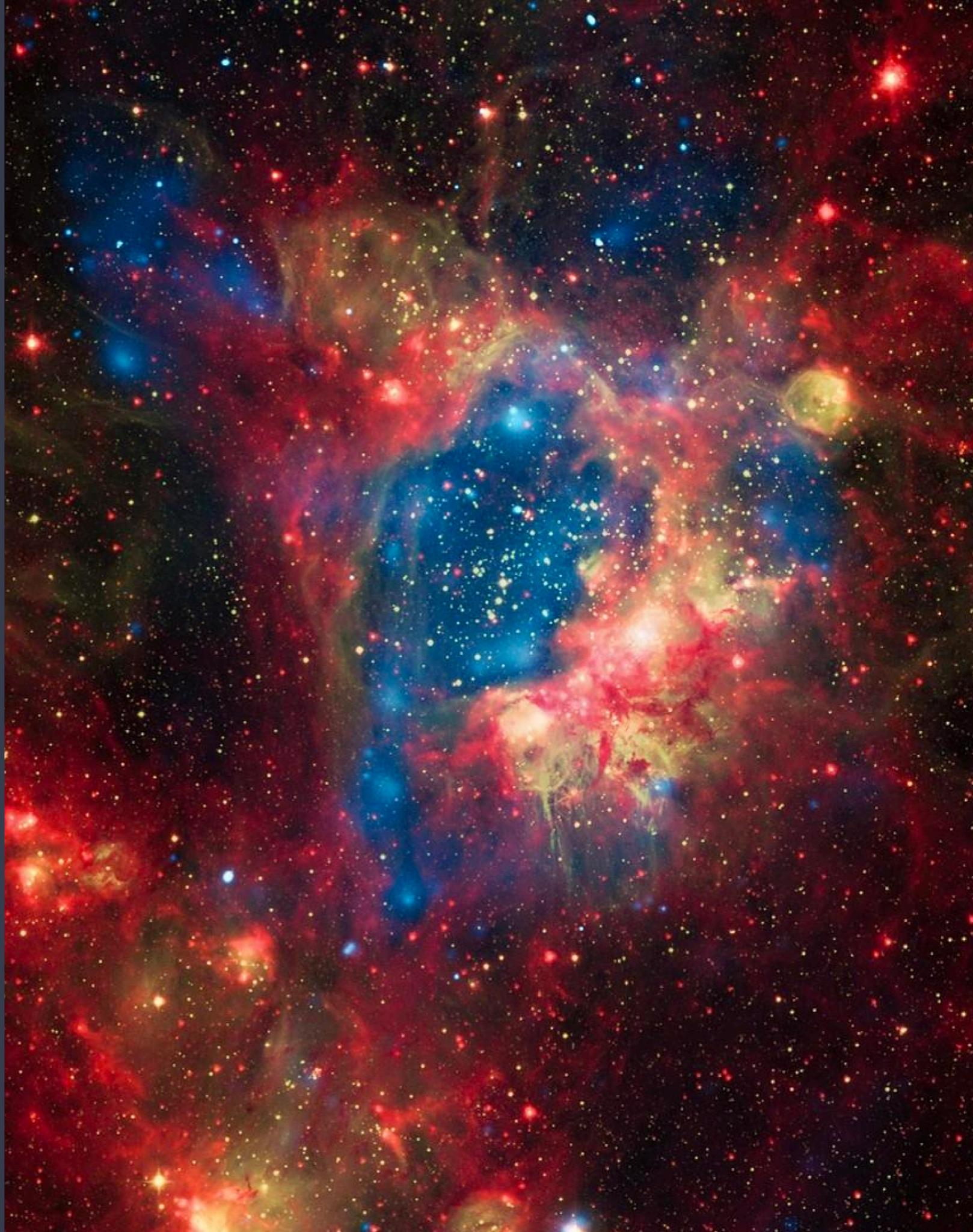


White Jaguars ®

GUÍA DE SEGURIDAD PARA WORDPRESS

Lo que debe saber para proteger
su sitio contra ciber ataques



CONTENIDO

- **Introducción**
- **Perímetro**
- **Sistema Operativo**
- **Servidor Web**
- **Servidor de Aplicación**
- **Wordpress**
- **Base de Datos**

White Jaguars Cyber Security ha creado este material gratuito con la finalidad de promover las prácticas de seguridad en las plataformas web de forma abierta y al alcance de todos.

