TECNOLÓGICO NACIONAL DE MÉXICO

INSTITUTO TECNOLÓGICO DE TLAXIACO

SEGURIDAD Y VIRTUALIZACIÓN

Investigación practica 3

Integrantes del Equipo:

Arnol Jesus Cruz Ortiz

Amilkar Vladimir Reyes Reyes

Rael Gabriel Bautista

Sandra Gabriela Velasco Guzmán

Docente:

Edward Osorio Salinas

Materia:

Seguridad y virtualización

Carrera:

Ingeniera en Sistemas Computacionales

Grupo: 7US

Semestre: Agosto – diciembre 2024

09/Septiembre/2024

Indicé

INYECCIÓN DE SQL: CONCEPTOS DE BASES DE DATOS SEGURAS Y CÓMO SE PUEDEN IMPLEMENTAR.

¿Qué es la inyección de SQL?

Los ataques de inyección de SQL son una de las vulnerabilidades de las aplicaciones web más antiguas, ya que se analizan desde fines de 1990, pero siguen siendo relevantes en la actualidad. En esta explicación, se describe qué son, cómo funcionan y cómo se pueden prevenir.

Una inyección de SQL, a veces abreviada como SQLi, es un tipo de vulnerabilidad en la que un atacante usa un trozo de código SQL (lenguaje de consulta estructurado) para manipular una base de datos y acceder a información potencialmente valiosa. Es uno de los tipos de ataques más frecuentes y amenazadores, ya que puede atacar prácticamente cualquier sitio o aplicación web que use una base de datos basada en SQL (la mayoría).

¿Cómo funcionan los ataques de inyección de SQL?

Para entender la inyección de SQL, es importante saber qué es el lenguaje de consulta estructurado (SQL). SQL es un lenguaje de consulta que se utiliza en programación para modificar y eliminar los datos almacenados en bases de datos relacionales y acceder a ellos. Debido a que la gran mayoría de los sitios y aplicaciones web utilizan bases de datos SQL, un ataque de inyección de SQL puede tener consecuencias graves para las organizaciones.

Una consulta de SQL es una solicitud enviada a una base de datos por algún tipo de actividad o función, como consultas de datos o una ejecución de código SQL que se debe realizar. Un ejemplo es cuando la información de inicio de sesión se envía a través de un formulario web para que el usuario pueda acceder al sitio. Normalmente, este tipo de formulario web está diseñado para aceptar solo tipos muy específicos de datos, como un nombre o una contraseña. Cuando se agrega esa información, esta se coteja contra una base de datos y, si coincide, se otorga acceso al usuario. Si no coincide, se niega el acceso.

Los posibles problemas surgen porque la mayoría de los formularios web no tienen forma de detener el ingreso de información adicional. Los atacantes pueden aprovechar esta debilidad y utilizar los cuadros de entrada del formulario para enviar sus propias solicitudes a la base de datos. Esto podría permitirles llevar a cabo una amplia gama de actividades maliciosas, desde el robo de datos confidenciales hasta la manipulación de la información de la base de datos para sus propios fines.

Debido a la prevalencia de sitios web y servidores que utilizan bases de datos, las vulnerabilidades de inyección de SQL son uno de los tipos de ciberataques más antiguos y generalizados. Varios avances en la comunidad hacker aumentaron el riesgo de este tipo de ataques; en especial, la llegada de herramientas para detectar y aprovechar la inyección de SQL. Disponibles de forma gratuita en desarrolladores de código abierto, estas herramientas les permiten a los cibercriminales realizar ataques automáticamente en tan solo minutos, ya que les permiten acceder a cualquier tabla o columna de la base de datos con tan solo un clic y un proceso de ataque.

Signos de SQLi

Es posible que un ataque de inyección de SQL exitoso no muestre ningún signo. Sin embargo, a veces hay algunas señales externas, como las siguientes:

- Recepción de una cantidad excesiva de solicitudes en un plazo breve. Por ejemplo, es posible que vea muchos correos electrónicos del formulario de contacto de su página web.
- Anuncios que redirigen a sitios web sospechosos.
- Ventanas emergentes desconocidas y mensajes de error.

