VULNERABILIDADES INFORMÁTICAS EN IMPLEMENTACIONES CON EL CMS WORDPRESS

LUZ ANGELA ROBAYO GARCÍA

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD
FACULTAD CIENCIAS BÁSICAS TECNOLOGÍA E INGENIERÍA - ECBTI
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
BOGOTÁ D.C
2021

VULNERABILIDADES INFORMÁTICAS EN IMPLEMENTACIONES CON EL CMS WORDPRESS

LUZ ANGELA ROBAYO GARCÍA

MONOGRAFÍA PARA OPTAR EL TÍTULO DE
ESPECIALISTA EN SEGURIDAD INFORMÁTICA

DIRECTORA DEL PROYECTO
YENNY STELLA NUÑEZ
ESPECIALISTA EN SEGURIDAD INFORMÁTICA

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD
FACULTAD CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA - ECBTI
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
BOGOTÁ D.C
2021

Nota de Aceptación

_____

_____

_____

_____

_____

_____

_____

Firma del presidente del Jurado

_____

Firma del Jurado

_____

Firma del Jurado

DEDICATORIA

Dedico este trabajo de grado a Dios por permitir culminar otro logro profesional, y a mi familia por el apoyo incondicional y emocional durante este tiempo de preparación y aprendizaje.

TABLA DE CONTENIDO

LISTA DE TABLAS

LISTA DE FIGURAS

GLOSARIO

- CMS: es un sistema de gestión de contenido que facilita crear, administrar y gestionar un sitio web.
- WordPress: es un gestor de contenido gratuito que permite crear blog, páginas web entre otros.
- Vulnerabilidad: es una debilidad informática que puede tener un sitio web el cual se puede presentar el riesgo de alterar la integridad, disponibilidad, y confidencialidad.
- Sucuri: empresa de seguridad informática reconocida a nivel mundial, el cual se enfoca en la seguridad de los sitios web.
- w3techs: es una Organización que analiza las diversas tecnologías que se utilizan, para el desarrollo de sitios web.
- Kali Linux: conjunto de herramientas que se utilizan para auditorias relacionadas con la seguridad informática.
- Plugin: son fragmentos de código que se utilizan como complementos, en el gestor de contenido de WordPress con una finalidad determinada.
- Herramienta Informática: conjunto de programas útiles para el análisis y escaneo de un aplicativo.
- Xampp: servidor web apache que tiene una base de datos, y el lenguaje de programación php.
- BuiltWith: es un portal web que por medio de la url de una página identifica aspectos importantes como: servidor, frameworks, javascript utilizados, y el gestor de contenido.
- Owasp Zap: herramienta de código abierto, que se utiliza para monitorear y auditar la seguridad de un aplicativo web.
- Enumeración de debilidades comunes (CWE): es una lista desarrollada por la comunidad de tipos de debilidades de software y hardware.

- Consorcio de seguridad de aplicaciones web (WASC): es una organización formada por un grupo internacional que producen estándares de seguridad de código abierto y ampliamente acordados sobre las mejores prácticas para la World Wide Web.
- Cross-site Request Forgery CSRF: consisten en forzar a un usuario a ejecutar peticiones no deseadas a una web en la que están autentificados sin que este se dé cuenta.

RESUMEN

El internet en la actualidad es indispensable en diferentes campos de la sociedad, ya que los usuarios interactúan con más frecuencia con las páginas web. Cabe resaltar que la web (World Wide Web) a lo largo del tiempo ha evolucionado. Inicialmente los ambientes de las páginas web eran estáticas, unidireccional se denominaba web 1.0, en el año 2004 surgió la web 2.0 bidireccional, con nuevas funcionalidades, como interacción y actualización de los datos ingresados por el usuario, foros, blogs entre otros, en el año 2010 aparece la web 3.0 más eficiente con la web semántica incorporando nuevas tecnologías como IA, y finalmente en el año 2016 surge la web 4.0 que es más eficiente y predictivo[1].

Teniendo en cuenta las diferentes versiones de la web, en el transcurso de la web 1.0 a la web 2.0 se vio la necesidad de utilizar herramientas informáticas, como fue los gestores de contenido que le facilito a los usuarios de internet, crear y publicar contenido sin tener conocimiento técnico de html, css, lenguajes de programación y base de datos. Los gestores de contenido es un tipo de software que permite administrar y gestionar diferente contenido como de texto, imágenes, video de un sitio web.

Finalmente, con el desarrollo y culminación de esta monografía se pretende unificar información verídica de diferentes estudios donde se destaque las principales causas del incremento, de las vulnerabilidades informáticas en los gestores de

[1] LATORRE, Mariano. HISTORIA DE LAS WEB, 1.0, 2.0, 3.0 y 4.0; [Sitio web]. [Citado el 31 de Enero del 2021].

Disponible en: https://d1wqtxts1xzle7.cloudfront.net/59947315/74_Historia_de_la_Web20190706-123188-141xd95.pdf?1562447444=&response-content-disposition=inline%3B+filename%3DHISTORIA_DE_LAS_WEB_1_0_2_0_3_0_y_4_0.pdf&Expires=1612364900&Signature=CGIYjWLiy3ZGe2a5HYi132w~rvOkxfgJyFkypWc-znEpXXWbBaR-K5KjJjhuhb2OzirqJokB7CcJen2RWbB68PXWm8iYGOzuwlLJD1Wj7OBivprFZgTg6zdH4nTZC5pFiA7-M2mNT3niOkEUqjznUeAVpqRCoVudUKZWRwRKnUUSKEL-r-VZni8tPHK8EtELBU2dhBiEU2B2oLwR77Ew4dbbF45z2BYqasnI3tuZnDSNzEdBeF2GdSNqHV0nad5tgsJTqS3CYKjbNjgyQmXu3H3gZxsKPnyvUbuFgBj2DswKJwXcZeoIGKMNT0IUdd3702pP9OesQiMF1VFsokZH2w__&Key-Pair-Id=APKAJLOHF5GGSLRBV4ZA

contenido y específicamente de WordPress, y fortalecer la seguridad informática en este aplicativo.

INTRODUCCIÓN

Los CMS (sistema de gestión de contenidos para páginas web), es un software que permite administrar y gestionar contenido como texto, imágenes, video de un sitio web. También los cms se clasifican en dos grupos uno para el diseño de páginas web y el otro para tiendas online, siendo WordPress el preferido por los usuarios para el diseño de sitios web[2].

Este CMS está compuesto por el lenguaje de programación PHP, el motor de Base de Datos MariaDB o MySQL y el Servidor Web Apache, cuenta con licencia GPL de código abierto, actualmente es muy popular a nivel local y empresarial. Así lo confirman organizaciones dedicadas a estas mediciones, que analizan las tecnologías que se utilizan para el desarrollo y ejecución de los sitios web, una de estas es W3Techs que en sus recientes estudios indica que el 39,0% de todos los sitios web están diseñados en WordPress[3].

Por otro lado, en la página web de estadísticas de sitios web WordPress indican "que el 14.7% de los 100 sitios web más importantes del mundo están basados en WP y más de 500 sitios nuevos se crean diariamente utilizando la versión gratuita en WordPress.org"[4].

Teniendo en cuenta lo anterior se puede destacar la utilidad que tiene los CMS open source en la actualidad, la necesidad de aplicar y mejorar frecuentemente la

[2] Departamento de Internet. Qué es un CMS y qué ventajas tiene; [Sitio web]. [Citado el 4 de Noviembre del 2020] Disponible en: https://www.departamentodeinternet.com/que-es-un-cms-y-que-ventajas-tiene/

[3] Web Technology Surveys: Estadísticas de uso y cuota de mercado de WordPress [Sitio web]. [Citado el 4 de Noviembre del 2020] Disponible en: https://w3techs.com/technologies/details/cm-wordpress

[4] Adicte. ¿Qué porcentaje de sitios web son WordPress en 2019?; [Sitio web]. [Citado el 4 de Noviembre del 2020] Disponible en: https://adictec.com/estadisticas-sitios-web-wordpress/

seguridad informática de los sitios web, debido a que este gestor de contenido presenta constantemente ataques de diccionario en las credenciales del administrador, vulnerabilidades en el núcleo, complementos y temas de WordPress, vulnerabilidades de software, vulnerabilidades en la configuración, vulnerabilidades de tipo directorio transversal que ocurre cuando no existe suficiente seguridad en cuanto a la validación de un usuario, permitiendo acceder a directorios superiores[5].

Finalmente es necesario implementar controles de seguridad, esto con el fin de evitar que se ejecuten las vulnerabilidades anteriormente nombradas, y adicional que los hackers intenten crear códigos maliciosos, encontrar agujeros en el código y robar o vulnerar la información, intentos de inicio de sesión por fuerza bruta, logrando que los sitios web se registre en las listas negras de Google y pierdan credibilidad ante los usuarios[6].

[5] BRITO GOBZALEZ, Raul Henry. PERURENA MONTESINO, Ray de. VELIZ ZULETA, Yeleny .CONTROLES DE SEGURIDAD PARA SISTEMAS DE GESTIÓN DE CONTENIDOS BASADOS EN SOFTWARE LIBRE; [Sitio web]. [Citado el 2 de Febrero del 2021].
Disponible en:http://www.informaticahabana.cu/sites/default/files/ponencia-2020/SEG14.pdf

[6] MURILLO, Bernardo. ¿Por qué es tan importante cuidar la seguridad de su sitio web de WordPress? ; [Sitio web]. [Citado el 15 de Diciembre del
2020] Disponible en: https://netquatro.com/por-que-es-tan-importante-cuidar-la-seguridad-de-su-sitio-web-de-wordpress

1. DEFINICIÓN DEL PROBLEMA

1.1. DESCRIPCIÓN

En la actualidad las páginas web son indispensables para usuarios convencionales como para las empresas, aproximadamente 18 millones de páginas web están diseñadas en WordPress, frente a otros gestores de contenido[7]. Este gestor de contenido es el más utilizado y vulnerado por los ciberdelincuentes como lo indica el informe presentado por sucuri.net, donde realizaron una muestra de más de 34 mil sitios web infectados y por medio de los resultados se pudo concluir que los 3 gestores de contenido con mayor grado de vulnerabilidad, eran: WordPress, Joomla y Magento, siendo WordPress el más vulnerable con un 83% en el año 2017 versus Joomla (13.1%), Magento (6.5%) y Drupal (1.6%), entre otros CMS descritos en el estudio[8].

Según el informe realizado por Imperva las vulnerabilidades en WordPress aumentaron en el año 2018, con un total de 542 vulnerabilidades, el 98% está relacionado con algún complemento de los 50,000 que están en la página oficial de WordPress, el 2% restante está relacionado con el código de WordPress[9].

---

[7] CANTO, Juan Carlos. Centro de Desarrollo de Competencias Digitales de Castilla-La Mancha Guía. [Sitio web]. Guía de los 7 mejores gestores de contenidos gratuitos de 2018. [Citado el 27 de diciembre de 2019] Disponible en: https://www.bilib.es/actualidad/blog/noticia/articulo/

[8] Sucuri Net.Informe de sitio web pirateado 2017, Las últimas tendencias de malware y piratería en sitios web comprometidos. [Citado el 27 de diciembre de 2019]. Disponible en: https://sucuri.net/reports/2017-hacked-website-report/

[9] Acunetix. Seguridad y Firewall. Wordpress revela que el 2018 triplicó vulnerabilidades. Fecha Revisión: [9 de enero del 2019], Fecha de Consulta: [27 de diciembre de 2019] Disponible en: https://www.seguridadyfirewall.cl/2019/01/wordpress-revela-que-el-2018-triplico.html

Según la CSIRT (Equipos de respuesta a incidentes de seguridad) en su página web indica que el “10 de julio del 2020, el equipo de Threat Intelligence (Inteligencia de amenazas) descubrió una vulnerabilidad en “All In One SEO Pack”, un plugin de WordPress instalado en más de 2 millones de sitios. Esta falla permitió a los usuarios autenticados con acceso de nivel de colaborador o superior tener la capacidad de inyectar scripts maliciosos que se ejecutarían si una víctima accedía a la página 'all posts' del panel wp-admin”[10].

A continuación, se destacan algunas de mayor criticidad, esta clasificación se hace teniendo en cuenta el gran volumen de vulnerabilidades en los últimos años. En el año 2018, la empresa Defiant descubrió aproximadamente 20 mil instancias de WordPress que ejecutaban ataques de fuerza bruta, con el fin de tener acceso a los aplicativos diseñados en este CMS. Por medio del plugin “wordfence” y de las listas negras de IP se logró bloquear 5 millones de solicitudes de login[11].

También la empresa WEBARX identificó una vulnerabilidad en el plugin Simple Social Buttons, cuya principal función era insertar botones para compartir en las redes sociales. La vulnerabilidad se ejecutaba en una escala de privilegios nivel administrador, ya que permitía modificar algunas configuraciones propias de la instalación de WordPress, obteniendo el control total del sitio web[12].

[10] Centro de respuestas a incidentes de seguridad informática. [Sitio web]. 2 millones de usuarios afectados por la vulnerabilidad en el plugin para WordPress “All In One SEO Pack”, Fecha Revisión: [19 de Julio de 2020], Fecha de Consulta: [9 de Noviembre de 2020] Disponible en: https://www.csirt-epn.edu.ec/como-tener/94-vulnerabilidad-plugin-wordpress

[11] Tecnonucleous. [Sitio web]. Una Botnet de 20,000 webs WordPress infectan otras webs basadas WordPress, Fecha Revisión: [7 diciembre 2018], Fecha de Consulta: [27 de diciembre de 2019]. Disponible en: https://tecnonucleous.com/2018/12/07/botnet-de-20000-webs-wordpress-infectan-otras-webs-wordpress/

[12] WebARX. [Sitio web]. Error de seguridad crítico del complemento de WordPress 'Botones sociales simples, Fecha Revisión: [29 de Octubre 2019], Fecha de Consulta: [11 de diciembre de 2019], Disponible en: https://www.webarxsecurity.com/wordpress-plugin-simple-social-buttons/

Los investigadores de RIPS Technologies GmbH identificaron la ejecución remota de código (RCE). Esta vulnerabilidad se ejecuta por medio de una cuenta de usuario tipo “autor”, que permite modificar la información de las imágenes y ejecutar código PHP en el servidor, logrando el control remoto de un aplicativo[13].

[13] Hispasec. [Sitio web]. Vulnerabilidad crítica en WordPress pasa desapercibida durante más de 6 años. Fecha Revisión. [21 de Febrero 2019], Fecha de Consulta: [Citado el 21 de febrero 2020] Disponible en: https://unaaldia.hispasec.com/2019/02/vulnerabilidad-critica-en-wordpress-pasa-desapercibida-durante-mas-de-6-anos.html

1.2. FORMULACIÓN DEL PROBLEMA

Basado en la problemática detallada en la descripción del problema respecto a las vulnerabilidades informáticas, presentes en diferentes versiones del gestor de contenido WordPress se genera la siguiente formulación:

¿Qué condiciones básicas de seguridad informática debe tener los CMS para su correcto funcionamiento?

2. JUSTIFICACIÓN

La facilidad de uso que brinda WordPress para el diseño de un aplicativo web es de agrado para las empresas y usuarios en general. Debido a esto, cada vez son más los sitios web diseñados en este CMS, algunos ejemplos son: Adobe Blogs, Noticias oficiales de la Universidad Harvard, Blogs de Skype entre otros[14].

Una de las principales causas de la ejecución de las vulnerabilidades informáticas, es la desactualización de las versiones de WordPress, permitiendo la ejecución de plugin o complementos falsos desarrollados por delincuentes informáticos[15].

Un hecho reciente fue el 1 de septiembre del año 2020 donde el grupo de seravo identificó en el plugin File Manager, una vulnerabilidad crítica el cual facilitaba el ingreso al aplicativo web, sin autenticación con el fin de ejecutar código de forma remota para robar datos confidenciales, o en su defecto alterar el sitio web.

También el equipo de Wordfence reporto que se han registrado 1.7 millones de ataques a sitios web, y aquellos que no tienen instalado este plugin están siendo revisados por bots que buscan detectar versiones vulnerables del plugin File Manager[16].

