

PRÁCTICA 2.

CONFIGURAR RESTRICCIONES DE ACCESO CON .HTACCESS EN LA PRÁCTICA 1

blog.francmirror.es

2º SMR

Fecha de realización: 11 - 01 - 23



En esta práctica voy a usar un servidor Ubuntu 18 servidor, ya que solo haré uso de la terminal de este. Y como cliente voy a usar mi distribución Linux que uso a diario, Parrot OS

1) Para crear restricciones de acceso usando un archivo `.htaccess` debemos añadir a la configuración de host virtual del archivo de `pagina1.com.conf` la directiva siguiente:

```
Ubuntu-18-Server Clone 1 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
GNU nano 2.9.3 /etc/apache2/sites-available/pagina1.com.conf Modified

<VirtualHost *:80>
    ServerAdmin admin@pagina1.com
    DocumentRoot /var/www/pagina1.com/public_html
    ServerName pagina1.com
    ServerAlias www.pagina1.com
    ErrorLog ${APACHE_LOG_DIR}/error.log
    CustomLog ${APACHE_LOG_DIR}/access.log combined

    <Directory /var/www/pagina1.com/public_html>
        AllowOverride all
    </Directory>
</VirtualHost>
```

De esta forma apache buscará el contenido `.htaccess` cuando se acceda al sitio web y controlará las restricciones de acceso que definamos en él. Una vez modificado recargamos la configuración con **`service apache2 reload`**

```
Ubuntu-18-Server Clone 1 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
root@ubu18:/home/ubu18# service apache2 reload
root@ubu18:/home/ubu18#
```



2) En el archivo `/etc/hosts` de la máquina cliente añade las resoluciones DNS directas. Guardalo y comprueba que funcionan bien las resoluciones usando `ping pagina1.com`.

Yo añadiré los siguientes parámetros en mi cliente Parrot OS y probaré si tenemos conexión

```
sudo vim /etc/hosts - Parrot Terminal
# Host addresses
127.0.0.1    localhost
127.0.1.1    parrot
192.168.1.150 pagina1.com
192.168.1.150 pagina2.com

::1          localhost ip6-localhost ip6-loopback
ff02::1      ip6-allnodes
ff02::2      ip6-allrouters

# Others

~
~
~ tml crearemos el
~ . es un archivo
~ usar ls -a.
~
~ entrada
~?id=9671 y
~ entes
~
~
~ /etc/hosts
"/etc/hosts" 10L, 216C written
```

Cómo podemos comprobar en la imagen tenemos conexión desde el cliente a la máquina



3) En la carpeta `/var/www/pagina1.com/public_html` crearemos el archivo `.htaccess`. Recuerda que al comenzar por `.` es un archivo oculto y para visualizarlo al hacer `ls` debemos usar `ls -a`. Comprueba en cada caso que se obtiene la restricción que has configurado.

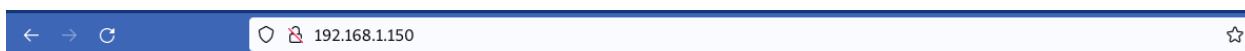
a. Permitir el acceso a todos.

```
Ubuntu-18-Server Clone 1 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
GNU nano 2.9.3 /var/www/pagina1.com/public_html/.htaccess
allow from all
```



Bien, el virtual host pagina1.com funciona perfectamente

b. Denegar el acceso a todos.



Forbidden

You don't have permission to access this resource.

Apache/2.4.29 (Ubuntu) Server at 192.168.1.150 Port 80

c. Denegar el acceso por ip al equipo cliente.

```
Ubuntu-18-Server Clone 1 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
GNU nano 2.9.3 /var/www/pagina1.com/public_html/.htaccess
Order allow,deny
Allow from all
Deny from 192.168.1.157
```



Forbidden

You don't have permission to access this resource.

Apache/2.4.29 (Ubuntu) Server at 192.168.1.150 Port 80



**Con esto ya habríamos finalizado la práctica de hoy, hemos configurado perfectamente el servidor Ubuntu 18 server y el cliente Parrot OS y hemos comprobado de qué maneras podemos configurar el archivo .htaccess.
Gracias por su tiempo.**