

5 ERRORES COMUNES EN WORDPRESS

TODOS LOS COMETEMOS POR QUE NO SOMOS PERFECTOS

Una charla de Salvador Aguilar

Analista de Seguridad en Sucuri.net

Email: sal.aguilar@sucuri.net

Twitter: @riper81

Blog: salrocks.com



ANTES DE EMPEZAR...

- 1. QUIEN SOY YO?**
- 2. PORQUÉ ÉSTA CHARLA?**
- 3. WORDPRESS: UN REPASO**
- 4. ERROR #1**
- 5. ERROR #2**
- 6. ERROR #3**
- 7. ERROR #4**
- 8. ERROR #5**
- 9. OTRAS SUGERENCIAS**
- 10. P & R**



¿QUIEN SOY YO?

- ALGUIEN QUE HA COMETIDO MILES DE ERRORES CON WORDPRESS
- ALGUIEN QUE SE HA SIDO HACKIADO
- ALGUIEN QUE SE HA PELEADO CON CLIENTES
- IMPLEMENTADOR DE WORDPRESS
- IT MANAGER DE CALL CENTERS: PRESS2, ETELECARE & STREAM.
- SYSADMIN DE EMPRESAS COMO KOM-1 & SEARS MEXICO.
- ANALISTA DE SEGURIDAD EN SUCURI.NET
- COORDINADOR EN SENORCODERS.COM



¿PORQUÉ ESTA CHARLA?

