

Índice

Prólogo	17
Capítulo I	
Introducción al ecosistema de WordPress	19
1. Un repaso por la historia de WordPress.....	19
Desarrolladores	20
2. Métricas que enamoran	22
3. Información y datos que preocupan	23
4. Funcionalidades	25
Multisitio	27
Plantillas y Themes	28
Widget	29
Plugins	29
5. Hooks, Acciones y Filtros	30
Hooks	30
Acciones	30
Filtros	31
6. Como colaborar con WordPress	31
7. Antes de Instalar WordPress	33
Capítulo II	
Instalación segura de WordPress.....	35
1. Donde obtener WordPress	35
2. Anatomía de WordPress.....	37
3. Definición de los Usuarios.....	41
4. Roles de Usuarios en WordPress.....	43
5. Cuentas de usuario sin verificar	45



6. Por qué se contrata un servicio de Hosting	47
7. Instalación	47
8. Docker WordPress	52
9. Docker Hub	53
10. Como instalar Docker	54
11. Docker Compose	56
12. Instalar Docker Compose	56
13. Instalación de WordPress con Docker Compose	57

Capítulo III

Configuración básica de Seguridad	61
1. Principios del Hardening	61
Defensa en Profundidad	61
Mínimo Privilegio Posible	61
Mínimo punto de exposición.....	62
2. Cambiar los permisos en Archivos y Directorios	62
Permisos básicos	62
Clases de usuarios	62
Los valores Octales	63
3. Como proteger el archivo wp-config.php	64
4. Políticas de cambio de contraseñas	65
5. Modificando los accesos al Dashboard de Administración	65
6. Restringir accesos a direcciones IP no deseadas	66
7. Medidas de Seguridad en .htaccess	66
8. Permisos especiales para Plugins	67
9. Los códigos de estados de HTTP	67
Códigos de estado 1XX.....	68
Códigos de estado 2XX.....	68
Códigos de estado 3XX.....	69
Códigos de estado 4XX.....	69
Códigos de estado 5XX.....	71
10. Desactivar los métodos Trace/Track de HTTP	72
11. Evitar la navegación por directorios	72
12. Aplicar reglas de una Blacklist	74
13. Como ocultar la versión de WordPress	75



Eliminar la versión en el Theme	76
Dejar sin acción la función que escribe la versión WordPress.....	76
14. Configurar la revisión en las publicaciones.....	76
15. Como desactivar REST API	77
Desactivar el enlace en el head de REST API.....	78
16. Puntos a revisar antes de desplegar WordPress en Producción.....	78
17. WordPress seguro con X-Frame-Options y cookies HTTPOnly.....	79
18. Como implementar X-Frame-Options Header en WordPress.....	80
19. Como implementar Cookies con HTTPOnly y Secure flag	81
Capítulo IV	
Plugins y Themes.....	83
1. Introducción a los Plugins	83
2. Consideraciones a tener en cuenta.....	83
3. Instalación de Plugins	84
¿Por qué es mejor implementar un procedimiento manual?	84
4. Listado de Plugins recomendado	85
Plugins de Seguridad.....	86
Plugins de Mantenimiento.....	86
Plugins de Optimización y Rendimiento.....	87
Plugins para realizar Migraciones.....	87
Plugins con herramientas Avanzadas	88
5. Cómo escribir el primer Plugins	88
Cuándo se debe escribir un Plugin.....	88
Sugerencias para el desarrollo de Plugin	89
Nombre del Plugin	89
Archivos del Plugin.....	89
Archivo Readme.....	89
Información Estándar del Plugin.....	90
¿Por qué es importante incluir el archivo index.php?	92
6. Desinstalar un Plugin	93
7. Implementación de los mecanismos de seguridad de Latch.....	93
¿Qué es Latch?	93
Requisitos previos	94
Pasos para realizar el pareado de una cuenta con Latch	94
Guía de instalación de Latch y el Plugins para WordPress.....	96
Obtención del identificador de la aplicación.....	96
Descarga del Plugin para WordPress.....	100



