VALENCIANAS POR EL MUNDO

Vacaciones de lujo en la playa

Ven con nosotras...

Cómo evitar que tu WordPress diga:

Diseño

Accesibilidad

Tipografía

Email marketing

Desarrollo

ADS

Servidores

Redes sociales

Podcasting

SEO

Analíticas

WPO

Los Clientes

Conocerlos es amarlos

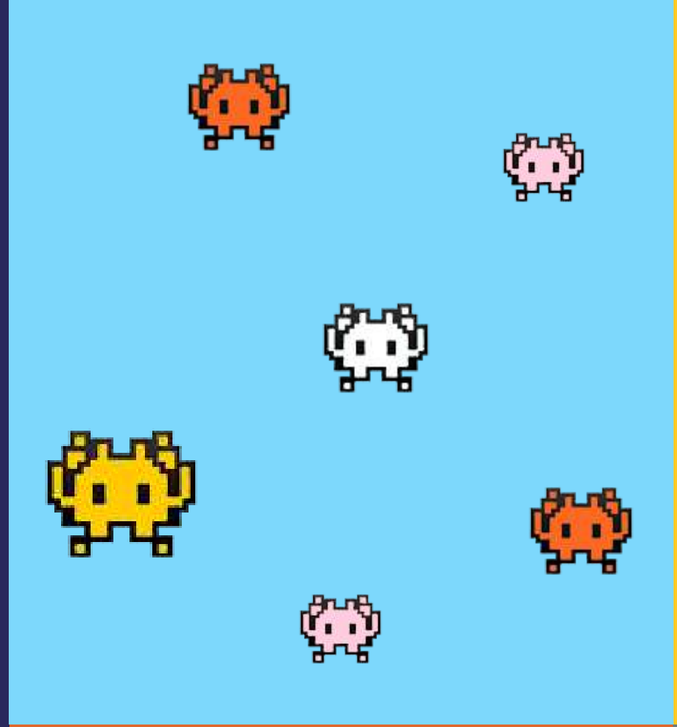
Twitter de Érica

Además está la SEGURIDAD

Que se nos olvida...