Tipos de inyección de SQL

Según la forma de acceso a los datos de backend y la extensión del posible daño provocado, las inyecciones de SQL se pueden dividir en las siguientes tres categorías:

SQLi en banda:

Este tipo de ataque SQLi es sencillo para los atacantes, porque usan el mismo canal de comunicación para lanzar ataques y obtener resultados. Este tipo de ataque SQLi tiene dos subvariantes:

SQLi basado en errores: la base de datos genera un mensaje de error por las acciones del atacante. El atacante obtiene información sobre la infraestructura de la base de datos en función de los datos que generaron estos mensajes de error.

SQLi basado en unión: el atacante usa el operador UNION SQL para obtener los datos deseados mediante la fusión de varias declaraciones Select en una única respuesta HTTP.

SQLi inferencial (también conocida como inyección de SQL ciega):

En este tipo de SQLi, los atacantes usan patrones de respuesta y comportamiento del servidor después de enviar cargas útiles de datos para obtener más información sobre su estructura. Los datos no se transfieren de la base de datos del sitio web al atacante, así que el atacante no ve la información sobre el ataque en banda (por eso se usa el término “SQLi ciega”). La SQLi inferencial se puede clasificar en dos subtipos:

SQLi basado en el tiempo: los atacantes envían una consulta de SQL a la base de datos, esto hace que la base de datos espere unos segundos antes de responder si la consulta es verdadera o falsa.

SQLi booleana: los atacantes envían una consulta de SQL a la base de datos, así permiten que la aplicación responda mediante la generación de un resultado verdadero o falso.

SQLi fuera de banda:

Este tipo de ataque de SQL se puede llevar a cabo en las siguientes dos situaciones:

- Cuando los atacantes no pueden usar el mismo canal para lanzar el ataque y compartir información; o

- Cuando un servidor es demasiado lento o inestable para realizar estas acciones.

Impacto de los ataques de inyección de SQL

Un ataque de inyección de SQL exitoso puede tener consecuencias graves para una empresa. Esto se debe a que un ataque de inyección de SQL puede lograr lo siguiente:

- **Exponer datos sensibles.** Los atacantes pueden extraer datos, lo que pone en riesgo la exposición de datos sensibles almacenados en el servidor SQL.
- Comprometer la integridad de los datos. Los atacantes pueden alterar o eliminar información del sistema.
- **Comprometer la privacidad de los usuarios.** En función de los datos almacenados en el servidor SQL, un ataque puede exponer información sensible del usuario, como direcciones, números de teléfono y detalles de tarjetas de crédito.
- **Otorgarle al atacante acceso de administrador al sistema**. Si un usuario de la base de datos tiene privilegios de administrador, un atacante puede acceder al sistema a través de un código malicioso.
- **Otorgarle a un atacante acceso general a su sistema.** Si usa comandos SQL débiles para verificar nombres de usuario y contraseñas, un atacante podría acceder a su sistema sin conocer las credenciales del usuario. De esta forma, el atacante puede causar problemas al acceder a información sensible y manipularla.

Ejemplos de inyección de SQL

A lo largo de los años, muchas organizaciones fueron víctimas de SQLi. Estos son algunos ejemplos de gran repercusión:

Fornite, 2019 Fornite es un juego en línea con más de 350 millones de usuarios. En 2019, se descubrió una vulnerabilidad de inyección de SQL que les permitía a los atacantes acceder a las cuentas de los usuarios. La vulnerabilidad se corrigió.

Cisco, 2018

En 2018, se encontró una vulnerabilidad de inyección de SQL en Cisco Prime License Manager. La vulnerabilidad permitía que los atacantes tuvieran acceso shell a los sistemas en los que estaba implementado el administrador de licencias. Cisco ya corrigió la vulnerabilidad.

Tesla, 2014

En 2014, investigadores de seguridad anunciaron que podían quebrantar el sitio web de Tesla con una inyección de SQL, lo que les permitiría obtener privilegios de administrador y robar datos de los usuarios en el proceso.

Preguntas frecuentes sobre los ataques de inyección de SQL

Las preguntas frecuentes sobre SQLi son las siguientes:

¿Qué es un ataque de inyección de SQL?

