

## 18. [Hardening Web + OWASP] htaccess EN APACHE (Control, Seguridad y SEO)

### Parte 1: Activación de .htaccess en Apache

Editar la configuración predeterminada del sitio Apache

- `sudo nano /etc/apache2/sites-available/000-default.conf`

```
ub@forense-ai:~$ sudo nano /etc/apache2/sites-available/000-default.conf
```

Contenido:

```
<Directory /var/www/html>
    Options Indexes FollowSymLinks
    AllowOverride All
    Require all granted
</Directory>
```

```
GNU nano 7.2 /etc/apache2/sites-available/000-default.conf *
<VirtualHost *:80>
    # The ServerName directive sets the request scheme, hostname and port that
    # the server uses to identify itself. This is used when creating
    # redirection URLs. In the context of virtual hosts, the ServerName
    # specifies what hostname must appear in the request's Host: header to
    # match this virtual host. For the default virtual host (this file) this
    # value is not decisive as it is used as a last resort host regardless.
    # However, you must set it for any further virtual host explicitly.
    #ServerName www.example.com

    ServerAdmin webmaster@localhost
    DocumentRoot /var/www/html

    <Directory /var/www/html>
        Options Indexes FollowSymLinks
        AllowOverride All
        Require all granted
    </Directory>
```

Guardar, cerrar y reiniciar Apache:

- `sudo systemctl restart apache2`

```
ub@forense-ai:~$ sudo systemctl restart apache2
```

### Parte 2: Autenticación Básica con .htaccess

Crear una carpeta /var/www/html/admin/ con un index.html.

- `sudo mkdir /var/www/html/admin`

```
ub@forense-ai:~$ sudo mkdir /var/www/html/admin
```

- `sudo nano /var/www/html/admin/index.html`

```
ub@forense-ai:~$ sudo nano /var/www/html/admin/index.html
```

```
GNU nano 7.2 /var/www/html/admin/index.html
<h1>Es una zona restringida</h1>
```

Crear /var/www/html/.htpasswd generando un usuario:

- htpasswd -c /var/www/html/.htpasswd admin

```
ub@forense-ai:~$ sudo htpasswd -c /var/www/html/.htpasswd admin
New password:
Re-type new password:
Adding password for user admin
```

Crear /var/www/html/admin/.htaccess:

- sudo nano /var/www/html/admin/.htaccess

```
ub@forense-ai:~$ sudo nano /var/www/html/admin/.htaccess
```

Contenido:

```
AuthType Basic
AuthName "Zona restringida"
AuthUserFile /var/www/html/.htpasswd
Require valid-user
```

```
GNU nano 7.2 /var/www/html/admin/.htaccess *
AuthType Basic
AuthName "Zona restringida"
AuthUserFile /var/www/html/.htpasswd
Require valid-user
```

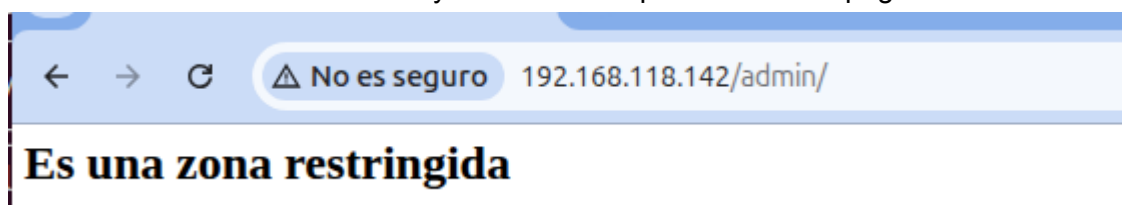
En el navegador:

- http://IP\_DEL\_SERVIDOR/admin



The screenshot shows a web browser window with the address bar displaying '192.168.118.142/admin'. The page content is a login form titled 'Iniciar sesión' (Log in). The form includes a warning message: 'http://192.168.118.142 Tu conexión con este sitio web no es privada' (Your connection to this website is not private). Below the warning, there are two input fields: 'Nombre de usuario' (Username) and 'Contraseña' (Password). At the bottom of the form, there are two buttons: 'Cancelar' (Cancel) and 'Iniciar sesión' (Log in).