El contenido de esta guía debe ser considerado como el punto de partida y no busca ser una guía exhaustiva o extensiva debido a que la tecnología cambia constantemente, lo cual podría dejar sin efecto algunas de las recomendaciones emitidas como parte de este contenido.

Esperamos que la guía le sea de utilidad y siéntase en la libertad de compartir este documento siempre y cuando sea de forma gratuita y conservando los créditos de autoría pertenecientes a WhiteJaguars ® Cyber Security.

INTRODUCCIÓN

34%



34% de los sitios web en internet utilizan Wordpress, hablamos de millones de servidores, lo cual resulta ser muy atractivo desde el punto de vista de un delincuente informático. Podemos decir que entre más visibilidad tenga una plataforma, más interés va a tener por parte de delincuentes, de la misma forma que ocurre con el sistema operativo Windows de Microsoft.

No es de sorprenderse entonces que el **83%** de los sitios web comprometidos utilizan Wordpress, muy por encima de otras plataformas CMS o eCommerce.

De hecho, hasta la fecha se han reportado más de

14900 vulnerabilidades

en Wordpress incluyendo su núcleo, plugins y temas.

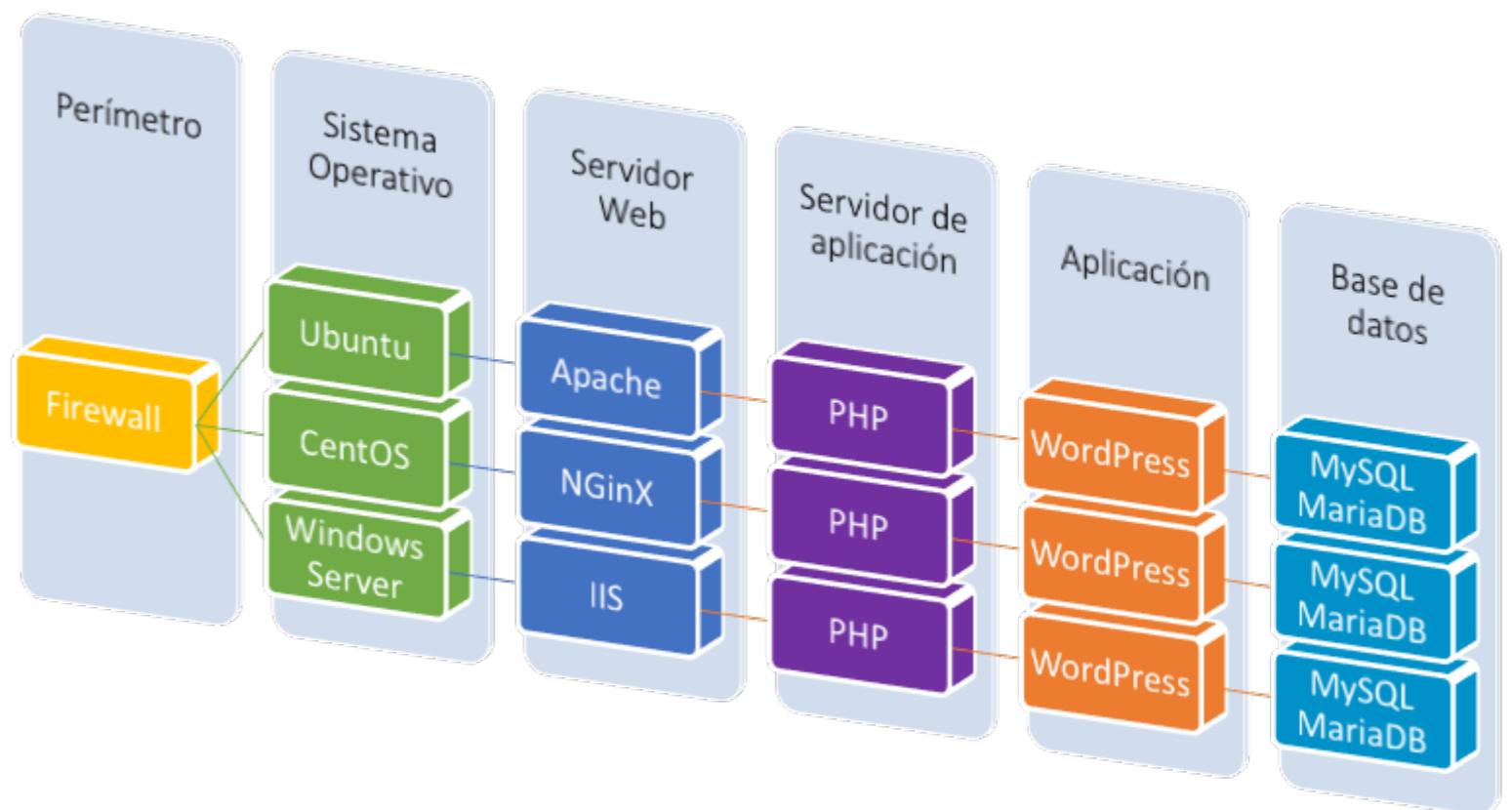
De las vulnerabilidades mencionadas, curiosamente, más del **55%** corresponde a plugins, siendo el vector de ataque más explotado.