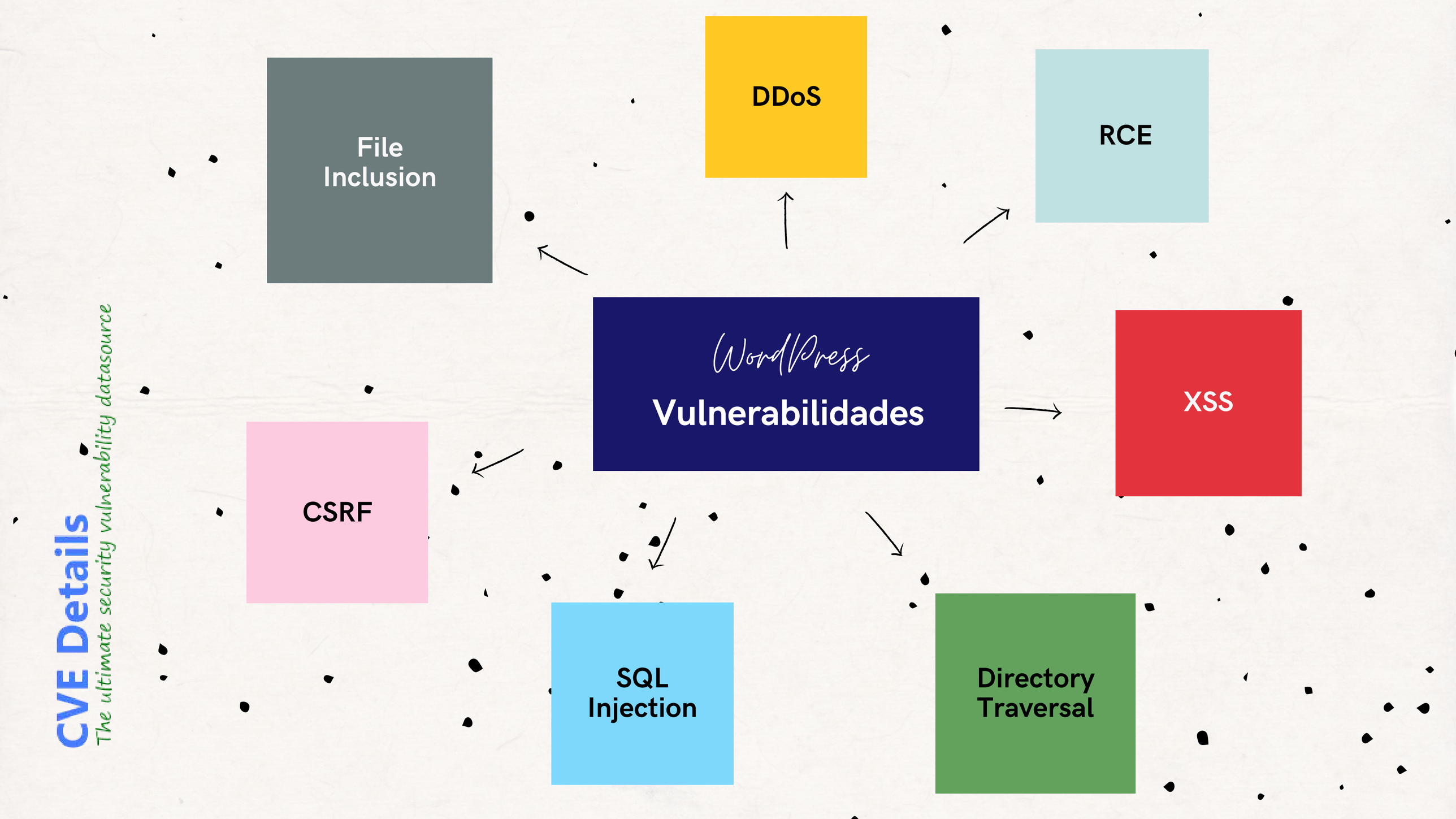
Por qué atacan a los sitios web con WP?

Respuesta "de cajón"...



Más webs

Más ataques


File Inclusion
DDoS
RCE
WordPress
Vulnerabilidades
XSS
CSRF
SQL Injection
Directory Traversal
CVE Details
The ultimate security vulnerability datasource

DDoS

Distributed Denial of Service (denegación de servicio distribuido).

Es un ataque que se lleva a cabo generando un gran flujo de información desde varios puntos de conexión hacia un mismo punto de destino, provocando la pérdida de conectividad por el elevado consumo de ancho de banda o por la sobrecarga de recursos.

La forma más común de realizar un DDoS es a través de una red de bots (botnet).

Cómo evitarlo

- **Bloquear XML-RCP**
- **Desactivar API Rest**
- **Limitar intentos de acceso**
- **Desactivar pinbacks**
- **Desactivar concatenación de scripts**
- **Activar WAF**

RCE

Remote Code Execution

La ejecución de código remoto se trata de una vulnerabilidad que permite la ejecución de código o comandos remotamente aprovechando un fallo en la programación o alguna función de PHP.

Cómo evitarlo

- **Actualizaciones al día**
- **Prohibir PHP en el directorio wp-includes**
- **Prohibir PHP en el directorio wp-content/uploads**
- **Desactivar la ejecución de PHP en directorios de la caché**
- **Desactivar lenguajes de scripting no usados (Python, perl, etc...)**
- **Bloquear análisis author**
- **Firewall**

XSS

Los ataques XSS también llamados en inglés Cross-site scripting son un tipo de ataque que aprovecha vulnerabilidades en el código que permitirían a una tercera persona inyectar, en páginas web visitadas por el usuario, código JavaScript no autorizado y ejecutarlo.

