5 Configuraciones De cPanel Esenciales Para Principiantes

cPanel es el líder en el panel de administración para los servicios de alojamiento web. El principal producto de **WHM/cPanel** ha sido utilizado por la mayoría de los proveedores de alojamiento web, debido a su flexibilidad y porque es fácil de administrar, personalizar y por el soporte de gran calidad.

La mayoría de quienes están involucrados en la industria de alojamiento web han oído hablar de lo que puede hacer. Si eres nuevo en cPanel, sin embargo, hay algunas cosas que le recomendamos que debe hacer durante la fase inicial. Destacamos 5 configuraciones de cPanel, recomendadas para aquellos usuarios que comiencen en el mundo de la administración de servicios web.

1. Obtener una contraseña segura

Cada usuario de forma predeterminada recibirá un nombre de usuario y contraseña para entrar en la interfaz del cPanel. El mismo nombre de usuario se aplica al usuario por defecto a la **base de datos mysql**, **cuenta FTP**, **correo electrónico** y **conexión del usuario al sistema**, que se puede utilizar para acceder al

servidor de forma remota utilizando **SSH** (si el administrador del servidor permite esta función).

El cambio de la contraseña de acceso al cPanel, es una primera acción crítica. Si alguien es capaz de recuperar o adivinar su contraseña, van a obtener todos los privilegios en el servidor, lo cual es peligroso.

Hay algunos casos en los que la cuenta de correo electrónico registrada de un usuario válido ha sido hackeada y tomada por un hacker. Dentro de la bandeja de entrada de correo electrónico era la credencial de inicio de sesión para su cuenta de cPanel. Cuando el dueño quería restablecer la contraseña (que había sido cambiado por el hacker), tuvo que ponerse en contacto con el proveedor de alojamiento web. El problema, es que tenía que utilizar la dirección de correo electrónico registrada para la verificación de que el titular de la cuenta, nada se puede hacer.

Una buena práctica para la contraseña debe aplicarse para evitar este tipo de problemas. Algunos consejos para la gestión de contraseñas:

- Cambie su contraseña con frecuencia
- Evite palabras de diccionario
- Evite los objetos familiares como fecha de nacimiento, número de matrícula del vehículo o el número de teléfono
- Use una combinación de letras, números y símbolos
- Utilice más de 8 caracteres
- No «recordar» la contraseña en el navegador

2. Comprender el entorno de servidor

Asegúrese de entender completamente el entorno del servidor antes de su uso. Algunas cosas importantes que usted necesita saber, es que sistema operativo tiene el servidor y la arquitectura, la versión del kernel, aplicaciones (***cpanel, apache, php, mysql, perl***), versión, dirección IP y caracteristicas del paquete de hosting. Usted puede obtener esta información en la página principal, que por lo general aparece en la barra lateral de la interfaz de cPanel. Un servidor de hosting bueno debe ejecutarse en la versión actualizada del kernel y las aplicaciones bajo arquitectura de 64 bits (x86_64).

El usuario cPanel también debe comprobar el estado del servicio cPanel (Panel > Stats > Service Status). Puedes saber cuántas tareas CPU se ejecutan en el servidor, el uso de memoria total y también el estado de espacio en disco de aquí. La inspección de esta función le dará más información sobre el estado en tiempo real del servidor. Asegúrese de que todos los servicios están funcionando como esperaba. Un servidor estable debería funcionar a menos del 80% del uso del disco y el 10% del intercambio, el promedio de carga del servidor debe ser inferior a 2 veces el número total de CPU.

3. Compruebe permisos (archivos y directorios)

Los usuarios de cPanel por defecto tendrán un directorio en **/home/{nombre de usuario}**. Todos los archivos y directorios bajo el directorio personal del usuario se debe ejecutar en el respectivo permisos y la propiedad. El directorio más importante que se debe ejecutar en permisos y la propiedad correcta es **public_html**. Pero, antes de proceder con la verificación, usted debe saber cómo se maneja PHP en el servidor de cPanel.