---

[14] Kinsta. [Sitio web]. 130 Sitios WordPress Principales Dominando la Web en 2020, Fecha Revisión: [Enero 7, 2020],
Fecha de Consulta: [14 de enero de 2020], Disponible en: https://kinsta.com/es/blog/ejemplos-de-sitios-wordpress/

[15] Sucuri, Informe de investigación sobre amenazas a sitios web de 2019 [Sitio web]. Un análisis de las últimas tendencias
en malware y sitios web pirateados detectados (o remediados) por Sucuri.Disponible en: https://sucuri.net/reports/2019-hacked- website-report/

[16] Welivesecurity, WordPress: importante crecimiento de ataques a sitios que utilizan el plugin File Manager, Fecha Revisión:
[7 Sep 2020], Fecha de Consulta: [14 de enero de 2020] Disponible en: https://www.welivesecurity.com/la-es/2020/09/07/wordpress-ataques-sitios-utilizan-plugin-file-manager/

Finalmente, debido a las altas cifras que publican los diferentes informes relacionados con las vulnerabilidades informáticas, en los sitios web diseñados en este CMS, es necesario unificar dicha información para elaborar un documento con información actual y organizada, para identificar a nivel general las causas de las vulnerabilidades informáticas, y proponer una guía de buenas prácticas relacionadas con la seguridad web, útil para los administradores de los aplicativos.

3. OBJETIVOS

3.1. OBJETIVO GENERAL

Analizar las principales causas de las vulnerabilidades informáticas presentadas en el CMS WordPress y su incidencia en la seguridad web.

3.2. OBJETIVOS ESPECIFICOS

- Estructurar la información publicada de las diferentes fuentes de información especializadas en la seguridad informática y relacionada con el CMS WordPress.
- Establecer las herramientas informáticas de auditoria adecuadas para analizar la seguridad del gestor de contenidos WordPress.
- Identificar las debilidades de seguridad informática presente en los CMS, estableciendo específicamente las vulnerabilidades de WordPress, proponiendo una guía de buenas prácticas de seguridad web.

4. MARCO REFERENCIAL

Se dará a conocer a nivel general las principales vulnerabilidades informáticas presentadas en WordPress, y las posibles causas que han alterado de una u otra forma la seguridad de los sitios web. Lo anterior tendrá como base información que será consultada, clasificada, y recopilada de diferentes fuentes de consulta confiables como libros, estudios de seguridad de los sitios web, foros de la comunidad de WordPress, entre otros.

4.1. MARCO TEÓRICO

Las páginas o sitios web en el transcurso del tiempo han sido una herramienta indispensable, en diferentes sectores como: educativos, empresariales, comerciales, entre otros. Estas páginas web en sus inicios, la información era estática la cual no se requería, de un webmaster constante para realizar las modificaciones en Html, CSS, JavaScript entre otros. Debido a que el volumen de la información fue creciendo y cambiando constantemente, se vio la necesidad de crear los gestores de contenidos, que en su mayoría son de código abierto y licencia GPL, el cual tiene algunas ventajas como:

- Cuenta con un entorno graficó amigable, con el fin de que cualquier persona con conocimientos básicos, pueda realizar modificaciones del sitio web.
- No tiene ningún costo por descargar, instalar y configurar el gestor de contenidos.
- Cada gestor de contenido cuenta con una página oficial donde se puede consultar información y realizar las descargas de los temas y plugin de forma gratuita.

Los gestores de contenido tienen dos entornos:

- Front Office: Es el ambiente que se muestra al digitar la url del sitio web, por lo general es lo que visualiza el usuario final.
- Back Office: Es el panel de administración del sitio web, en el cual se puede diseñar, modificar diferentes componentes del sitio web.

Según el portal web W3Techs encargado de recopilar y generar estadísticas de los sitios web y las tecnologías que más se utilizan en estos sitios, determinó que el gestor de contenido que en la actualidad se utiliza más es WordPress. Como se puede observar en las siguientes estadísticas. El cual indica que 34.1% de los sitios web son diseñados en WordPress.

Tabla 1.Sistemas de Gestión de Contenido más Populares

Sistemas de Gestión de Contenido más Populares		
No.	CMS	Uso
1	WordPress	34.1%
2	Joomla	2.8%
3	Drupal	1.9%
4	Shopify	1.6%

Fuente: El Autor

Otro análisis que genero resultados similares al anterior fue el portal web “BuiltWith” el cual se pudo identificar que aproximadamente el 48 % de los sitios web están soportados sobre el gestor de contenido WordPress.

4.1.1. GENERALIDADES DE WORDPRESS

Los programadores estadounidense Matt Mullenweg y Mike Little tomaron como base el CMS b2/cafelog para crear el nuevo gestor de contenido WordPress en el año 2003. La finalidad era ofrecer una herramienta para elaborar Blogs, gracias a los desarrollos técnicos que este CMS tuvo, permitió que muchos usuarios crearan sitios web, tiendas online, foros entre otros, los cuales a lo largo del tiempo han sido vulnerados por los delincuentes informáticos.

A continuación, se destacan algunas vulnerabilidades que se han presentado a lo largo del tiempo en diferentes versiones WordPress.

- Versión 1.0: Fue la primera versión de WordPress lanzada el 3 de enero 2004, con el nombre de Miles.
- Versión 2.0 Duke: Presento algunas mejoras como:
    - Se incluyó el editor WYSIWYG.
    - Se agrego el complemento antispam y finalmente se habilito la opción de subir imágenes.
- Versión 2.6 Tyner: Lanzada el 15 de Julio del 2008, entre las configuraciones se incluyó dos parches de seguridad con el fin de minimizar las vulnerabilidades que se estaban ejecutando en la generación de contraseñas aleatoriamente.
- Versión 2.6.2 Tyner: Parche dirigido prácticamente en exclusiva a solucionar vulnerabilidades en el registro de usuarios, relacionadas con la generación aleatoria de contraseñas y el posible reseteo de las mismas para otros usuarios. Afecta por lo tanto sólo a sistemas con el registro de usuarios habilitado.
- Vulnerabilidad en el plugin GDPR Complance: Fue creado con el fin de aportar al reglamento general de protección de datos (GDPR). Pero fue utilizado por parte de los ciberdelincuentes que por medio de la instalación

de scripts de backdoors (puertas traseras) y la creación de cuentas de usuarios utilizando nombres como t2trollherten y t3trollherten, con una escala de privilegios de administrador, lograron tener el control de los sitios web y cambiar la configuración de WordPress generando un alto riesgo aproximadamente a 100.000 sitios web. Cabe resaltar que esta vulnerabilidad afecta a gran cantidad de versiones hasta la 1.4.2, lo recomendable fue actualizar a la versión parcheada 1.4.3 y verificar los nombres de usuario.

- (Una vulnerabilidad de WordPress pone en riesgo a 100.000 sitios web, 2018). Vulnerabilidad Path Traversal (Directorio Tranversal): Según un estudio de Seguridad de RIPS Technologies esta vulnerabilidad no fue parcheada en su momento, tuvo un lapso de tiempo aproximado de 6 años en los ambientes web diseñados sobre WordPress, afectando las versiones anteriores a 4.9.9 y 5.0.1.Esta vulnerabilidad se ejecuta cuando el atacante manipula los puntos de entrada, y accede con una cuenta de usuario con privilegios de autor, con el fin de ejecutar RCE (Ejecución Remota de Código), código php desde el servidor, logrando el acceso y control del sitio web.

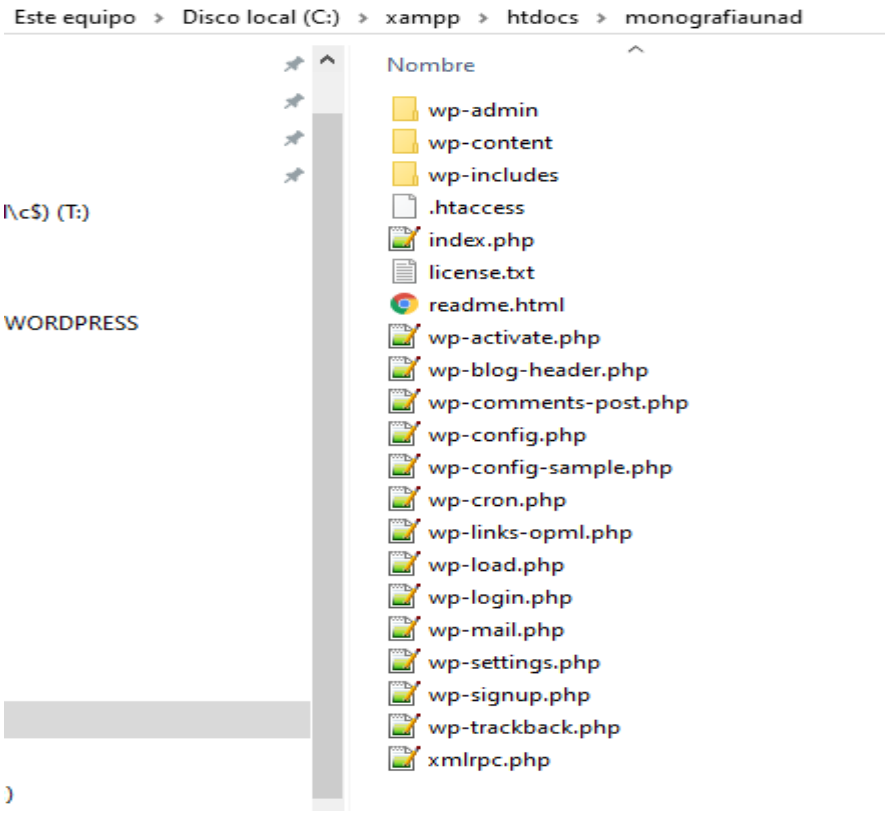
También es necesario resaltar que dependiendo la finalidad del sitio web, estos deben cumplir unos estándares como es el caso de las páginas web enfocadas al comercio electrónico y negocio. Estos sitios web deben cumplir con el estándar de seguridad de datos para la industria de tarjetas de pago o PCI DSS, que por lo general se basan en el cumplimiento de 6 categorías y 12 requisitos plasmados en un documento titulado “Normas de seguridad de datos de la industria de tarjetas de pago (PCI). Cuestionario de autoevaluación C-VT y atestación de cumplimiento.”[17]

[17] Wpwhitesecurity, Cumplimiento de PCI DSS para sitios comerciales y de comercio electrónico de WordPress Fecha Revisión: [23 de julio 2020], Fecha de Consulta: [5 de septiembre 2020], Disponible en: https://www.wpwhitesecurity.com/pci-dss-compliance-wordpress-sites-business

4.1.2. ESTRUCTURA DE WORDPRESS

Al realizar la instalación de WordPress de forma local, se crean 3 carpetas wpadmin, wp-content, wp-includes y 18 archivos.

Figura 1. Archivos y carpetas de Wordpress



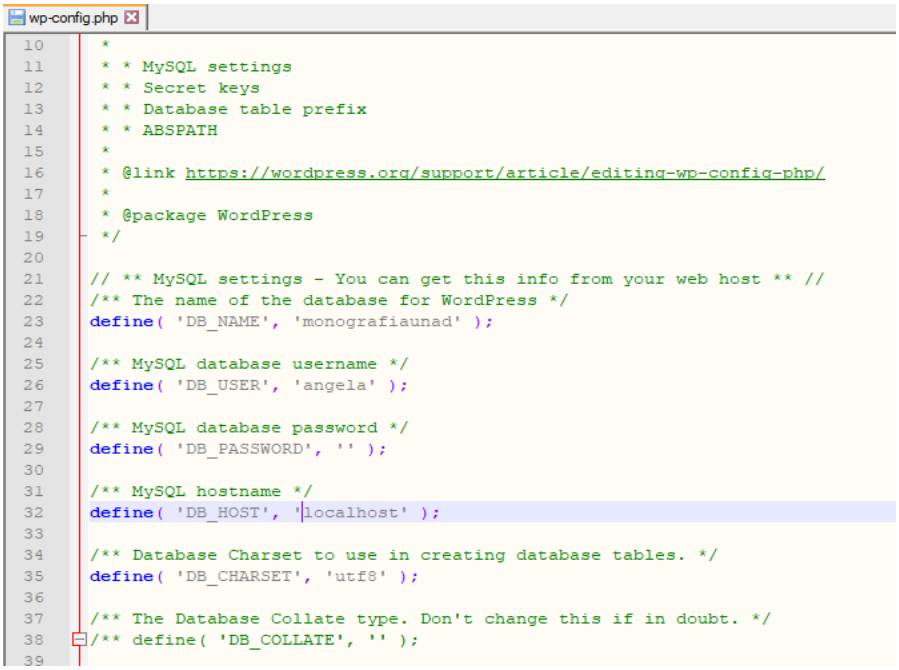
Fuente: El Autor

- wp_admin: Contiene archivos y carpetas relacionadas con el backend de wordpress.
- wp_content: En esta carpeta se almacena información relacionada con languages, plugins, themes, upgrade, uploads. Al realizar copias de wordpress se debe incluir esta carpeta.

- wp_includes: Contiene archivos php y clases importantes de wordpress. Cada vez que se actualiza a una nueva versión esta información también se actualiza.
- index.php: Archivo principal que tiene información de WordPress.
- wp-config.php: Archivo que se crea en la instalación de wordpress y contiene información de la conexión de la BD.
- xmlrpc.php: Archivo que incluye el protocolo de comunicación XML-RPC con el lenguaje XML para su codificación y el protocolo http.

La información de la base de datos, el usuario y contraseña esta guardada en el archivo wp-config.php, el cual utiliza la función define () y unas constantes en el que se almacena, información confidencial por este motivo es necesario que este tipo de archivo este protegido.

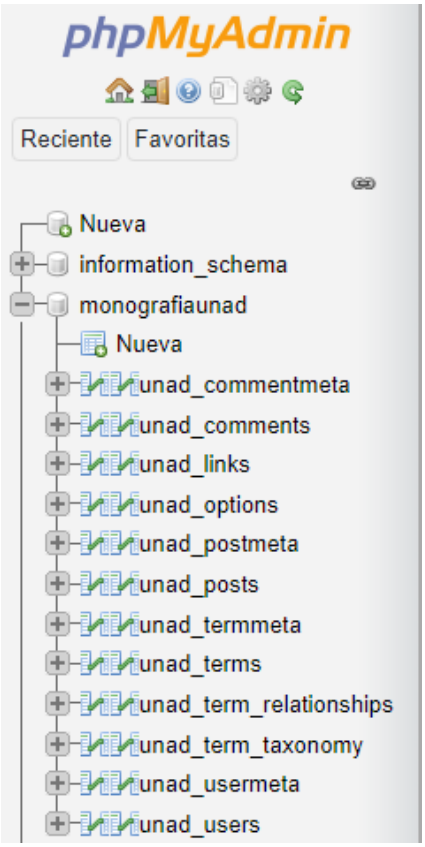
Figura 2. Archivo wp.config.php de WordPress



Fuente: El Autor

También en la herramienta de administración y gestión PhpMyAdmin, se puede consultar información relacionada con el CMS WordPress, como: La Base de Datos, usuarios entre otros.

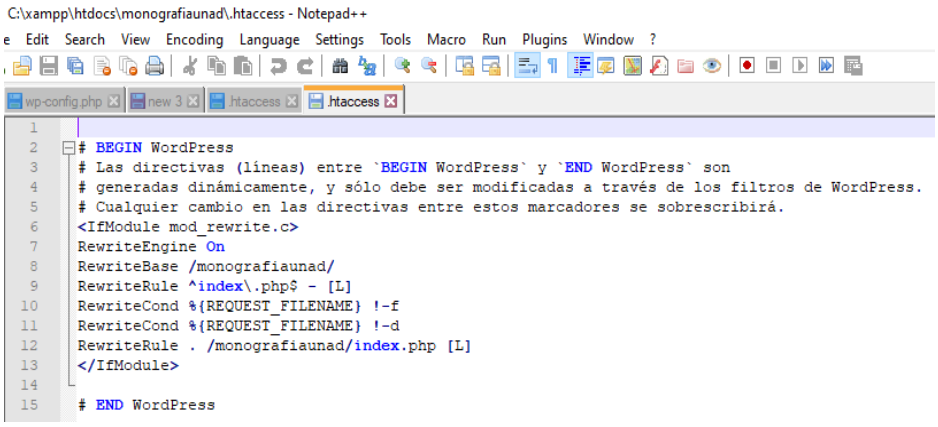
Figura 3 .Tablas de la Base de Datos de WordPress



Fuente: El Autor

El archivo .htaccess por defecto contiene la siguiente información.

Figura 4. Archivo .htaccess



Fuente: El Autor

Se puede editar con el fin de restringir el acceso a carpetas o archivos propios de WordPress tales como:

La wp-includes que contiene el cor de WordPress.

4.1.3. COMPLEMENTOS DE SEGURIDAD

WordPress tiene un conjunto de complementos o plugin los cuales son desarrollados con diferentes fines, a continuación, se enuncian algunos complementos de seguridad.

BackWPup: Es un complemento, que se integra en el backend de WordPress con el fin de realizar copias de seguridad, que se pueden guardar en un servidor FTP, Dropbox.

