¿QUÉ ES INYECCIÓN SQL?

AUTOR: RICARDO CASTILLO

NOVIEMBRE: 2020

San Marcos

Introducción

Aunque sea fácil prevenirlos, los ataques de inyección SQL son una gran amenaza que ha afectado a muchas compañías de renombre y medios de comunicación, así como a sus usuarios. Los expertos estiman que más de la mitad de todos los ciber ataques hoy en día se realizan con técnicas de inyección SQL. La mayoría ataca blogs de WordPress y sitios de comercio electrónico.

Conforme a lo anterior es de suma importancia conocer los tipos de ataques a los que están expuestos las grandes, medianas o pequeñas empresas, así como a los usuarios individuales que hacen uso de las redes, debido a que los ataques de inyección SQL se pueden organizar en cinco tipos principales, mismos que serán detallador en el siguientes documento, asimismo se brindan ejemplos de este tipo de ataques y su prevención.

Contenido

Antes de entrar en materia con la temática de la inyección SQL, se debe comprender qué es un SQL, para posteriormente retomar los elementos conectados con los ataques al lenguaje SQL

¿Qué es un SQL?

La programación SQL permite interactuar con una base de datos. El lenguaje de consulta estructurado (SQL) es el lenguaje de base de datos más implementado y valioso para cualquier persona involucrada en la programación informática o que usa bases de datos para recopilar y organizar información.
En la actualidad el estándar SQL, sea cual sea su entorno de ejecución, es imprescindible para cualquier desarrollador de aplicaciones informáticas centradas en la especialidad de la informática de gestión. Lo que hace que el dominar el lenguaje SQL sea tan importante para el desempeño de la labor de un programador.

Una vez comprendido qué es el SQL, se puede iniciar con el tema de la inyección SQL, mismo que se explica a continuación.

¿Qué es Inyección SQL?

La inyección SQL es el alojamiento del código malicioso en aplicaciones alojadas en páginas web con el fin de atacar esas páginas web y/o recoger los datos de los usuarios. Además de las filtraciones de datos, pueden usar esta técnica para alimentar con información falsa la base de datos de la aplicación, retirar información importante o denegar el acceso a los propietarios o creadores de la base de datos de la aplicación. Para hacer esto, deben encontrar y explotar alguna vulnerabilidad de la seguridad en el software de la aplicación objetivo.

Acortamiento de Lenguajes de Consulta Estructurada, SQL es un lenguaje creado especialmente para introducir datos y modificar los contenidos de las bases de datos. Las páginas web y las aplicaciones alojadas en ellas dependen de las bases de datos para almacenar todos sus datos y proporcionar servicio al usuario final. EL SQL juega un papel crucial en este proceso porque permite al usuario localizar contenido específico en la base de datos, por ejemplo, si usted está buscando un producto en concreto en

una tienda online, su término de búsqueda y sus preferencias (talla, peso, etc.) serán formateados en SQL.

Tal y como su nombre indica, los ataques de inyección SQL atacan esas bases de datos de SQL. Los hackers responsables de los ataques explotan la falta de filtros de validación de input por los llamados caracteres de escape (por ejemplo, respuesta negativa) para inyectar su propio código en el sistema. Dependiendo de sus objetivos, los hackers pueden poner un código para que cada vez que un usuario final introduzca una petición de búsqueda, ellos tengan el acceso a sus datos de registro o una parte de la base de datos se destruya completamente. Las inyecciones SQL también se pueden usar para expandir malware a través de páginas infectadas.

¿Qué Tipos de Ataques de Inyección SQL existen?

Basados en la forma de realizarse, los ataques de inyección SQL se pueden organizar en cinco tipos principales.

Inyección SQL de Unión: La inyección SQL de unión es un tipo de ataque de inyección SQL dentro de la banda que usa un operador de UNION SQL para extraer fácilmente la información solicitada de la base de datos atacada. El operador UNION permite al usuario extraer datos simultáneamente de múltiples tablas que consisten en el mismo número de columnas e idéntico tipo de datos. Los hackers pueden recoger la información que necesitan si inyectan la sentencia SELECT, pero para que el ataque sea exitoso, tienen que saber el número exacto de la tabla, el número de columnas y el tipo de datos.

SQL Inyección De Error: Otro tipo de ataque de inyección SQL dentro de la banda, la inyección SQL de error es una técnica que permite a los hackers aprovechar los mensajes de error devueltos por el servidor para sacar información sobre la estructura del servidor atacado. Los hackers realizan peticiones no válidas a propósito para desencadenar mensajes de error. Sin embargo, estos mensajes a menudo contienen, o bien resultados completos de la petición, o bien la información sobre cómo mejorar la petición para conseguir los resultados deseados, ambos ayudan a los hackers a llevar a cabo su ataque con éxito.

