



# CURSO Seguridad en Aplicaciones Web

## Práctica VH

Billy diaz de Luis



## Índice

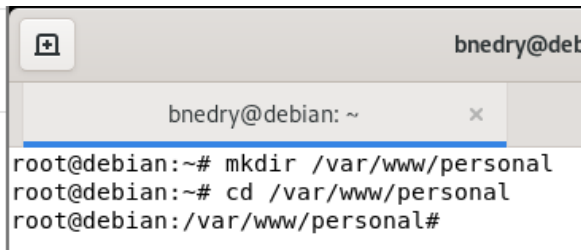
<b>Dar de alta el sitio : <a href="http://www.paginapersonal.unam.mx">www.paginapersonal.unam.mx</a></b>	<b>1</b>
<b>Configuración DocumentRoot</b>	<b>2</b>
<b>Configuración de bitácora error y acces propias para el VH</b>	<b>3</b>
<b>Remover la firma del servidor y del encabezado</b>	<b>4</b>
<b>Configuración de un mensaje de error genérico en error.html para los códigos más comunes</b>	<b>7</b>

Dar de alta el sitio : [www.paginapersonal.unam.mx](http://www.paginapersonal.unam.mx)

Crear directorio en /var/www/personal

```
#mkdir /var/www/personal
```

```
#cd /var/www/personal
```



```

bnedry@debian: ~
root@debian:~# mkdir /var/www/personal
root@debian:~# cd /var/www/personal
root@debian:/var/www/personal#
  
```

Creamos una nueva configuración para mi página.

```
cp 000-default.conf personal.conf
```

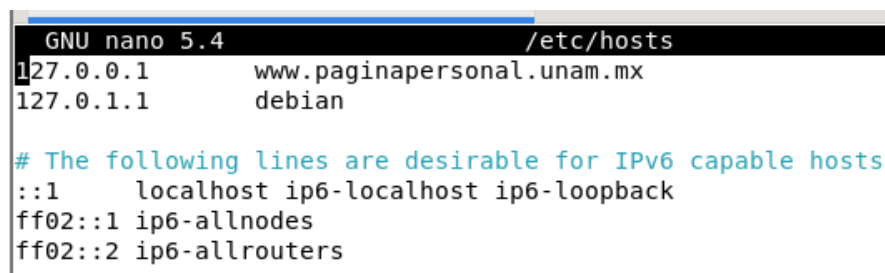


```

root@debian:/etc/apache2# cd sites-enabled/
root@debian:/etc/apache2/sites-enabled# ls
000-default.conf index.html portal.conf sitioIP.conf
root@debian:/etc/apache2/sites-enabled# cp 000-default.conf personal.conf
root@debian:/etc/apache2/sites-enabled# ls
000-default.conf index.html personal.conf portal.conf sitioIP.conf
root@debian:/etc/apache2/sites-enabled#
  
```

Abrimos el archivo /etc/hosts y agregamos la linea:

```
127.0.0.1 www.sitio1.unam.mx
```



```

GNU nano 5.4 /etc/hosts
127.0.0.1 www.paginapersonal.unam.mx
127.0.1.1 debian

# The following lines are desirable for IPv6 capable hosts
::1 localhost ip6-localhost ip6-loopback
ff02::1 ip6-allnodes
ff02::2 ip6-allrouters
  
```

## Configuración DocumentRoot

Editamos personal.conf y agregamos nombre de servidor

```
#nano personal.conf
```

```
ErrorDocument 404 "Recurso no disponible"
```

```
<Directory /var/www/sitio1>
```

```
Options -Indexes
```

```
AllowOverride
Require all granted
</Directory>
```

```
GNU nano 5.4 personal.conf
VirtualHost *:80>
# The ServerName directive sets the request scheme, hostname and
# 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)
# 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.paginapersonal.unam.mx

ServerAdmin billydilu@gmail.com
DocumentRoot /var/www/personal
ErrorDocument 404 "Recurso no disponible"

<Directory /var/www/sitio1>
    Options -Indexes
    AllowOverride
    Require all granted
</Directory>
```