Figura 5. Plugin BackWPup

Fuente: El Autor

UpdraftPlus: Permite hacer copias de seguridad manual o programadas, y determinar el lapso (diario, semanal, mensual) en que se realizaran las copias de seguridad.

Themes Security: Es un plugin que tiene como función proteger el sitio web de los hackers, intrusos, identificar vulnerabilidades, software obsoleto y contraseñas débiles.

Jetpack: Es un complemento que se enfoca a la seguridad de las redes sociales y protección contra el spam.

SecuPress: Dentro sus funciones ofrecen el inicio de sesión de fuerza bruta, direcciones ip bloqueadas, visitas bloqueadas de los bots.

BulletProof Security: Este complemento se encarga de la seguridad de los inicios de sesión de una página web, herramientas anti-spam y anti-piratería.

Google Authenticator: Brinda una segunda capa de seguridad en el módulo de inicio de sesión enviando una notificación automática al teléfono.

4.2. MARCO CONCEPTUAL

Se lista una serie de conceptos relacionados con las vulnerabilidades informáticas, en el gestor de contenido WordPress.

Sistema de Gestión de Contenido (CMS): Plataforma gratuita que facilita crear y publicar contenidos web, de forma sencilla[18].

Blog: Es un espacio web para publicar, texto ideas, tutoriales, entre otros contenidos.

Código Abierto: Software que puede ser visualizado, editado, y modificado por cualquier tipo de usuario sin ningún costo monetario.

Plugin: Complemento de WordPress que tiene como función principal, agregar nuevas características o modificar la funcionalidad de un módulo en específico.

Tema (Theme): Es un complemento que permite cambiar la interfaz de un sitio web diseñado en WordPress, sin tener que modificar el código fuente.

Actualización: Código publicado en la página oficial de WordPress modificado o parcheado, por un desarrollador con el fin de brindar mejoras de seguridad a la versión actual de WordPress.

Administrador: Tipo de usuario que tiene todos los permisos para realizar cualquier tipo de modificación en WordPress, y asignar permisos a otros tipos de usuario[19].

Vulnerabilidad: Es un fallo que presenta un sistema de información o aplicativo web, el cual puede poner en riesgo la confidencialidad, integridad, disponibilidad de la información[20].

---

[18] Diccionario GLOSARIO de términos WordPress 2019 - Fecha de Consulta: [10 de enero de 2020], Ibid. 18,23
Disponible en: https://wpinsideout.com/que-es-wordpress/glosario/.

[19] *Xplora,* Glosario de términos y palabras de WordPress para principiantes, Fecha de Consulta: [5 de septiembre 2020], Disponible en: https://www.xplora.eu/glosario-wordpress/

[20] Net cloud engineering. Ciberseguridad: Amenaza vs. Vulnerabilidad, [Sitio web]. Conceptos de amenaza y vulnerabilidad, Disponible en: https://netcloudengineering.com/ciberseguridad-amenaza-vulnerabilidad/

4.3. MARCO HISTÓRICO

Por medio de diferentes consultas de fuentes confiables, se pudo identificar informes relacionados con algunas posibles causas por la cuales, se han presentado vulnerabilidades en los aplicativos diseñados en WordPress durante el transcurso del tiempo.

En el año 2015 la entidad webempresa realizó un estudio por medio de la herramienta de auditoria Wp Doctor, en el cual evaluó varios aspectos relacionados con la seguridad, algunos datos relevantes fueron[21].

El 66.97% de los sitios web no tenían protegido el archivo wp-login.
El 67.64% de los sitios web no tenían protegido el archivo wp-admin.
El 47.69% de los sitios web no tenían protegido el archivo User Agent, el cual tiene como función principal analizar las peticiones que llegaban a la web, con el fin de bloquear vistas masivas.
El 30.13% de los sitios web no tenían protegido el archivo wp-config el cual contiene información crítica como, usuario de la BD, nombre de la BD y contraseña.
El 95.78% de los sitios web diseñados en wordpress no utilizan el protocolo de seguridad SSL.
El 0,14% de los sitios web tiene el protocolo SSL caducado.
El 4,06% de los sitios web tiene el protocolo SSL correcto.

Adicional se resaltan las principales causas por las cuales wordpress es vulnerada la seguridad:[22]

[21] webempresa, Informe sobre el uso de wordpress 2015, Fecha de Consulta: [5 de septiembre 2019], Disponible en: https://www.wpdoctor.es/wp-content/uploads/2015/12/ESTUDIO-SOBRE-EL-USO-DE-WORDPRESS-2015.pdf

[22] Webempresa. Aumenta la seguridad en WordPress, ¡protege tu inversión!, Fecha Revisión: [Dic 15, 2014], Fecha de Consulta: [5 de septiembre 2019], Disponible en: https://www.webempresa.com/blog/aumenta-la-seguridad-en-wordpress-protege-tu-inversion.html

El 41% este cms es atacado por las vulnerabilidades no parcheadas en su hosting.
El 29% es atacado por utilizar temas no actualizados.
El 22 % es atacado por utilizar plugins infectados.
También la empresa Cisco anualmente publica un informe a nivel general relacionado con la seguridad, como es el caso del informe del año 2016 donde cita algunos aspectos relacionados con el gestor de contenido WordPress. En este informe, señala las principales causas por las cuales los aplicativos de WordPress son vulnerables.

- La versión de WordPress no está actualizada.
- Las contraseñas de administrador son débiles.
- Instalación de plugin que no cuentan con parches de seguridad.
- Adicional a esto, los investigadores de Cisco identificaron un grupo de malware que se ejecutaban en aplicativos diseñados en este CMS como:[23]
- Malware Dridex: La principal función es el robo de información.
- Malware Pony: La principal función es almacenar usuario y contraseña con el fin de enviarlos a servidores remotos, controlados por los ciberdelincuentes.
- Malware Necurs: Su principal función es infectar a los pc que tengan instalado el sistema operativo Windows, con el fin de pasarlos a un botnet y robar la información.
- Ransomware Cryptowall: Se infiltra en el sistema operativo por medio de correos electrónicos, o descargar fraudulentas con el fin de encriptar la información.
- Por otro lado, el 29 de mayo del 2019 se reportó una vulnerabilidad crítica, en el plugin convert plus con un estimado de 100.000 instalaciones activas. Esta vulnerabilidad permitía al atacante registrar nuevos usuarios con rol de

[23] Cisco, Cisco 2016 informe anual de seguridad, Fecha de Consulta: [5 de septiembre 2019], Disponible en: https://www.cisco.com/c/dam/m/es_mx/assets/offers/pdfs/cisco_2016_asr_011116_es-xl.pdf

administrador. Como posible solución se lanzó una regla de firewall que se podía utilizar después de los 30 días, para versiones gratuitas de WordPress[24].

Finalmente, el investigador en seguridad Sam Thomas, descubrió un fallo deserialización en PHP que pone en riesgo a millones de sitios web WordPress. Este tipo de riesgo consiste en que el atacante manipula la función serialize () que se utiliza para almacenar valores y la función unserialize () para recuperar dichos valores[25].

4.4. ESTADO ACTUAL

En diferentes países existen comunidades en pro de mejorar frecuentemente el gestor de contenido WordPress, y los aplicativos diseñados en este. En Colombia en diferentes ciudades existen grupos de profesionales, desarrolladores, que se reúnen para intercambiar ideas relacionadas con WordPress con el fin de fomentar un aprendizaje colectivo, y aportar frecuentemente mejoras.[26]Entre estas mejoras están los plugin de seguridad los cuales cada uno tiene una funcionalidad, como el rastreo de los elementos web, análisis de archivos para comprobar modificaciones, análisis de malware entre otros, todos en pro de mejor la seguridad de los aplicativos webs.

[24] Entelgy.Accelerating the change. [sitio web], Nuevas vulnerabilidades en diferentes plugins de WordPress, Fecha Revisión: [Dic 15, 2014], Fecha de Consulta: [3 de junio 2019], Disponible en: https://www.entelgy.com/divisiones/innotec-security/innotec-security-actualidad/innotec-security/noticias-del-sector-innotecsecurity/nuevas-vulnerabilidades-en-diferentes-plugins-de-wordpress

[25] MuySeguridad, [sitio web], Un fallo de deserialización en PHP pone en riesgo a millones de sitios web WordPress, Fecha Revisión:[17 agosto 2018], Fecha de Consulta: [16 de enero de 2020], Disponible en: https://www.muyseguridad.net/2018/08/17/fallo-deserializacion-php-riesgo-wordpress/

[26] Comunidadestech. WordPress Medellín, Fecha de Consulta: [16 de enero de 2020], Disponible en: https://www.rutanmedellin.org/comunidadestech/wordpress-medellin/

4.5. MARCO LEGAL

Teniendo en cuenta la importancia y utilidad que día a día tiene las páginas web diseñadas en diferentes plataformas o gestores de contenido como WordPress, es necesario que los administradores del sitio web apliquen las leyes expedidas por el gobierno nacional que respalden la seguridad y confidencialidad de los datos e información. En Colombia el 5 de enero del 2009 el congreso de la republica publicó la ley 1273 " de la protección de la información y de los datos" en el cual se estipula una serie de artículos, uno de estos es:

- Artículo 269A: Acceso abusivo a un sistema informático.
- Artículo 269E: Uso de software malicioso.
- Artículo 269F: Violación de datos personales.
- Artículo 269G: Suplantación de sitios web para capturar datos personales.

Los cuales se enfocan a nivel general de la penalidad que causa los delitos informáticos, el uso de software malicioso, violación de datos personales, daños informáticos, suplantación de sitios web, entre otros[27].

También la ley 1581 del 2012 trata del derecho constitucional que tiene los colombianos, a conocer, actualizar y rectificar la información que se haya archivo en las bases de datos de una entidad, y de igual forma la autorización y tratamiento de datos personales y tratamiento de datos sensibles. Algunos de los artículos que se relacionan con el desarrollo de esta monografía son: [28]

Artículo 2°. Ámbito de aplicación.

Artículo 3°. Definiciones.

[27] Ley 1273 de 2009, [sitio web], Fecha de Consulta: [19 de enero de 2020], Disponible en: https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=34492

[28] Ley 1581 de 2012, [Sitio web].[Citado el 2 de Febrero del 2021].Disponible en: https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=49981

Artículo 4°. Principios para el Tratamiento de datos personales.

Artículo 5°. Datos sensibles.

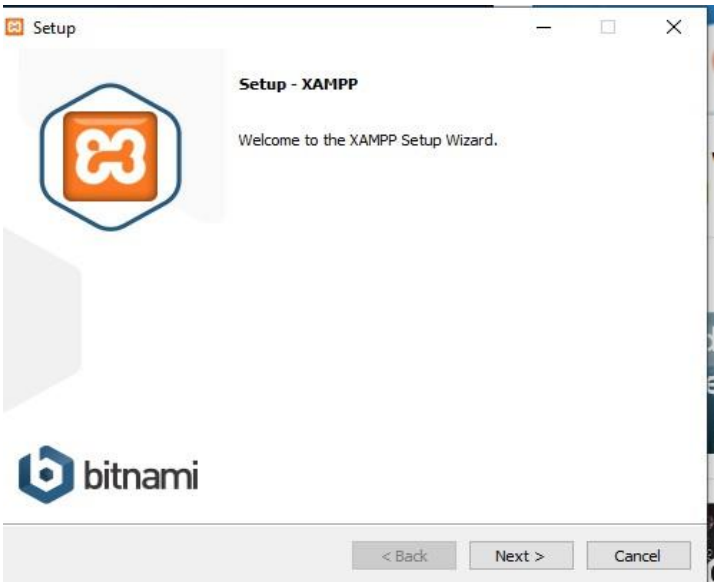
Artículo 6°. Tratamiento de datos sensibles.

4.6. MARCO TECNOLÓGICO

Para esta monografía se utilizará algunas herramientas informáticas como son:

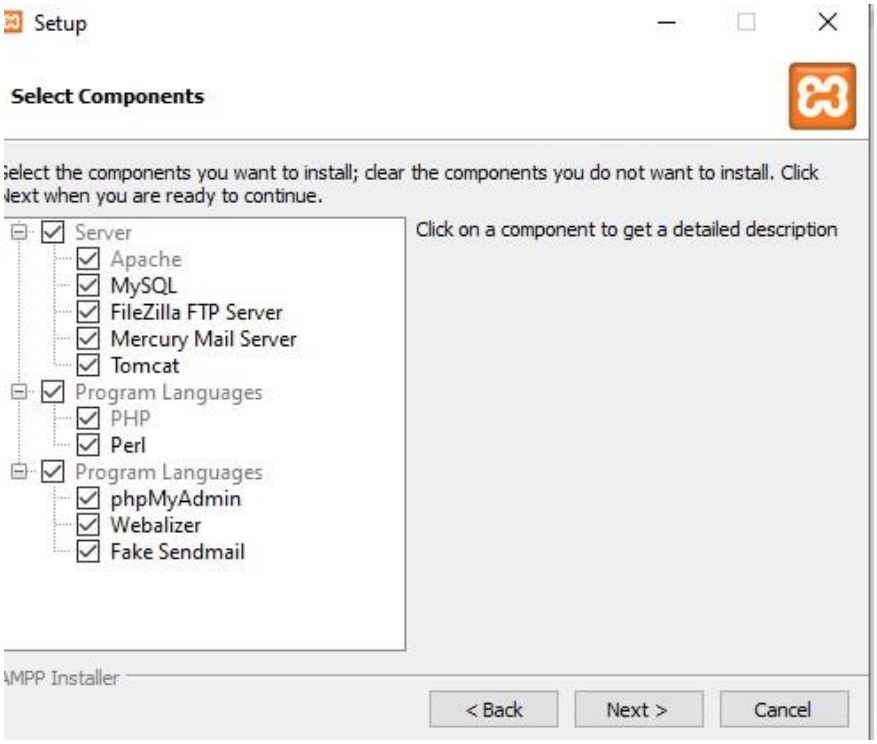
- El servidor gratuito de Xampp.
- PhpMyadmin donde se crea la Base de Datos.
- Instalación de WordPress.
- A continuación, se adjunta algunas evidencias de la instalación.

