido a tu nuevo Virtual Host!</title>  
</head>  
<body>  
<h1>Hecho! El dominio 'news.ddaw.es/nationalnews.html' funciona correctamente!</h1>  
</body>  
</html>
```

- Se crea un archivo de host virtual con las directivas correctas:

```
cd /etc/apache2/sites-available/  
sudo nano 004-es.ddaw.news.conf  
<VirtualHost *:80>  
ServerAdmin webmaster@localhost  
ServerName news.ddaw.es
```

```
ServerAlias www.news.ddaw.es
DocumentRoot /var/www/news/html
ErrorLog ${APACHE_LOG_DIR}/004-es-ddaw-news-error.log
CustomLog ${APACHE_LOG_DIR}/004-es-ddaw-news-access.log combined
</VirtualHost>
```

- Se habilita el vhost con la herramienta a2ensite:

```
sudo a2ensite 004-es.ddaw.news.conf
```

- Comprobamos que el archivo no tiene errores:

```
sudo apache2ctl configtest
```

- Se reinicia apache:

```
sudo systemctl restart apache2
```

- Ahora hay que cambiar el archivo hosts y añadimos una nueva relación del ip de la maquina con el nombre del dominio.

- Comprobar que funciona correctamente:



Hecho! El dominio 'news.ddaw.es/index.html' funciona correctamente!



Hecho! El dominio 'news.ddaw.es/sportsnews.html' funciona correctamente!



Hecho! El dominio 'news.ddaw.es/nationalnews.html' funciona correctamente!

- Una vez que todo funciona correctamente, modificamos la configuracion de vhost para añadir una directiva:

```
cd /etc/apache2/sites-available/
```

```
sudo nano 004-es.ddaw.news.conf
```

(Lo que aparece remarcado, es lo que se ha añadido al fichero)

```
<VirtualHost *:80>
    <Directory "/var/www/news/html">
        AuthType Basic
        AuthName "Restricted Files"
        # (Following line optional)
        AuthBasicProvider file
        AuthUserFile "/etc/apache2/passwd/passwords"
        Require valid-user
    </Directory>
```

```
ServerAdmin webmaster@localhost
```

```
ServerName news.ddaw.es
```

```
ServerAlias www.news.ddaw.es
```

```
DocumentRoot /var/www/news/html
```

```
ErrorLog ${APACHE_LOG_DIR}/004-es-ddaw-news-error.log
```

```
CustomLog ${APACHE_LOG_DIR}/004-es-ddaw-news-access.log combined
```

```
</VirtualHost>
```

- Se crean los usuarios:

```
sudo htpasswd -c /etc/apache2/passwd/passwords reader
```

```
sudo htpasswd /etc/apache2/passwd/passwords sports
```

```
sudo htpasswd /etc/apache2/passwd/passwords national
```

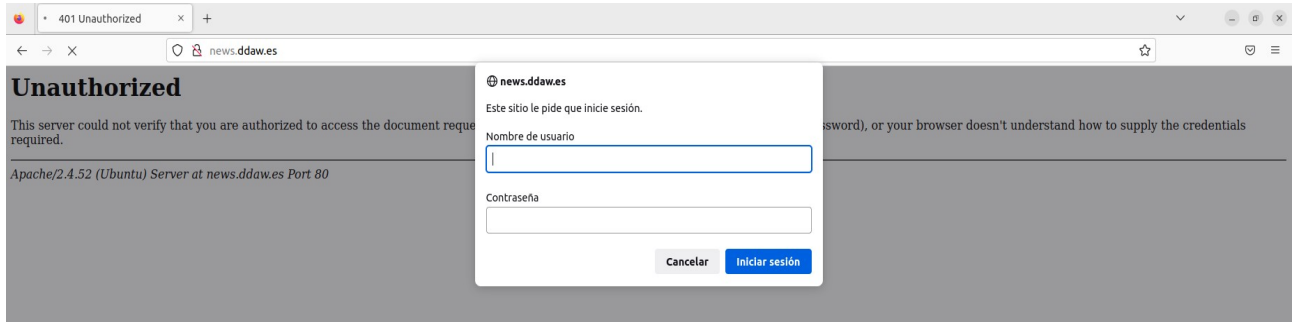
El terminal te pedirá ingresar una contraseña y luego que la confirmes

Si aparece un error diciendo que no se tienen permisos para crear el directorio, entonces, habrá que crear el directorio a mano, cambiando los permisos

- Se reinicia apache:

```
sudo systemctl restart apache2
```

- Ahora, al entrar, te solicita el usuario:



Actividad 2.1

- Se va a crear un archivo .htaccess en el directorio /var/www/01-es-ddaw-intranet:

```
cd /var/www/01-es-ddaw-intranet
```

```
sudo nano .htaccess
```

```
AuthType Basic
AuthName "By Invitation Only"
# Optional line:
AuthBasicProvider file
AuthUserFile "/etc/apache2/passwd/pass-intranet"
Require valid-user
```

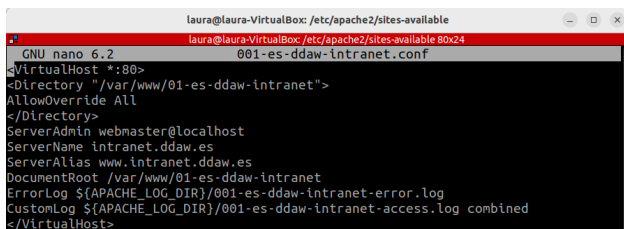
- Se modifica el archivo de configuracion de intranet.ddaw.es

```
cd /etc/apache2/sites-available
```

```
sudo nano 001-es-ddaw-intranet.conf
```

Y añadimos esta directiva en el archivo:

```
<Directory /var/www/01-es-ddaw-intranet>
AllowOverride All
</Directory>
```



```
laura@laura-VirtualBox: /etc/apache2/sites-available
GNU nano 6.2 001-es-ddaw-intranet.conf
<VirtualHost *:80>
<Directory "/var/www/01-es-ddaw-intranet">
AllowOverride All
</Directory>
ServerAdmin webmaster@localhost
ServerName intranet.ddaw.es
ServerAlias www.intranet.ddaw.es
DocumentRoot /var/www/01-es-ddaw-intranet
ErrorLog ${APACHE_LOG_DIR}/001-es-ddaw-intranet-error.log
CustomLog ${APACHE_LOG_DIR}/001-es-ddaw-intranet-access.log combined
</VirtualHost>
```

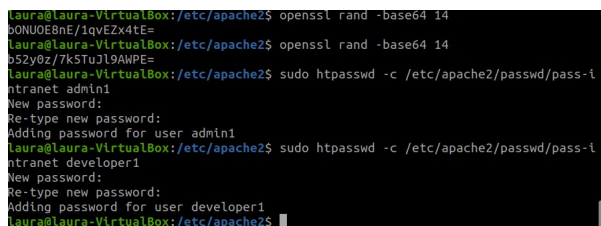
- Se crean los usuarios, pero en esta ocasión, utilizando la herramienta openssl:

Se generan con el comando “openssl rand -base64 14” dos contraseñas

Se crean los usuarios:

```
sudo htpasswd -c /etc/apache2/passwd/pass-intranet admin1
```

```
sudo htpasswd /etc/apache2/passwd/pass-intranet developer1
```



```
laura@laura-VirtualBox: /etc/apache2$ openssl rand -base64 14
bONUOE8nE/1qvEZx4tE=
laura@laura-VirtualBox: /etc/apache2$ openssl rand -base64 14
b52y0z/7k5TuJl9AWPE=
laura@laura-VirtualBox: /etc/apache2$ sudo htpasswd -c /etc/apache2/passwd/pass-i
intranet admin1
New password:
Re-type new password:
Adding password for user admin1
laura@laura-VirtualBox: /etc/apache2$ sudo htpasswd -c /etc/apache2/passwd/pass-i
intranet developer1
New password:
Re-type new password:
Adding password for user developer1
laura@laura-VirtualBox: /etc/apache2$
```

Cuando te pida las contraseñas, utilizarás las generadas, en nuestro caso:

bONUOE8nE/1qvEZx4tE=

b52y0z/7k5TuJl9AWPE=

- Se reinicia el servidor apache, ya que se han cambiado archivos de configuración:

```
sudo systemctl restart apache2
```

- Ahora se puede entrar nuevamente al sitio con estos usuarios