Introduzca el nombre de usuario y la contraseña para mostrar la página



The screenshot shows a web browser window with the address bar displaying '192.168.118.142/admin/'. The page content is a message that reads 'Es una zona restringida' (It is a restricted area).

### Parte 3: Gestión de Errores Personalizados

Crear y en la raíz.404.html 403.html

- sudo nano /var/www/html/404.html

```
ub@forense-ai:~$ sudo nano /var/www/html/404.html
```

```
GNU nano 7.2 /var/www/html/404.html
<h1>Error 404 - Pagina no encontrada</h1>
```

- sudo nano /var/www/html/403.html

```
ub@forense-ai:~$ sudo nano /var/www/html/403.html
```

```
GNU nano 7.2 /var/www/html/403.html
<h1>Error 403 - Acceso prohibido</h1>
```

Añadir en :/var/www/html/.htaccess

- sudo nano /var/www/html/.htaccess  
ErrorDocument 404 /404.html  
ErrorDocument 403 /403.html

```
ub@forense-ai:~$ sudo nano /var/www/html/.htaccess
```

```
GNU nano 7.2 /var/www/html/.htaccess *
ErrorDocument 404 /404.html
ErrorDocument 403 /403.html
```

Probar:

← → ↻ ⚠ No es seguro 192.168.118.142/404.html

## Error 404 - Pagina no encontrada

← → ↻ ⚠ No es seguro 192.168.118.142/403.html

## Error 403 - Acceso prohibido

### Parte 4: Cabeceras de Seguridad

Añadir en :/var/www/html/.htaccess

- Header set X-Frame-Options "DENY"
- Header set X-Content-Type-Options "nosniff"
- Header set X-XSS-Protection "1; mode=block"
- Header set Referrer-Policy "no-referrer-when-downgrade"
- Header set Permissions-Policy "geolocation=()"

```

GNU nano 7.2 /var/www/html/.htaccess *
ErrorDocument 404 /404.html
ErrorDocument 403 /403.html
Header set X-Frame-Options "DENY"
Header set X-Content-Type-Options "nosniff"
Header set X-XSS-Protection "1; mode=block"
Header set Referrer-Policy "no-referrer-when-downgrade"
Header set Permissions-Policy "geolocation=()"

```

## Parte 5: Redirecciones HTTP

Redirección permanente (301):

Redirect 301 /viejo.html /nuevo.html

Temporal (302):

Redirect 302 /promo /promo-2026

- sudo nano /var/www/html/.htaccess

```

ub@forense-ai:~$ sudo nano /var/www/html/.htaccess

```

```

GNU nano 7.2 /var/www/html/.htaccess *
ErrorDocument 404 /404.html
ErrorDocument 403 /403.html
Header set X-Frame-Options "DENY"
Header set X-Content-Type-Options "nosniff"
Header set X-XSS-Protection "1; mode=block"
Header set Referrer-Policy "no-referrer-when-downgrade"
Header set Permissions-Policy "geolocation=()"

Redirect 301 /viejo.html /nuevo.html
Redirect 302 /promo /promo-2026

```

Probando 301:

Crear nuevo.html

- sudo nano /var/www/html/nuevo.html

```

ub@forense-ai:~$ sudo nano /var/www/html/nuevo.html

```

Contenido:

<h1>Esta es la nueva pagina</h1>

```

GNU nano 7.2 /var/www/html/nuevo.html
<h1>Esta es la nueva pagina</h1>

```

Crear viejo.html

- sudo nano /var/www/html/viejo.html

```

ub@forense-ai:~$ sudo nano /var/www/html/viejo.html

```

Contenido:

<h1>Pagina vieja</h1>

```
GNU nano 7.2 /var/www/html/viejo.html *
<h1>Pagina vieja</h1>
```