Figura 6. Setup de Xampp



Fuente: El Autor

Figura 7. Componentes a instalar

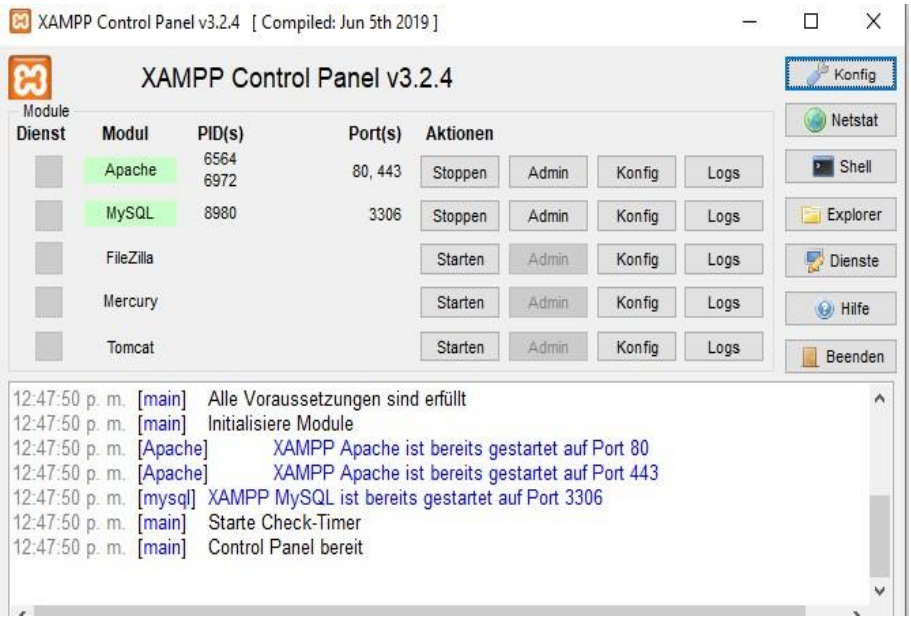


Fuente: El Autor

Figura 8. Inicio de la instalación de Xampp

Fuente: El Autor

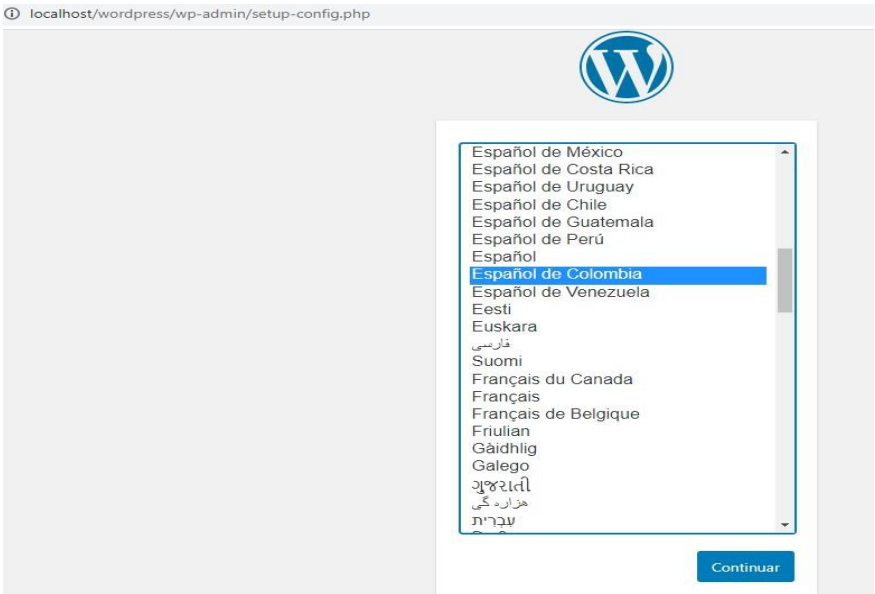
Figura 9. Panel de Control de Xampp



Fuente: El Autor

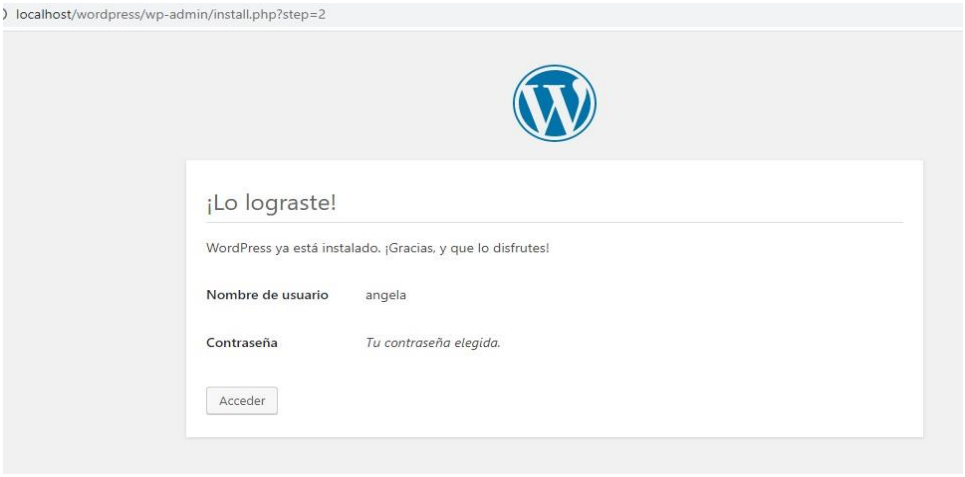
4.6.1. INSTALACIÓN DE WORDPRESS

Figura 10. Inicio de la instalación de wordpress



Fuente: El Autor

Figura 11.Instalación con éxito



Fuente: El Autor

Figura 12. Página de prueba en Wordpress local

Fuente: El Autor

La finalidad de instalar el gestor de contenido WordPress de forma local, es para realizar simulaciones de ataques por medio de kali linux.

5. METODOLOGIA PARA DESARROLLAR OBJETIVOS

5.1. ANÁLISIS DE LA INFORMACIÓN SOBRE LA SEGURIDAD INFORMÁTICA DEL CMS WORDPRESS

Metodología: Para este objetivo se cita información extraída de informes y estudios realizados por parte de empresas dedicadas a la seguridad informática. A nivel general se da a conocer información que ha impactado la seguridad informática en el gestor de contenido WordPress.

A continuación, se da inicio al desarrollo haciendo referencia a los estudios de seguridad informáticas en WordPress.

Según la fundación Linux, y el científico informático Nicko Van Someren consideran que la principal ventaja de los CMS Open Source, es tener el código disponible el cual facilita al amplio grupo de desarrolladores, a generar una pronta solución en caso de presentar algún tipo de bug de seguridad en algún aplicativo[29].

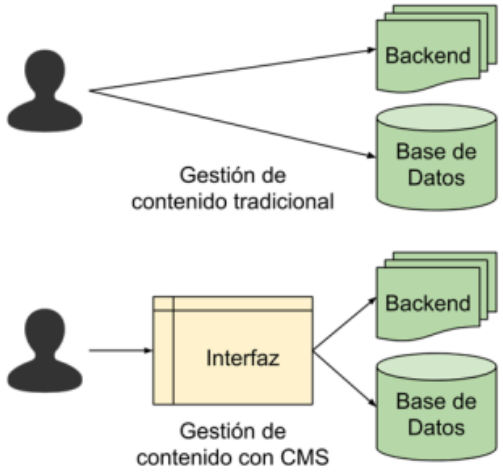
Siendo la seguridad un item fundamental de un sitio web, a nivel general algunas empresas como sucuri indica en uno de sus informes, las principales causas por el cual los CMS son atacados o vulnerados, se debe a la deficiente gestión de la plataforma por parte de los administradores, ya que en el año 2016 el 61% de los sitios web diseñados en WordPress fueron vulnerados el cual tenían la versión desactualizada.

[29] CREATIVE DESIGNER.Sobre la seguridad de los CMS Open Source, Fecha Revisión: [28 mayo 2018], Fecha de Consulta: [16 de enero de 2020], Disponible en: https://www.fcomoreno.net/sobre-la-seguridad-de-los-cms-open-source

Otra forma que utilizan los hackers para vulnerar los CMS, es ejecutando ataques de fuerza bruta o ataques de diccionario con el fin de tener acceso al aplicativo [30].

5.1.1. ESQUEMA BÁSICO DE UN CMS FRENTE A UN APLICATIVO WEB SIN CMS

Figura 13. Esquema básico de un cms frente a un aplicativo web sin cms



Fuente: Errores comunes en los CMS (en línea) 6 febrero, 2015 (Consultado 5 de noviembre 2020) Disponible en: https://empresas.blogthinkbig.com/errores-comunes-en-los-cms/

En el esquema anterior se puede resaltar el componente intermedio “Interfaz” que tiene los CMS. Este componente ha incrementado el porcentaje de puntos de acceso potencialmente vulnerables al sistema.

A continuación, se listan algunas vulnerabilidades relacionadas con los CMS:

1) Búsqueda de versiones antiguas: Es necesario tener actualizado todos los componentes del CMS, ya que tener versiones desactualizadas del gestor de contenido WordPress está más vulnerable a los ataques informáticos.

[30] Powered by prestigia, Seguridad en internet, Fecha de Consulta: [16 de enero de 2020], Disponible en: https://seguridad.prestigia.es/seguridad-en-los-cms/

2) Copias de Seguridad: Es recomendable hacer copias de seguridad periódicamente, verificando que ningún plugin guarde copias en directorios públicos.
3) Copias de archivos de configuración: Al duplicar archivos como wp_config.php que contiene información crítica, es recomendable borrar estas copias.
4) Plugin Inseguros: Los CMS utilizan plugin que en algunos casos son desarrollados por los mismos atacantes o aficionados sin habilidades de programación, por tal motivo estos plugin contienen vulnerabilidades que se convierten en un punto de acceso al CMS[31].

Finalmente, Sucuri público un informe sobre amenazas a sitios web del año 2019, donde indico que el 56 % de las aplicaciones diseñadas por un CMS tenía una versión desactualizada. Por otro lado, el CMS más utilizado fue WordPress con un 94.23% frente a otros gestores de contenido[32].

VULNERABILIDADES INFORMÁTICAS EN WORDPRESS

Tabla 2. Vulnerabilidades informáticas en WordPress

FECHA	AUTOR	DESCRIPCIÓN	ORIGEN
2016	Sucuri	En el 2016 la empresa de seguridad Sucuri indico que aproximadamente 11.000 sitios web resultaron infectados, el 75% de estos sitios estaban diseñados en WordPress y el 50 % tenían	https://sucuri.net/reports/2016-q1-hacked-website-report/

[31] Telefónica CYBER SECURITY COMPANY,Errores comunes en los CMS Fecha Revisión: [6 Febrero 2015], Fecha de Consulta: 16 de enero de 2020], Disponible en: https://empresas.blogthinkbig.com/errores-comunes-en-los-cms/
[32] Sucuri, Informe sobre amenazas a sitios web pirateados - 2019, Fecha Revisión: [28 Enero 2020], Fecha de Consulta: [5 de Noviembre de 2020], Disponible en: https://blog.sucuri.net/2020/01/hacked-website-threat-report-2019.html

		una versión desactualizada. Otra causa de infección en sitios web fue la explotación de vulnerabilidades del software, relacionado con los componentes de la plataforma como: plugin, plantillas, complementos entre otros.	
2017	Sucuri	En el 2017 según un informe de la empresa de seguridad web, Sucuri indico que los 3 CMS más vulnerables fueron WordPress (83%), Joomla (13,1%) y Magento (6,5%). Una de las principales causas de estas vulnerabilidades fue por la mala gestión de la plataforma desde una óptica de seguridad y protección por parte del administrador del sitio web.	https://sucuri.net/reports/Sucuri-Hacked-Report-2017.pdf

Tabla 3. (Continuación)

2018	Sucuri	En el 2018 según un informe de la empresa de seguridad web, Sucuri indico que las infecciones informáticas aumentaron de un 83% en el año 2017 al 90% del 2018.Algunas de las causas del incremento se debe a problemas de configuración de seguridad, falta de conocimientos o recursos sobre seguridad, mantenimiento general del sitio entre otros.	https://sucuri.net/reports/2018-hacked-website-report/
2019	Sucuri	En el 2019 según un informe de la empresa de seguridad web, Sucuri indico que las amenazas informáticas estaban más complejas y los atacantes estaban utilizando vulnerabilidades conocidas, en campañas de automatización masivas con el fin de atacar a sitios web de grandes y medianas empresas. Por otro lado, el 47% de sitios web se infectaron por medio de puertas traseras y el 53% por inyecciones sql.	https://sucuri.net/reports/2019-hacked-website-report/

		Por medio de sucuri Firewall se mitigo 170 millones de intentos de ataques de tipo bots maliciosos, ataques DDos y parches virtuales para vulnerabilidades conocidas.	

Fuente: El Autor

Tabla 4. Resumen de algunas Vulnerabilidades en WordPress

Fecha de Publicación	Versión de WordPress	Tipo de Vulnerabilidad	Descripción de la Vulnerabilidad	Versión corregida	Origen
22 de junio de 2016	WordPress 4.5.2	Denegación de servicio (DoS) oEmbed	Un atacante puede aprovechar este problema para provocar condiciones de denegación de servicio.	WordPress 4.5.3	https://wpscan.com/vulnerability/2ca0753d-6ae1-43f2-8a8b-e61a32c34b91

Tabla 5. Continuación

07 de marzo de 2017	WordPress 4.7.2 y anteriores	Ejecución de comandos maliciosos	Esta vulnerabilidad redirigía el sitio web del usuario a otra página para robarle información mediante phishing.	WordPress 4.7.3	https://www.incibe.es/protege-tu-empresa/avisos-seguridad/solucion-vulnerabilidades-wordpress-473
05 de febrero de 2018	WordPress 4.9.2 y anteriores	Vulnerabilidad de denegación de servicio	El atacante bloquea la aplicación afectada, logrando la denegación de servicio.		https://www.securityfocus.com/bid/103060/references
24 de julio de 2019	WordPress 5.2.3 y versiones anteriores	Denegación de servicio remota.	Vulnerabilidades de tipo Cross-site scripting (XSS), que permitía a un atacante ejecutar código malicioso en el equipo de la víctima.	WordPress 5.2.4	https://www.incibe.es/protege-tu-empresa/avisos-seguridad/actualizacion-seguridad-wordpress-0

Fuente: El Autor

5.2. HERRAMIENTAS INFORMÁTICAS DE AUDITORIA ADECUADAS PARA ANALIZAR LA SEGURIDAD DEL GESTOR DE CONTENIDOS WORDPRESS

Metodología: Debido a que existe un amplio grupo de herramientas informáticas, se clasifican las que se enfocan en el análisis de vulnerabilidades en el gestor de contenido WordPress.

Los sitios web en la actualidad, son de gran importancia para cualquier empresa u organización por esta razón el porcentaje de páginas web publicadas en la internet va en aumento. Debido a esto es indispensable realizar escaneos a los sitios web por medio de herramientas informáticas, con el fin obtener un informe a nivel general de los posibles riesgos y vulnerabilidades, que se puedan estar presentando en los sitios web.

A continuación, se lista algunas herramientas informáticas las cuales realizan escaneos de seguridad web.

Sqlmap: Es una herramienta Open Source que se utiliza para hacer pruebas de penetración, una de sus principales funciones es identificar posibles vulnerabilidades en los aplicativos webs [33] .

Nikto: Es una herramienta Open Source que se utiliza para el análisis de seguridad de red y buscar vulnerabilidades en servidores web, para identificar errores de configuración, verificación de versiones no actualizadas.

[33] Sqlmap, herramienta automática para pruebas de penetración (Sql Injection) Fecha Revisión: [20/04/2018], Fecha de Consulta: [5 de Noviembre de 2020], Disponible en: https://securityhacklabs.net/articulo/sqlmap-herramienta-automatica-para-pruebas-de-penetracion-sql-injection Ibid.

Vega: Herramienta Open Source que se utiliza para escanear la seguridad de aplicaciones web, ya que funciona como proxy con el fin de identificar las peticiones que se realizan durante la navegación[34].

Acunetix: Es un complemento gratuito diseñado para monitorear los sitios web en búsqueda de vulnerabilidades informáticas. Una de las principales funciones de este complemento en pro de la seguridad de los aplicativos diseñados en el gestor de contenido WordPress es:

- Agrega index.php automáticamente a los directorios de WordPress para evitar la divulgación de información.
- Eliminación de la versión de WordPress.
- Eliminación de la información de actualización de WordPress para usuarios no administradores de WordPress.
- Eliminación de la información de actualización del tema de WordPress para usuarios no administradores de WordPress.
- Desactiva el informe de errores de la base de datos.
- Deshabilita el informe de errores de PHP.[35]

Owasp Zap: Es una herramienta Open Source que se utiliza para realizar pruebas de penetración, con el fin de identificar vulnerabilidades en un sitio web[36].

Esta herramienta es un escáner de seguridad para aplicaciones web. Tiene varios módulos como Proxy para capturar, fuzzer para identificar vulnerabilidades

[34] Universitat Oberta de Catalunya, [sitio web], Generación de reportes de vulnerabilidades y amenazas para aplicaciones web, Fecha de Consulta: [5 de Noviembre de 2020], Disponible en: http://openaccess.uoc.edu/webapps/o2/bitstream/10609/26821/6/evagonzalezTFM0114memoria.pdf

[35] Acunetix. Complemento de seguridad de WordPress de Acunetix, Fecha de Consulta: [5 de Noviembre de 2020], Disponible en: https://www.acunetix.com/websitesecurity/wordpress-security-plugin/

[36] Caballero Eduardo, Pruebas de Penetración con Zed Attack Proxy, https://owasp.org/www-pdf-archive//OWASP_ZAP_Alonso_ReYDeS.pdf , [Citado el 6 de Noviembre de 2020]

informáticas, araña para descubrir las web aplicaciones, escáner para ataque activo y pasivo y método de diccionario para acceder a los archivos. [37].

Wpscan: Es un escáner web que puede detectar la siguiente información de un sitio web:

- Detecta vulnerabilidades de seguridad.
- Identifica el listado de plugin utilizados en un aplicativo web y clasifica los plugin posiblemente, vulnerables a la explotación.
- Descubrimiento de contraseñas débiles [38].

También existe algunos escáneres de vulnerabilidades web en línea como:

Escáner Geekflare: Realiza un análisis del sitio web identificando vulnerabilidades del núcleo, tema, complementos y las bibliotecas de JavaScript del lado del cliente que son vulnerables.

Este escáner permite hacer una prueba gratis, la url es https://gf.dev/wordpress-security-scanner[39].