SEGURIDAD BASADA EN CAPAS

La primera recomendación que se puede dar es que la seguridad se debe aplicar por capas. El camino de un atacante debe atravesar múltiples mecanismos antes de llegar a las aplicaciones o lo que es más importante, a las bases de datos donde se encuentra la información que se busca extraer.

Esta guía esta compuesta por diferentes capas, las cuales podrían en la mayoría de los casos, corresponder a diferentes personas responsables, departamentos o inclusive proveedores de servicios, lo más importante es que usted conozca las medidas que se pueden aplicar en cada capa para que pueda ser vigilante de las buenas prácticas que se deben dar en su sitio web.

La buena noticia es que estos mismos principios son aplicables a cualquier plataforma web.



PERÍMETRO

- Introducción
- Perímetro
- Sistema Operativo
- Servidor Web
- Servidor de Aplicación
- Wordpress
- Base de Datos

El perímetro es toda la superficie que es externa a su propiedad, al igual que su casa esta rodeada por un muro que la separa del dominio público, el perímetro expuesto en internet es esa superficie que usuarios buenos y malos pueden acceder.

FIREWALL

Los muros de fuego son los encargados de controlar el tráfico que ingresa a su infraestructura, para un servidor web, solo deberían exponerse los puertos de comunicación 80 y 443 con el protocolo de transporte TCP.

FIREWALL DE CAPA DE APLICACIÓN (WAF)

Los Firewall tradicionales se encargan de regular el transporte sin analizar el contenido de la información, de forma similar a un policía de tránsito que se preocupa porque las reglas viales se cumplan. Los Firewall de capa de aplicación realizan una inspección más detallada, siendo capaces de analizar los datos para detectar y bloquear patrones conocidos como maliciosos.

PROTECCIÓN CONTRA DDOS

Algunos fabricantes de WAF también ofrecen servicios de protección contra ataques de denegación de servicio (DoS), estos ataques buscan enviar a los servidores, mas solicitudes de las que son capaces de responder, con lo cual el servicio de respuesta a solicitudes reales se ve interrumpido perjudicando la disponibilidad del sitio web. En casos más agresivos, los ataques provienen desde muchos puntos diferentes, lo cual es conocido como ataques distribuidos de denegación de servicios (DDoS).

SISTEMA OPERATIVO

- Introducción
- Perímetro
- Sistema Operativo
- Servidor Web
- Servidor de Aplicación
- Wordpress
- Base de Datos

Las siguientes recomendaciones aplican para todos los diferentes tipos de sistema operativo.

