Listas de verificación de la configuración de seguridad recomendada

Esta sección contiene dos listas de verificación que usted puede usar como referencia rápida para ver si usted usa nuestra configuración de seguridad recomendada. Puede encontrar información adicional sobre cada una de estas opciones de configuración en este set de documentos.

La lista de verificación de Tweak Settings

Esta lista de verificación corresponde con la interfaz de *Tweak Settings* de WHM. Puede acceder la interfaz Tweak Settings bajo *Home >> Server Configuration >> Tweak Settings*.

Configuración	Recomendación
Enable HTTP Authentication – Activar autenticación de HTTP Desactivar esta opción activa la autenticación de cookies, lo que les ayuda a prevenir algunos tipos de ataques XSRF.	**Off**
Cookie IP Validation – Validación de IP con *cookies* Activar esta opción limita la habilidad de los atacantes que capturan las *cookies* de sesiones de cPanel y tratan de acceder las interfaces de cPanel & WHM. Para que esta configuración funcione mejor, también debe desactivar los dominios intermediarios (*proxy*).	**On**
Proxy Subdomain Creation – Crear subdominios intermediarios Desactivar esta opción evita que cPanel, webmail, el disco de web y las entradas DNS de subdominio intermediario de WHM se añadan a las cuentas nuevas.	**Off**
Require SSL – Requerir SSL Activar esta opción requiere entradas desde ubicaciones remotas para usar SSL.	**On**
Security Tokens – *Tokens* de seguridad Activar esta opción requiere que los *tokens* de seguridad se usen para acceder cualquier interfaz asociada con cPanel & WHM. Esto ayuda a prevenir ataques XSRF.	**On**
Block Common Domains Usage – Bloquear dominios comunes Activar esta opción previene a los usuarios de añadir o aparcar dominios de Internet comunes, como `hotmail.com` o `google.com`.	**On**
Initial default/catch-all forwarder destination – Destino del reenviador predeterminado/_catch-all_ inicial Seleccionar **Bounce** para esta opción causa que el servidor descarte automáticamente los correos electrónicos no enrutables enviados a las cuentas nuevas de su servidor. Esta es la mejor opción para proteger su servidor contra ataques de correo.	**Bounce**

La lista de verificación de Security Center

Usted puede acceder las características de *Security Center* de WHM bajo *Main >> Security Center*. Muchas de estas características le ayudarán a asegurar su servidor.

Configuración	Recomendación
Password Strength Configuration – Configuración de la fortaleza de contraseña Esta característica le permite especificar una fortaleza mínima de contraseña para cuentas alojadas por su servidor.	**Valor de 50 o más.**
PHP open_basedir Tweak – El ajuste de PHP open_basedir Activar esta opción les requiere a los usuarios especificar manualmente la configuración `open_basdir` en sus archivos `php.ini` pertinentes si se configura PHP para correr como un proceso CGI, SuPHP o FastCGI.	**Enabled**
Apache mod_userdir Tweak – El ajuste de Apache mod_userdir Activar esta opción les previene a los usuarios evadir los límites de banda ancha al acceder sus sitios con una tilde (~), nombre de usuario y nombre de anfitrión (*hostname*) (por ejemplo, `http://ejemplo.com/~usuario`).	**Enabled**
Compiler Access – Acceso al compilador Desactivar acceso al compilador para usuarios no especificados le ayudará a prevenir ataques en su servidor.	**Disabled**

Manage Wheel Group Users – Administrar usuarios del *Wheel Group* Esta característica le permite definir los usuarios que pueden usar el comando `su` para convertirse en el usuario *root*.	**Elimine todos los usuarios excepto por root y su cuenta principal.**
Shell Fork Bomb Protection – Protección contra *Shell Fork Bomb* Activar esta opción les previene a los usuarios con acceso de terminal usar todos los recursos en el servidor. **¡Ojo!:** Activar esta opción puede causar problemas de escasez de recursos y esta configuración limita fuertemente varios recursos.	**Enabled**
FTP Configuration – Configuración de FTP	**Disable Anonymous FTP**
Manage Shell Access – Administrar acceso *shell*	**Desactive el acceso shell para todos los otros usuarios.**
cPHulk Brute Force Protection – Protección contra fuerza bruta de cPHulk Si usted activa esta opción, usted debe añadir múltiples IP de confianza con la pestaña *White/Black List Management*. Esto evitará de que usted quede bloqueado si alguien trata un ataque de fuerza bruta contra su servidor.	**Enabled**

Desactivar la salida de identificación para Apache

1. Entre a WHM y acceda la característica *Apache Global Configuration* (bajo *Main >> Service Configuration >> Apache Configuration >> Global Configuration*).
2. Seleccione *Off (PCI Recommended)* del menú desplegable *ServerSignature*.
3. Pulse *Save* para guardar.

Configuración de EasyApache

Cuando usted configura EasyApache, usted debe incluir los siguientes módulos:

- **suPHP** — Este módulo causará que los *scripts* de PHP corran como el usuario que es propietario del *script* en vez del usuario de sistema conocido como **nobody**.
- **Suhosin** — Este módulo es un sistema avanzado de protección para instalaciones de PHP. Obtenga más información en la página de Suhosin (en inglés).
- **mod_security** — Este módulo es un cortafuegos para aplicación de web de fuente abierta. Lea más en modsecurity.org (en inglés). También puede leer nuestro mensaje en el foro sobre mod_security (en inglés).

Para más información, lea nuestra documentación de EasyApache (en inglés).