[37] Testing for Security Weakness of Web Applications using Ethical Hacking, Fecha de Consulta: [5 de Noviembre de 2020], Disponible en: https://ieeexplore-ieee-org.bibliotecavirtual.unad.edu.co/stamp/stamp.jsp?tp=&arnumber=9143018

[38] Herramientas Kali Linux, Fecha Revisión: [9 Octubre 2016], Fecha de Consulta: [5 de Noviembre de 2020], Disponible en: https://seguridadkalilinux.wordpress.com/author/seguridadkalilinux/

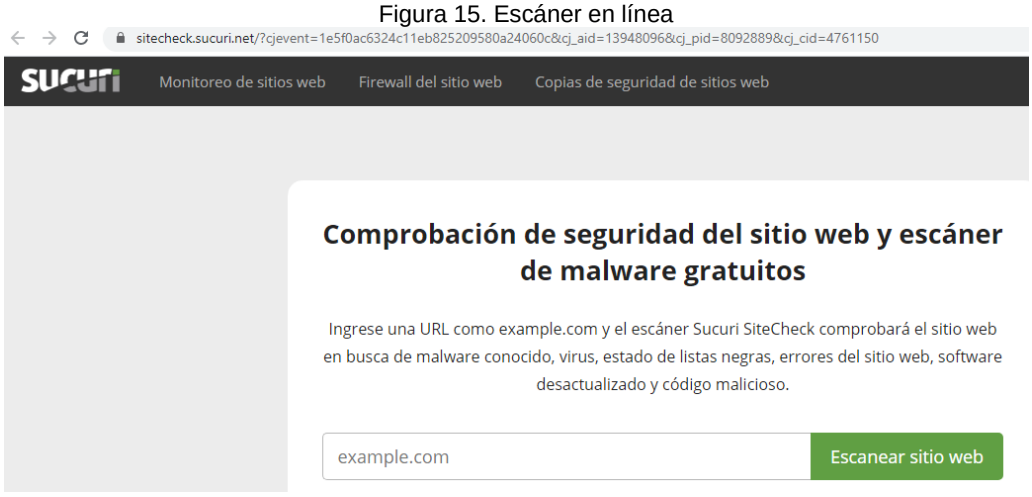
[39] Geekflare, Escáner de seguridad de WordPress, Fecha de Consulta: [5 de Noviembre de 2020], Disponible en: https://gf.dev/wordpress-security-scanner

Figura 14. Escáner de seguridad

Fuente: Escáner de seguridad de WordPress (en línea) (Consultado el 23 de noviembre 2020). Disponible en: https://gf.dev/wordpress-security-scanner

Sucuri: Realiza un análisis del sitio web identificando algunos item como: listas negras, malware, software desactualizado[40].

Figura 15. Escáner en línea

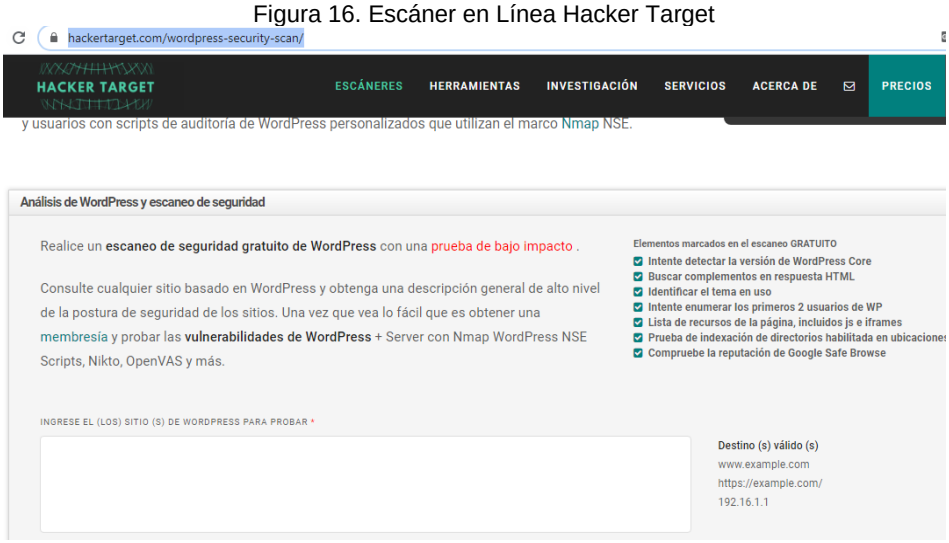


Fuente: El Autor

[40] Sucuri, Comprobación de seguridad del sitio web y escáner de malware gratuitos, Fecha de Consulta: [2 de Noviembre de 2020] Disponible en: https://sitecheck.sucuri.net/?cjevent=f8521b5f324e11eb829a09e40a24060f&cj_aid=13948096&cj_pid=8092889&cj_cid=4761150

Destino hacker: Este escáner mediante el análisis de páginas web puede identificar versión tanto de WordPress, complementos y temas. También lista los elementos de la página incluyendo los iframes y js[41].

Figura 16. Escáner en Línea Hacker Target



Fuente: El Autor

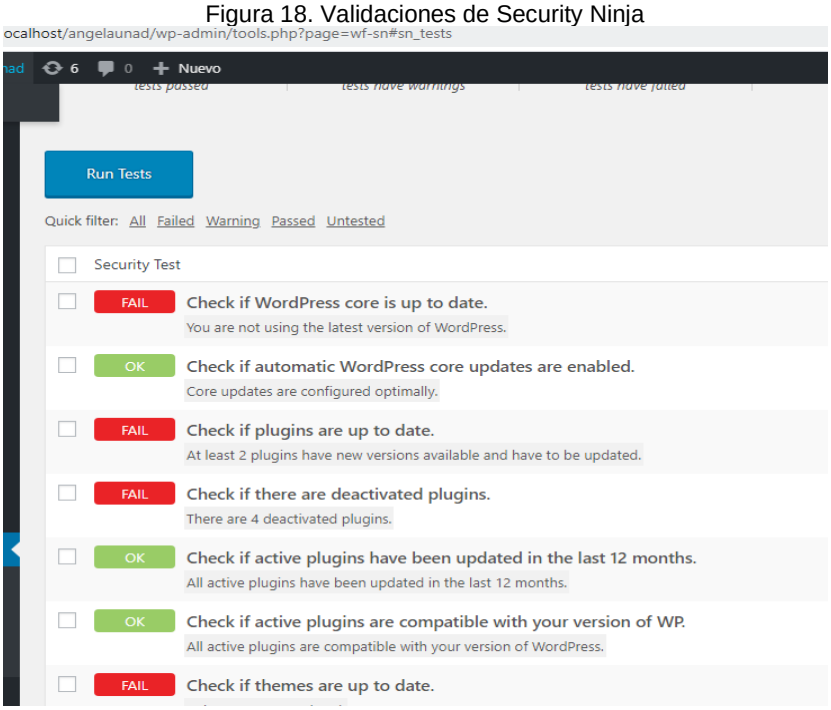
Security Ninja: Es un complemento de seguridad de WordPress que realiza un análisis de un sitio web, y genera un listado de las vulnerabilidades encontradas.

[41] HACKER TARGET. Análisis De Seguridad De WordPress, Fecha de Consulta: [5 de Octubre de 2020], Disponible en: https://hackertarget.com/wordpress-security-scan/

Figura 17. Complemento de seguridad

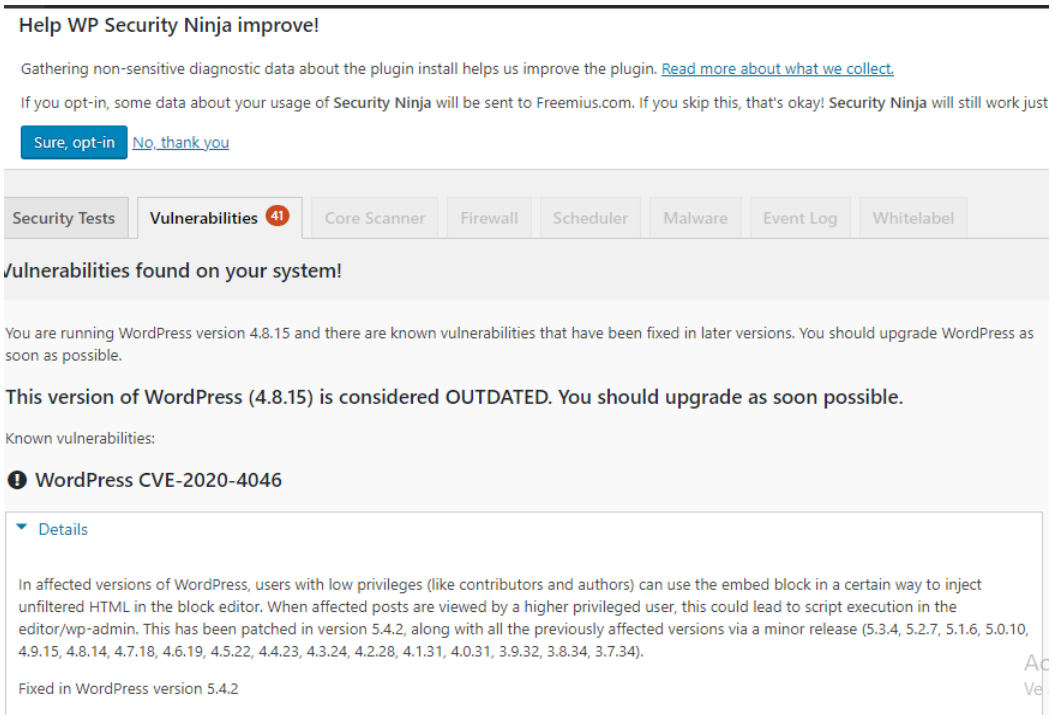
Fuente: El autor

Figura 18. Validaciones de Security Ninja



Fuente: El autor

Figura 19. Lista de Vulnerabilidades en WordPress



Fuente: El autor

Escáner Pentest: Realiza análisis de sitios web identificando y generando un informe con la siguiente información:

- Identifica la versión de WordPress del tema y complementos.
- Lista las vulnerabilidades y exploits.
- Indica posibles problemas de configuración y las rutas de las carpetas y archivos[42].

[42] Pentest-Tools, Escáner de vulnerabilidad de sitios web, Fecha de Consulta: [5 de Octubre de 2020], Disponible en: https://pentest-tools.com/website-vulnerability-scanning/website-scanner

Figura 20. Escáner en línea WPScan

Fuente: Escáner de vulnerabilidades de WordPress – WPScan. (en línea). (Consultado el 29 de noviembre 2020). Disponible en: https://pentest-tools.com/cms-vulnerability-scanning/wordpress-scanner-online-wpscan

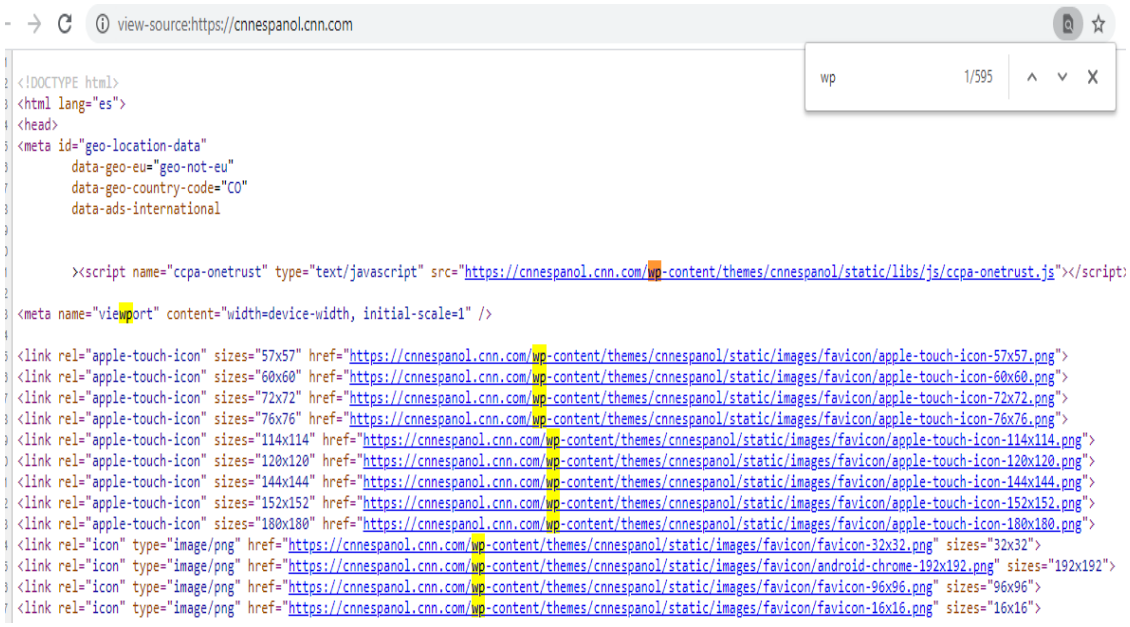
ANÁLISIS DE UNA PÁGINA WEB DISEÑADA EN WORDPRESS CON OWASP ZAP

Teniendo en cuenta el listado de las herramientas y escáner de vulnerabilidades que existe, para esta monografía se realizó un escaneo con la herramienta OWASP ZAP, a una página diseñada en WordPress el cual se obtuvo una lista de algunas url vulnerables, como se evidencia en las imágenes.

Antes de utilizar la herramienta OWASP ZAP se realizó unas verificaciones manuales como:

Se consulta el código fuente de la página web https://cnnespanol.cnn.com/ y se busca información relacionada con WordPress, como la carpeta, wp-content.

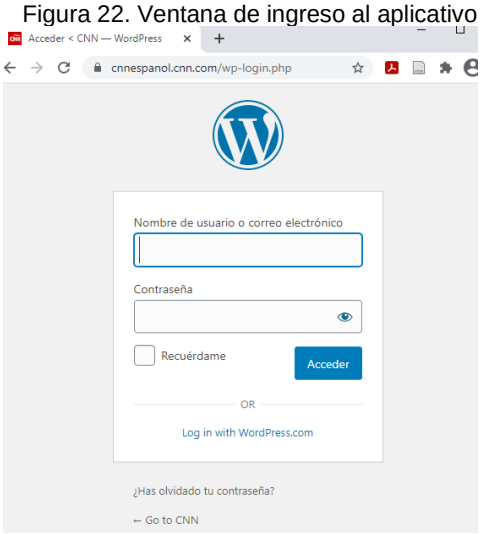
Figura 21.Código Fuente



Fuente: El Autor

Al ingresar la url https://cnnespanol.cnn.com/wp-login.php se visualiza la ventana de logueo, el cual si se tiene el usuario y la contraseña se podrá realizar modificaciones al aplicativo.

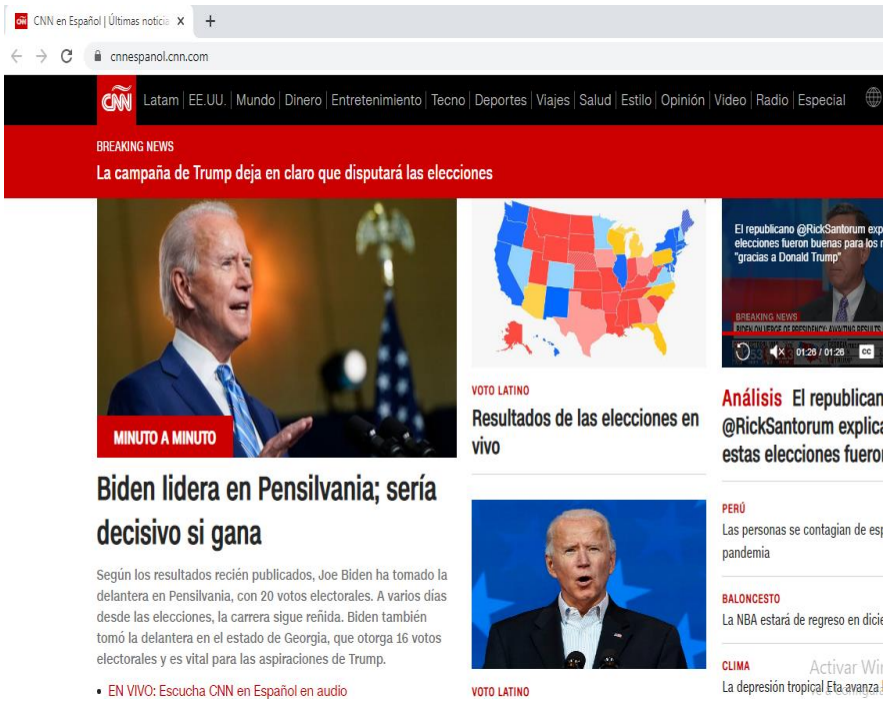
Figura 22. Ventana de ingreso al aplicativo



Fuente: El autor

Se ingresa a la página web https://cnnespanol.cnn.com/

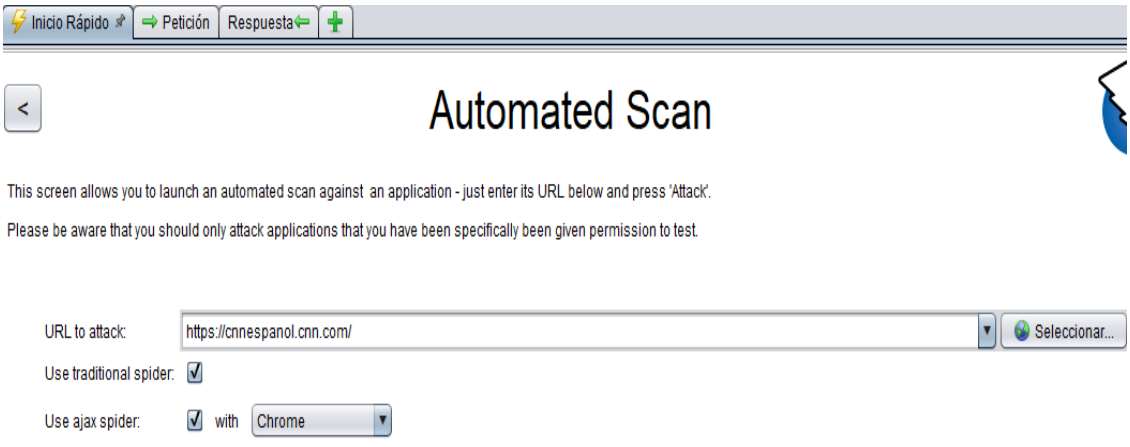
Figura 23. Página web cnn.com



Fuente: El Autor

Luego se copia la url https://cnnespanol.cnn.com/ a la herramienta OWASP ZAP donde inicia el escaneo.

