Dirección General de Cómputo y de
Tecnologías de Información y Comunicación

UNAM-CERT
Plan de Becarios en Seguridad Informática

Seguridad en aplicaciones web

Ejercicio

Página web

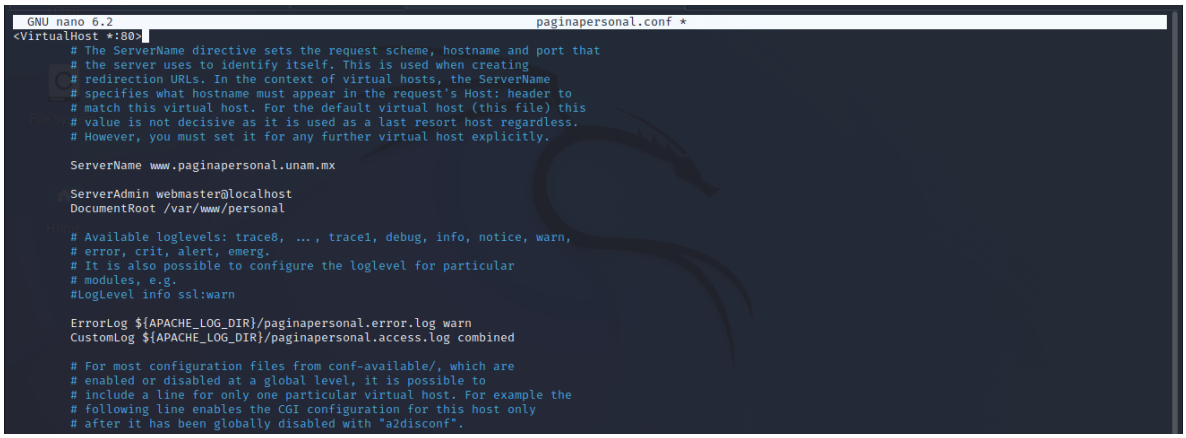
Ivan Daniel Galindo

Profesora Angie Aguilar

28/04/2022

Primero hacemos una copia del .conf

Ahora hacemos la configuración de `paginapersonal.conf` donde añadimos el `ServerName` , indicamos el `DocumentRoot` y lo referente a los logs



Después configuramos el `/etc/hosts` para que el navegador sepa a dónde buscar el recurso cuando lo solicitemos luego

Realizamos las configuraciones en `/etc/apache2/apache2.conf` para remover la firma del servidor y del encabezado.

```
 GNU nano 6.2                                                    /etc/apache2/apache2.conf
# (the actual bytes sent including headers) instead of %b (the size of the
# requested file), because the latter makes it impossible to detect partial
# requests.
#
# Note that the use of %{X-Forwarded-For}i instead of %h is not recommended.
# Use mod_remoteip instead.
#
LogFormat "%v:%p %h %l %u %t \"%r\" %>s %O \"%{Referer}i\" \"%{User-Agent}i\"" vhost_combined
LogFormat "%h %l %u %t \"%r\" %>s %O \"%{Referer}i\" \"%{User-Agent}i\"" combined
LogFormat "%h %l %u %t \"%r\" %>s %O" common
LogFormat "%{Referer}i -> %U" referer
LogFormat "%{User-agent}i" agent

# Include of directories ignores editors' and dpkg's backup files,
# see README.Debian for details.

# Include generic snippets of statements
IncludeOptional conf-enabled/*.conf

# Include the virtual host configurations:
IncludeOptional sites-enabled/*.conf

ServerSignature Off

ServerTokens ProductOnly

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

Posteriormente creamos el directorio raíz de la página:

```
┌──(kali㉿kali)-[/etc/apache2/sites-available]
└─$ sudo mkdir /var/www/personal
```

En `paginapersonal.conf` añadimos la directiva de los errores

```
        ErrorLog ${APACHE_LOG_DIR}/personal/paginapersonal.error.log
        CustomLog ${APACHE_LOG_DIR}/personal/paginapersonal.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

        ErrorDocument 404 /customerror.html
        ErrorDocument 401 /customerror.html
        ErrorDocument 410 /customerror.html
        ErrorDocument 500 /customerror.html
        ErrorDocument 502 /customerror.html
        ErrorDocument 301 /customerror.html