FIREWALL LOCAL

Todos los sistemas operativos posee muros de fuego que se pueden habilitar localmente en el servidor, es importante configurarlos correctamente no solo para el tráfico entrante, también se debe considerar el tráfico saliente donde se permite únicamente los servicios mínimos necesarios para el funcionamiento correcto del servicio.

ACTUALIZACIONES Y PARCHES DE SEGURIDAD

Los fabricantes publican correcciones para vulnerabilidades detectadas de forma constante, es de suma importancia poseer un proceso para la instalación de actualizaciones de forma recurrente.

SISTEMA OPERATIVO

- Introducción
- Perímetro
- **Sistema Operativo**
- Servidor Web
- Servidor de Aplicación
- Wordpress
- Base de Datos

CONFIGURACIÓN

Lamentablemente algunos sistemas operativos no poseen configuraciones seguras de forma predeterminada, existen muchos aspectos que se deben considerar como la gestión de usuarios, contraseñas, privilegios y parámetros de configuración de servicios.

ENDURECIMIENTO (HARDENING)

Las guías de hardening o endurecimiento nos ayudan a tener un proceso repetible y documentado con todos los pasos requeridos al instalar un nuevo servidor, esto incluye tareas como deshabilitar servicios, remover herramientas inseguras o no utilizadas, habilitar protecciones, etc.

Estos procesos manuales han sido reemplazados por herramientas automatizadas de “Orquestación” que permiten aplicar “recetas” pre-configuradas donde ya se incluyen las prácticas de seguridad de forma automática, cada vez que un nuevo servidor o contenedor es puesto en funcionamiento.

SERVIDOR WEB

- Introducción
- Perímetro
- Sistema Operativo
- Servidor Web
- Servidor de Aplicación
- Wordpress
- Base de Datos

CIFRADO EN EL TRANSPORTE

Todos estamos familiarizados con el concepto general de que HTTPS significa que el sitio es seguro, aunque lamentablemente eso no es del todo cierto.

El uso de HTTP sobre un canal seguro (HTTPS) solamente garantiza que la información viaja de forma cifrada entre el navegador y el servidor, esto significa que si un servidor es comprometido, los ataques serán enviados a través de HTTPS porque no le corresponde a la capa de cifrado velar por la integridad o confiabilidad de los datos almacenados en el servidor.

SSL / TLS

Existen actualmente dos protocolos de transporte seguro de información, la capa de conectores seguros (Secure Socket Layer SSL) y la seguridad de capa de transporte (Transport Layer Security TLS), el navegador negociará el protocolo y algoritmo de cifrado a utilizar basándose en los que están disponibles en el servidor y los que son soportados por el navegador.

Lamentablemente algunas versiones de protocolos y algoritmos de cifrado han sido vulnerados por lo que parte de la tarea de protección es desactivar esas versiones inseguras en el servidor.

SERVIDOR WEB

- Introducción
- Perímetro
- Sistema Operativo
- Servidor Web
- Servidor de Aplicación
- Wordpress
- Base de Datos

CIFRADO EN EL TRANSPORTE

Reglas básicas para la protección en la capa de transporte de HTTP:

- Decidir si se debe utilizar HTTPS no esta en discusión, es obligatorio y actualmente los navegadores marcan los sitios que no lo utilizan como inseguros.
- A la hora de generar el certificado digital, asegúrese de que la llave sea como mínimo de 2048 bits de longitud.
- De momento solo el protocolo TLS 1.2 es considerado como seguro, esto significa que los protocolos TLS 1.3, TLS 1.1, SSL 3 y SSL 2 deben estar desactivados.
- Hay muchos algoritmos de cifrado que deben desactivarse y esto tienen tendencia a cambiar, se recomienda utilizar herramientas gratuitas como SSL Labs de Qualys para verificar la configuración cada cierto tiempo.
<https://www.ssllabs.com>

SERVIDOR WEB

- Introducción
- Perímetro
- Sistema Operativo
- Servidor Web
- Servidor de Aplicación
- Wordpress
- Base de Datos

ENCABEZADOS DE SEGURIDAD

Los encabezados de seguridad deben ser la línea base de la configuración de todo servidor web debido a que le evitará problemas innecesarios sobre las actividades de escaneo constante que es típica en internet, algunos ejemplos:

