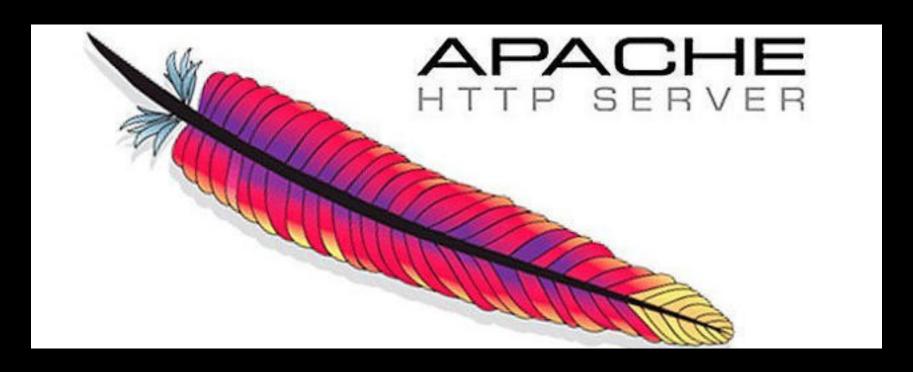


## Hardening de Apache









## 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 exposición. Exite una herramienta para desactivarlos llamada a2dismod.
- Deshabilitar la información ofrecida por el servidor:
  Cuando Apache responde a una petición, en las cabeceras muestra información sobre la version de Apache. Este tipo de infromación tambien se muestra cuando se produce un error.



## Deshabilitar la información ofrecida por el servidor

En el dichero /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.



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



### 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.



### Options:

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



#### Access Control (ACL):

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

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



#### .htaccess:

Los ficheros .htaccess se colocan dentro de directorios donde se desee apkicar una configuración especifica 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 especificas. AllowOverrride None.



### mod\_security

mod\_security es un módulo que permite filtrar petiones maliciosas recibidas por el servidor web Apache. Se comodera un sistema de deteccion 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 codigo (XSS). Es util para minimizar los riesgos en aplicaciones web inseguras.

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