Instalación del Plugin.....	100
Configurar el Plugin instalado.....	101
Uso del Plugin “Latch” por el usuario	102
¿Cómo parrear un usuario?.....	102
8. Agrupar el control de varios WordPress bajo un solo Latch	104
Escenario de trabajo	104
Limpiando	108
Conclusiones	109
9. Introducción a los Themes	109
10. Instalación de Theme	110
Editar el Theme desde el Dashboard no es la mejor opción	111
11. Como escribir el primer Theme	112
12. Desinstalar un Theme.....	113
13. Plugins de seguridad	113
14. Recomendaciones Finales	115
15. Doble Factor de Autenticación Temporal con Latch.....	115

Capítulo V

Crónicas de un ataque a WordPress	119
¿Cómo fue que sucedió?	125
Recopilando información de Plugins en WordPress	126
Los objetivos del ataque.....	126
Aprender de los errores	127

Capítulo VI

Políticas de actualización en WordPress.....	129
1. Tipos de actualizaciones.....	129
2. Configuraciones preestablecidas	130
¿Qué es un cron?	132
3. Actualizaciones automáticas.....	133
Desactivar todas las actualizaciones	133
¿Cuál es la razón para desactivar las actualizaciones automáticas?	133
Opciones de actualización del núcleo (core).....	134
Las funciones <code>__return_true</code> y <code>__return_false</code>	135
Actualizaciones automáticas en Plugins y Themes.....	135
Actualizaciones automáticas de traducciones	135
4. El mito de las actualizaciones.....	136



5. Crear un inventario	137
6. Monitoreo	138
¿Qué es lo que interesa monitorear?	139
7. Entornos de Prueba y Producción	141
8. Ejecutando las actualizaciones	141
9. Documento de actualización	142

Capítulo VII

Asegurando las Bases de Datos	143
1. Introducción y Configuración de MySQL	143
2. Administración de MySQL	145
Consultar los usuarios	146
Crear un usuario en MySQL	146
Como eliminar un usuario.....	146
Cambiar el nombre de un usuario	147
Modificar la contraseña de Usuario.....	147
Asignación de Permisos	147
Elimina privilegios de un usuario	147
El archivo ~/.mysql_history	148
Crear y Eliminar Bases de Datos	149
3. Ejecutar y restaurar copias de seguridad con MySQLDump	150
4. Monitoreo	151
5. Consultas útiles para aplicar en WordPress	152
Obtener el tamaño de la base de datos	152
Cambio de los atributos siteurl y home de wp_options	153
Cambiar el atributo guid de wp_posts.....	153
Cambiar URL en contenido del sitio web.....	153
Cambiar el PATH de las imágenes publicados en los artículos.....	153
Actualización en los valores de wp_postmeta	153
Cambiar el nombre de usuario admin	154
Restablecer la Contraseña	154
Eliminar la revisión de artículos y páginas publicadas	154
Eliminar todo Pingback.....	155
Eliminar todos los comentarios spam	155
6. Hackear un WordPress con Network Packet Manipulation	155
Analizando las consultas de WordPress	156
Ataque 1: Cambiando las passwords a los usuarios.....	157
Ataque 2: Crear usuarios en WordPress.....	158



7. Fortificación de comunicación entre WordPress y MySQL para Evitar los ataques de NPM (Network Packet Manipulation)	160
WordPress por defecto	160
Punto 1. Fortificando la conexión a MySQL con SSL	160
Punto 2. Configurar WordPress para que cifre con SSL la conexión a MySQL	162
8. Wordpress in Paranoid Mode	163
9. Seguridad en phpMyAdmin	165
10. Cadena de conexión de WordPress a MySQL	167
Dividiendo las cadenas de conexión para usuarios autenticados y no autenticados	168
Configuración de WordPress	169

Capítulo VIII

Copias de Seguridad171

1. Tipos de Backups	171
¿Cada cuánto tiempo debería hacer una copia de seguridad?	171
¿Se puede usar este método para respaldar otros datos?.....	172
¿Cuántas copias de seguridad se debe hacer?	172
¿Es posible reducir el espacio de las copias de seguridad?.....	172
¿Se puede automatizar la copia de seguridad?.....	172
¿En qué dispositivo se debe alojar las copias de Seguridad?.....	173
¿Cuánto tiempo se debe almacenar un respaldo?.....	173
Backups completos.....	173
Backups incrementales.....	173
Backups diferenciales.....	174
2. Copias de Seguridad en WordPress	174
¿Por qué simplemente se propone respaldar la base de datos y los archivos generados en el directorio wp-content/uploads/?.....	176
3. Plugins para realizar copias de seguridad en WordPress	178
Xcloner - Backup and Restore	178
BackUpWordPress	179
WordPress Backup to Dropbox	180
BackWPup Free - WordPress Backup Plugin	180
4. Pruebas en la restauración de Backups	181
5. Conclusiones	182