Habilitar el sitio

```
# sudo a2ensite portal.conf
```

releer los archivos de configuración:

```
#systemctl reload apache2
```

Validar la sintaxis de configuración:

```
# sudo apache2ctl configtest
```













## Configuración de bitácora error y acces propias para el VH

```
# Available loglevels: trace8, ..., trace1, debug, info, notice, warn,
# error, crit, alert, emerg.
# It is also possible to configure the loglevel for particular
# modules, e.g.
#LogLevel info ssl:warn

ErrorLog ${APACHE_LOG_DIR}/www.paginapersonal.unam.mx-error.log
CustomLog ${APACHE_LOG_DIR}/www.paginapersonal.unam.mx-access.log combined

# For most configuration files from conf-available/, which are
# enabled or disabled at a global level, it is possible to
# include a line for only one particular virtual host. For example the
# following line enables the CGI configuration for this host only
# after it has been globally disabled with "a2disconf".
#Include conf-available/serve-cgi-bin.conf
</VirtualHost>

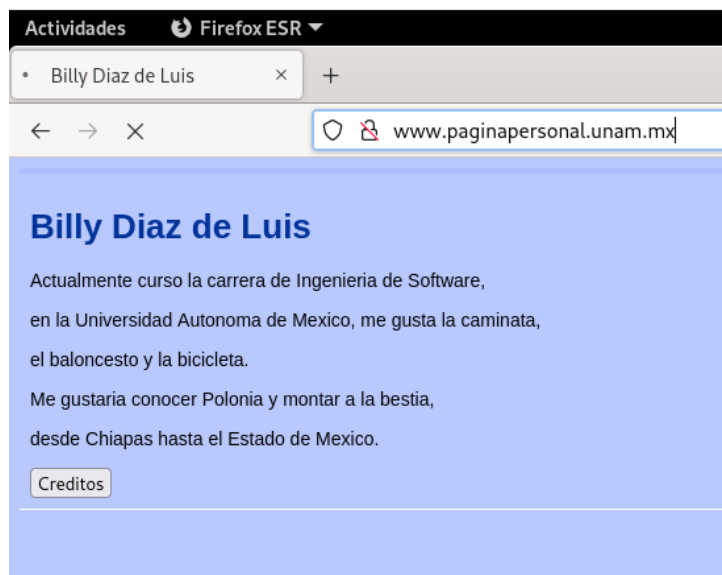
# vim: syntax=apache ts=4 sw=4 sts=4 sr noet
```

 Ayuda	 Guardar	 Buscar	 Cortar	 Ejecutar	
 Salir	 Leer fich.	 Reemplazar	 Pegar	 Justificar	

si la configuración es correcta se mostrará el siguiente mensaje:

```
root@debian:/etc/apache2/sites-enabled# sudo apache2ctl configtest
AH00558: apache2: Could not reliably determine the server's fully qualified domain name, using 127.0.1.1. Set the 'ServerName' directive globally to suppress this message
Syntax OK
root@debian:/etc/apache2/sites-enabled#
```

probar en el navegador  
[www.paginapersonal.unam.mx](http://www.paginapersonal.unam.mx)



## Remover la firma del servidor y del encabezado

La directiva ServerSignature

Habilitada de forma predeterminada, se debe deshabilitar de la siguiente manera para ocultar la firma del servidor:

Abrir la configuración principal de apache.

```
#nano /etc/apache2/apache2.conf
```

agregamos la siguiente línea al final del archivo.

ServerSignature off

```
# vim: syntax=apache ts=4 sw=4 sts=4 sr noet
#Eliminar firma de servidor
ServerSignature off
```

```

^G Ayuda      ^O Guardar    ^W Buscar     ^K (
^X Salir      ^R Leer fich. ^\ Reemplazar  ^U I

```

Nuevamente Habilitar el sitio

```
# sudo a2ensite portal.conf
```

Nuevamente releer los archivos de configuración:

```
#systemctl reload apache2
```

Utilizando el siguiente comando logramos observar información importante acerca de nuestro servidor, esto vulnera nuestro sistema se debe ocultar dicha información:

```
root@debian:/etc/apache2# sudo curl -vk# -X HEAD www.paginapersonal.unam.mx
Warning: Setting custom HTTP method to HEAD with -X/--request may not work the way you want. Consider using -I/--head instead.
* Trying 127.0.0.1:80...
* Connected to www.paginapersonal.unam.mx (127.0.0.1) port 80 (#0)
> HEAD / HTTP/1.1
> Host: www.paginapersonal.unam.mx
> User-Agent: curl/7.74.0
> Accept: */*
>
* Mark bundle as not supporting multiuse
< HTTP/1.1 200 OK
< Date: Fri, 29 Apr 2022 10:15:01 GMT
< Server: Apache/2.4.53 (Debian)
< Last-Modified: Fri, 29 Apr 2022 08:50:01 GMT
< ETag: "52b-5ddc720bfb447"
< Accept-Ranges: bytes
< Content-Length: 1323
< Vary: Accept-Encoding
< Content-Type: text/html
<
* transfer closed with 1323 bytes remaining to read
* Closing connection 0
curl: (18) transfer closed with 1323 bytes remaining to read
root@debian:/etc/apache2#
```

Abrir la configuración principal de apache.

```
#nano /etc/apache2/apache2.conf
```

agregamos la siguiente línea al final del archivo y guardamos.

```
ServerTokens ProductOnly
```

```
# vim: syntax=apache ts=4 sw=4 sts=4 sr noet
#Eliminar firma de servidor
ServerSignature off
ServerTokens ProductOnly
```