</VirtualHost>

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

Y creamos el archivo `customerror.html` (A modo de prueba inicialmente se llama `custom_404.html` pero luego se cambia el nombre)

```
┌──(kali㉿kali)-[/etc/apache2]
└─$ echo "<h1 style='color:red'> Are you a lost monkee? :-(</h1>" | sudo tee /var/www/personal/custom_404.html
<h1 style='color:red'> Are you a lost monkee? :-(</h1>
```

Creamos el `index.html` y `creditos.html`:

```
 GNU nano 6.2                                                    /var/www/personal/index.html
<!DOCTYPE html>
<html>
<body>

<h1>About the Odyssey</h1>

<p> Sing to me of the man, Muse, the man of twists and turns, driven time and again off course, once he had plundered the hallowed heights of Troy.</p>
<a href="http://www.paginapersonal.unam.mx/creditos.html">Creditos</a>

</body>
</html>
```

```
 GNU nano 6.2                                creditos.html *
<!DOCTYPE html>
<html>
<body>

<h1>About the Odyssey... I mean, this page</h1>

<p> Ivan [dot] Galindo [at] bec [dot] cert [dot] unam [dot] mx </p>
<a href="http://www.paginapersonal.unam.mx/">Index</a>

</body>
</html>
```

Una vez terminado esto habilitamos el sitio con `a2ensite`:

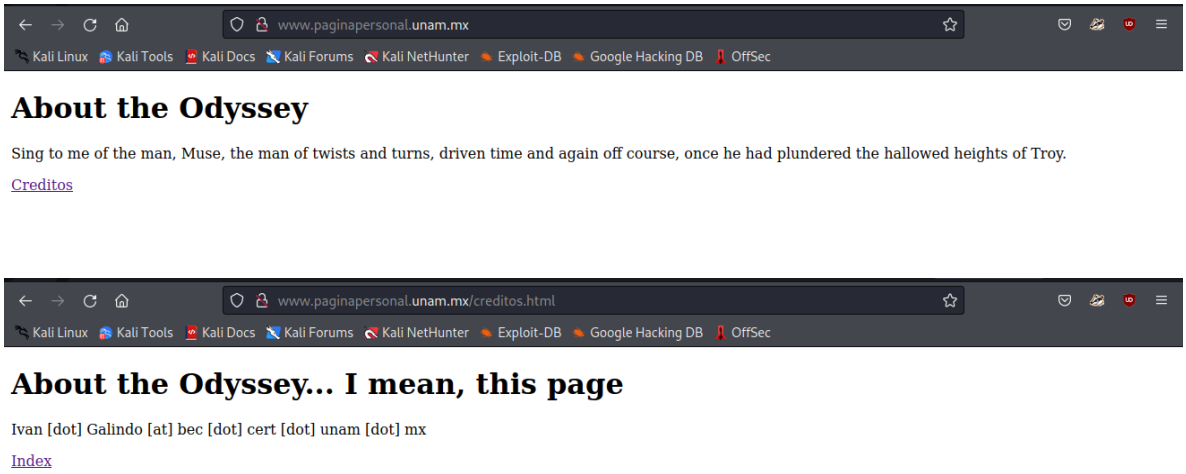
```
┌──(kali㉿kali)-[~]
└─$ sudo a2ensite paginapersonal.conf
Enabling site paginapersonal.
To activate the new configuration, you need to run:
  systemctl reload apache2
```

También tenemos que dar `reload` al servicio de Apache:

```
┌──(kali㉿kali)-[/var/www/personal]
└─$ 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 th
is message
Syntax OK

┌──(kali㉿kali)-[/var/www/personal]
└─$ sudo systemctl reload apache2
```

Ahora se puede ver nuestra página y créditos:



¿Qué pasa si no tengo un `index.*`? ¿Cómo indico que home.html debe servirse al solicitar la raíz del sitio?

De no estar bloqueado, se muestra un listado de los archivos del directorio. Se puede indicar con una directiva en el .conf "`DirectoryIndex home.html`"