

Hardening de Apache



Hardening de Apache

- Configuraciones Globales
- Deshabilitar la información ofrecida por el servidor
- Configuraciones por contexto
- mod_security



Configuraciones Globales

Existen algunas configuraciones generales de Apache que ayudan a aumentar su seguridad:

- Ejecutarlo con un **usuario** con los privilegios justos. Tipicamente en entornos debian es `www-data`, para cercionarnos de que esta configurado de forma correcta podemos en *`/etc/apache2/apache2.conf`*



Configuraciones Globales

- **Deshabilitar los modulos innecesarios:** Es posible que algunos modulos configurados para cargarse en el inicio sean innecesarios y por lo tanto contradicen la norma de la minima exposici3n. Existe una herramienta para desactivarlos llamada a2dismod.
- **Deshabilitar la informaci3n ofrecida por el servidor:** Cuando Apache responde a una petici3n, en las cabeceras muestra informaci3n sobre la version de Apache. Este tipo de informaci3n tambien se muestra cuando se produce un error.



Deshabilitar la información ofrecida por el servidor

En el fichero */etc/apache2/conf.d/security* se encuentran las directivas *ServerTokens* (que viene por defecto como *OS* y deberíamos cambiarla a *ProductOnly*) y *ServerSignature* (por defecto *On* y debemos desactivarla) que nos permiten dejar de mostrar dicha información.



Deshabilitar la información ofrecida por el servidor

En el fichero */etc/apache2/conf.d/security* se encuentran las directivas *ServerTokens* (que viene por defecto como *OS* y deberíamos cambiarla a *ProductOnly*) y *ServerSignature* (por defecto *On* y debemos desactivarla) que nos permiten dejar de mostrar dicha información.

Deshabilitar la información ofrecida por el servidor

En el fichero */etc/apache2/conf.d/security* se encuentran las directivas *ServerTokens* (que viene por defecto como *OS* y deberíamos cambiarla a *ProductOnly*) y *ServerSignature* (por defecto *On* y debemos desactivarla) que nos permiten dejar de mostrar dicha información.

Configuraciones por contexto

En la definición de contexto de cada sitio */etc/apache2/sites-available/enabled* existen una gran variedad de parámetros para modificar el comportamiento de los sitios servidos por Apache. Entre dichos parametros destacariamos:

Configuraciones por contexto

Options:

- FollowSymLinks Permite a Apache seguir los enlaces simbolicos que se encuentren dentro del directorio.
- SymLinksIfOwnweMatch Hace lo mismo que el anterior siempre que dichos enlaces sean del mismo propietario que el recurso enlazado. Si los enlaces pertenecieran a www-data no hay mucho peligro.



Configuraciones por contexto

Options:

- MultiViews Tratará de ofrecer un recursos aunque este no disponga de la extensión.
- Indexes En el caso de no existir un fichero index mostrará el contenido del directorio. Esta configuración no tendrá efecto si desactivamos el modulo autoindex.
- None hay que indicar esta opción siempre que no exista otra.

Configuraciones por contexto

Access Control (ACL):

Es posible restringir el acceso para determinadas direcciones o redes. Esto puede ser útil para restringir una intranet, bloquear un rango de IPs, etc...

Para conseguir esta funcionalidad se utilizan las directivas *Order*, *Allow* y *Deny*.

Configuraciones por contexto

.htaccess:

Los ficheros .htaccess se colocan dentro de directorios donde se desee aplicar una configuración específica definida por el desarrollador web y no por el administrador de apache. En mi caso lo desaconsejo y creo que es mejor definir en la configuración de apache (probablemente mediante includes) las configuraciones específicas.
AllowOverride None.



mod_security

mod_security es un módulo que permite filtrar peticiones maliciosas recibidas por el servidor web Apache. Se considera un sistema de detección de intrusos (IDIS) para aplicaciones web y es capaz tanto de prevenir los ataques como de crear un registro de los mismos. Mediante los filtros y patrones que implementa puede detectar gran cantidad de ataques entre los que se encuentran las inyecciones a la base de datos (SQLi) o las de código (XSS). Es útil para minimizar los riesgos en aplicaciones web inseguras.

Consta de dos partes, la primera es el módulo en sí y la segunda las reglas o filtros CRS.

