Los riesgos de las inyecciones SQL en WordPress

Saib García Morales, José Ney Garrido Vázquez, José Manuel Gómez Zea, Alejandro Hernández Cadena, José Ángel Jesús Magaña

Tecnológico Nacional de México/Instituto Tecnológico de Villahermosa, División de Estudios de Posgrado e Investigación, Carretera Villahermosa - Frontera Km. 3.5 Ciudad Industrial Villahermosa, Tabasco, México. C.P. 86010.

Resumen

El desarrollo de contenido web tiene gran demanda en el mercado laboral, y el sistema de gestor de contenido WordPress es uno de los más populares a la hora de desarrollar este tipo de proyectos, debido a su fácil uso y baja curva de aprendizaje; sin embargo posee algunas vulnerabilidades que la hacen blanco fácil para hackers que desean obtener información mediante inyecciones SQL, esta situación ha generado muchos problemas a todo tipo de sitios desarrollados con esta tecnología, ya que es un ataque en el que se inserta código malintencionado en cadenas que posteriormente pasan a una instancia de SQL Server para su análisis y ejecución; ya que todos los procedimientos generan instrucciones de SQL deben revisarse en busca de vulnerabilidades, ya que el programa ejecutara todas las consultas recibidas que sean válidas desde el punto de vista sintáctico.

Abstract

Web content development is in great demand in the labor market, and the content manager system WordPress content is one of the most popular when it comes to developing this type of project, due to its easy to use and low learning curve; however, it has some vulnerabilities that make it an easy target for hackers who want to obtain information through SQL injections. This situation has generated many problems for all kinds of sites developed with this technology, since it is an attack in which malicious code is inserted into strings. which are subsequently passed to an instance of SQL Server for analysis and execution; Since all procedures generate SQL statements, they must be checked for vulnerabilities, since the program will execute all received queries that are valid from the syntactic point of view.

Palabras clave: SQL, WordPress, Gestor de contenido
Keywords: SQL, WordPress, Content manager.

1. INTRODUCCIÓN

Lo que hoy en día llamamos sistemas de gestión de contenido, son aquellas herramientas tecnológicas que permiten crear y mantener ya sea un blog u otro tipo de web mediante código abierto, estas poseen diversos tipos de plantillas y diseños para páginas web. Dentro de este rubro WordPress sobresale ya que tiene características de aprendizaje no tan complicado y tiene gran variedad de cosas para implementar, su facilidad de uso es recomendable para aquellos que estén empezando a crear o desarrollar páginas y sitios web.

Pero si hay algo que toda persona que trabaja en las áreas de tecnologías, desempeñándose ya sea como desarrollador de software o productos, es reconocer la importancia que tiene la seguridad de las cosas, así como la disponibilidad de la página de manera permanente, que no entren virus, malware y que no se vaya a perder información almacenada en la nube.

Una de estas preocupaciones son las inyecciones de SQL, ya que es un ciberataque en el cual el hacker introduce código ajeno en un sitio web para romper o quebrar las medidas de seguridad y lograr acceder a los datos que están protegidos; una vez logrado esto, el individuo puede controlar la base de datos del sitio web y obtener información de los múltiples usuarios, así como otro tipo información que esté buscando, inclusive dañar el sitio cambiando su comportamiento para perjudicar a los usuarios o a los administradores.

Estos ataques apuntan directamente a la base de datos y a los gestores de base de datos, que son un conjunto de datos y de programas que contienen información relevante de la empresa; su principal función es proporcionar una forma de almacenar y recuperar la información de una base de datos que sea tanto práctica como eficiente, ya que están diseñados para almacenar grandes cantidades de información (Tovar Valencia, 2014).