Inyección SQL Ciega de Tiempo: La inyección SQL ciega de tiempo es una técnica que implica el envío medido de peticiones SQL a la base de datos para evaluar el resultado de la petición. La consulta en cuestión forzará la base de datos a que espere antes de devolver un resultado, que será o VERDADERO o FALSO. Basada en el tiempo de espera, así como en la respuesta misma, el hacker puede evaluar si su carga se ha enviado correctamente. El mayor inconveniente de esta inyección SQL es su duración, ya que el hacker tiene que enumerar un carácter de la base de datos a la vez.

Inyección SQL Ciega de Boolean: Una inyección SQL ciega Boolean es una técnica de inyección inferencial muy similar a la inyección SQL ciega de tiempo. Concretamente, los hackers enviarán una petición SQL cada vez, con el intento de enumerar la base de datos. En base a la respuesta que obtengan, evaluará si su carga se ha enviado correctamente. Sin embargo, en lugar de medir sus peticiones, combinarán las expresiones VERDADERO y FALSO. Tal y como sucede con la inyección SQL de tiempo, estos ataques pueden ser muy lentos, especialmente cuando un hacker está atacando una base de datos grande.

Inyección SQL Fuera de Banda: La inyección SQL fuera de banda es una técnica usada por los hackers para generar peticiones DNS y/o HTTP que les entregarían los datos directamente a ellos. En ocasiones se usa como alternativa para ataques de inyección SQL ciega de tiempo, normalmente cuando están tratando con una respuesta lenta del servidor o cuando es imposible recoger datos a través del mismo canal usado para lanzar el ataque. Como su éxito depende de los elementos que solo puede activar el administrador del servidor, los ataques de inyección SQL fuera de banda son muy raros.

Ejemplos de Ataques de Inyección SQL

Durante las últimas dos décadas, un gran número de ataques de inyección SQL han sido dirigidos hacia grandes páginas web, empresas y plataformas de redes sociales. Algunos de estos ataques han resultado en grandes filtraciones de datos. Algunos de los ejemplos más notorios incluyen los siguientes:

En 2008, dos hackers nacidos en Rusia usaron técnicas de inyección SQL para atacar Heartland Payment Systems, un proveedor entonces exitoso de soluciones de tramitación de pagos. Clasificada como la filtración de datos de tarjetas de crédito más grande hasta el momento, el ataque dio a los hackers acceso a la información de más

de 150 millones de tarjetas de crédito y costó a la empresa afectada más de 300 millones de dólares. En 2018, los hackers fueron condenados a una sentencia conjunta de más de 16 años.

En 2016, un grupo de hackers explotó 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, los hackers consiguieron robar datos de registro de más de 27 millones de cuentas.

También en 2016, los hacker usaron métodos de inyección SQL para lanzar un ciber ataque contra el banco nacional de Qatar. Los hackers consiguieron robar más de 1.4 GB de datos, que fueron publicados poco después. Estos datos implicaban la información de cuentas de miles de clientes, incluidos los miembros de la familia real del país, oficiales de la inteligencia, polémicos líderes religiosos, así como varios ciudadanos británicos, franceses y estadounidenses que estaban indicados como espías en la base de datos del banco.

Cómo Prevenir los Ataques de Inyección SQL

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. 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.

Conclusiones y recomendaciones

Durante las últimas dos décadas, un gran número de ataques de inyección SQL han sido dirigidos hacia grandes páginas web, empresas y plataformas de redes sociales. Algunos de estos ataques han resultado en grandes filtraciones de datos, no obstante, cualquier usuario puede ser atacado. Los hackers llevan a cabo los ataques de inyección de SQL por varias razones, no obstante, ninguna de ellas tendrá buenas intenciones, por lo tanto los usuarios deben asegurarse instalar el mejor software antivirus, este contribuirá a mantener su computador y sus datos a salvo de los virus, malware y muchas otras amenazas potenciales.

Lo anterior se recomienda, debido a que al visitar una página web infectada, el malware empezará a descargarse sin el consentimiento del usuario y peor aún sin darse cuenta de que está siendo atacado, así que el no utilizar antivirus, es arriesgarse a que los hackers puedan efectuar ataques de inyección SQL para comprometer páginas web fiables con software malicioso y puesto que una vez que este ha instalado, dará a los hackers acceso a su historial de búsquedas, datos personales e incluso sus pulsaciones sobre el teclado.

De ahí la importancia de asegurar la instalación de programas que prevengan el acceso a los códigos malisiosos.

Referencias bibliográficas

- SoftwareLab.org (2020) ¿Qué es Inyección SQL? Recuperado de: https://softwarelab.org/es/que-es-inyeccion-sql/

- RED/PROYDESA (2020) ¿Qué es y para qué sirve el Lenguaje SQL? https://www.proydesa.org/portal/noticias/1553-que-es-y-para-que-sirve-el-lenguaje-sql

San Marcos

www.usanmarcos.ac.cr

San José, Costa Rica