Crear una página phpinfo bajo public_html. Acceda a la página a través del navegador y compruebe el valor de «API Server».

Si el valor CGI / FastCGI, entonces el controlador de PHP es, ya sea suPHP, FastCGI o CGI. La mayoría de proveedores de alojamiento web utiliza suPHP debido a la verificación de la seguridad y por ser el manejador por defecto para los servidores que ejecutan cPanel. En este controlador, PHP ejecuta como un proceso diferente al lado de Apache. Todo permiso de archivo se debe ejecutar en 644, y el permiso de directorio, bajo 755. Para Permisos más altos que esto se

traducirá en «Internal Server Error» cuando se ejecuta el script PHP.

Si el valor es Apache 2.0 Handler, entonces usted está ejecutando PHP bajo DSO. Este controlador no requiere permisos de archivo estrictos y de propiedad, porque el archivo PHP esta totalmente a cargo de Apache. Sin embargo, todavía se recomienda tener la misma práctica de permisos como se aconseja en el método CGI / FastCGI.

Usted puede utilizar el Administrador de archivos de cPanel, cliente FTP o acceso SSH (si está permitido) para fijar el permiso y la cuestión de la propiedad. No olvide borrar la página phpinfo después de la información que desea recuperar.

4. Añadir un poco de protección

A pesar de que la protección y la seguridad es totalmente bajo la responsabilidad administrador del servidor, los usuarios de cPanel pueden hacer uso de las flexibilidades cPanel en añadir algún tipo de protección de su sitio web, dominio y cuenta de cPanel.

Asegúrese de que el servicio spam Assassin (cPanel > Mail >

Spam Assassin) está activado. Algunos proveedores de alojamiento web no activan esta opción por defecto, porque el dominio recién registrado, por lo general, no reciben muchos mensajes de spam. Deseche todo el correo electrónico sin enrutamiento bajo la dirección predeterminada (cPanel> Correo> Default Address) con el error al remitente en el momento de SMTP. No utilice el «blackhole» o «forward to email address» a menos que realmente lo necesite. Los hackers pueden aprovechar estas 2 funciones para crear un ataque DOS para el servicio SMTP.

Desactivar Frontpage si no se utiliza (cPanel> Avanzado> Extensiones de FrontPage). Microsoft ha descontinuado el soporte de extensión de FrontPage para la plataforma Unix y recientemente muchos proveedores de alojamiento web habían observado intentos de intrusión a través de graves vulnerabilidades de FrontPage.

Compruebe disabled_function PHP usando la página phpinfo. Asegúrese de que todas las funciones críticas se han deshabilitado en el servidor. Si no es así, cree un archivo php.ini bajo public_html y agregue la siguiente línea:

disable_functions=exec, passthru, shell_exec,system, proc_open, popen, curl_exec, curl_m ulti_exec, parse_ini_file, show_source

Activación de la protección hotlink (**cPanel> Seguridad> Protección Hotlink**) para evitar que otros roben su ancho de banda. Las personas sólo pueden vincular sus imagenes a sus sitios web, por lo que es parte de su contenido. Sólo permita que su sitio web acceda a los contenidos estáticos como. Jpg,. Jpeg,. Gif,. Png y. Bmp.

5. Notificación y Monitoreo

Es necesario poner un correo electrónico alternativo para recibir una notificación por cPanel. De forma predeterminada, el correo electrónico registrado del usuario siempre será el contacto principal. Bajo actualización de Contacto (cPanel> Preferencias> Actualizar información de contacto), añadir un correo electrónico alternativo como respaldo en caso de que no tenga acceso a el correo electrónico principal.

Suscríbete a las herramientas de seguimiento disponibles en línea para monitorear su sitio web y la disponibilidad del dominio. A pesar de que algunos proveedores de alojamiento web ofrecen este servicio de forma gratuita, puede que tenga que tener otro punto de control externo para obtener resultados más precisos. Asegúrese de configurar el sistema de control para activar y enviar alertas a su correo electrónico para que reciba notificaciones de inmediato.