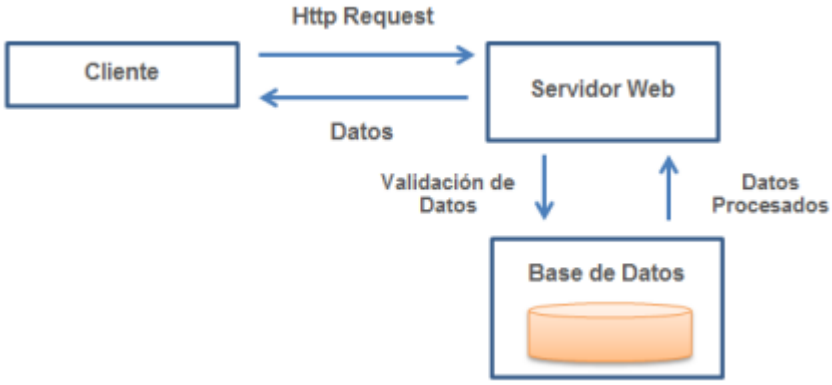

Figura 1. Arquitectura Web, Fuente: http://www.andromeda-proyect.org

La relevancia de este artículo se basa en la siguiente premisa: "El Internet se ha convertido en una herramienta invaluable que permite al mundo corporativo mostrar sus capacidades. Si bien las aplicaciones web han ganado importancia en Internet, la seguridad es lo único que preocupa. Los datos empresariales son muy críticos y flotan en la nube y es por eso que la seguridad de las aplicaciones web se está convirtiendo rápidamente en una preocupación creciente para todas las empresas." (Onishi, 2013)

1.1 Estadística de uso de Gestión de contenido

De acuerdo a las estadísticas proporcionadas por la W3techs "El peligro de las inyecciones SQL se conoce desde hace más de una década, pero los ataques de inyección han liderado el top 10 de OWASP (Open Web Application Security Project) durante años y siguen siendo una de las principales razones de ataques devastadores en sitios web. Como alrededor del 24% por ciento de los 10 millones de sitios web principales se basan en el sistema de gestión de contenido WordPress, no es de extrañar que los sistemas de gestión de contenido en general y WordPress en particular sean frecuentemente dirigidos. Para comprender cómo los atacantes pueden descubrir y explotar los errores de seguridad subyacentes, se han analizado 199 exploits de inyección SQL divulgados públicamente para WordPress y sus complementos." (W3Techs, 2022)

Sistemas de gestión de contenidos

Sistemas de gestión de contenido más populares

© W3Techs.com	uso	cambio desde el 1 de mayo de 2022	cuota de mercado	cambio desde el 1 de mayo de 2022
1. WordPress	43.0%		64.2%	
2. Shopify	4.2%	-0.1%	6.3%	-0.2%
3. Wix	2.3%		3.4%	
4. Espacio cuadrado	2.0%		3.0%	
5. Joomla	1.6%	-0.1%	2.5%	

porcentajes de sitios

Figura 2. Porcentajes de gestores de contenidos más populares. (W3Techs, 2022)

El 33,1% de los sitios web no utilizan ninguno de los sistemas de gestión de contenido que monitoreamos. WordPress es utilizado por el 42,9% de todos los sitios web, es decir, una cuota de mercado del sistema de gestión de contenido del 64,2%. (https://w3techs.com)

Como gestor de contenido WordPress ha crecido en la actualidad y es el favorito entre los usuarios por muchas razones, y esto se ve reflejado en los diversos contenidos que hay en Internet, con diseños más profesionales, mejor estructura, calidad más alta etc.

2. ATAQUE DE INYECCIÓN SQL

Este tipo de ataques tienen una metodología a seguir para llevarse a cabo, que es muy sencilla de entender si se tiene conocimiento básico de SQL. Como bien sabemos la metodología son un conjunto de diferentes técnicas que permiten realizar diversas actividades de un proyecto, esto permite tener un control de todas las actividades que se cometen.

Así también funcionan los ataques cibernéticos, siguiendo diferentes pasos, cumpliendo con diferentes actividades, hasta lograr el objetivo principal, que va desde, obtención de información de cuentas, robo de información, accesos no autorizados, robo de dinero, difamación, hasta daños al sitio web.

Según OWASP, la inyección SQL es una de las diez vulnerabilidades más peligrosas y populares que pueden presentarse en entornos web, los cuales generalmente son difíciles de proteger debido a su alta personalización, complejidad, escala, tecnología y desarrollo por programadores con poca experiencia en seguridad, causan serios daños a los negocios de las víctimas (Crespo Martínez, 2020).

2.1 Cómo funciona una inyección de SQL.

Explicaremos esto de manera fácil de entender y en pocos pasos:
El hacker identifica algún sitio que pueda ser vulnerable, ya sea que el sitio web este relativamente nuevo, o que este en desarrollo o de bajo presupuesto, esto sucede ya que muchas veces se invierte más en el diseño que tenga una buena calidad, a que tenga mejor seguridad y algo que hay en todo sitio web es un “login”.

