UNIVERSIDAD “GERARDO BARRIOS”

FACULTAD DE CIENCIA Y TECNOLOGIA

Asignatura:

ADMON DE BASES DE DATOS II

Nombre del Docente:

GISELA YASMÍN GARCÍA ESPINOZA

Integrantes:

SMSS096022 - Edin Iván Saravia Vigil

SMIS020521 - Joel Cristopher Turcios Turcios

Smis024117 - Anderson Emmanuel Morales Lazo

INTRODUCCION

Al hablar de términos de seguridad informática se debe entender a las bases que conforman los cimientos de esta ciencia, para las partes más complejas de esta disciplina, una de estas bases es el concepto de seguridad, La seguridad siempre busca la gestión de riesgos, esto quiere decir que se tenga siempre una forma de evitarlo o prevenirlo y que se pueda realizar ciertas acciones para evitar esas situaciones de la mejor forma.

vulnerabilidades de SQL es un servicio que proporciona visibilidad sobre el estado de seguridad e incluye acciones recomendadas para resolver problemas de seguridad y mejorar la seguridad de la base de datos ya que Una amenaza a una base de dato es una circunstancia que tiene el potencial de causar un daño o una perdida, es decir, las amenazas, riesgos o vulnerabilidades.

Las organizaciones son más dependientes de sus redes informáticas y un problema que las afecte, por pequeño que sea, puede llegar a comprometer la continuidad de las operaciones, situación que inevitablemente se traduce en pérdida económica, retraso en las operaciones y crisis de confianza por parte de los usuarios.

Seguridad en bases de datos SQL y NoSQL

Las bases de datos son una de las principales herramientas que se utilizan hoy en día para el almacenamiento de datos y procesamiento de información.

Al igual que todos los otros componentes informáticos son vulnerables a taques, veremos dos de los ataques más comunes y la mejor manera de poder prevenirlos.

Amenaza	DB´s RELACIONALES	DB´s NoSQL
Inyección SQL	Por errores en programación se puede permitir la inyección SQL en una base de datos.	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.
Seguridad	La seguridad de las bases de datos puede ser atacada por problemas en configuración y manejo de roles en los datos.	Las Bases de Datos NoSQL tienen deficiencias en seguridad.

Inyección SQL:

Se utilizan los campos de texto en formularios que envían información a la base de datos, con el fin de generar consultas válidas que muestren información o den acceso al sistema.

Seguridad:

Al manejar sistemas complejos de bases de datos, se presentan errores de configuración en la seguridad, lo que en manos expertas puede presentar riesgos graves para el sistema.

Ejemplo de ataques:

Inyección SQL DB:

En un campo de texto cualquiera que ingrese información, se agrega una sentencia SQL que permita ejecutar código externo.
Un hacker puede tener acceso a nombres de usuarios o contraseñas en la base de datos simplemente insertando " OR ""=" en el campo de texto de usuario o contraseña:

Usuario:

Contraseña:

El Código del servidor creará una sentencia SQL válida que se verá así:
SELECT * FROM Users WHERE Name ="" or ""="" AND Pass ="" or ""=""

Lo que le da acceso a la información al hacker.

Inyección en bases de datos NoSQL

Si un atacante puede manipular los datos pasados al operador $ where, ese atacante podría incluir JavaScript arbitrario para ser evaluado como parte de la consulta de MongoDB. Un ejemplo de vulnerabilidad se expone en el siguiente código, si la entrada del usuario se pasa directamente a la consulta MongoDB sin verificar.

db.myCollection.find({ active: true, $where: function() { return obj.credits - obj.debits < $userInput; } });;

Inyección en bases de datos NoSQL

Si un atacante puede manipular los datos pasados al operador $ where, ese atacante podría incluir JavaScript arbitrario para ser evaluado como parte de la consulta de MongoDB. Un ejemplo de vulnerabilidad se expone en el siguiente código, si la entrada del usuario se pasa directamente a la consulta MongoDB sin verificar.

```
db.myCollection.find( { active: true, $where: function() { return obj.credits - obj.debits < $userInput; } } );;
```

Ataques de inyección SQL:

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

Seguridad de base de datos:

La seguridad se mejora al implementar medidas que permitan realizar un control estricto de las consultas realizadas por los usuarios, adicionalmente la asignación de permisos generalizados y la falta de control en la parametrización generan riesgos de acceso a la base de datos.

Punto 2

Investiga como solucionar y aporta nuevas ideas sobre como solucionas los problemas identificados en el punto.

1.1 Auditoría de acceso y autenticación

¿Quién accedió a qué sistemas, cuándo y cómo?

1.2 Auditoría de usuario y administrador

Qué actividades realizaron en la base de datos tanto usuarios como administradores

1.3 Monitoreo de actividad de seguridad

Identifique y marque cualquier acceso sospechoso, inusual o anormal a datos confidenciales o sistemas críticos

1.4 Auditoría de vulnerabilidad y amenazas

Detecta vulnerabilidades en la base de datos, luego monitorea a los usuarios que intentan explotarlas

1.5 Cambiar la auditoría

Establecer una política de base para la base de datos; configuración, esquema, usuarios, privilegios y estructura, luego rastrear desviaciones de esa línea base.

Conclusiones

-Con esto aprendimos que la seguridad informática su principal objetivo es la protección de los reactivos informáticos del usuario.

-Diferenciamos los mecanismos de la seguridad de nuestras bases de datos, así como su clasificación entre otras cosas, así como los tipos de vulnerabilidad y de riesgo.

-Este trabajo nos da diferentes opciones para asegurar nuestros datos, así como para protegerlos.

-Por seguridad de base de dato conjunto de normas, procedimientos y herramientas, que tienen como objetivo garantizar la disponibilidad, integridad, confidencialidad y buen uso de la información que reside en un sistema de información.