Seguridad en Apache Web Server 2.0.x

gaper
BRIO
ayzax

http://www.icenetx.cjb.net

Seguridad ...

Seguridad informática: Mantener protegida la información

Podemos entender como seguridad una característica de cualquier sistema (informático o no) que nos indica que ese sistema está libre de todo peligro, daño o riesgo.

En criptografía y seguridad informática, seguridad por ocultación (a veces seguridad mediante ocultación) es un controvertido principio de ingeniería de seguridad, la cual intenta utilizar el secreto (de diseño, de implementación, etc.) para asegurar la seguridad. Un sistema que se apoya en la seguridad por ocultación puede tener vulnerabilidades de seguridad teóricas o prácticas, pero sus propietarios o diseñadores creen que estos puntos débiles no se conocen, y que es probable que los atacantes no los descubran.

Compilando Apache

Entramos en modo super usuario o root:

su -
password:

Descomprimimos el archivo:

tar -xvzf httpd-2.0.55.tar.gz

Configuramos y compilamos:

cd httpd-2.0.55
./configure --
prefix=ruta_de_instalacion
make
make install

Creando grupo y usuario:

groupadd apache
useradd -g apache apache

Arrancando apache:
/usr/local/apache2/bin/apachectl start

Configuración de apache web server

El archivo de configuración de apache se encuentra en la carpeta conf dentro de la ruta donde se encuentra instalado. Es denominado httpd.conf

Como encontrar el archivo de configuración?
1.- updatedb && locate httpd.conf
2.- find /etc -iname httpd.conf

Por defecto en después de una compilación lo podemos encontrar en la ruta:

/usr/local/apache2/conf/httpd.conf

Para modificarlo usamos nuestro editor preferido:

1.- nano /usr/local/apache2/conf/httpd.conf
2.- vi /usr/local/apache2/conf/httpd.conf
3.- xhost+ && su -c “gedit /usr/local/apache2/conf/httpd.conf”

.htaccess

Restringir accesso:
Permite htaccess, colocando en httpd.conf

AllowOverride AuthConfig

Crear la contraseña con la utilidad de apache, en un directorio no accesible para http

htpasswd -c /usr/local/apache/passwd/passwords usuario1
htpasswd /usr/local/apache/passwd/passwords usuario2

crear archivo de grupo con el siguiente formato:

GroupName: usuario1 usuario2 usuario3

Dar permiso en el .htaccess o httpd.conf

AuthType Basic
AuthName "Restricted Files"
AuthUserFile /usr/local/apache/passwd/passwords
Require [user rbowen,Require group GroupName,valid-user]

ServerTokens

Opciones: [Full | OS | Minor | Minimal | Major | Prod]
ServerTokens []

Esto incrementa la seguridad por OBSCURIDAD al servidor, en caso de que un hacker pretenda revisar la versión de apache con algún script ordinario, esto provoca que si olvidamos actualizar el servidor por alguna vulnerabilidad, el hacker no intentara explotarla.

La variable ServerTokens le indica a apache que cantidad de información debe proporcionar a la petición de las cabeceras HTTP.

Default: ServerTokens Full

Recomendado: ServerTokens Minimal

ServerAdmin

Opciones: [mail]
ServerAdmin []

La variable ServerAdmin le indica a apache que dirección de correo del administrador mostrar al publico con el fin de reportar un error.

Cambiar el valor de ServerAdmin por una dirección de correo especial designada para recibir correo referente al servidor.
En caso de que un hacker pretenda hacer ingeniería social, **PHYSING,** xploits, hacer spam o bombardear la dirección del administrador, sera posible obtener información y mantenernos enterados sobre lo que concierne Apache.

Default: you@example.conf

User & Group

Opciones: [usuario] & [grupo]
User []
Group []

Al correr apache en una plataforma linux, automáticamente adquiere las propiedades de su sistema de archivos, la arquitectura RWX le permite a apache restringir el acceso a los sitios web como todo archivo en linux bajo el criterio Read | Write | Execute tanto para Usuario como para el Grupo al que pertenece; estas 2 variables de apache afectan a todas las paginas web que este tenga dentro de “htdocs”.

Default:

User nobody
Group #-1

Recomendado:

User apache
Group apache

chown -R apache /usr/local/apache2/htdocs

KeepAlive

Opciones: [On | Off]

Permite o no conexiones persistentes de una sola dirección o una o mas peticiones por conexión

Default: KeepAlive On

Recomendado: KeepAlive Off

Options Indexes

Cuando una carpeta no tiene index.html, muestra la lista de archivos y carpetas en forma indexada, esto se presta a que se expongan archivos y directorios que no se desean mostrar. Cada bloque de carpetas compartidas por el servidor apache deberá especificar si desea o no mostrar este valor. Para este caso Document Root.

Default: Options Indexes FollowSymLinks

Recomendado: Options FollowSymLink

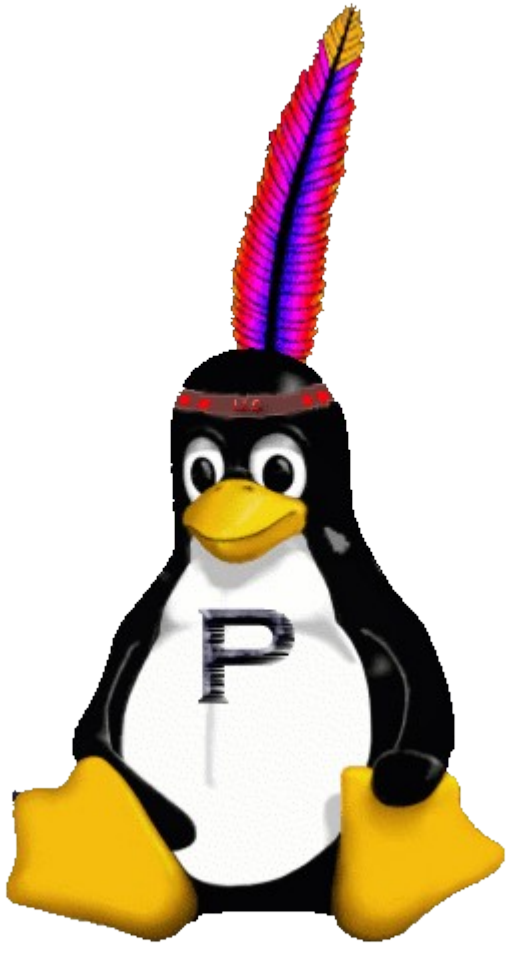
Creación de un directorio publico

Si se desea contar con un directorio publico o permitir y aceptar índices en determinadas rutas, sera necesario indicarlo una por una en el archivo de configuración de apache.

```
<Directory “/usr/local/apache2/htdocs/dir_publico”>
        Options FollowSymLinks Indexes
        AllowOverride None
        Order allow,deny
        Allow From all
</directory>
```

Esto permite tener índices en la carpeta especificada, útil si hemos denegado el índice en todo el servidor.

Parte de Lamp Live CD project !



http://www.icenetx.cjb.net