****

**UNIVERSIDAD GERARDO BARRIOS SAN MIGUEL**

Facultad de Ciencia y Tecnología.

**Actividad:**

Amenazas, riesgos y vulnerabilidades de las bases de datos

**Ingeniera:**

Gisela Espinoza

**Materia:**

Administración y Base de Datos II

**Alumno:**

Manfredy José Quintanilla Chávez - SMIS021120

Jhonatan Josué Benítez Turcios – SMIS024420

Introducción

En este documento vamos a recopilar información de algunas amenazas, riesgos y vulnerabilidades en las bases de datos SQL y NoSQL y así mismo darle solución y prevenciones para evitar la pérdida de datos o filtraciones de datos personales.

Inyección SQL

Este lo podemos encontrar en cualquier campo que requiera información, en este se agrega una sentencia SQL esta permitirá que se ejecute un código externo.

Un ejemplo claro es que un hacker puede acceder a los nombres de usuarios y contraseñas de la base de datos con el simple hecho de llenar ambos campo de texto con “OR””=”

El código del servidor creará una sentencia SQL válida que se verá así:

SELECT \* FROM Users WHERE Name = “or””=” AND Pass = “or””=”

# Solución:

* Para la prevención de ataques SQL se requiere que el programador de la interfaz y de la aplicación, generen métodos que validen las sentencias SQL y los datos ingresados en los formularios.

# Otras soluciones:

* Podemos prevenir estos fallos con softwares especiales que nos permitan hacer pruebas de impregnación estos hacen el trabajo de analizar y ejecutar detenciones y explotaciones de fallas en la base de datos. SQLmap es perfecto para realizar y ejecutar las pruebas de fallos de inyección SQL, cabe recalcar que es una herramienta de código libre.
* Podemos utilizar DataDome este detecta bots de análisis de vulnerabilidades SQLi y los bloquea antes de que alcance su aplicación y evita que continúen ataque de inyección SQL.

Inyección NoSQL

Como las bases de datos NoSQL tienen menos restricciones en relaciones y chequeos de consistencia, son más vulnerables a ataques de inyección, sin embargo, el atacante debe ser experto en programación y sintaxis del lenguaje atacado.

## Solución:

* En SQL si hubiera soluciones, por ejemplo, el control de acceso de nivel de consulta, gracias a ello restringe los privilegios a operaciones y datos requeridos. Pero, en NoSQL la mayoría de los motores de búsqueda NoSQL las medidas de seguridad no están habilitadas por defecto, por ejemplo: Debilidad de autenticación, Debilidades en la autorización, y Debilidad de autorización de administrador.

# Otras soluciones:

* El uso de herramientas externas que brindad una solución a ataques y escaneo de vulnerabilidades, Por ejemplo, está la herramienta scuba, esta herramienta es gratuita que permite escanear vulnerabilidades y fallas de configuración, incluye Oracle, Microsoft SQL Server, MySQL y entre otros más.

Auditoria de acceso y autenticación.

En esta podremos saber quién accedió a cuál sistema, cuando y como.

* Auditoria de usuario y administrador.
  + En ella se podrá observar que tipo de actividades realizaron los usuarios y los administradores en la base de datos.
* Monitoreo de actividad de seguridad.
  + Es se encarga de identificar y marcar cualquier acceso sospechoso, inusual o anormal.
* Auditoria de vulnerabilidad y amenazas.
  + Este detecta primero las vulnerabilidades y después monitorea a los usuarios que intentan explotarlas.
* Cambiar la auditoria.
  + Esta establece una política de base para la base de datos; configuración, esquema, usuarios, privilegios y estructura, luego rastrea desviaciones de esa línea base.

Correo electrónico Pishing malicioso.

Ahora hablemos de un ataque más común por correo electrónico, los mensajes en pishing que contiene un enlace hacia un sitio malicioso son los más comunes y usados, con un solo clic equivocado puede desencadenar una descarga peligrosa.

# Solución.

Evitar no abrir correos que no sean verídicos o de confianza.

Privilegios de acceso excesivos o inutilizados uso abusivo de los privilegios asignados.

Esta amenaza es muy común cuando no hay un control de nivel de acceso, en una base de datos siempre hay privilegios para cada usuario, observador, editor y administrativo, y esta amenaza viene cuando hay un error en los privilegios y el usuario se aprovecha de este problema y aprovecha a acceder a toda la información confidencial de la base de datos, intentando editar o eliminar la información. Incluso llegando a tirar la misma base de datos.

Desprotección de los soportes o destinos de las copias de seguridad

Una mala administración de las copias de seguridad por medio de las personas encargadas puede llevar a catástrofe todos los datos que hacen que la empresa este en pie y que se pueda laborar.

# Solución:

* Se debe asignar una copia de seguridad automática y que se genere diariamente para que los datos que se van agregando sean asegurados y poder utilizarlos en algún caso que se pierdan.
* Se debe proteger el dispositivo en el que se hacen las copias de seguridad para que este no sea un punto directo para ser atacado y vulnerado.

Conclusiones

Las medidas antes mencionadas deben servir de recomendación para futuros trabajos y para advertir si nuestros datos están en riesgo y poder evitar perdidas “repentinas” que se pueden dar en alguna amenaza que podamos recibir por medio de correos electrónicos o por las mismas personas que se han contratado ya que pueden ocurrir daños irreparables para la información sensible que podemos manejar.