Un ataque de inyección de SQL usa un código SQL malicioso para manipular la base de datos de backend y acceder a información privada. Esta información puede incluir datos sensibles de empresas, listas de usuarios o detalles de los clientes. SQL significa “lenguaje de consulta estructurado” e inyección de SQL a veces se abrevia como SQLi.

¿Qué hace una inyección de SQL?

Los ataques de inyección de SQL les permiten a los atacantes falsificar identidades, alterar datos existentes, exponer datos del sistema, eliminar datos o quitar su disponibilidad y convertirse en administradores del servidor de la base de datos. Los ataques de inyección de SQL pueden provocar daños graves a las empresas, como la pérdida de confianza de los clientes si se quebrantan datos confidenciales de los usuarios.

¿Cómo son los ataques de inyección de SQL habituales?

Debido a que son relativamente fáciles de implementar y que la posible recompensa es grande, los ataques de inyección de SQL son comunes. Las estadísticas varían, pero se estima que los ataques de inyección de SQL

constituyen la mayoría de los ataques en las aplicaciones de software. Según el Open Web Application Security Project (Proyecto abierto de seguridad de aplicaciones web), los ataques de inyección, que incluyen las inyecciones de SQL, fueron el tercer riesgo de seguridad más grave en las aplicaciones web en 2021.

Cómo prevenir los ataques de inyección de SQL

Para las empresas interesadas en la prevención de la inyección de SQL, los principios clave para ayudar a proteger los sitios y las aplicaciones web son los siguientes:

Capacitar al personal: Concientizar al equipo responsable de la aplicación web sobre los riesgos relacionados con la SQLi y brindar la capacitación necesaria para todos los usuarios en función del puesto.

Mantener el control de la entrada de los usuarios: Cualquier entrada de usuario utilizada en una consulta de SQL genera un riesgo. Aborda las entradas de los usuarios autenticados o internos de la misma manera que las entradas públicas hasta que se verifiquen. Otórgales a las cuentas que se conectan a la base de datos SQL solo los privilegios mínimos necesarios. Utilice listas blancas como práctica estándar en lugar de listas negras para verificar y filtre la entrada de los usuarios.

Utilizar las versiones más recientes: Es importante usar la versión más reciente del entorno de desarrollo para maximizar la protección, ya que es posible que a las versiones anteriores les falten funciones de seguridad. Asegúrese de instalar el software y los parches de seguridad más recientes cuando estén disponibles.
Analizar de forma continua las aplicaciones web:
Use herramientas integrales de administración del rendimiento de las aplicaciones. Analizar regularmente las aplicaciones web permite identificar y abordar posibles vulnerabilidades antes de que provoquen daños graves.

Usar un firewall: El firewall de una aplicación web (WAF) a menudo se usa para filtrar SQLi, así como otras amenazas en línea. Un WAF confía utiliza una extensa lista de firmas que se actualiza con frecuencia y le permite filtrar

CONCEPTOS DE BASES DE DATOS SEGURAS Y CÓMO SE PUEDEN IMPLEMENTAR.

¿Qué es la seguridad de las bases de datos?

La seguridad de las bases de datos se refiere al conjunto de herramientas, medidas y controles diseñados para establecer y mantener la confidencialidad, la integridad y la disponibilidad de las bases de datos. Este artículo se va a centrar principalmente en la confidencialidad, ya que es el elemento que se ve comprometido en la mayoría de las infracciones de datos.

La seguridad de las bases de datos debe tratar y proteger lo siguiente:

- Los datos de la base de datos
- El sistema de gestión de bases de datos (DBMS)
- Cualquier aplicación asociada
- El servidor de base de datos físico y/o el servidor de base de datos virtual, y el hardware subyacente
- La infraestructura informática y/o de red utilizada para acceder a la base de datos

¿Por qué es importante?

Por definición, una infracción de datos es la incapacidad de mantener la confidencialidad de los datos en una base de datos. La cantidad de daño que las infracciones de datos infligen a su empresa depende de varios factores o consecuencias:

Propiedad intelectual comprometida: la propiedad intelectual —secretos comerciales, invenciones, prácticas propietarias— puede ser fundamental para poder mantener una ventaja competitiva en el mercado. Si dicha propiedad intelectual es robada o queda expuesta, su ventaja competitiva puede ser difícil o imposible de mantener o recuperar.