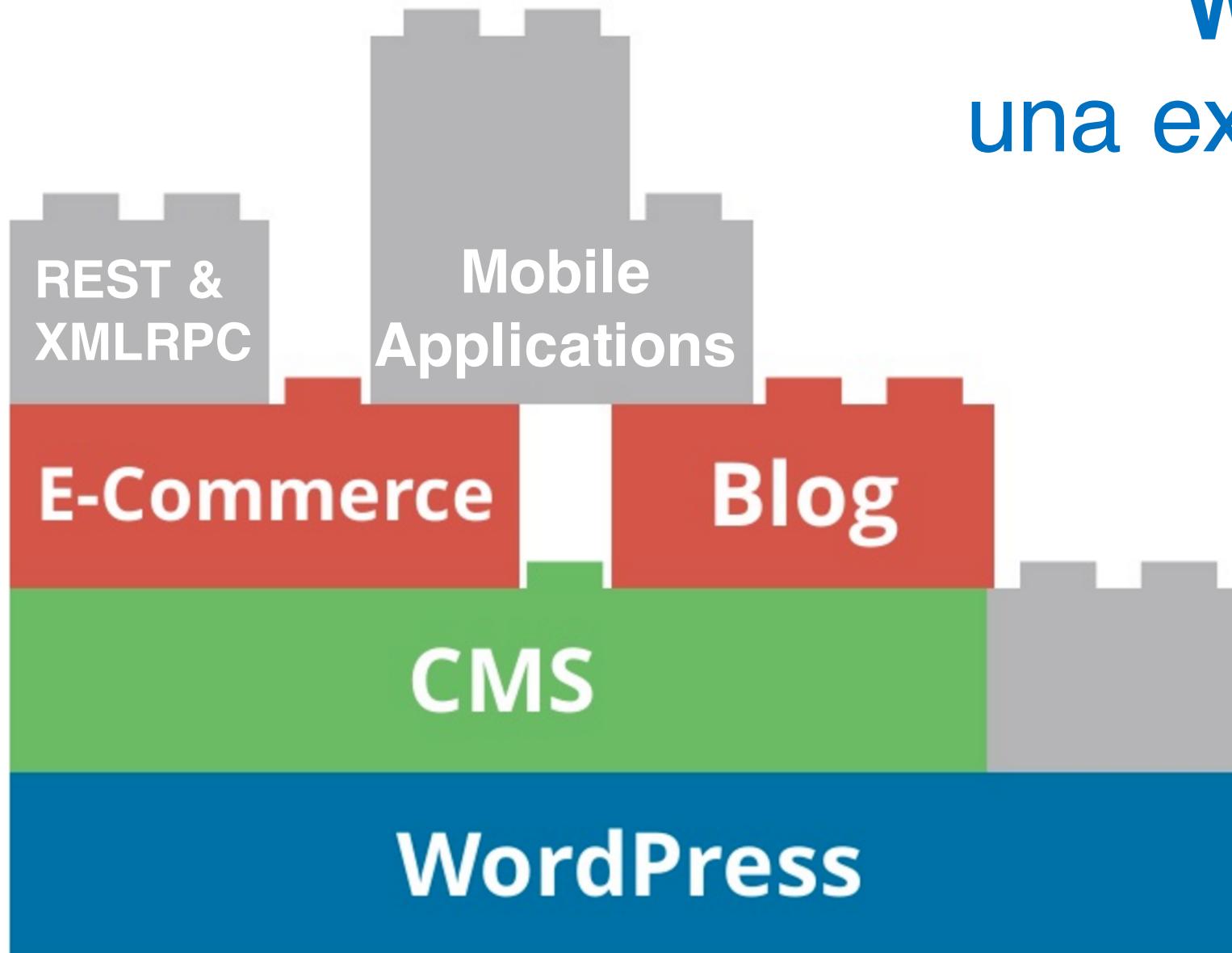
- HE ESTADO EN VARIOS ROLES: APRENDIZ, DISEÑADOR, ADMINISTRADOR, SOPORTE TÉCNICO EN UNA COMPAÑÍA DE HOSTING & ANALISTA DE SEGURIDAD
- PARA QUE LOS PRINCIPIANTES VEAN TODOS LOS ERRORES QUE SE PUEDEN COMETER CON LA ESPERANZA DE QUE NO LOS COMETAN.
- PARA LOS QUE TIENEN EXPERIENCIA Y REVIVAN ERRORES PASADOS, PRESENTES Y FUTUROS
- LOS ERRORES QUE COMETEMOS COMÚNMENTE TIENEN IMPACTOS NEGATIVOS PARA TODOS: USUARIOS, DUEÑOS DEL NEGOCIO, DISEÑADORES & ADMINISTRADORES.
- AHORRAR TIEMPO, ESFUERZO & DINERO = REDUCIR STRESS + MEJORAR LA CALIDAD DE NUESTRO TRABAJO + DAR UN VALOR AGREGADO.
- PARA MEJORAR NUESTRO CONOCIMIENTO SOBRE WORDPRESS Y MEJORAR LA CALIDAD DE NUESTRO TRABAJO Y PODER OFERTAR MEJORES PRODUCTOS Y COBRAR MEJOR (\$\$\$).

WORDPRESS: UN BREVE REPASO

- WORDPRESS ES UN FORK DE OTRO CMS LLAMADO B2 CAFELOG. (2003)
- DEPENDE DE PHP & MySQL
- USADO POR MÁS DEL 26% DE LOS SITIOS WEB DEL MUNDO.
- TIENE ALTA ACEPTACIÓN POR PARTE DE USUARIOS FINALES Y MARKETEROS (SI ESOS QUE ENGAÑAN A LA GENTE Y ESTUDIAN LA MAGIA NEGRA DEL MARKETING).
- PERMITE TENER UN SITIO WEB SIN TENER CONOCIMIENTOS DE HTML NI JAVASCRIPT.
- ULTIMOS GRANDES AVANCES: IMAGENES RESPONSIVAS, CALYPSO & REST API
- AUTOMATIC, LA COMPAÑIA DETRAS DE WORDPRESS.ORG OFRECE WORDPRESS.COM, WOOCOMMERCE, JETPACK, ETC. NO TODO ES GRATIS EN ESTA VIDA
- FUTURO DE WORDPRESS: JAVASCRIPT: REACT, ANGULAR & NODE, REST API, REACT
- EL REPOSITORIO DE PLUGINS TIENE MAS DE 1 BILLON DE DESCARGAS