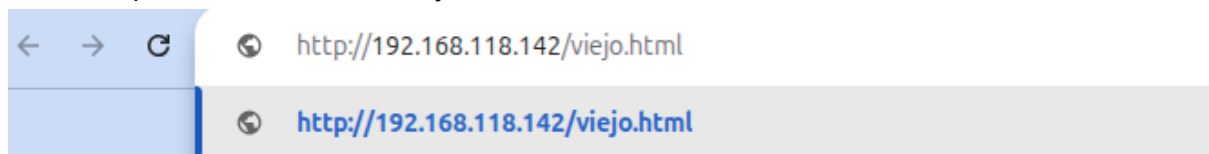
Habilite los siguientes módulos y reinicie Apache:

- sudo a2enmod alias
- sudo a2enmod headers
- sudo a2enmod rewrite
- sudo systemctl restart apache2

```
ub@forense-ai:~$ sudo a2enmod alias
Module alias already enabled
ub@forense-ai:~$ sudo a2enmod headers
Enabling module headers.
To activate the new configuration, you need to run:
    systemctl restart apache2
ub@forense-ai:~$ sudo a2enmod rewrite
Enabling module rewrite.
To activate the new configuration, you need to run:
    systemctl restart apache2
ub@forense-ai:~$ sudo systemctl restart apache2
```

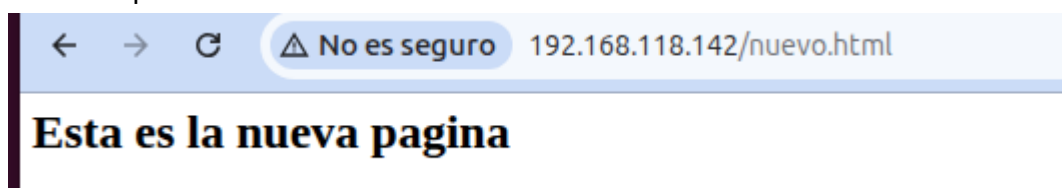
En el navegador:

- http://192.168.118.142/viejo.html



Redireccionar automáticamente a:

- http://192.168.118.142/nuevo.html



Prueba 302:

- sudo mkdir /var/www/html/promo-2026
- sudo nano /var/www/html/promo-2026/index.html

```
ub@forense-ai:~$ sudo mkdir /var/www/html/promo-2026
ub@forense-ai:~$ sudo nano /var/www/html/promo-2026/index.html
```

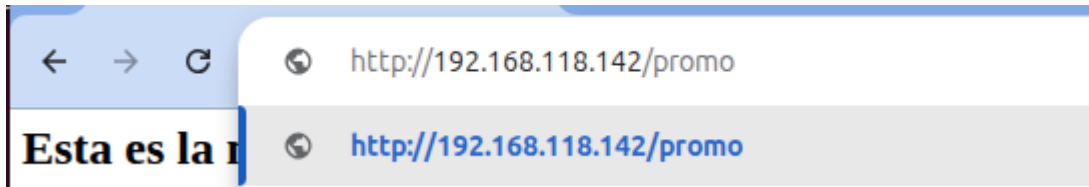
Contenido:

<h1>Promo 2026</h1>

```
GNU nano 7.2 /var/www/html/promo-2026/index.html *
<h1>Promo 2026</h1>
```

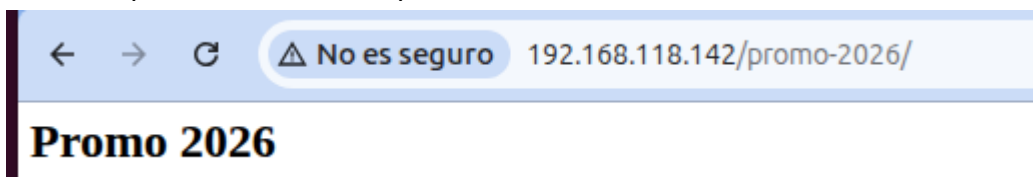
En el navegador:

- `http://192.168.118.142/promo`



Redireccionar automáticamente a:

- `http://192.168.118.142/promo-2026`



## Parte 6: Reescritura de URLs con mod\_rewrite

Habilite el módulo de rewrite

- `sudo a2enmod rewrite`
- `sudo systemctl restart apache2`

```
ub@forense-ai:~$ sudo a2enmod rewrite
Enabling module rewrite.
To activate the new configuration, you need to run:
    systemctl restart apache2
ub@forense-ai:~$ sudo systemctl restart apache2
```