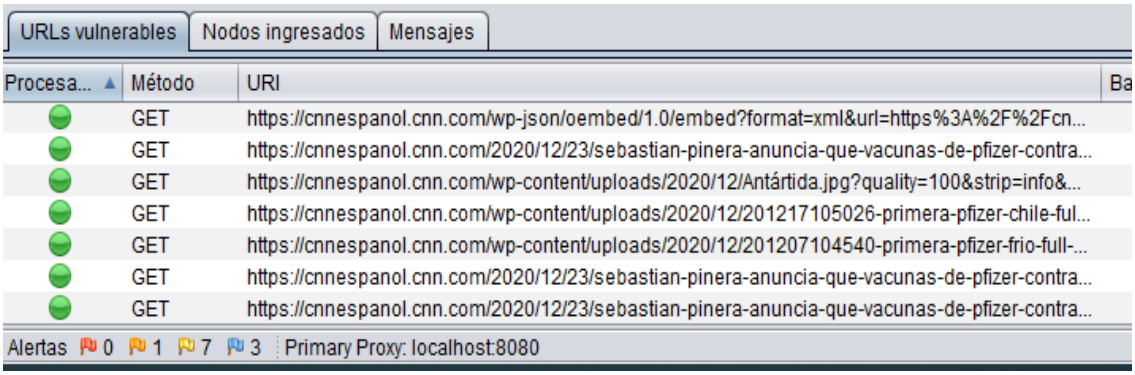
Figura 24. Ventana de escaneo OWASP ZAP



Fuente: El Autor

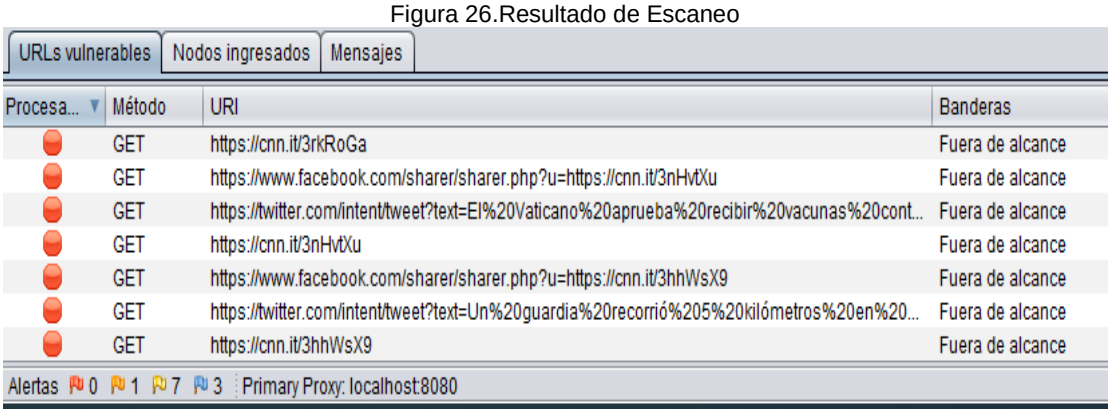
Por medio del escaneo con la herramienta OWASP ZAP se obtiene un listado de algunas posibles vulnerabilidades, y el detalle de cada una de estas, ejemplo Absence of Anti-CSRF Tokens (Ausencia de tokens anti-CSRF), como se evidencia en la imagen y descripción.

Figura 25. Resultado de Escaneo



Fuente: El Autor

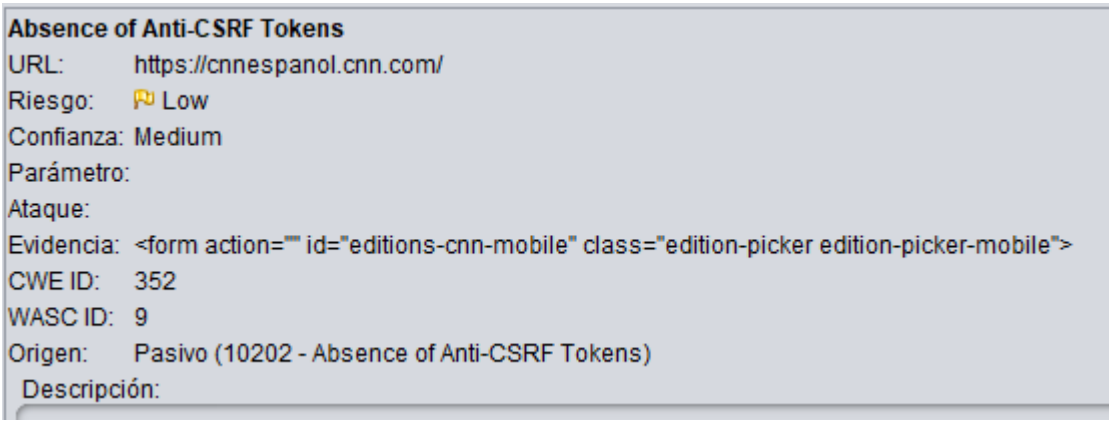
Figura 26.Resultado de Escaneo



Fuente: El Autor

Absence of Anti-CSRF Tokens (Ausencia de tokens anti-CSRF)

Figura 27. Descripción de una Vulnerabilidad



Fuente: El Autor

Descripción generada por la Herramienta OWASP ZAP

Una solicitud falsa entre sitios en un ataque que compromete y obliga a una víctima a enviar su solicitud HTTP a un destino objetivo sin su conocimiento o intención para poder realizar una acción como víctima. La causa oculta es la funcionalidad de la aplicación utilizando acciones de URL/formulario que pueden ser adivinados de forma repetible. La naturaleza del ataque es que CSRG explota la confianza que un sitio web proporciona a un usuario. Por el contrario, las cadenas de comandos de los sitios cruzados (XSS) explotan la confianza que un usuario proporciona en un sitio web. Al igual que XSS, los ataques CSRG no son de forma necesaria de sitios cruzados, pero hay la posibilidad de que si pueden serlo. La falsificación de las solicitudes ente los sitios también se conocen como CSRF, XSRG, ataques con un solo clic.

Los ataques de CSRG son muy efectivos en varias situaciones, que incluyen:

- La victima tiene una sesión activa en el sitio de destino.

- La víctima se autoriza por medio de la autenticación HTTP en el sitio de destino.
- La víctima se encuentra en la misma red local que el sitio de destino.

CSRF se ha utilizado especialmente para poder realizar una acción contra un sitio objetivo utilizando los privilegios de la víctima, pero se han revelado técnicas recientes para difundir información al obtener el acceso a la respuesta. El riesgo de divulgación de información aumenta de forma drástica cuando el sitio de destino se encuentra vulnerable a XSS, porque XSS se puede utilizar como una plataforma para CSRF, lo que le permite al atacante que opere desde adentro de los límites de la misma política de origen.

Enumeración de debilidades comunes (CWE) 352: Falsificación de solicitudes entre sitios. La aplicación web no puede, verificar suficientemente si el usuario que envió la solicitud proporcionó intencionalmente una solicitud coherente, válida y bien formada[43].
WASC-9 (Falsificación de solicitud entre sitios): Es un ataque que implica forzar a una víctima a enviar una solicitud HTTP a un destino objetivo sin su conocimiento o intención para realizar una acción como víctima[44].

5.2.1. PRUEBAS REALIZADAS CON KALI LINUX

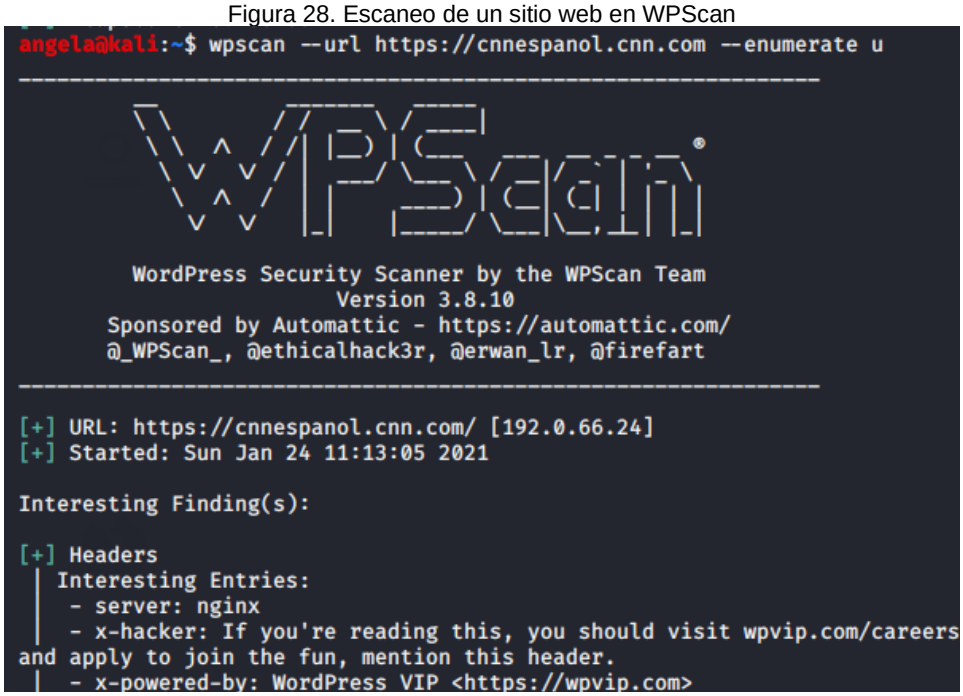
A continuación, se dará a conocer por medio de imágenes las pruebas de seguridad que se realizaron, con algunas de las herramientas de Kali Linux.

[43] CWE Enumeración de debilidades comunes, [Sitio web], CWE-352: Falsificación de solicitudes entre sitios (CSRF), Fecha de Consulta: [Citado el 22 de enero 2021] Disponible en: https://cwe.mitre.org/data/definitions/352.html
[44] Falsificación de solicitud entre sitios, [Sitio web], Fecha de Consulta: [Citado el 22 de enero 2021] Disponible en: http://projects.webappsec.org/w/page/13246919/Cross%20Site%20Request%20Forgery

En la herramienta WPSCAN se ejecutó el siguiente comando ***wpscan --url https://cnnespanol.cnn.com --enumerate u***, con el fin de obtener la siguiente información:

Nombre del servidor web de código abierto nginx.