El script malicioso se podría ejecutar almacenándolo en el servidor o directamente en el lado del usuario en el navegador.

Cómo evitarlo

- **Cookies de sesión con HTTPOnly y Secure Flag**
- **Desactivar/limitar cabecera HTTP X-Frame-Options**
- **Encabezado HTTP seguros, como Content Security Policy (CSP)**
- **Desactivar el HTTP TRACE / TRACK**
- **Firewall**

Directory Traversal

Los ataques por cruce de directorios son un ataque HTTP que permite a un atacante aprovechar una vulnerabilidad en el recorrido de directorios para acceder a archivos, directorios y/o comandos.

Cómo evitarlo

- Bloquear exploración de directorios
- Permisos de ficheros
- Bloquear el acceso a archivos confidenciales
- Bloquear análisis author
- Ocultar versiones
- Firewall

SQL Injection

Los ataques por Inyección SQL aprovechan vulnerabilidades para infiltrar o incrustar código SQL intruso aprovechando la falta de comprobación de las variables con el fin de quebrantar las medidas de seguridad y acceder a datos protegidos.

Cómo evitarlo

- **Actualizaciones**
- **Configuración de las Security Keys**
- **Cambia el prefijo de la base de datos**
- **Evita la inyección de scripts**
- **Proteger htaccess y wp-config.php**
- **Prevenir el indice de directorios en robots.txt**

CSRF

Cross-site request forgery o falsificación de petición en sitios cruzados.

Fuerza al navegador web de un usuario registrado a enviar una petición que pasa por otra aplicación, y la utiliza para realizar una acción maliciosa en nombre del usuario.

Se suele usar para estafas por Internet y el proceso se lleva a cabo mediante solicitudes HTTP.

Cómo evitarlo

- **HTTPS (HSTS)**
- **Usar última versión de PHP**
- **Configuración cabeceras HTTP seguras**
- **Impedir acceso a servidores externos**
- **Evitar subida de ficheros en formularios**
- **Firewall**

File Inclusion

Ataque por RFI (del inglés Remote File Inclusion, traducido al español como Inclusión Remota de Archivos)

Es un tipo de ataque que aprovecha una vulnerabilidad existente en páginas dinámicas en PHP que permiten el enlace de archivos remotos situados en otros servidores a causa de una mala programación de la página que contiene funciones de inclusión de archivos.

Cómo evitarlo

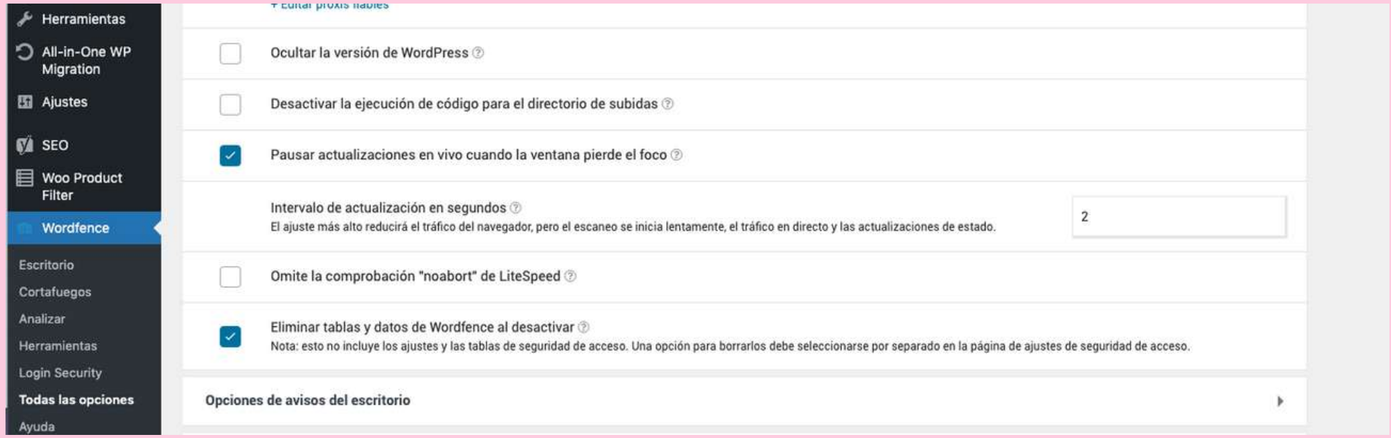
- Actualizaciones
- Permisos de ficheros
- Utilizar últimas versiones de PHP
- Prohibir PHP en el directorio wp-includes
- Prohibir PHP en el directorio wp-content/uploads
- Desactivar la ejecución de PHP en directorios de la caché