Wordpress

una explicación visual



Los 5 + comunes



Empecemos



ERROR #1 – WORDPRESS ES FÁCIL

- MENTIRA. MENTIRA. MENTIRA.
- ES UN CMS VERSATIL PERO NO FÁCIL.
- TIENE MÁS DE 100,000 PLUGINS, PERO CADA UNO ES DIFERENTES, HAY VARIOS PLUGINS PARA UN SOLO PROPOSITO, PERO TIENEN DIFERENTES IMPACTOS EN SEGURIDAD & RENDIMIENTO.
- TIENE VARIOS PAGE BUILDERS COMO: VISUAL COMPOSER DE WP BAKERY, ETC ETC - PERO SE ROMPEN FÁCILMENTE AL ACTUALIZAR WORDPRESS.
- VARIOS PLUGINS SON INCOMPATIBLES CON OTROS Y CAUSAN MUCHOS DOLORES DE CABEZA.
- TEMAS POR AQUÍ, TEMAS POR ALLÁ. HAY MILES DE TEMAS PERSONALIZADOS, TANTO GRATIS COMO PAGADOS, PERO IGUAL MUCHOS TIENEN CONFLICTOS CON VERSIONES DE WORDPRESS E INCLUSO PLUGINS. :(
- **SOLUCIÓN: TENER BACKUPS POR CUALQUIER EVENTUALIDAD. MANTENER WORDPRESS CORE, TEMAS & PLUGINS SIEMPRE ACTUALIZADOS.**

ERROR #2 – WP SE INSTALA EN 5 MINUTOS

- OH DIOS QUE INGENUIDAD!
- SI INSTALAS WORDPRESS CORE, Y LO DEJÁS ASÍ, ES COMO CONSTRUIR UN CASA, DEJARLA EN OBRA GRIS Y NO PONERLE LLAVE A LA PUERTA PRINCIPAL.
- WORDPRESS CORE, AL SER OPEN SOURCE, TRAE EL RIESGO DE QUE TODO MUNDO SABE DONDE LOGIARSE COMO ADMIN: WP-ADMIN
- NO TRAE PROTECCIÓN CONTRA ATAQUES DE FUERZA BRUTA QUE INTENTAN ADIVINAR TU USUARIO & CONTRASEÑA
- NO TRAE UNA BITÁCORA PARA PODER AUDITAR LOS ERRORES DE INICIO DE SESIÓN
- **SOLUCIÓN: UNA VEZ WORDPRESS CORE ESTÉ INSTALADO, INSTALAR UN PLUGIN DE SEGURIDAD: WORDFENCE, SUCURI O BULLETPROOF SECURITY, O MEJOR AUN UN FIREWALL EXTERNO PARA LIMITAR EL INTENTO DE ACCESO Y PODER TENER LOGS. INSTALAR Y CONFIGURAR CUALQUIER SOLUCIÓN DE CACHÉ.**

ERROR #3 – USUARIOS: ADMIN & ADMINISTRATOR

- USAR EL USUARIO POR DEFECTO 'ADMIN' ES UN ERROR ESPANTOSO!
- HAY SCRIPTS, BOTS, CRAWLERS QUE ESTAN CONSTANTEMENTE BUSCANDO INTERNET POR SITIOS WORDPRESS Y CUAL ES EL PRIMER USUARIO QUE INTENTAN USAR PARA BRUTE FORCE?
- UNA VEZ QUE TIENEN EL USUARIO ES SÓLO CUESTIÓN DE TIEMPO PARA QUE LOGREN ENTRAR A TU SITIO WEB! BUENA SUERTE!
- **SOLUCIÓN: NO USAR ADMIN O ADMINISTRATOR COMO USUARIO. ASÍ DE SENCILLO!**