Figura 28. Escaneo de un sitio web en WPScan

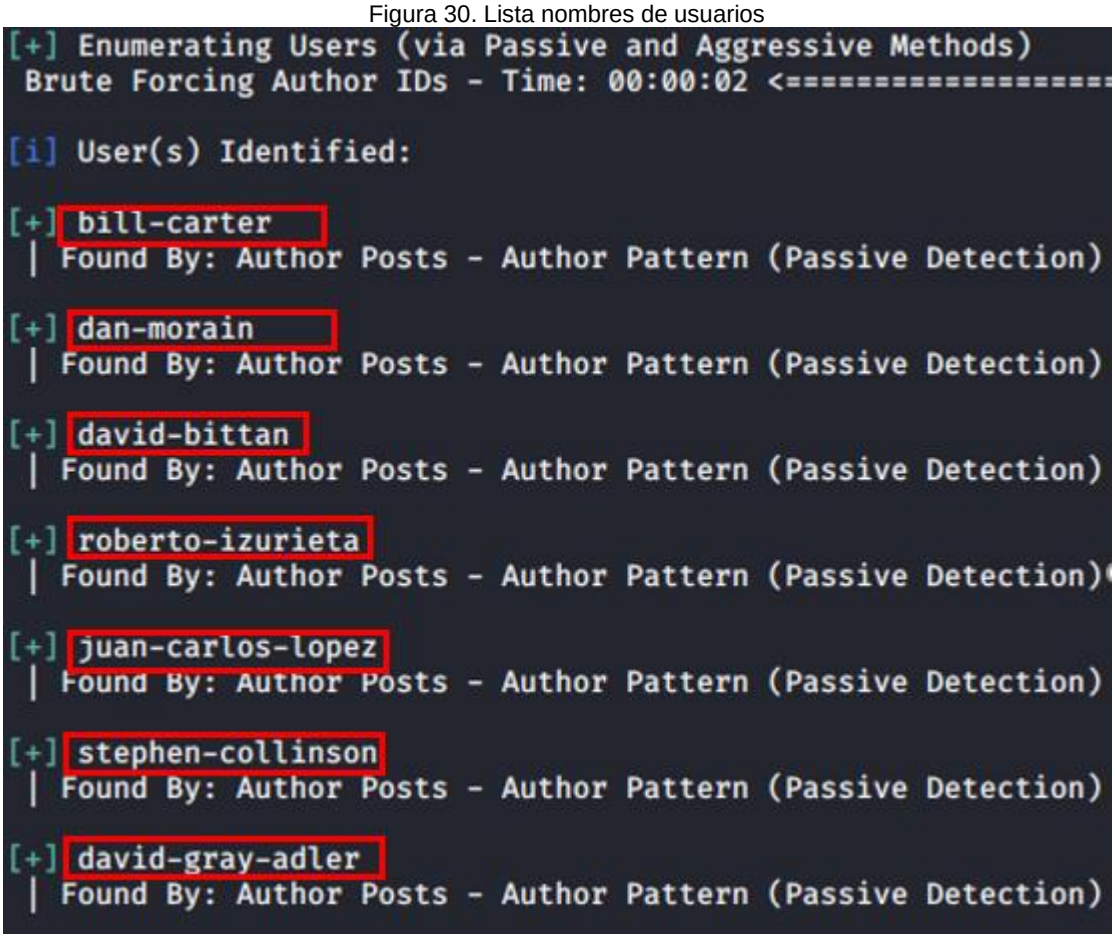


Fuente: El Autor

Figura 29. Versión de Wordpress

Fuente: El Autor

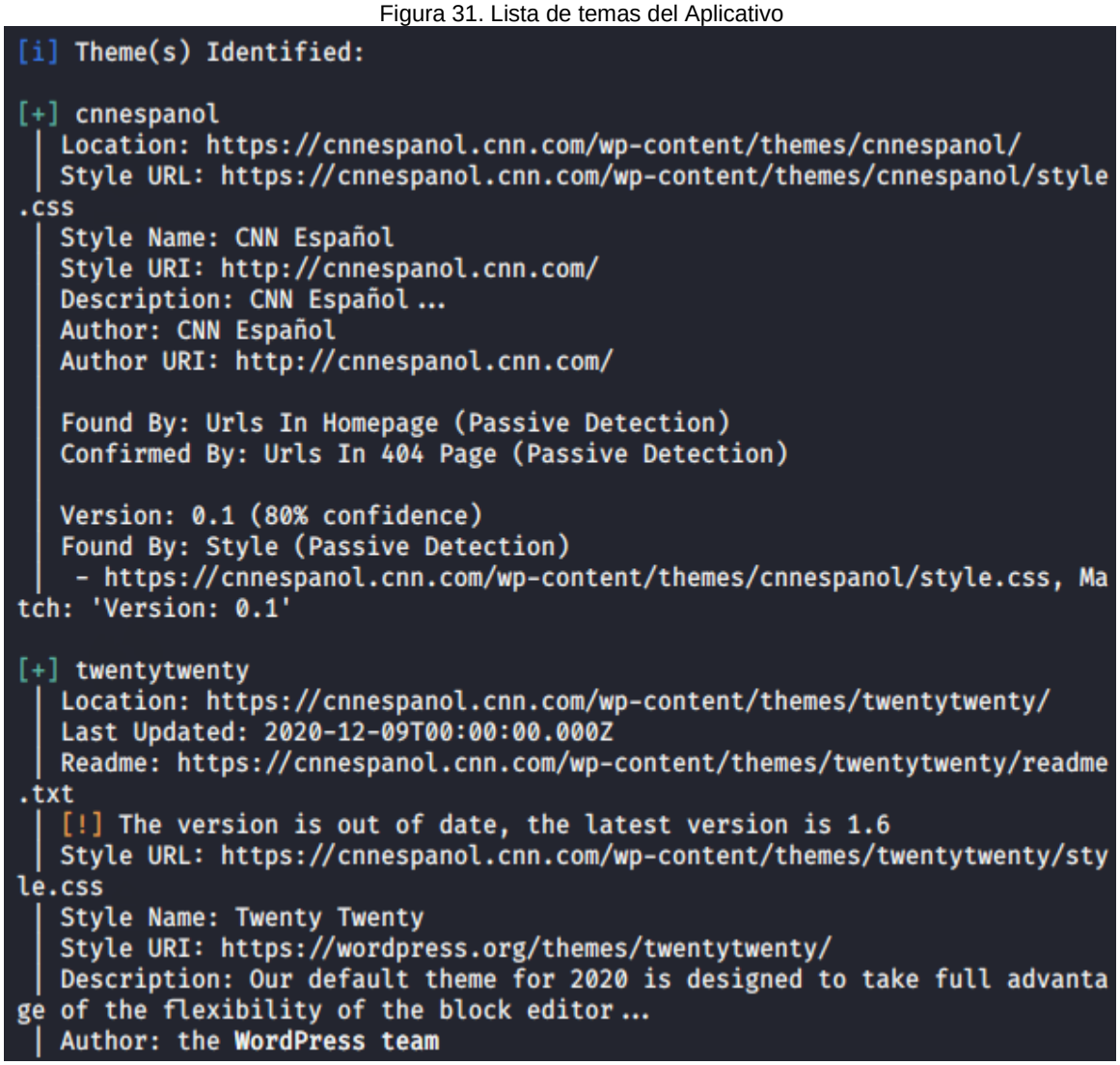
Figura 30. Lista nombres de usuarios



Fuente: El Autor

Con la siguiente línea wpscan --url https://cnnespanol.cnn.com --enumerate t, lista algunos temas de la página web.

Figura 31. Lista de temas del Aplicativo

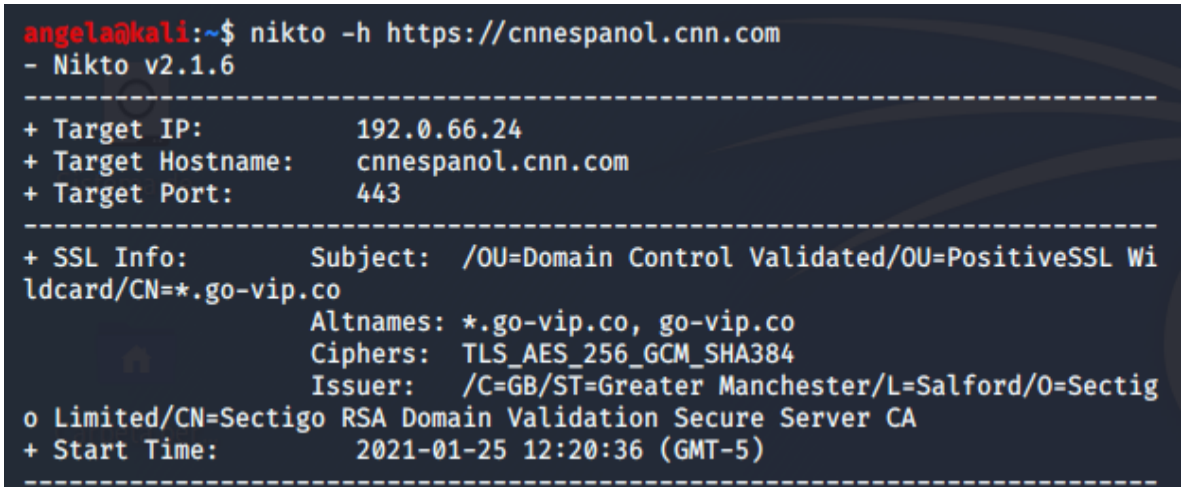


Fuente: El Autor

PRUEBAS CON LA HERRAMIENTA NIKTO

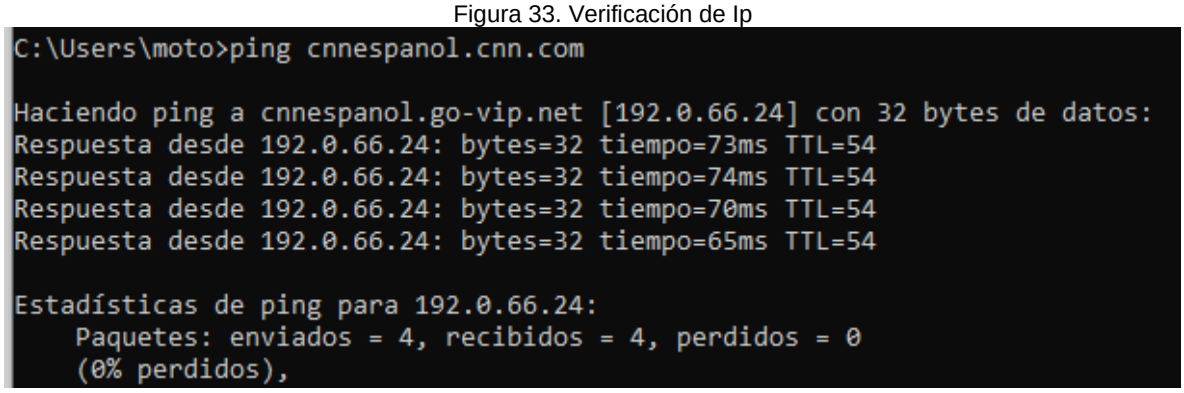
Al ejecutar la línea nikto -h https://cnnespanol.cnn.com se obtiene la dirección ip de la página 192.0.66.24 y el puerto de navegación 443.

Figura 32. Resultados del escaneo en Nikto



Fuente: El Autor

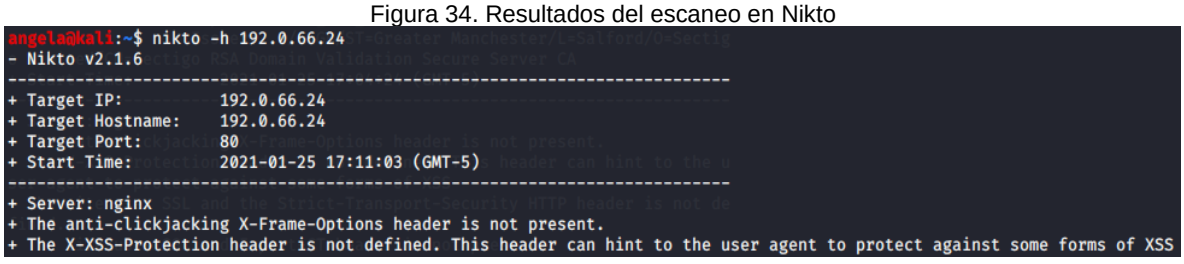
Figura 33. Verificación de Ip



Fuente: El Autor

Con la siguiente línea nikto -h 192.0.66.24 indica que la cabecera X-Frame-Options, no está presente debido a esto facilitaría a un atacante abrir la página por medio de un frame o iframe.

Figura 34. Resultados del escaneo en Nikto

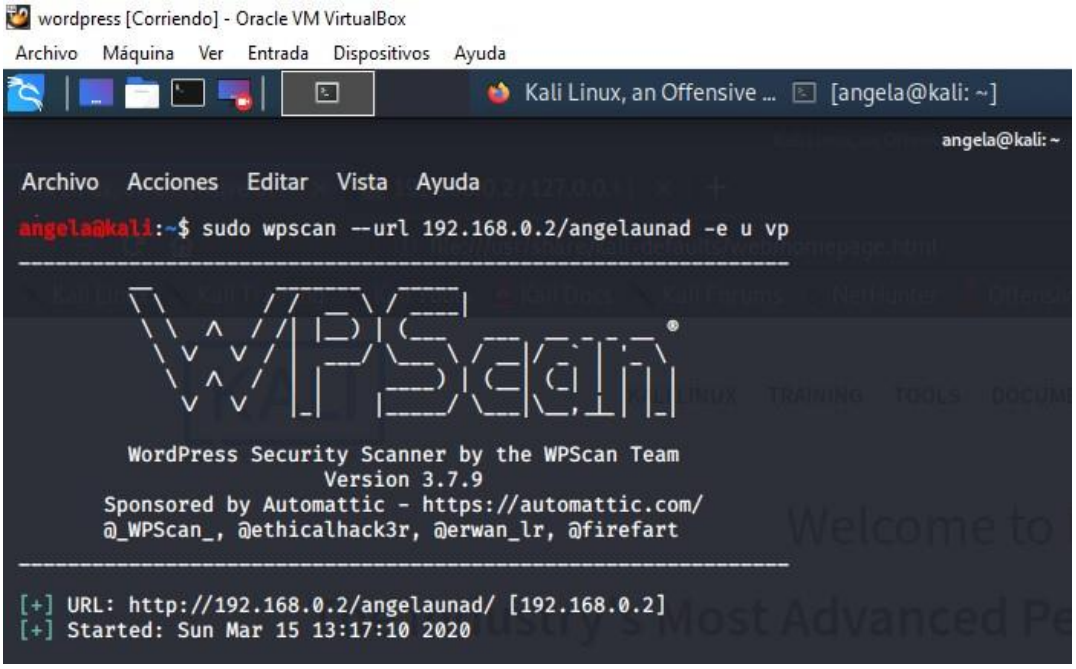


Fuente: El Autor

WORDPRESS LOCAL

Ejecutando la línea sudo wpscan –url 192.168.0.2/angelaunad -e u vp se listan los nombres de usuarios creados en WordPress.

Figura 35. Escaneo de Usuarios en WordPress local

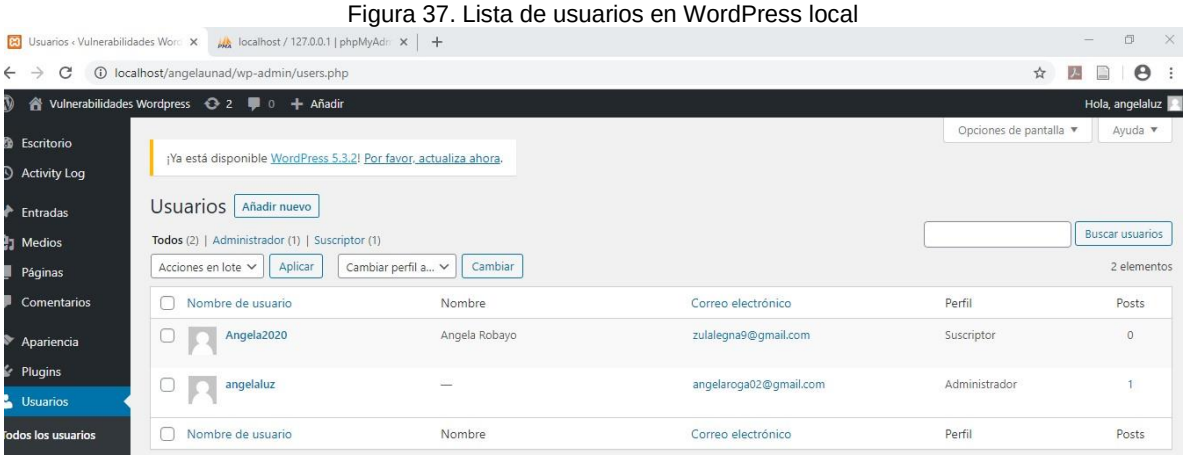


Fuente: El Autor

Figura 36. Lista de Usuarios en WordPress local

Fuente: El Autor

Figura 37. Lista de usuarios en WordPress local



Fuente: El Autor

5.3. GUIA DE BUENAS PRÁCTICAS DE SEGURIDAD WEB TENIENDO EN CUENTA LAS DEBILIDADES INFORMÁTICAS, DE LOS CMS Y VULNERABILIDADES DE WORDPRESS

Metodología: Por medio de las diferentes consultas realizadas se identificó que una de las principales causas por las cuales WordPress es vulnerable, es porque tiene versiones obsoletas de los complementos, temas, y el núcleo de WordPress.

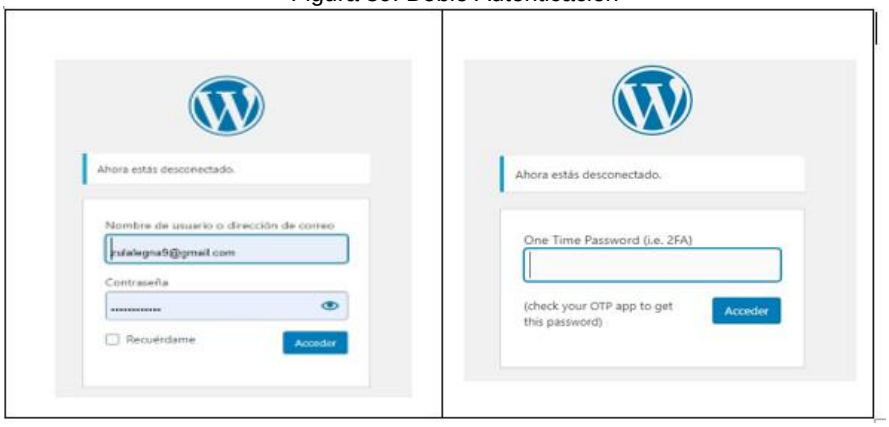
A continuación, se dará una serie de recomendaciones útiles para los administradores de los sitios web. El siguiente manual de recomendaciones de seguridad, se elabora con base en la información de la metodología OWASP WordPress y algunos controles de la norma ISO 27002.

1) Utilizar el complemento Two Factor Authentication para evitar ataques de fuerza bruta. Utilizando doble autenticación en el inicio de sesión.

Figura 38. Complemento Two Factor Authentication

Fuente: El Autor

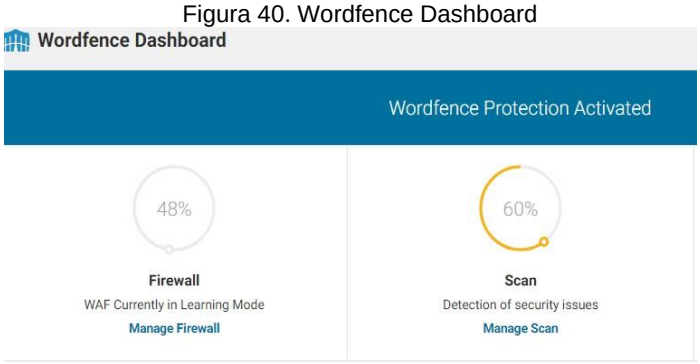
Figura 39. Doble Autenticación



Fuente: El Autor

2) Utilizar un firewall por medio del complemento Wordfence Security el cual ofrece diversas configuraciones de seguridad, entre estas restringir el número de accesos a una página con el fin de evitar un bot.

Figura 40. Wordfence Dashboard



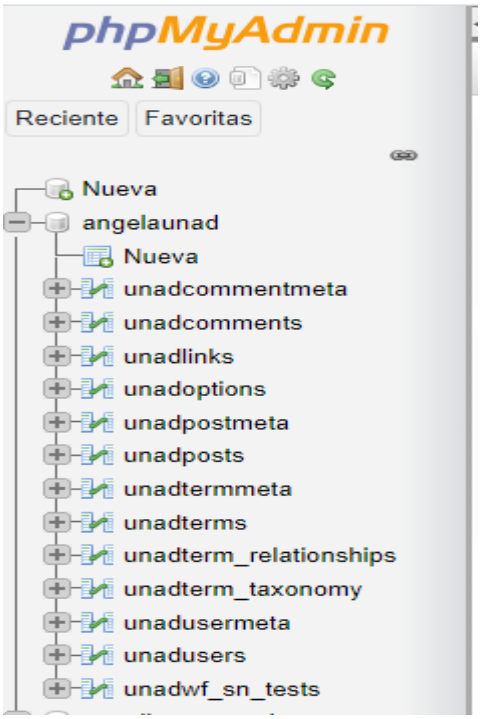
Fuente: El Autor

3) Cuando se esté configurando la Base de datos eliminar el prefijo wp, que viene por defecto de WordPress.