- **HSTS**: Strict Transport Security, indica a los navegadores que el sitio web debe accederse únicamente por HTTPS.
- **CSP**: Content Security Policy, establece reglas que restringen el acceso a recursos remotos junto con acciones de ejecución de código en el navegador.
- **CORS**: Cross Origin Resource Sharing, se utiliza para establecer niveles de confianza entre dominios diferentes.
- **X-Frame Options**: Limita el uso de iFrames debido a su vinculación con ataques de Clickjacking o Cross-Frame Scripting (XFS)
- **X-Content-Type-Options**: Protección contra el abuso de tipos MIME.
- **Cache-Control / Pragma**: Control de cache para protección de información de formularios.
- **Expires**: Expiración de contenido para formularios o contenido protegido.

APACHE

Es muy común encontrarse los sitios Wordpress utilizando el servidor web Apache, aquí una muestra de como configurar los encabezados de seguridad por medio de archivos .htaccess.

```
<IfModule mod_headers.c>
## CSP
Header set Content-Security-Policy: default-src 'self'; img-src 'self' https://i.imgur.com;
object-src 'none'; script-src 'self'; style-src 'self'; frame-ancestors 'self'; base-uri
'self'; form-action 'self';

## General Security Headers
Header set X-XSS-Protection: 1; mode=block
Header set Access-Control-Allow-Origin: http://www.one.site.com
Header set X-Frame-Options: deny
Header set X-Content-Type-Options: nosniff
Header set Strict-Transport-Security: max-age=3600; includeSubDomains

## Caching rules
# Don't cache by default
Header set Cache-Control no-cache
Header set Expires: 0

# Cache static assets for 1 day
<filesMatch ".(ico|css|js|gif|jpeg|jpg|png|svg|woff|ttf|eot)$">
  Header set Cache-Control "max-age=86400, public"
</filesMatch>
</IfModule>

<\IfModule mod_gzip>
<\IfModule mod_deflate>
  Header set Cache-Control "max-age=86400"
```

NGINX

En otros casos nos podemos encontrar Wordpress siendo accesible por medio de servidores web NginX, aquí una muestra de como configurar los encabezados de seguridad.

```
## CSP
add_header Content-Security-Policy: default-src 'self'; img-src 'self' https://i.imgur.com;
object-src 'none'; script-src 'self'; style-src 'self'; frame-ancestors 'self'; base-uri
'self'; form-action 'self';

## General Security Headers
add_header X-XSS-Protection: 1; mode=block;
add_header Access-Control-Allow-Origin: http://www.one.site.com;
add_header X-Frame-Options: deny;
add_header X-Content-Type-Options: nosniff;
add_header Strict-Transport-Security: max-age=3600; includeSubDomains;

## Caching rules # Don't cache by default
add_header Cache-Control no-cache;
add_header Expires: 0;

# Cache static assets for 1 day
location ~* \.(?:ico|css|js|gif|jpe?g|png|svg|woff|ttf|eot)$ {
    try_files $uri @rewriteapp;
    add_header Cache-Control "max-age=86400, public";
}

#qq-peaqei Cache-Control "max-age=86400" baptric
#rry-ttjeas snti rewriteapp;
location ~* \.(?:ico|css|js|gif|jpe?g|png|svg|woff|ttf|eot)$ {
    # Cache static assets for 1 day
}
```

SERVIDOR DE APLICACIÓN

- Introducción
- Perímetro
- Sistema Operativo
- Servidor Web
- Servidor de Aplicación
- Wordpress
- Base de Datos

PHP

Wordpress fue creado en el lenguaje PHP y como consecuencia, existen consideraciones que se deben tener en cuenta a la hora de instalar y configurar PHP.

ACTUALIZACIONES

Aunque suene trivial porque ya se menciono antes para el caso del sistema operativo, hay que tener en cuenta que PHP es el lenguaje más utilizado en el mundo de las aplicaciones web y es por eso que es el más atacado también, instalar las actualizaciones de forma semanal es de suma importancia para evitar que PHP sea el causante de una brecha de seguridad en su sitio.