<b>^G</b> Ayuda	<b>^O</b> Guardar	<b>^W</b> Buscar	<b>^K</b> Cortar	<b>^T</b> Ejecutar
<b>^X</b> Salir	<b>^R</b> Leer fich.	<b>^N</b> Reemplazar	<b>^U</b> Pegar	<b>^J</b> Justificar

Nuevamente Habilitar el sitio

```
# sudo a2ensite portal.conf
```

Nuevamente releer los archivos de configuración:

```
#systemctl reload apache2
```

Si ejecutamos nuevamente el código de consulta de cabecera observamos que la información de nuestro servidor se ha ocultado.

```
root@debian:/etc/apache2# sudo curl -vk# -X HEAD www.paginapersonal.unam.mx
Warning: Setting custom HTTP method to HEAD with -X/--request may not work the way you want. Consider using -I/--head instead.
* Trying 127.0.0.1:80...
* Connected to www.paginapersonal.unam.mx (127.0.0.1) port 80 (#0)
> HEAD / HTTP/1.1
> Host: www.paginapersonal.unam.mx
> User-Agent: curl/7.74.0
> Accept: */*
>
* Mark bundle as not supporting multiuse
< HTTP/1.1 200 OK
< Date: Fri, 29 Apr 2022 10:22:14 GMT
< Server: Apache
< Last-Modified: Fri, 29 Apr 2022 08:50:01 GMT
< ETag: "52b-5ddc720bfb447"
< Accept-Ranges: bytes
< Content-Length: 1323
< Vary: Accept-Encoding
< Content-Type: text/html
<
* transfer closed with 1323 bytes remaining to read
* Closing connection 0
curl: (18) transfer closed with 1323 bytes remaining to read
root@debian:/etc/apache2#
```

Habilitamos el módulo a2enmod headers para modificar los encabezados y agregamos los siguientes comandos en el archivo /etc/apache2/conf-enabled/security.conf:

```
#a2enmod headers
```

```
#
Header set X-Content-Type-Options: "nosniff"

#
# Setting this header will prevent other sites from embedding pages
# site as frames. This defends against clickjacking attacks.
# Requires mod_headers to be enabled.
#
Header set X-Frame-Options: "sameorigin"

Header set X-XSS-Protection "1; mode=block"
$ vim: syntax=apache ts=4 sw=4 sts=4 sr noet
```

Ejecutamos un curl para observar el nuevo comportamiento mostrado en la siguiente imagen:

```
e2
root@debian:/etc/apache2/conf-enabled# sudo curl -vk# -X HEAD www.
paginapersonal.unam.mx
Warning: Setting custom HTTP method to HEAD with -X/--request may
not work the
Warning: way you want. Consider using -I/--head instead.
* Trying 127.0.0.1:80...
* Connected to www.paginapersonal.unam.mx (127.0.0.1) port 80 (#0)
> HEAD / HTTP/1.1
> Host: www.paginapersonal.unam.mx
> User-Agent: curl/7.74.0
> Accept: */*
e>
y* Mark bundle as not supporting multiuse
< HTTP/1.1 200 OK
< Date: Fri, 29 Apr 2022 10:56:36 GMT
< Server: Apache
< Last-Modified: Fri, 29 Apr 2022 08:50:01 GMT
< ETag: "52b-5ddc720bfb447"
< Accept-Ranges: bytes
< Content-Length: 1323
< Vary: Accept-Encoding
< X-Content-Type-Options: nosniff
< X-Frame-Options: sameorigin
< X-XSS-Protection: 1; mode=block
< Content-Type: text/html
<
* transfer closed with 1323 bytes remaining to read
* Closing connection 0
curl: (18) transfer closed with 1323 bytes remaining to read
root@debian:/etc/apache2/conf-enabled#
```

## Configuración de un mensaje de error genérico en error.html para los códigos más comunes

El archivo que se desea configurar es `/etc/apache2/sites-enabled/personal.conf`

Considere los errores más comunes y los redireccione a la página `error.html`

```
ErrorDocument 301 /error.html
ErrorDocument 302 /error.html
ErrorDocument 400 /error.html
ErrorDocument 401 /error.html
ErrorDocument 403 /error.html
ErrorDocument 404 /error.html
ErrorDocument 500 /error.html
ErrorDocument 503 /error.html
ErrorDocument 504 /error.html
```

Intentamos acceder a un recurso inexistente en nuestra página, por lo tanto se arrojó el siguiente mensaje genérico:





Universidad Nacional  
Autónoma de México

DGTIC

Coordinación de  
Seguridad de la Información