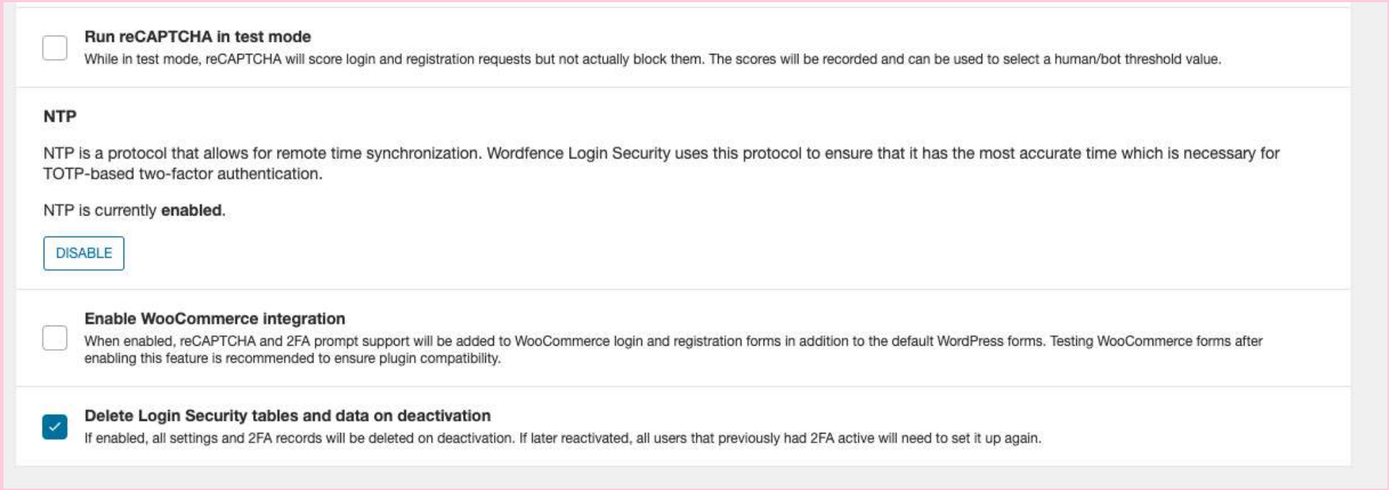
Pon Wordfence

Es coña

Canva

Quita Wordfence





Protégete

INSTITUTO NACIONAL DE CIBERSEGURIDAD

Conciencia, analiza y resuelve

Portal: Protege tu empresa

Teléfono gratuito: 017

Herramienta: Autodiagnóstico

INSTITUTO NACIONAL DE CIBERSEGURIDAD

Análisis de casos gestionados

(más de 100.000 casos gestionados en 1 año)

Uno de los principales objetivos de los ciberataques:

- **Autónomos**
- **PYMES**

1° Fraudes por falsas ventas

2° Ataques a equipos no actualizados

3° Infecciones de malware (robar o borrar datos, espiar al usuario, etc.)