PHP

La configuración de PHP debe realizarse teniendo consideraciones sobre las aplicaciones y los plugins utilizados por Wordpress, como regla base, se deben desactivar los módulos no utilizados, las funciones peligrosas y remover el encabezado **X-Powered-By** que divulga la versión de PHP instalada en el servidor.

Este es un ejemplo base que puede aplicar en su configuración:

```
## php.ini
expose_php = Off
enable_dl = Off
disable_functions = system, exec, shell_exec, passthru, phpinfo, show_source,
highlight_file, popen, proc_open, fopen_with_path, dbmopen, dbase_open, putenv,
move_uploaded_file, chdir, mkdir, rmdir, chmod, rename, filepro, filepro_rowcount,
filepro_retrieve, posix_mkfifo

disable_classes =

## Uploads
file_uploads = On
upload_tmp_dir = /path/PHP-uploads/
upload_max_filesize = 2M
max_file_uploads = 2

max_execution_time = 3
max_input_time = 30
max_input_size = \bafy\bfy-objosqas\
trtje-objosqas = On
```

WORDPRESS

- Introducción
- Perímetro
- Sistema Operativo
- Servidor Web
- Servidor de Aplicación
- **Wordpress**
- Base de Datos

ACTUALIZACIONES

Si para el caso de PHP la tarea de actualización es semanal, para Wordpress estamos hablando de un ejercicio diario debido a que usualmente se reportan vulnerabilidades por lo menos tres veces por semana.

Algunos aspectos importantes a tener en cuenta:

- Más de 14900 vulnerabilidades han sido reportadas en Wordpress, la gran mayoría en plugins.
- Se deben realizar respaldos automáticos no solo de la base de datos, debe tener una forma confiable para poder restaurar el sitio completo en caso de ataque debido a que es muy común que se reemplace el código de algunas secciones para injectar funciones maliciosas una vez que el sitio a sido comprometido.
- Actualice el núcleo de forma constante, las vulnerabilidades en el núcleo ya no son muy frecuentes pero cuando aparecen usualmente son de severidad Crítica.

WORDPRESS

- **Introducción**
- **Perímetro**
- **Sistema Operativo**
- **Servidor Web**
- **Servidor de Aplicación**
- **Wordpress**
- **Base de Datos**

TEMAS Y PLUGINS

El gran crecimiento que ha tenido Wordpress es gracias a la cantidad de plugins y temas que existen, esto a su vez posee un lado negativo debido a que es más difícil controlar la calidad y seguridad de los componentes hechos por la comunidad.

Algunos aspectos importantes a tener en cuenta:

- Remover los plugins y los temas que no se están utilizando reduce la posibilidad de ser afectado por vulnerabilidades descubiertas allí.
- En vista de que la mayoría de ataques provienen de los plugins, es de suma importancia seleccionar con cuidado los que se van a utilizar.
- Considere la reputación del desarrollador, que tan activo es el proyecto y las calificaciones dadas por la comunidad antes de instalar un plugin, crear una dependencia a un proyecto abandonado puede generarle dolores de cabeza si se llegará a necesitar la corrección de algún problema por parte del creador.
- Nuevamente, mantener los plugins actualizados diariamente.

WORDPRESS

- Introducción
- Perímetro
- Sistema Operativo
- Servidor Web
- Servidor de Aplicación
- Wordpress
- Base de Datos

PLUGINS DE SEGURIDAD

No todo son malas noticias alrededor de los plugins, por suerte existe una creciente tendencia a crear plugins dedicados a proteger su sitio, aquí una lista de algunos recomendados:

- Wordfence: Es probablemente el primer plugin de seguridad que debe tener habilitado en su sitio, posee versiones gratuitas y de pago e incluye muchas características indispensables para proteger su sitio, como por ejemplo el bloqueo de ataques por enumeración y la notificación de actualizaciones de seguridad.
<https://wordpress.org/plugins/wordfence/>
- Limitar la cantidad de intentos de login para prevenir los ataques por fuerza bruta
<https://wordpress.org/plugins/limit-login-attempts-reloaded/>
- Revisiones de configuración y scanner de malware
<https://wordpress.org/plugins/sucuri-scanner/>
- iThemes Security: Seguridad de temas
<https://wordpress.org/plugins/better-wp-security/>
- Google Authenticator para habilitar el segundo factor de autenticación
<https://wordpress.org/plugins/miniorange-2-factor-authentication/>
- Escaneos diarios de seguridad
<https://wordpress.org/plugins/wpscan/>