Figura 41. Tablas de la Base de Datos de Wordpress

Fuente: El Autor

Figura 42. Tablas de la Base de Datos de Wordpress sin el wp



Fuente: El Autor

4) Ocultar el archivo wp-config.php que tiene información confidencial como el nombre de la Base de Datos, el nombre del super usuario, y el hostname.

Figura 43. Archivo wp-config.php

```
// ** MySQL settings - You can get this info from your web host ** //
/** The name of the database for WordPress */
define( 'DB_NAME', 'monografia' );

/** MySQL database username */
define( 'DB_USER', 'root' );

/** MySQL database password */
define( 'DB_PASSWORD', '' );

/** MySQL hostname */
define( 'DB_HOST', 'localhost' );

/** Database Charset to use in creating database tables. */
define( 'DB_CHARSET', 'utf8' );

/** The Database Collate type. Don't change this if in doubt. */
define( 'DB_COLLATE', '' );
```

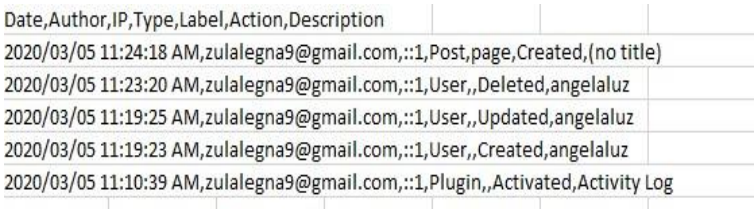
Fuente: El Autor

5) Llevar un control de los diferentes eventos que se realiza como: creación y eliminación de usuarios, creación de nuevos sitios web entre otros. Por medio del plugin Activity Log, el cual muestra un listado de los eventos tanto en WordPress como en un archivo CSV.

Figura 44. Resultados de Activity Log

Fuente: El Autor

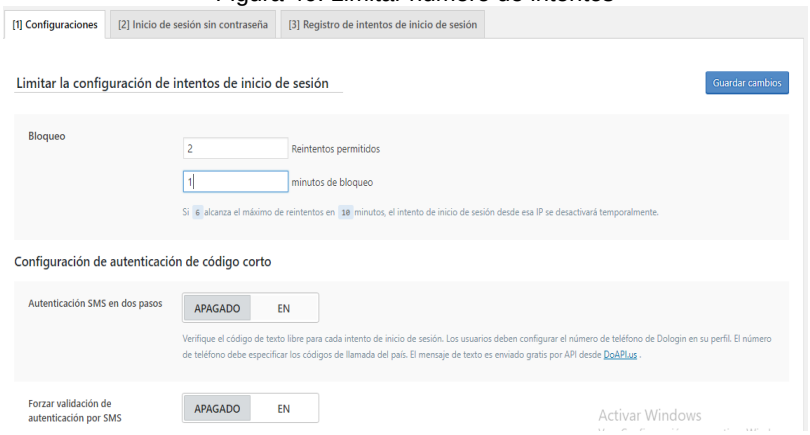
Figura 45. Resultados de Activity Log en archivo CSV



Fuente: El Autor

Limitar el número de intentos de ingreso al sistema por medio del plugin Seguridad DoLogin.

Figura 46. Limitar número de intentos



Fuente: El Autor

- Tener actualizada la última versión de WordPress en los aplicativos webs.
- Usar claves aleatorias, alfanuméricas y utilizar caracteres especiales.
- Cambiar prefijo wp de las tablas de la base de datos.
- Ocultar la versión de WordPress.
- Mantener el ordenador con el antivirus actualizado, para evitar la instalación de posibles keylogger que capturan la información que se ingresa por teclado.
- Instalación y actualización regular del software de detección y reparación de código malicioso.
- Verificar los sitios web para comprobar la presencia de código malicioso.
- Implementación de procedimientos para recolectar información clave, como la suscripción a sitios web de verificación que informe acerca de los nuevos códigos maliciosos.
- Auditar y registrar algunos eventos como fecha y hora de ingreso y cierre del aplicativo.

- Activación de log que registren los eventos del administrador y operador de WordPress.
- Registro de todos los usuarios y los privilegios asignados.
- Confidencialidad en las contraseñas asignadas por parte de los usuarios.
- Restringir el acceso a las carpetas y archivos del sistema como wp-config,wp-admin, .htaccess entre otros.
- Definir los riesgos que podría causar la instalación o actualización de un parche.
- Al identificar una vulnerabilidad en el aplicativo se debe identificar los riesgos y acciones a ejecutar45.

[45] NORMA TÉCNICA NTC-ISO/IEC COLOMBIANA 27002, [Sitio web], Fecha de Consulta: [Citado el 26 de enero 2021] Disponible en:

6. RESULTADOS

A través del desarrollo de esta monografía se pudo identificar que actualmente el gestor de contenido WordPress, está presente en diferentes y reconocidas páginas web a nivel mundial, por tal motivo se realizó unas verificaciones de seguridad informática a nivel general, por medio de algunas herramientas de Kali linux como wpscan, nikto y OWASP ZAP, las cuales arrojaron datos confidenciales como, versión de WordPress, nombre del servidor, listado de nombres de usuarios, entre otras fallas de seguridad, que le facilitaría al atacante ingresar a los aplicativos con el rol de administrador y vulnerar la configuración e información del aplicativo web. Adicional este cms también es vulnerado por que los administradores de los sitios web, instalan plugin o complementos de sitios web no autorizados o poco confiables, y mantiene desactualizada la versión de WordPress.

Cabe resaltar que este cms cuenta con una comunidad de profesionales y desarrolladores quienes se encargan de mejorar constantemente, la estructura y seguridad de WordPress y dar soluciones a los incidentes de seguridad informática que se presentan en los aplicativos webs

http://gmas2.envigado.gov.co/gmas/downloadFile.public?repositorioArchivo=000000001070&ruta=/documentacion/0000001358/0000000107

7. CONCLUSIONES

- El gestor de contenido WordPress tiene un grupo de colaboradores que están dispuestos a dar soluciones en un mínimo tiempo a cualquier falla de seguridad que se pueda presentar.
- La información en la web relacionada con la seguridad y las vulnerabilidades del cms WordPress no está unificada ni organizada.
- La información de la metodología OWASP y la norma ISO 27002 son útiles en el momento de crear un manual de recomendaciones.
- Por medio de las herramientas Nikto y Wpscan se pudo obtener datos confidenciales del gestor de contenido WordPress como: Apache/2.4.41, OpenSSL/1.1.1c, PHP/7.2.28, motor de la base de datos, phpmyadmin, y finalmente los nombres de los usuarios que están creados en WordPress.

8. RECOMENDACIONES

Por medio del desarrollo de esta monografía se evidencia que la información a nivel general de WordPress está muy dispersa, por eso es aconsejable clasificar la información y plasmarla en manuales de recomendaciones, y más puntualmente para los temas relacionados con los problemas de seguridad, vulnerabilidades y mejoras.

- Adicional a esto, tener en cuenta lo siguiente:
- Tener actualizadas la versión de WordPress y PHP.
- Descargar los plugin y complementos de seguridad de la página oficial de WordPress.
- No utilizar nombre de usuario por defectos “**Admin**” y contraseñas débiles.
- Asignar permisos al as carpetas y archivos q contengan información confidencial, como usuario y contraseña de la base de datos.
- Limitar el número de intentos en el momento de ingresar al ambiente de administración de WordPress.
- Realizar frecuentemente copias de seguridad tanto de la aplicación, como de la base de datos.
- Utilizar un firewall y limitar conexiones en el archivo .htaccess.

REFERENCIAS BIBLIOGRÁFICAS

Adicte. ¿Qué porcentaje de sitios web son WordPress en 2019?; [Sitio web]. [Citado el 4 de Noviembre del 2020] Disponible en: https://adictec.com/estadisticas-sitios-web-wordpress/

Alejo, Luis Méndez. Aumenta la seguridad en WordPress, ¡protege tu inversión {En línea}.{Accedido 14 de enero de 2020}. Disponible.https://www.webempresa.com/blog/aumenta-la-seguridad-en-wordpress-protege- tu-inversion.html.

Aumenta la seguridad en WordPress, ¡protege tu inversión. {En línea}. Accedido {13 de enero de 2020}. Disponible https://www.webempresa.com/blog/aumenta-la-seguridad-enwordpress-protege-tu-inversion.html

BRIAN, Jackson.130 Sitios WordPress de Marcas Grandes que Dominan la Web en 2019 2017. {En línea}. {Accedido 14 de enero de 2020}. Disponible. https://kinsta.com/es/blog/ejemplos-de-sitios-wordpress/

BRIAN, Jackson. Los 16 Mejores Plugins de Seguridad de WordPress para Bloquear a los Malos. 2018. Kinsta WordPress Hosting Gestionado. 23 de abril de 2018.{En línea}.{Accedido 4 de marzo de 2020}. Disponible en: https://kinsta.com/es/blog/plugins-seguridad-wordpress/

BRITO GOBZALEZ, Raúl Henry. PERURENA MONTESINO, Raydel.VELIZ ZULETA,Yeleny .CONTROLES DE SEGURIDAD PARA SISTEMAS DE GESTIÓN DE CONTENIDOS BASADOS EN SOFTWARE LIBRE; [Sitio web].[Citado el 2 de Febrero del 2021].

Disponible en: http://www.informaticahabana.cu/sites/default/files/ponencia-2020/SEG14.pdf

Carlos. Glosario de términos y palabras de WordPress para principiantes. {En línea}. {Accedido 14 de enero de 2020}. Xplora (blog). 14 de marzo de 2017. Disponible. https://www.xplora.eu/glosario-wordpress/.

cisco_2016_asr_011116_es-es.pdf. {En línea}. {Accedido 11 de enero de 2020}. Disponible https://www.cisco.com/c/dam/m/es_es/internet-of-everythingioe/iac/assets/pdfs/security/cisco_2016_asr_011116_es-es.pdf

Departamento de Internet. Qué es un CMS y qué ventajas tiene; [Sitio web]. [Citado el 4 de Noviembre del 2020] Disponible en: https://www.departamentodeinternet.com/que-es-un-cms-y-que-ventajas-tiene/

Diccionario GLOSARIO de términos WordPress 2019 - 2020 s. f. {En línea}. {Accedido 14 de enero de 2020}. Disponible. https://wpinsideout.com/que-eswordpress/glosario/#Sistema_de_gestion_de_contenidos_CMS

Engineering, NetCloud. 2017. Ingeniería de redes, telecomunicaciones y ciberseguridad en Barcelona». Net Cloud Engineering (blog). 26 de junio de 2017. {En línea}. {Accedido 14 de enero de 2020}. Disponible. https://netcloudengineering.com/ciberseguridad-amenaza-vulnerabilidad/.

ESTUDIO-SOBRE-EL-USO-DE-WORDPRESS-2015.pdf. {En línea}. {Accedido 13 de enero de 2020}. Disponible https://wpdoctor.es/wp-content/uploads/2015/12/ESTUDIO-SOBRE-EL-USO-DE-WORDPRESS-2015.pdf

Fake Plugins, Fake Security, Sucuri Blog, 28 de septiembre de 2017, https://blog.sucuri.net/2017/09/fake-plugins-fake-security.html. {En línea} {Accedido 14 de enero de 2020}. Disponible. https://blog.sucuri.net/2017/09/fake-plugins-fakesecurity.html

FERNANDEZ PEREZ, Daniel. Botnet de 20,000 webs WordPress infectan otras webs basadas WordPress, Tecnonucleous, 7 de diciembre de 2018, {En línea}. {Accedido 13 de Enero de 2020}. Disponible. https://tecnonucleous.com/2018/12/07/botnet-de-20000-webswordpress-infectan-otras-webs-wordpress/.

FONTELA, Alvaro. Guía básica de seguridad informática para Wordpress s. f. {En línea}. {Accedido 14 de enero de 2020}. Disponible. https://es.semrush.com/blog/seguridad-informaticawordpress/

Guía de los 7 mejores gestores de contenidos gratuitos de 2018. {En línea}. {Accedido 27 de diciembre de 2019}. Disponible https://www.bilib.es/actualidad/blog/noticia/articulo/guia-de-los-7-mejores-gestoresde-contenidos-gratuitos-de-2018/

Hacked Website Report 2017 Statistics s. f. {En Línea}. {Accedido 14 de enero de 2020}. Disponible. https://sucuri.net/reports/2017-hacked-website-report/

LATORRE, Mariano. HISTORIA DE LAS WEB, 1.0, 2.0, 3.0 y 4.0; [Sitio web]. [Citado el 31 de Enero del 2021].
Disponible en: https://d1wqtxts1xzle7.cloudfront.net/59947315/74_Historia_de_la_Web20190706-123188-141xd95.pdf?1562447444=&response-content-disposition=inline%3B+filename%3DHISTORIA_DE_LAS_WEB_1_0_2_0_3_0_y_4_0.pdf&Expires=1612364900&Signature=CGIYjWLiy3ZGe2a5HYi132w~rvOkxfgJyFkypWc-znEpXXWbBaR-K5KjJjhuhb2OzirqJokB7CcJen2RWbB68PXWm8iYGOzuwlLJD1Wj7OBivprFZgTg6zdH4nTZC5pFiA7-M2mNT3niOkEUqjznUeAVpqRCoVudUKZWRwRKnUUSKEL-r-VZni8tPHK8EtELBU2dhBiEU2B2oLwR77Ew4dbbF45z2BYqasnI3tuZnDSNzEdBe

F2GdSNqHV0nad5tgsJTqS3CYKjbNjgyQmXu3H3gZxsKPnyvUbuFgBj2DswKJwXcZeolGKMNT0IUdd3702pP9OesQiMF1VFsokZH2w__&Key-Pair-Id=APKAJLOHF5GGSLRBV4ZA

MURILLO, Bernardo. ¿Por qué es tan importante cuidar la seguridad de su sitio web de WordPress?; [Sitio web]. [Citado el 15 de Diciembre del 2020] Disponible en: https://netquatro.com/por-que-es-tan-importante-cuidar-la-seguridad-de-su-sitio-web-de-wordpress

OWASP for WordPress - Using OWASP Top 10 on WordPress». 2018. WP White Security (blog). {En línea}. {Accedido 4 de marzo de 2020}. Disponible en: 22 de agosto de 2018. https://www.wpwhitesecurity.com/owaspwordpress-security-owasp-top-10/.

Plugins de WordPress para la seguridad de tu web. s. f. IONOS Digitalguide. {En línea}. {Accedido 4 de marzo de 2020}.https://www.ionos.es/digitalguide/hosting/blogs/plugins-de-wordpress-para-laseguridad-de-tu-web/

ROBLES CORTES, Diego. Wordpress revela que el 2018 triplicó vulnerabilidades. {En línea} {Accedido 28 de diciembre de 2019}. Disponible http://www.seguridadyfirewall.cl/2019/01/wordpressrevela-que-el-2018-triplico.html

SALINAS, M. Vulnerabilidad crítica en WordPress pasa desapercibida durante más de 6 años 2019. {En línea}. {Accedido 14 de enero de 2020}. Disponible. https://unaaldia.hispasec.com/2019/02/vulnerabilidad-critica-en-wordpress-pasadesapercibida-durante-mas-de-6-anos.html

SILD, Oliver. WordPress Plugin “Simple Social Buttons” Critical Security Bug 2019. {En línea}. {Accedido 14 de enero de 2020}. Disponible.

https://www.webarxsecurity.com/wordpress-plugin-simple-social-buttons/

Sucuri-Hacked-Report-2017.pdf. {En línea} {Accedido 27 de diciembre de 2019}. https://sucuri.net/reports/Sucuri-Hacked-Report-2017.pdf

TELLADO, Fernando. Seguridad O.W.A.S.P. y WordPress • Ayuda WordPress. {En línea} {Accedido 14 de enero de 2020}. Disponible . https://ayudawp.com/owasp-wordpress/.

Vulnerabilidad crítica parcheada en el popular complemento Convert Plus. s. f. {En línea}. {Accedido 13 de enero de 2020}. Disponible. https://www.wordfence.com/blog/2019/05/critical-vulnerability-patched-in-popularconvert-plus-plugin/

Web Technology Surveys: Estadísticas de uso y cuota de mercado de WordPress [Sitio web]. [Citado el 4 de Noviembre del 2020] Disponible en: https://w3techs.com/technologies/details/cm-wordpress

WordPress Medellín – Comunidades Tech. s. f. {En línea}. {Accedido 14 de enero de 2020}. Disponible.https://www.rutanmedellin.org/comunidadestech/wordpress-medellin/.