Mención especial a las Apps de salud (COVID) fantásticas para recopilar datos de usuarios

Pasos a seguir ante un hackeo

Asegúrate de tener un Plan de Contingencia para reanudar la actividad lo antes posible y si lo crees necesario una póliza de ciberseguridad, antes de que nada suceda.

IDENTIFICAR

Identificación clara de qué ha ocurrido, qué daños hemos sufrido y su repercusión. Y sobre todo, encontrar la vulnerabilidad.

COMUNICAR

Comunicarlo a la Agencia Española de Protección de Datos. Especialmente si se han comprometido datos de clientes, empleados o proveedores. Denunciarlo y aportar pruebas.

RECUPERAR

Recuperación de los sistemas que se hayan visto afectados y paliar sus efectos cuanto antes.

Muchas gracias!

erica_aguado

erica-aguado-exposito

@erica_aguado

erica@reanimandowebs.com

MeetUp WordPress Valencia

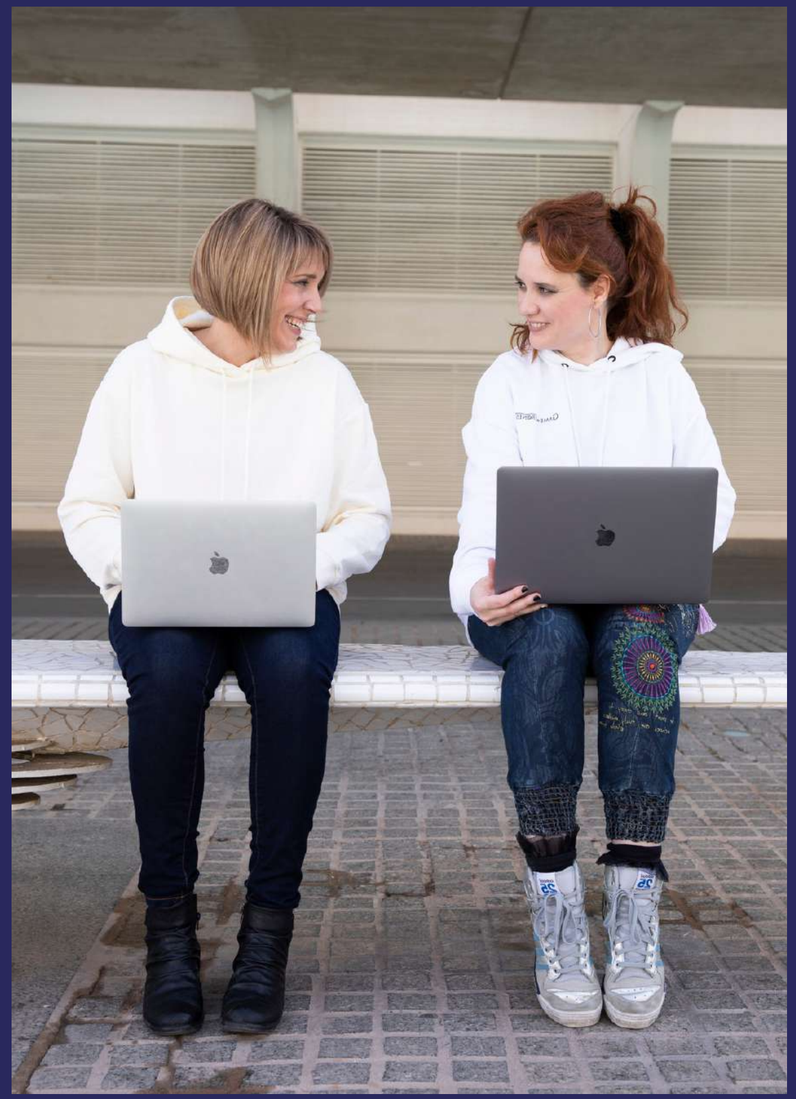
patrinavarrosanz

patricianavarrosanz

@Patri_TSW

patri@thesuperwaywebs.com

MeetUp WordPress Valencia




GAME
OVER