Daño a la reputación de la marca: los clientes o los socios pueden no estar dispuestos a comprar sus productos o servicios (o a hacer negocios con su empresa) si no sienten que pueden confiar en usted para proteger los datos.

Continuidad del negocio (o falta de ella): algunas operaciones de negocio no pueden continuar hasta que se resuelva la infracción.

Multas o sanciones por falta de conformidad: el impacto financiero por no cumplir con las normativas globales, como la Sarbannes-Oxley Act (SAO) o eñ Payment Card Industry Data Security Standard (PCI DSS); las normativas de privacidad de datos específicas del sector, como la HIPAA, o las normativas regionales de privacidad de datos, como el Reglamento General de Protección de Datos (RGPD) de Europa, puede ser devastador, con sanciones superiores, en el peor de los casos, a varios millones de dólares por violación.

Costes de reparación de infracciones y notificación a los clientes: además del coste de comunicar una infracción al cliente, la organización que sufre la infracción debe abonar las actividades forenses y de investigación, de gestión de crisis, triaje, reparación de los sistemas afectados, etc.

IMPLEMENTACIÓN DE MEDIDAS DE SEGURIDAD AVANZADAS

Además de las mejores prácticas básicas, existen medidas de seguridad avanzadas que se pueden implementar para fortalecer aún más la protección de las bases de datos:

Uso de cifrado de datos en reposo y en tránsito

El cifrado de datos en reposo y en tránsito implica encriptar los datos tanto cuando están almacenados en la base de datos como cuando se transmiten a través de la red. Esto garantiza que incluso si un atacante logra acceder a los datos, no podrá leerlos ni utilizarlos sin la clave de desencriptación adecuada.

Configuración de listas de control de acceso

Las listas de control de acceso permiten definir y gestionar los permisos de acceso a nivel de usuario y objeto en la base de datos. Al utilizar estas listas, se pueden establecer reglas detalladas sobre qué usuarios pueden acceder a qué

datos y qué operaciones están permitidas. Esto proporciona un mayor control sobre los accesos y reduce los riesgos.

Monitoreo y detección de intrusiones

Implementar soluciones de monitoreo y detección de intrusiones permite identificar y responder rápidamente a posibles amenazas. Estas soluciones analizan los registros de actividad, buscan patrones anormales y generan alertas en caso de actividad sospechosa. El monitoreo constante ayuda a detectar y mitigar los ataques antes de que causen un daño significativo.

Respuesta ante incidentes

Es importante contar con un plan de respuesta ante incidentes bien definido. Esto incluye la identificación de roles y responsabilidades, la creación de procedimientos de manejo de incidentes y la realización de simulacros periódicos. Tener un plan establecido agiliza la respuesta y minimiza el impacto en caso de una brecha de seguridad.

Seguridad en bases de datos en la nube

La seguridad en bases de datos en la nube presenta desafíos adicionales debido a la naturaleza compartida de la infraestructura. Al utilizar bases de datos en la nube, es importante considerar las siguientes consideraciones específicas:

- Asegurarse de comprender las responsabilidades compartidas entre el proveedor de la nube y el usuario. El proveedor generalmente se encarga de la seguridad física de los servidores y la infraestructura, mientras que el usuario es responsable de garantizar la seguridad de los datos y la configuración de la base de datos.
- Utilizar medidas de seguridad específicas para la nube, como el cifrado de datos y las soluciones de seguridad proporcionadas por el proveedor. Estas medidas ayudan a proteger los datos almacenados en la nube y a garantizar la confidencialidad y disponibilidad de la información.

BIBLIOGRAFÍA

- Seguridad de las bases de datos: guía básica. (2023, mayo 10). *Ibm.com*. https://www.ibm.com/es-es/topics/database-security
- Seguridad en bases de datos: conceptos y mejores prácticas. (2023, junio 29). *Informática y Tecnología Digital*. https://informatecdigital.com/bases-de-datos/seguridad-en-bases-de-datos/