3 Sencillos Pasos Para Proteger Una Página Web De Los Hackers

Como **webmaster**, es una pesadilla total enfrentar la vulneración de un sitio web que este bajo nuestra administración. La idea básica es realizar copias de seguridad periódicamente para que puedas respaldar en el momento indicado, pero sin duda, esto es una tediosa tarea.

Actualmente existen **herramientas que pueden ayudar** a saber el hosting a cualquier persona, las tecnología web que usa, el CMS y datos de este. Para evitar vulneraciones en un sitio web, te compartimos 3 útiles **consejos para proteger una página web**.

1. Mantenga Las Plataformas Y Scripts Actualizados

Hoy en día se ha convertido algo común las vulnerabilidades en el mundo de la web. Estos fallos de seguridad son usados por atacantes informáticos para poder tomar el control de la web, y muchas veces esto se evita con algo tan sencillo como una actualización ;)

Como ejemplo, si estas usando WordPress en tu sitio web, y con el algunos plugins, tu web puede ser vulnerada ya sea por el fallo del CMS o de los plugins. Tener siempre las últimas versiones de tu CMS y los scripts instalados minimiza el

riesgo de que suceda un hackeo.

2. Instala Plugins De Seguridad, Cuando Sea Necesario

Una vez más, tomaré como ejemplo el **CMS WordPress**, lo hago, ya que este es uno de los gestores de contenido mas populares actualmente. En los CMS puedes encontrar útiles **plugins para mejorar la seguridad** de los sitios web, como lo es iThemes Security.

Si estás desarrollando un sitio en HTML, de seguro SiteLock te será de gran utilidad. SiteLock va más allá del simple bloqueo, brinda monitoreo diario para todo, desde la detección de malware a la identificación de la vulnerabilidad de análisis de virus activo y más.

3. Permisos Adecuados De Archivos Y Directorios

En el **sistema operativo Linux**, los permisos se pueden ver como un código de tres dígitos y cada dígito es un número entero entre el 0 y 7. El primer dígito representa los **permisos para el propietario del archivo**, el segundo dígito representa los **permisos para cualquier persona asignada al grupo al que pertenece el archivo**, y el tercer dígito representa los **permisos para todos los demás**. Las asignaciones funcionan de la siguiente manera:

- 4 es igual a Leer
- 2 es igual Escribir
- 1 es igual Ejecutar
- 0 es igual a no permisos para ese usuario

A modo de ejemplo, tomar el código de autorización «644.» En este caso, un «6» (o «4 + 2») en la primera posición da el propietario del archivo la capacidad de leer y escribir en el archivo. El «4» en la segunda y tercera posiciones significa que tanto los usuarios de grupos y usuarios de Internet en general pueden leer el archivo sólo, con esto se protege el archivo de manipulaciones inesperadas.

Una buena regla de oro para establecer los permisos, es de la siguiente manera:

- Carpetas y directorios = 755
- Archivos individuales = 644