Crear archivo

- `sudo nano /var/www/html/hola.html`

```
ub@forense-ai:~$ sudo nano /var/www/html/hola.html
```

Contenido:

Hola mundo

```
GNU nano 7.2 /var/www/html/hola.html *
<h1>Hola mundo</h1>
```

Editar .htaccess

```
RewriteEngine On
RewriteRule ^hola$ hola.html [L]
```

```

GNU nano 7.2 /var/www/html/.htaccess *
ErrorDocument 404 /404.html
ErrorDocument 403 /403.html

Header set X-Frame-Options "DENY"
Header set X-Content-Type-Options "nosniff"
Header set X-XSS-Protection "1; mode=block"
Header set Referrer-Policy "no-referrer-when-downgrade"
Header set Permissions-Policy "geolocation=()"

# 永久重定向 301
Redirect 301 /viejo.html /nuevo.html

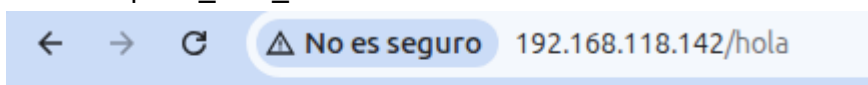
# 临时重定向 302
Redirect 302 /promo /promo-2026

RewriteEngine On
RewriteRule ^hola$ hola.html [L]

```

En el navegador:

- `http://IP_DEL_SERVIDOR/hola`



# Hola mundo

## Ejemplo avanzado: patrón MVC (Front Controller)

Abre el archivo .htaccess

- `sudo nano /var/www/html/.htaccess`

```
ub@forense-ai:~$ sudo nano /var/www/html/.htaccess
```

Contenido:

```
RewriteEngine On
```

```
RewriteCond %{REQUEST_FILENAME} !-f
```

```
RewriteCond %{REQUEST_FILENAME} !-d
```

```
RewriteRule ^(.+)$ index.php?route=$1 [L,QSA]
```

```

GNU nano 7.2 /var/www/html/.htaccess *
RewriteEngine On

RewriteCond %{REQUEST_FILENAME} !-f
RewriteCond %{REQUEST_FILENAME} !-d
RewriteRule ^(.+)$ index.php?route=$1 [L,QSA]

```

Abre el archivo

- `sudo nano /var/www/html/index.php`

```
ub@forense-ai:~$ sudo nano /var/www/html/index.php
```

Contenido:

```
<?php
```

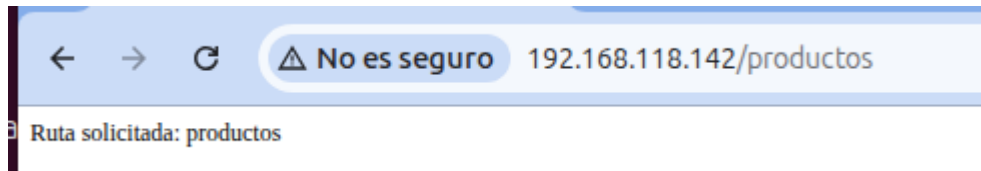
```
echo "Ruta solicitada: " . ($_GET['route'] ?? 'ninguna');
```

```
GNU nano 7.2 /var/www/html/index.php *
<?php
echo "Ruta solicitada: " . ($_GET['route'] ?? 'ninguna');
```

Prueba 1: Acceso a una ruta inexistente

En el navegador:

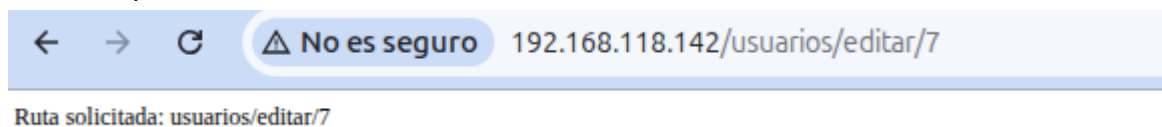
- `http://192.168.118.142/productos`



Prueba 2: Acceso a rutas de varios niveles

En el navegador:

- `http://192.168.118.142/usuarios/editar/7`



## Parte 7: Control del Listado de Directorios

Editar .htaccess

- `sudo nano /var/www/html/.htaccess`

```
ub@forense-ai:~$ sudo nano /var/www/html/.htaccess
```

Añade esta línea

Options -Indexes

```
GNU nano 7.2 /var/www/html/.htaccess *
Options -Indexes
RewriteEngine On
```

Crear directorio de prueba

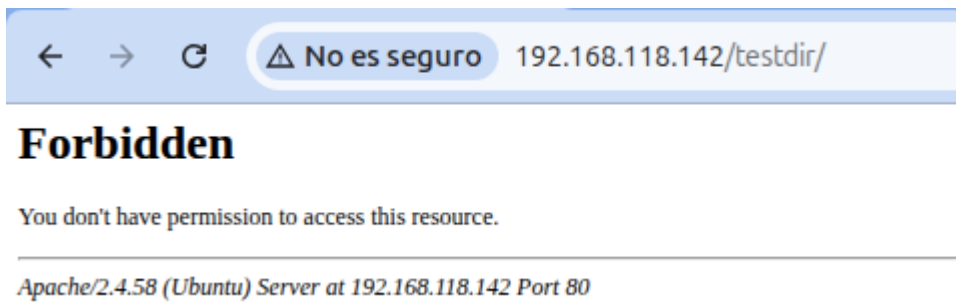
- `sudo mkdir /var/www/html/testdir`

```
ub@forense-ai:~$ sudo mkdir /var/www/html/testdir
```

En el navegador:

- `http://192.168.118.142/testdir`





## Parte 8: Forzar HTTPS

Editar .htaccess

- `sudo nano /var/www/html/.htaccess`

Añade:

```
RewriteEngine On
RewriteCond %{HTTPS} !=on
RewriteRule ^ https://%{HTTP_HOST}%{REQUEST_URI} [L,R=301]
```

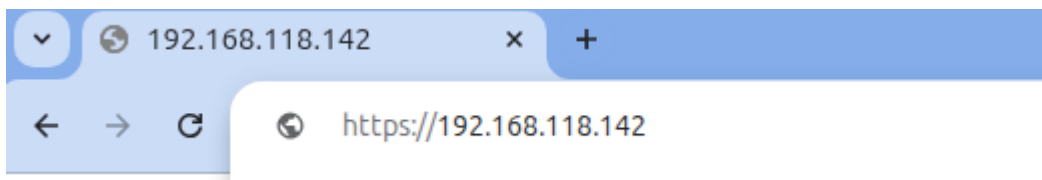
```
GNU nano 7.2 /var/www/html/.htaccess
# Options -Indexes

RewriteEngine On

RewriteCond %{HTTPS} !=on
RewriteRule ^ https://%{HTTP_HOST}%{REQUEST_URI} [L,R=301]
```

En el navegador:

- `192.168.118.142`



## Parte 9: Cacheo y Compresión

Cache de archivos (si activado):mod\_expires

Habilitar módulo

- `sudo a2enmod expires`
- `sudo systemctl restart apache2`

```
ub@forense-ai:~$ sudo a2enmod expires
Enabling module expires.
To activate the new configuration, you need to run:
systemctl restart apache2
ub@forense-ai:~$ sudo systemctl restart apache2
```

Añadir a .htaccess:

```
<IfModule mod_expires.c>
```

```
ExpiresActive On
ExpiresByType image/jpeg "access plus 30 days"
ExpiresByType text/css "access plus 7 days"
ExpiresByType application/javascript "access plus 7 days"
</IfModule>
```

```
GNU nano 7.2 /var/www/html/.htaccess *
# Options -Indexes

RewriteEngine On

RewriteCond %{HTTPS} !=on
RewriteRule ^ https://%{HTTP_HOST}%{REQUEST_URI} [L,R=301]

<IfModule mod_expires.c>
  ExpiresActive On
  ExpiresByType image/jpeg "access plus 30 days"
  ExpiresByType text/css "access plus 7 days"
  ExpiresByType application/javascript "access plus 7 days"
</IfModule>
```

