Aumentar la seguridad de Apache

ÍNDICE

1. Configuración básica en Apache **3**

Edita el archivo de configuración de Apache 3

Configura las directivas de ServerTokens y ServerSignature 3

Reinicia Apache para aplicar los cambios 3

2. Desactivar módulos que exponen información **4**

Desactiva mod_status (que podría exponer información sensible) 4

Desactiva otros módulos innecesarios 4

3. Configurar seguridad adicional con mod_security **5**

Instalar mod_security 5

Activar mod_security 5

Configurar reglas para modificar el encabezado Server 5

En este manual vamos a ocultar nuestra versión de Apache para protegernos frente posibles ataques, vamos a partir desde una página web ya configurada y funcional, para llegar a este punto puedes consultar mi otro manual en este enlace.

Lo primero que vamos a realizar es un “status” de apache.

```
sudo service apache2 status
```

Una vez comprobemos que todo está funcionando correctamente proseguimos con el manual.

1. Configuración básica en Apache

Primero, asegúrate de que Apache no revele información sobre su versión en los encabezados HTTP.

Edita el archivo de configuración de Apache:

En sistemas Debian/Ubuntu:
```
sudo nano /etc/apache2/apache2.conf
```

En sistemas CentOS/RHEL:
```
sudo nano /etc/httpd/conf/httpd.conf
```

Configura las directivas de `ServerTokens` y `ServerSignature`

Agrega o modifica estas líneas en el archivo de configuración principal:
```
ServerTokens Prod
ServerSignature Off
```

- `ServerTokens Prod`: Oculta detalles del sistema operativo y muestra sólo "Apache".
- `ServerSignature Off`: Desactiva la firma del servidor en las páginas de error.

Reinicia Apache para aplicar los cambios:

```
sudo systemctl restart apache2  # En Debian/Ubuntu

sudo systemctl restart httpd    # En CentOS/RHEL
```

2. Desactivar módulos que exponen información

Desactiva `mod_status` (que podría exponer información sensible):

Verifica si está habilitado:

```
apachectl -M | grep status
```

Si está habilitado, desactívalo:

```
sudo a2dismod status
sudo systemctl restart apache2
```

Desactiva otros módulos innecesarios:

```
sudo a2dismod autoindex
sudo a2dismod info
sudo systemctl restart apache2
```

3. Configurar seguridad adicional con mod_security

Instalar `mod_security`:

```
sudo apt install libapache2-mod-security2  # En Debian/Ubuntu
sudo yum install mod_security              # En CentOS/RHEL
```

Activar `mod_security`:

```
sudo a2enmod security2
sudo systemctl restart apache2
```

Configurar reglas para eliminar el encabezado `Server`:

Edita el archivo de configuración de `mod_security`:
`sudo nano /etc/modsecurity/modsecurity.conf`

Añade:
`SecServerSignature "Variable*"`

Reinicia Apache para aplicar las reglas:
`sudo systemctl restart apache2`

Variable*: Aqui podemos añadir lo que queramos que aparezca en vez de la versión de apache, es muy importante no añadir ningún tipo de espacio ya que no están soportados, en esta caso vamos a poner "Hola"

Comprobaciones de versión

Una vez hayamos completado todos los pasos, nuestra página web de Apache debería de ocultar la versión de Apache y muchos otros datos.

Para comprobar que funcione todo correcto podemos probar los siguientes comandos:

`curl -I (ip: fjlr.ddns.net)`

```
C:\Users\Daen>curl -I fjlr.ddns.net
HTTP/1.1 200 OK
Date: Mon, 25 Nov 2024 19:00:45 GMT
Server: Hola
Last-Modified: Mon, 25 Nov 2024 18:12:49 GMT
ETag: "29af-627c0ae2534df"
Accept-Ranges: bytes
Content-Length: 10671
Vary: Accept-Encoding
Content-Type: text/html
```

`whatweb (ip:fjlr.ddns.net)`

```
fcojoaquin@manualapache:~$ whatweb fjlr.ddns.net
http://fjlr.ddns.net [200 OK] Country[SPAIN][ES], HTTPServer[Hola], IP
[87.222.14.114], Title[Apache2 Ubuntu Default Page: It works]
```

`nmap -sV (ip:fjlr.ddns.net)`

```
fcojoaquin@manualapache:~$ nmap -sV fjlr.ddns.net
Starting Nmap 7.80 ( https://nmap.org ) at 2024-11-25 20:04 CET
Stats: 0:00:58 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan
Service scan Timing: About 66.67% done; ETC: 20:05 (0:00:29 remaining)
Nmap scan report for fjlr.ddns.net (87.222.14.114)
Host is up (0.026s latency).
rDNS record for 87.222.14.114: 114.14.222.87.dynamic.jazztel.es
Not shown: 994 closed ports
PORT      STATE    SERVICE       VERSION
80/tcp    open     http          Hola
443/tcp   open     ssl/http      DD-WRT milli_httpd
```

Como es obvio para realizar estas comprobaciones necesitamos tener instalado las apt(nmap, curl & whatweb).

`sudo apt install (nmap, curl & whatweb)`

¡Muchas gracias por utilizar mi manual !