WORDPRESS

- Introducción
- Perímetro
- Sistema Operativo
- Servidor Web
- Servidor de Aplicación
- Wordpress
- Base de Datos

CONFIGURACIÓN

La configuración base de Wordpress es clave como el primer paso para toda nueva instalación, algunas recomendaciones son:

- Restringir el acceso a la consola de administración por medio de archivos **.htaccess** para el caso de Apache. Para cualquier atacante, la sección administrativa es la llamada a ejecutar ataques por fuerza bruta para intentar obtener acceso, esto no solo representa un riesgo para la administración del sitio, también ese tipo de ataques degradan el rendimiento del servidor considerablemente.
- Eliminar los archivos **readme.html** e **install.php**, ambos no se necesitan una vez que el sitio ya se encuentra en funcionamiento y contienen información valiosa desde el punto de vista de un atacante.
- Eliminar o cambiar el nombre del usuario **admin** predeterminado. Desde la perspectiva de un atacante, saber que el usuario predeterminado es "admin", ya representa el 50% del proceso de obtener acceso y se puede enfocar solo en la contraseña.
- Habilitar la protección contra enumeración con Wordfence y el segundo factor de autenticación con Google Authenticator.

BASE DE DATOS

- Introducción
- Perímetro
- Sistema Operativo
- Servidor Web
- Servidor de Aplicación
- Wordpress
- Base de Datos

RECOMENDACIONES

La base de datos es usualmente el objetivo principal de todo atacante, es por eso que se deben seguir muchas prácticas importantes con respecto a la protección de la información:

- Bajo ninguna circunstancia se debe compartir el mismo servidor para los servicios web y de bases de datos.
- Tampoco deben estar los servidores en el mismo segmento de red, idealmente el servidor web debe estar ubicado en una zona desmilitarizada que es la que posee acceso desde internet para servicios publicados, los servidores de bases de datos deben estar en segmentos privados resguardados por protecciones adicionales.
- No utilizar usuarios ni contraseñas fáciles de adivinar, esto aplica tanto para la plataforma misma de Wordpress como para el usuario utilizado para conexión de base de datos.
- Si existen múltiples aplicaciones utilizando el mismo servicio de base de datos, se deben utilizar usuarios separados para cada aplicación de manera que el ataque de una no pueda afectar a las demás.
- De igual forma, para cada usuario se deben delimitar y asignar los permisos mínimos requeridos para el funcionamiento de la aplicación.

White Jaguars ®

GUÍA DE SEGURIDAD PARA WORDPRESS

<https://www.whitejaguars.com>
info@whitejaguars.com
+506 2505-5402
Escazú, San José, Costa Rica

NOTAS FINALES

Como ya vimos existen muchos aspectos que se deben considerar en materia de seguridad para proteger los sitios Wordpress.

Usted mismo puede evaluar la seguridad de su sitio utilizando diferentes mecanismos gratuitos y comerciales aunque algunos clientes solicitan revisiones realizadas por terceros, aquí algunas opciones:

- WPScan que es una herramienta de línea de comandos gratuita.
- Existen escáneres comerciales especializados en seguridad para Wordpress, un ejemplo es Sucuri.
- Si su cliente le solicita evidencia o certificación de la seguridad del sitio, probablemente va a requerir de un tercero que realice una revisión no solo utilizando herramientas automatizadas, sino también aplicando pruebas de penetración manuales para verificar toda la seguridad de la infraestructura, a esto se le conoce como análisis de penetración o Pentest, y es una de las áreas en las que nos hemos especializado en WhiteJaguars.

De parte de WhiteJaguars esperamos que esta guía le sea de utilidad y en caso de cualquier duda nos puede contactar en el momento que guste.