# Seguridad en Apache Web Server 2.0.x


gaper
BRIO
ayzax

http://www.icenetx.cjb.net

# Personalizar mensajes de error

Es importante dar la menor cantidad de información posible, ya que un atacante puede llegar a comprometer la seguridad del servidor con un poco de información que obtenga de este. Los mensajes de error pueden ser una fuente importante de información, y para evitar esto, lo podemos personalizar. Creamos una página de error general (error.html) y enviamos cualquier error a ésta página.

*ErrorDocument 400 /error/error.html*
*ErrorDocument 401 /error/error.html*
*ErrorDocument 403 /error/error.html*
*ErrorDocument 404 /error/error.html*
*ErrorDocument 405 /error/error.html*
*etc...*

# Virtual Hosts

Si vamos a tener varias páginas web alojadas en el mismo servidor, una de las opciones es usar virtual hosts. Lo primero es activar la siguiente línea:

*NameVirtualHost *:80*

Y luego usar el siguiente modelo para cada virtual host

```
<VirtualHost *:80>
ServerName www.domain.tld
ServerAlias domain.tld *.domain.tld
DocumentRoot /www/domain
</VirtualHost>

<VirtualHost *:8080>
ServerName www.otherdomain.tld
DocumentRoot /www/otherdomain
</VirtualHost>
```

# Safe Mode

Cuando safe_mode está en On, el PHP verifica si el dueño del script actual coincide con el dueño del fichero a ser operado por una función de fichero. Por ejemplo:

*-rw-rw-r--  1 ayzax  ayzax  33 Jul  1 19:20 script.php*
*-rw-r--r--  1 root  root  1116 May 26 18:01 /etc/passwd*

Corriendo este script.php

```
<?php
 readfile('/etc/passwd');
?>
```

resulta in este error cuando Modo Seguro está habilitado:

*Warning: SAFE MODE Restriction in effect. The script whose uid is 500 is not allowed to access /etc/passwd owned by uid 0 in script.php on line 2*

Para activar el safe mode, tenemos que editar el archivo php.ini que se encuentra en /etc/php.ini y nos queda así:

```
safe_mode = On
safe_mode_gid = Off
safe_mode_include_dir =
safe_mode_exec_dir =
```

# Versión de PHP

Para agregar un poco de seguridad, impedimos que se muestre la versión de PHP en los headers del servidor web. También editando php.ini , queda así:

*expose_php = Off*

# Errores de PHP

Debemos habilitar que solamente se muestren los errores graves de php, de modo que si ocurre alguna falla en un script de php no se exponga cierta información que podría ser vital para un atacante

*error_reporting = E_COMPILE_ERROR | E_ERROR | E_CORE_ERROR*
*display_errors = Off*

Parte del proyecto Lamp Live CD