ISSN: 2007-4786

Todo formulario cuando alguien lo rellena y pulsa el botón de "Log In" se envía información en una sentencia de SQL que será ejecutada en la base de datos como, por ejemplo:

- "$sql = SELECT * FROM usuarios WHERE usuario = '$usuario' and password = '$pass';"

Si entendemos algo de SQL entendemos que la sentencia quedaría así:

- "$sql = SELECT * FROM usuarios WHERE usuario = 'Silvia' and password = '12345';"

Pero, ¿qué ocurriría si un atacante en el campo "password" agregara "' OR '1' = '1"? Es decir: password = '12345' OR '1' = '1'; (W3Techs, 2022)

Lo que pasa a continuación es la inyección SQL y esto permite entrar a los sitios donde no se hubieran tomado las medidas correspondientes de seguridad necesarias, esa simple instrucción va a comparar si el usuario "Silvia" existe y aparte, como el password tiene la instrucción de 1 es igual a 1 entraria al sistema sin saber realmente la contraseña, esto es algo muy sencillo de entender, pero ahora, cambiemos a que se pide información de una tabla de salarios, número de cuentas bancarias, etc. Esto ya se pone algo más serio y nos da a entender que la seguridad en nuestro sitio es muy importante.

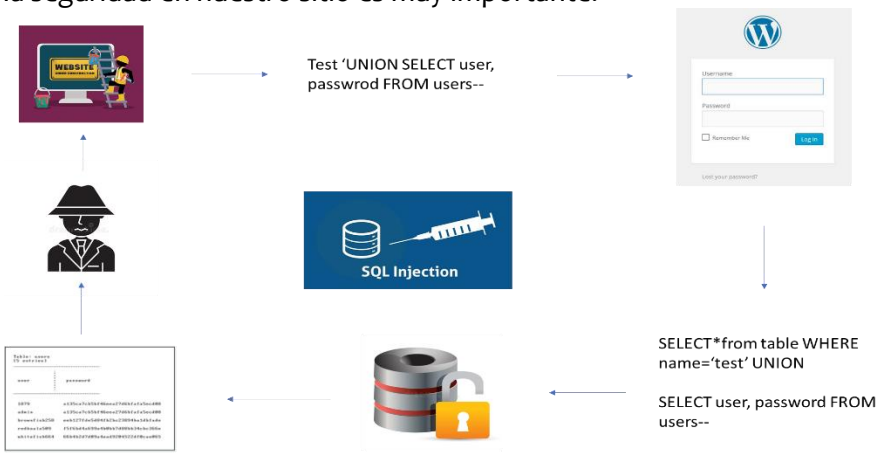

Figura 3. Metodología de inyección SQL

Con esto vemos lo sencillo que es realizar ataques de inyecciones de SQL en sitios web que no tenga desarrollado una buena seguridad, es una metodología en ciclo que se puede repetir muchas veces. Lo siguientes son casos reales de ataques usando inyecciones de SQL:

- En el año 2016 hackers usaron métodos de inyección SQL para lanzar un ciber ataque contra el banco nacional de Qatar. Asia consiguieron robar más de 1.4 GB de datos, que fueron publicados poco después. Estos datos implicaban información de miles clientes, incluidos miembros de la familia real del país, oficiales de la inteligencia, polémicos lideres religiosos, así como varios ciudadanos británicos, franceses y estadounidenses que estaban indicados como espías en la base de datos del banco. (Moes, 2021)
- Igualmente, en 2016 otro grupo de hackers exploto las vulnerabilidades de vBulletin, un popular software de tablón de mensajería online, para atacar a 11 tableros de mensajes dedicados a los juegos,

la mayoría de ellos en ruso. Durante el ataque, consiguieron robar datos de registros de mas de 27 millones de cuentas en el proceso. (Moes, 2021)

Como vemos en el siguiente gráfico; los ataques de inyecciones de SQL son el segundo que más afecta a todo sitio web hecho en WordPress:

