Bienvenido a WordPress Granollers

Próxima meetup

21 de Julio

Meetup Party at ZOOM: Fiesta final de temporada

Próxima temporada en 3r Martes de cada mes:

22 de septiembre

20 de octubre

17 de noviembre

WordPress es seguro, y si te dicen lo contrario, mienten

Tipos de hacks

- Servidor web
- Base de datos
- Ficheros
- SEO

Servidor web: DDOS

- Se ataca al servidor desde muchos ordenadores simultáneamente .
- Objetivo: denegar el servicio, que el servidor deje de funcionar.
  - https://es.wordpress.org/plugins/limit-login-attempts-reloaded/
  - https://wordpress.org/support/article/brute-force-attacks/

Base de datos

- Hackear base de datos y escalar privilegios.
- Hosting malo.
- **admin id, prefijo de tabla**

Ficheros

De WordPress o no (hosting compartido)

Código preparado (fuentes desconocidas)

Código sin preparar (bugs)

SEO

Envío de sitemap incorrecto a Google con cientos de páginas inexistentes que llenan los resultados de búsqueda de páginas fantasma en chino.

La web en sí no se ve afectada, pero si la imagen de la empresa y el tráfico procedente del buscador

¿Cómo prevenirlo?

- Hosting de calidad. Ojo con los compartidos.
- WordPress: actualización frecuente de core, plugins y themes.
- Copia de seguridad.
- Gestión prudente de usuarios y contraseñas.
- Configuración adecuada (permisos de ficheros, plugins y themes de calidad, protección por códigos o plugins).

¿Cómo arreglarlo?

- Entender qué pasa
- Copia de seguridad
- Limpiar
- Instalación nueva
- Configuración

Doctor ¿qué me pasa?

Detectar por donde ha entrado el error es vital ya que va a permitir tapar ese agujero. Si no se tapa, seguramente te volverá a pasar.

Doctor ¿qué me pasa?

Sospecha de :

Plugins

Versión WP

Config server

Tema

PHP

Tu ordenador

Doctor ¿qué me pasa?

https://wpvulndb.com/

https://www.cvedetails.com/

https://nvd.nist.gov/

https://cwe.mitre.org/

Volvamos a un punto que funciona

Detectar en qué momento aproximado fue el hackeo y cargar una copia de seguridad funcional.

Trabajar en local o capar el acceso a la web a tu IP.

```
order allow, deny
allow from *.*.*.*(sustituye por tu IP)
deny from all
```

Limpieza general

Si te han atacado los ficheros habrá mucha cosa...

- Intentar reemplazarlos por una copia limpia

Si te han atacado la bd

- reemplazar tablas

Volvamos de 0

- Empezar con una copia limpia de WordPress
- Instalar el tema
- Instalar los plugins
- Poner la base de datos (o en su defecto, posts y post_meta)

Configuración

- Aplicar toda la prevención que hemos explicado.
- Actualizar todo
- Cruzar los dedos ;)

¡Gracias!

WordPress Granollers | wpgranollers.com | @wpgranollers