Compresión (si activado):mod\_deflate

Habilitar módulo

- sudo a2enmod deflate
- sudo systemctl restart apache2

```
ub@forense-ai:~$ sudo a2enmod deflate
Considering dependency filter for deflate:
Module filter already enabled
Module deflate already enabled
ub@forense-ai:~$ sudo systemctl restart apache2
```

Añadir a .htaccess:

SetOutputFilter DEFLATE

```
</IfModule>
SetOutputFilter DEFLATE
```

## Parte 10: Interacción con Buscadores (SEO y Indexación)

Crear archivo

- sudo nano /var/www/html/robots.txt

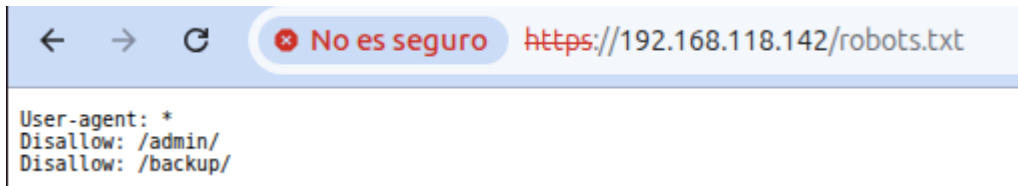
Contenido:

```
User-agent: *
Disallow: /admin/
Disallow: /backup/
```

```
GNU nano 7.2 /var/www/html/robots.txt *
User-agent: *
Disallow: /admin/
Disallow: /backup/
|
```

Prueba:

En el navegador: <http://192.168.118.142/robots.txt>



Evitar indexación con HTTP (X-Robots-Tag)

Habilitar el módulo headers

- sudo a2enmod headers
- sudo systemctl restart apache2

Añadir a .htaccess:

Header set X-Robots-Tag "noindex, nofollow"

```
Header set X-Robots-Tag "noindex, nofollow"
```

Bloquear bots por User-Agent

RewriteEngine On

RewriteCond %{HTTP\_USER\_AGENT} googlebot [NC]

RewriteRule ^ - [R=403]

```
GNU nano 7.2 /var/www/html/.htaccess *
# Options -Indexes

RewriteEngine On

RewriteCond %{HTTPS} !=on
RewriteRule ^ https://%{HTTP_HOST}%{REQUEST_URI} [L,R=301]

RewriteCond %{HTTP_USER_AGENT} googlebot [NC]
RewriteRule ^ - [R=403]
```

## Parte 11: Ocultación y Restricción de Carpetas

Impedir acceso web a una carpeta:

Dentro de la carpeta crear .htaccess

- sudo nano /var/www/html/backup/.htaccess

```
ub@forense-ai:~$ sudo nano /var/www/html/backup/.htaccess
```

Contenido:

Require all denied

```
GNU nano 7.2 /var/www/html/backup/.htaccess *
Require all denied
```

Bloquear tipos de archivos específicos

```
<FilesMatch "\.(sql|bak|zip|tar)$">
    Require all denied
</FilesMatch>
```

```
GNU nano 7.2 /var/www/html/backup/.htaccess *
Require all denied

<FilesMatch "\.(sql|bak|zip|tar)$">
    Require all denied
</FilesMatch>
```

Restringir el acceso por dirección IP  
Require ip 192.168.1.0/24

```
GNU nano 7.2 /var/www/html/backup/.htaccess *
Require all denied

<FilesMatch "\.(sql|bak|zip|tar)$">
    Require all denied
</FilesMatch>

Require ip 192.168.1.0/24
```

Impedir la ejecución de PHP en directorios de carga

- sudo nano /var/www/html/uploads/.htaccess

```
ub@forense-ai:~$ sudo nano /var/www/html/uploads/.htaccess
```

Contenido:

```
<FilesMatch "\.(php|phtml)$">
    Require all denied
</FilesMatch>
```

```
GNU nano 7.2 /var/www/html/uploads/.htaccess *
<FilesMatch "\.(php|phtml)$">
    Require all denied
</FilesMatch>
|
```