ERROR #4 – USAR USUARIOS CON NIVEL DE ADMINISTRADOR COMO AUTORES DE POSTS & PAGINAS

- A QUE ME REFIERO ?
- WORDPRESS TIENE VARIOS NIVELES DE USUARIOS, USAR EL USUARIO ADMIN COMO AUTOR ES UN PROBLEMA, PORQUE ESTÁS REVELANDO EL NOMBRE DEL USUARIO, Y VAN A HABER MENOS PROBLEMAS SI SE USA UN USUARIO DE BAJO NIVEL COMO AUTOR QUE EL ADMINISTRADOR.
- **SOLUCIÓN: TENER 2 USUARIOS & BLOQUIAR PETICIONES DE INICIO DE SESIÓN A USUARIOS QUE NO EXISTEN & LIMITAR LOS INTENTOS DE INICIO DE SESIÓN DE USUARIOS VÁLIDOS A 5 INTENTOS, LUEGO BLOQUIAR EL IP. TAMBIÉN ES BUENA IDEA USAR AUTENTICACIÓN DE 2 NIVELES COMO UN CAPTCHA.**

ERROR #5 – NO USAR CACHE

- WP NO SÓLO DEPENDE DE APACHE/NGINX & PHP. TAMBIÉN DEPENDE DE MySQL.
- CADA VEZ QUE SE CARGA UNA PÁGINA DE WP, SE HACEN POR LO MENOS 5 QUERIES A LA BASE DE DATOS.
- MIENTRAS MÁS PLUGINS & FUNCIONALIDADES, MÁS QUERIES A LA BASE DE DATOS.
- AHORA ESTO AL PRINCIPIO NO PUEDE SER MUCHO PROBLEMA, PERO CUANDO TENES 100, 500, 1000, 2000 USUARIOS HACIENDO LO MISMO, SE HACE UNA TRAGEDIA.
- **SOLUCIÓN PRÁCTICA: CACHÉ A NIVEL APLICATIVO. W3 TOTAL CACHE, WP SUPER CACHE, WP ROCKET, WORDFENCE, ETC.**
- **SOLUCIÓN INTERMEDIA: CACHÉ APLICATIVO CON INTEGRACIÓN A UN CACHE NOSQL COMO MEMCACHE OR REDIS.**
- **SOLUCIÓN ÓPTIMA: CACHÉ EXTERNO TIPO LOAD BALANCER PARA QUE TODO EL TRAFICO ESTÁTICO ESTE EN UN CDN Y SOLO SE HAGAN LLAMADAS AL SERVIDOR CUANDO SEA NECESARIO. EJEMPLOS: CLOUDFRONT, CLOUDFLARE & SUURI CLOUDPROXY.**

OTRAS SUGERENCIAS

- ESTAR PENDIENTES DE LOS PLUGINS Y SUS VULNERABILIDADES
- AUDITAR REGULARMENTE LOS LOGS TANTO DE INICIO DE SESIÓN DE COMO DE LAS PÁGINAS MÁS VISITADAS
- MANENER UNA POLÍTICA COHERENTE DE BACKUPS. BACKUPS EN EL MISMO SERVIDOR ES UN GRAN ERROR
- USAR HERRAMIENTAS GRATUITAS COMO: UPTIME ROBOT, PERFORMANCE (PERFORMANCE.SUCURI.NET O TOOLS.PINGDOM.COM O GTMETRIX.COM)
- SI NO SE CUENTA CON EL TIEMPO PARA ESTO, ADQUIRIR SERVICIOS QUE NOS SIMPLIFIQUEN LA VIDA COMO SUCURI, QUE TE DA UN FIREWALL, ANTIVIRUS, CACHE + CDN, AYUDA EN RESTAURAR EL SITIO EN CASO DE HACKS.

PREGUNTAS Y RESPUESTAS



**GRACIAS
TOTALES**