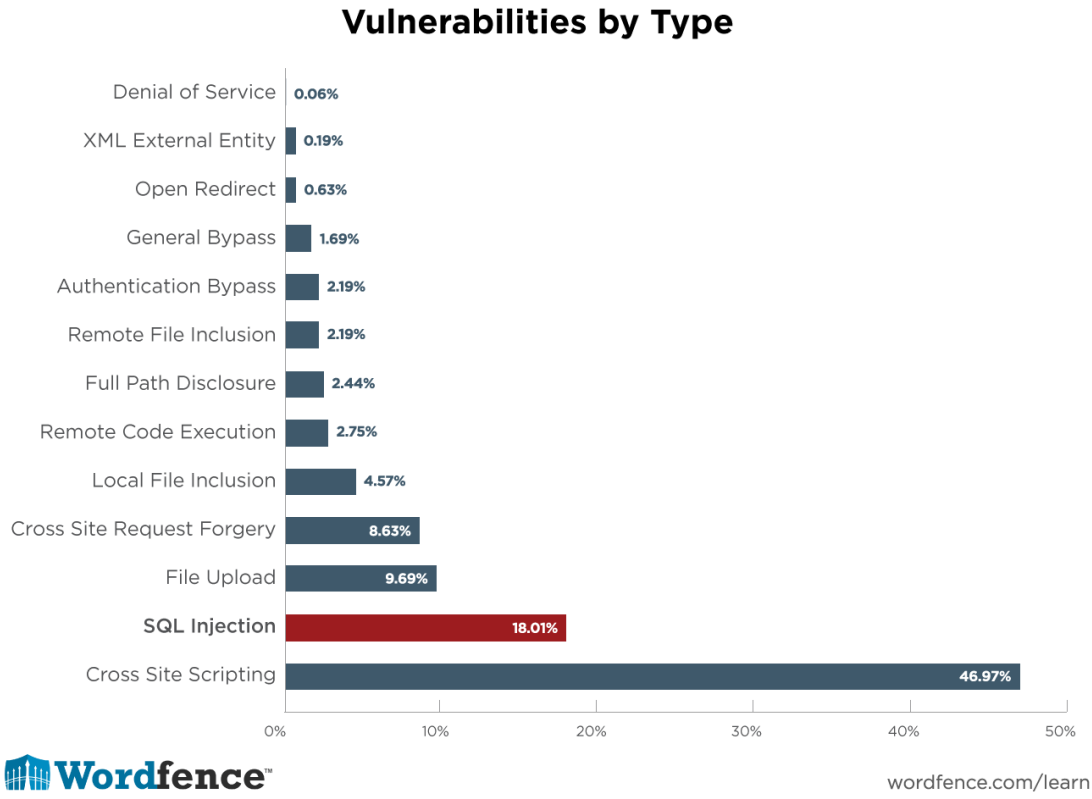

Figura 4. Porcentaje de Vulnerabilidades (www.wordfence.com, 2020)

3. COMO PREVENIR ESTOS ATAQUES

Siempre que se desarrolle algún sitio web con WordPress se busca que el sitio tenga un diseño llamativo que atraiga la atención y no se enfoca en la seguridad, el principal problema de estos ataques es que, si dejamos que el usuario del programa introduzca libremente caracteres sin control ninguno, puede llegar a aprovecharse de las comillas.

Por lo tanto, la solución sería evitar que se pudieran introducir caracteres especiales, como comillas sin haberlas transformado antes, por ejemplo, una comilla doble: " debería de transformarse en \" que así se interpretará como texto la comilla y no como el carácter que cierra o abre el un texto en la consulta, pero según el lenguaje se puede implementar de distintas formas y algunas son *automáticas* y más optimizadas.

Otra medida sería Utilizar el escáner de vulnerabilidad web de Burp Suites. Se Puede usar este escáner estableciendo pruebas contra cada punto de entrada de la aplicación, permite buscar errores, diferencias sistemáticas y comprobar las respuestas que se reciben por parte de la aplicación.

Validación de entrada y WAF escribe un código que puede identificar a los usuarios ilegítimos. Sin embargo, cuando se utiliza solo, este no es un método infalible. Puede generar muchos falsos positivos. La implementación de este método junto con el uso de un firewall de aplicaciones web (WAF) puede ser efectivo. El WAF filtrará la inyección SQL y otras amenazas online.

Cuando el WAF detecta un posible usuario ilegítimo, verificará los datos de la IP antes de bloquear la solicitud. Así, se bloquearán los datos de las IP's que tengan mala fama.

Los ataques de inyección SQL son fáciles de prevenir con un mantenimiento apropiado de la página web. Esto incluye controles constantes de declaraciones SQL de las aplicaciones conectadas a la base de datos, aplicación regular de actualizaciones y parches de la base de datos, así como la compra de un software fiable de ciberseguridad para proteger la base de datos. Como esos ataques se dirigen a las páginas web con el uso de SQL dinámicas, debería dar una serie de pasos para minimizar la necesidad del input del usuario en la construcción de sus peticiones. (Schüring, 2020)

Siempre que sea posible, ofrezca a los usuarios declaraciones preparadas y una lista de opciones, en lugar de darles la opción de introducir su propia consulta. También es importante usar la validación de input para evitar problemas con los caracteres de escape. Es más, asegúrese de habilitar el filtrado de datos basado en el contexto. Por ejemplo, debería permitir solo dígitos para números de teléfono. (Schüring, 2020)

No se puede lograr impedir que se realicen los ataques de inyecciones de SQL, pero podemos realizar algo que ayude a minimizar los riesgos de que ocurran y así poder mitigar los efectos que estos producen con estos pequeños pasos. (proporcionados por (Belcic, 2020)

