SERVICIO WORDPRESS SAFE

WP-SAFE

SERVICIO DE SEGURIDAD, PROTECCIÓN Y MONITOREO PARA WORDPRESS

TECNOVAN LATAM PERU
del Grupo Araya & Cía.

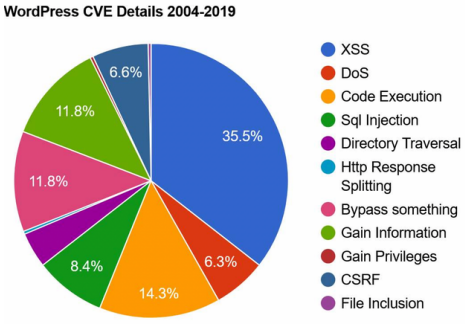
WORDPRESS, EL GESTOR DE CONTENIDOS MÁS UTILIZADO

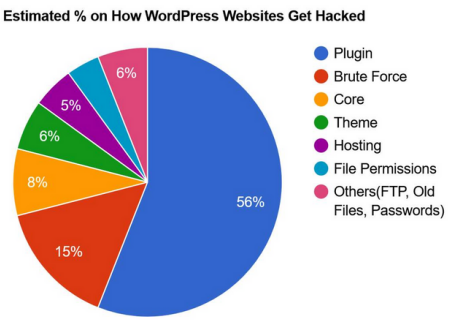
POR QUÉ SE DEBEN PROTEGER LOS SITIOS EN PLATAFORMAS WORDPRESS

El ser el gestor de contenidos más utilizado a nivel mundial, conlleva también riesgos, Wordpress es el que más ataques recibe, por lo que se requiere de configuraciones adicionales para mejorar su seguridad.
Por otra parte, este gestor de contenidos, consta de diferentes elementos, que deben ser actualizados en forma independiente, lo que hace más complicada su correcta administración.
A su vez, muchos de los plugins utilizados para su funcionamiento, son desarrollados por distintas empresas o personas, las cuales tienen distintos estándares de seguridad y desarrollo, por lo que generalmente se pierde el control de los mismos.
Si no se tiene una correcta y controlada administración de Wordpress, como cualquier software, puede aparecer una vulnerabilidad de día cero que ponga en riesgo la seguridad o la integridad del sitio.
Todo lo expuesto con anterioridad provoca lo que varios estudios demuestran, que entre el 95% y el 98% de los sitios en Wordpress son vulnerables.
Los sitios en Wordpress son seguros como cualquier otra plataforma, siempre que se tomen las medidas correctas para su seguridad.

¿QUÉ TIPO DE ATAQUE PODRÍA RECIBIR MI SITIO EN WORDPRESS?

A continuación, describimos algunos tipos de ataques de los cuales su sitio podría ser víctima si es que no toma los debidos resguardos:





Authentication Bypass: Agujero de seguridad que permite saltarse el formulario de acceso y acceder al sitio.
Fuerza Bruta: Se intenta iniciar sesión adivinando el nombre de usuario y la contraseña de la cuenta de administrador (o de un usuario).
Cross-Site Request Forgery (CSRF): El código se introduce y ejecuta desde la URL.
Cross-site Scripting (XSS): Se puede inyectar código en un sitio, normalmente a través de un campo de formulario.
Denial of Service (DoS): Ataque con constante de tráfico y que suele proceder de una red de máquinas controladas.
Distributed Denial of Service (DDoS): Similar a un ataque DoS, excepto que el ataque proviene desde muchos atacantes.
Path Traversal: Posibilidad de listar los directorios de un sitio y ejecutar comandos fuera del directorio raíz del servidor.
File Upload: Se puede subir un fichero con código malicioso en un servidor sin restricciones.
Full Path Disclosure (FPD): Se expone la ruta de acceso a la carpeta raíz del sitio; habitualmente es debido a que están activos los mensajes de error que las muestran.
Local File Inclusion (LFI): Un atacante es capaz de controlar qué archivo se ejecuta en una hora programada que fue configurada anteriormente.
Open Redirect: El sitio redirige a otro debido a alguna vulnerabilidad, a menudo un sitio de spam o de suplantación de identidad.
Remote Code Execution (RCE): Capacidad de ejecutar código en un sitio desde una máquina diferente.
Remote File Inclusion (RFI): Posibilidad de ejecutar un script externo en un sitio al que se suele cargar malware, desde un sitio diferente.
Security Bypass: Similar al Authentication Bypass, pero en este caso permite saltarse algún sistema de seguridad establecido.
Server-side Request Forgery (SSRF): Toma de control de un servidor, ya sea parcial o total, para obligarlo a ejecutar peticiones de forma remota.
Inyección SQL (SQLI): Se produce cuando se pueden hacer consultas SQL desde el sitio web.
Enumeración de usuarios: Posibilidad de encontrar la lista de usuarios de un sitio desde la zona pública, para posteriormente realizar un ataque de Fuerza Bruta.
XML External Entity (XXE): Un fichero XML que por la generación de errores deja expuesto algún tipo de ruta, mensaje o acceso a información confidencial.

