



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

```
(kali@kali)-[/etc/apache2/sites-available]
└─$ sudo cp 000-default.conf paginapersonal.conf
[sudo] password for kali:
(kali@kali)-[/etc/apache2/sites-available]
└─$
```

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

```
GNU nano 6.2 paginapersonal.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.paginapersonal.unam.mx

    ServerAdmin webmaster@localhost
    DocumentRoot /var/www/personal

    # 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}/paginapersonal.error.log warn
    CustomLog ${APACHE_LOG_DIR}/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".
```

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

```
(kali@kali)-[/var/www/personal]
└─$ cat /etc/hosts
127.0.0.1 localhost
127.0.0.1 kali
127.0.0.1 www.paginapersonal.unam.mx

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

(kali@kali)-[/var/www/personal]
└─$
```

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%h %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

```

Sing to me and again off course, once he had plundered the hallowed heights of Troy.
CustomLog ${APACHE_LOG_DIR}/personal/paginapersonal.access.log combined
Credits
# 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 "azdisconf".
#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 501 /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>
(kali@kali)-[/etc/apache2]

```

Creamos el index.html y credits.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/credits.html">Credits</a>
</body>
</html>

```

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

<h1>About the Odyssey... I mean, this page</h1>e? :-(</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:



## About the Odyssey

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.

[Creditos](#)



## About the Odyssey... I mean, this page

Ivan [dot] Galindo [at] bec [dot] cert [dot] unam [dot] mx

[Index](#)

¿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”