- No proporcione información personal en sitios web sospechosos. Al introducir datos confidenciales, asegúrese de hacerlo solo en sitios web de confianza que cuenten con fuertes medidas de seguridad. Ni siquiera esto es garantía infalible para evitar ser víctima de un ataque de este tipo, pero es un comienzo.
- Manténgase informado de las noticias sobre seguridad tecnológica. Cuando se producen ataques de hackers y filtraciones en sus bases de datos, las empresas lo anuncian. Esté al tanto de las noticias sobre los sitios web que utiliza y, si ve algo en referencia a una SQL, cambie sus credenciales de inicio de sesión sin demora.
- Acostúmbrese a crear contraseñas seguras. Si utiliza una contraseña distinta para cada cuenta, reducirá el riesgo. Siga las prácticas recomendadas de creación de contraseñas para ir siempre un paso por delante de los hackers.
- Utilice un administrador de contraseñas. Muchos administradores de contraseñas alertan al usuario cuando un sitio web que utiliza ha sufrido un ataque. Si es el caso, podrá cambiar rápidamente una contraseña difícil de averiguar por otra igual de segura. Busque un administrador que proporcione funcionalidad en varias plataformas para poder usar las contraseñas en todos sus dispositivos.

3.1 Detección de ataques

Para la detección, en un array se enumeran los tipos de operaciones que se pueden realizar y cuando la consulta de inyección coincide con un dato de la matriz, este se puede rastrear hacía la lista de operaciones mediante la dirección IP y la fecha y hora en particular se registran aquí en la tabla (Abhay K. Kolhe, 2014).

Id	Ip Address	Injection Type	Date & Time
46	127.0.0.1	%	2013-11-14 22:08:56
47	127.0.0.1	=	2013-11-14 22:20:36
48	127.0.0.1	LIKE	2013-11-14 22:21:02
49	127.0.0.1	UPDATE	2013-11-14 22:21:52
50	127.0.0.1	INSERT	2013-11-14 22:22:41
51	127.0.0.1	1	2013-11-14 22:25:48
52	127.0.0.1	DELETE	2013-11-14 22:26:38
53	127.0.0.1	1	2013-11-14 22:27:37

Figura 5. Tabla de detección mediante IP (Abhay K. Kolhe, 2014)

4. DISCUSIÓN Y CONCLUSIONES

Los ataques de SQL en WordPress son de los más peligros que pueden existir, ya que en su mayoría son muy fáciles de llevar a cabo y pueden generar daños desastrosos, en especial a los sitios web pequeños de ventas de muchas empresas. La entrada del usuario debe ser revisada y limpiada, también debe enmascarar los datos para evitar la ejecución de código malicioso.

A este proceso se denomina saneamiento y validación de datos, agregar algunos plug-ins de seguridad también ayudan en estos casos. En si la automatización de WordPress, su facilidad ha hecho que muchos nuevos desarrolladores de contenido crezcan, pero eso también ha hecho que no se enfoque mucho en la codificación y eso ha facilitado e incrementado los ataques de inyección de SQL.

5. REFERENCIAS

[1] A, O. (2013). *Seguridad y Rendimiento en pro: WordPress.* Berkely, CA.
[2] Abhay K. Kolhe, P. A. (2014). Injection, Detection, Prevention of SQL Injection Attacks. *International Journal of Computer Applications*, 40-43.
[3] Belcic, I. (22 de Septiembre de 2020). *¿Qué es la inyección de SQL y cómo funciona?* Obtenido de Seguridad - OTRAS AMENAZAS: https://www.avast.com/es-es/c-sql-injection
[4] D., W. (2022). *WordPress Bible.*
[5] Guardado, J. J. (22 de Julio de 2011). Identificación y Clasificación de las Mejores Prácticas para Evitar la Inyección SQL. Zacatecas, Zacatecas, México.
[6] Moes, T. (2021). *Softwarelab*. Obtenido de https://softwarelab.org/es/que-es-inyeccion-sql/
[7] Schüring, T. (15 de Enero de 2020). *raidboxes*. Obtenido de https://raidboxes.io/
[8] Tovar Valencia, O. (2014). International Journal of Computer Applications. Bogotá, Colombia.
[9] W3Techs. (2022). *W3Techs*. Obtenido de https://w3techs.com/
[10] www.wordfence.com. (2020). *www.wordfence.com*. Obtenido de https://www.wordfence.com/

Correo del autor: ***saib.gamo@gmail.com***