Capítulo IX

Políticas de restauración ante desastres185

1. Continuidad del negocio	185
2. Control de cambios	185



Stream	186
Simple History	187
3. Gestión de incidentes.....	189
4. Plan de recuperación ante desastres	190
5. Hacer uso del Plan de Recuperación ante Desastres.....	191
Plan de recuperación multiusuario	192
6. Informe de resultado	192
Dirección.....	193
Gerencia	193
Técnicos	193
7. RansomWare.....	193
Listado de RansomWare.....	195
8. RansomWare en WordPress	195
9. Recomendaciones finales.....	197
Conclusiones Finales.....	198

Capítulo X

Fortificando la instalación de WordPress con WPHardening	199
1. El camino a la automatización	199
2. ¿Qué es WPHardening?.....	200
3. Instalación	200
El administrador de Paquetes pip.....	201
Actualización.....	201
4. Primeros pasos con WPHardening	202
5. Cambiar los permisos en Archivos y Directorios.....	204
6. Cambiar dueño y grupo en Archivos y Directorios.....	205
7. Eliminar componentes que no son necesarios.....	205
8. Crear un archivo robots.txt correcto y a medida	206
9. Eliminar todo Fingerprinting de un proyecto.....	208
10. Crear el archivo wp-config.php a medida	210
11. Descargar los Plugins de Seguridad.....	211
12. Evitar la navegación en directorios y ocultar errores	211
13. Realizar un escaneo de malware	212
14. Revisar las librerías TimThumb	213



15. Trabajo en Conjunto	214
16. Colaborar con WPHardening	214

Capítulo XI

Auditoría en WordPress con WP-CLI	215
1. Conociendo wp-cli.phar	215
2. Requerimientos de Sistema.....	216
3. Instalación de wp-cli.phar	216
4. Escenario de Trabajo	217
Cómo obtener la versión de WordPress	218
Chequear actualizaciones de WordPress	218
Ejecutar una actualización WordPress	218
5. Administrar las Bases de Datos	219
6. Como obtener información de los usuarios.....	221
7. Cómo obtener información de los Plugins	222
8. Cómo obtener información de los Themes	224
9. Como buscar backdoor, webshell o código ofuscado	226
10. Acciones en segundo plano	227

Capítulo XII

Los ataques más frecuentes en WordPress	231
1. Ataques de Phishing a WordPress con enlaces en target=”_blank”	231
Un servidor para hacer Phishing	232
2. Cómo comprometer las contraseñas a los Administradores de WordPress con XSS	234
3. Proteger la ejecución de acciones planificadas en WordPress.....	237
4. Ataque en WordPress: Time-Based XSPA (Cross-Site Port Attack)	240
Time-Based XSPA [Cross-Site Port Attack]	242
5. Controlar el caché PHP de un sitio web en WordPress.....	245
6. Fortificar WordPress frente ataques de fuerza bruta	248
7. Escaneo de Vulnerabilidades con WPScan	250
Como obtener WPScan	250
Comprobación de Plugins vulnerables.....	251
Comprobación de Themes vulnerables	252
Enumeración de Usuario	252



Fuerza Bruta en contraseñas.....	252
8. Auditoría en sistemas WordPress con Plecost.....	253
Como instalar Plecost.....	253
9. El escaner de vulnerabilidades CMSmap	254
Como obtener CMSmap.....	254
10. Detectar vulnerabilidades en WordPress con w3af.....	254
Como obtener w3af.....	255
Automatización de pruebas.....	256
11. Como obtener información de WordPress con WhatWeb	257
Cómo obtener WhatWeb.....	258
12. Pruebas de contraseñas y Brutforcing con BLACKBOX.....	260
Cómo obtener BLACKBOX.....	260
13. Metasploit para WordPress.....	261
Cómo obtener metasploit frameworks.....	262
Índice alfabético	265
Índice de imágenes	269