QUÉ CONTEMPLA NUESTRO SERVICIO

CARACTERÍSTICAS DEL SERVICIO

Nuestro servicio permite conocer el nivel de seguridad de su página web y mejorarlo evitando los riesgos que podrían afectar su reputación corporativa e incluso su operación comercial on line. Este servicio contempla lo siguiente:

- Actualizaciones de plugins.
- Actualizaciones de Wordpress.
- Configuración de seguridad.
- Recomendaciones de seguridad.
- Análisis de seguridad inicial para el servidor.
- Monitoreo 24X7.
- Detección y notificación ante ataques críticos.
- Informes mensuales.
- Informes ante eventos críticos.
- Respaldos diarios de la configuración de Wordpress.
- Monitoreo Uptime y de recursos de Hardware.

FIREWALL DE APLICACIONES WEB

Nuestro servicio también contempla un Firewall de aplicaciones web especializado para ser utilizado en Wordpress con protección de WordPress y todos sus subdirectorios. Sus características son:

- Escaneo de malware incluyendo escaneos programados.
- El escaneo incluye una variedad de otros controles, incluidos los controles de la lista negra.
- Protección contra ataques de fuerza bruta.
- Autenticación de dos factores.
- Bloqueo por país de origen.
- Bloqueos por IPs•
- Protección contra rastreadores agresivos.
-

Una vez que se configura, cualquier solicitud que llegue, sin importar a qué archivo PHP intente acceder, primero será procesada por la solución para verificar si es segura o no.
El firewall de WordPress ejecutará la solicitud a través de su conjunto de reglas, realizando un análisis detallado de alto rendimiento y tomará la decisión de bloquear la solicitud o permitirla.El código de firewall que toma esta decisión se
ejecuta antes que cualquier otra cosa, incluido WordPress. Eso significa que el código de WordPress no se ha cargado y la base de datos aún no está conectada. Esto hace que el código del cortafuegos de la solución sea increíblemente rápido . Podemos bloquear una solicitud maliciosa incluso antes de que se conecte a su base de datos y antes de que se cargue el voluminoso código de WordPress y el entorno API.

ALCANCES DEL SERVICIO

- El servicio no incluye la administración ni la operación de Wordpress.
- Hay actualizaciones que requieren de la confirmación del administrador del sitio para ser realizadas.
- Las normas, políticas, procedimientos y metodologías generadas como producto de esta consultoría son de carácter confidencial y de exclusiva propiedad del cliente.

ACERCA DE TECNOVAN LATAM PERÚ

QUIENES SOMOS

TECNOVAN LATAM PERÚ, es el resultado de la alianza de dos grupos empresariales con basta experiencia en sus respectivas áreas y con una fuerte orientación a entregar servicios de excelencia.

TECNOVAN LATAM se formó en Chile con el firme propósito de ser un aporte para nuestros clientes, entregando Soluciones TI de vanguardia junto a un equipo humano con un alto grado de compromiso hacia los servicios y en constante perfeccionamiento.

Su foco principal en ciberseguridad y siempre en búsqueda de nuevas tendencias e innovación para dar solución a las actuales problemáticas y los posibles futuros riesgos. Su equipo de profesionales multi disciplinario con amplia experiencia en el área TI y especialmente en ciberseguridad, buscan brindar al cliente un servicio de excelencia, logrando relaciones de largo plazo con nuestros clientes.

Por otra parte, ARAYA & CÍA. ABOGADOS , fundado en el 2004, es un estudio jurídico destacado por brindar asesoramiento especializado en el ámbito corporativo y de comercio internacional posicionándose como líderes en Chile y Perú. Respaldados por su reconocida experiencia y amplia trayectoria, prestan servicios en diversas áreas del derecho empresarial asesorando y representando a clientes nacionales y extranjeros en los negocios e inversiones que realizan.

El estudio está integrado por profesionales con un alto nivel de especialización y conocimiento profundo de los sectores económicos en los que se desenvuelven, lo cual les permite garantizar a sus clientes un servicio integral de primer nivel en todos los aspectos relacionados con los diferentes rubros de sus negocios.

En búsqueda de contribuir de forma activa al desarrollo del mercado de soluciones y servicios de ciberseguridad en Perú, ambas empresas unieron fuerzas y conocimientos para entregarles servicios y soluciones de vanguardia, apoyados por un equipo de profesionales de excelencia en constante desarrollo para enfrentar el dinámico mundo de las ciber amenazas y con una fuerte vocación hacia el servicio de excelencia.

Tecnovan Latam Perú : Av. Armendáriz 424 piso 4, oficina 401, Miraflores.
Lima, Perú.
Fono:(511) 270-7449 (511) 683-2938
Email contacto@tecnovan.com

WWW.TECNOVAN.COM