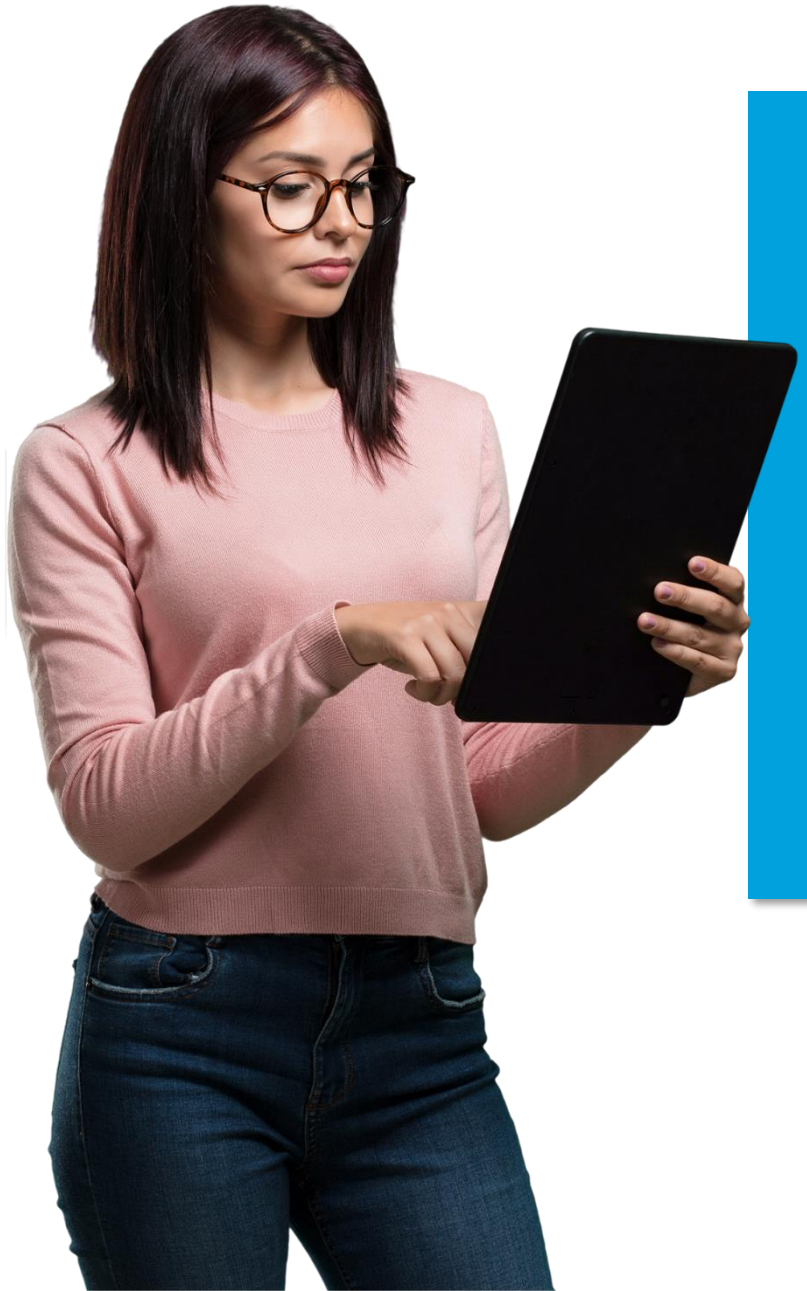


Unidad # 2
Nombre del contenido: Amenazas, riesgos y vulnerabilidades de las bases de datos

Administración de Base de Datos II

UNIVERSIDAD GERARDO BARRIOS
Líderes en Gestión del Conocimiento

Comisión de Acreditación de la Calidad de la Educación Superior
UNIVERSIDAD GERARDO BARRIOS (UGB)
ACREDITADA
2019- 2024

Contenidos a desarrollar

- Amenazas, riesgos y vulnerabilidades de las bases de datos

¿Cuales son las amenazas mas comunes de seguridad en bases de datos?

.

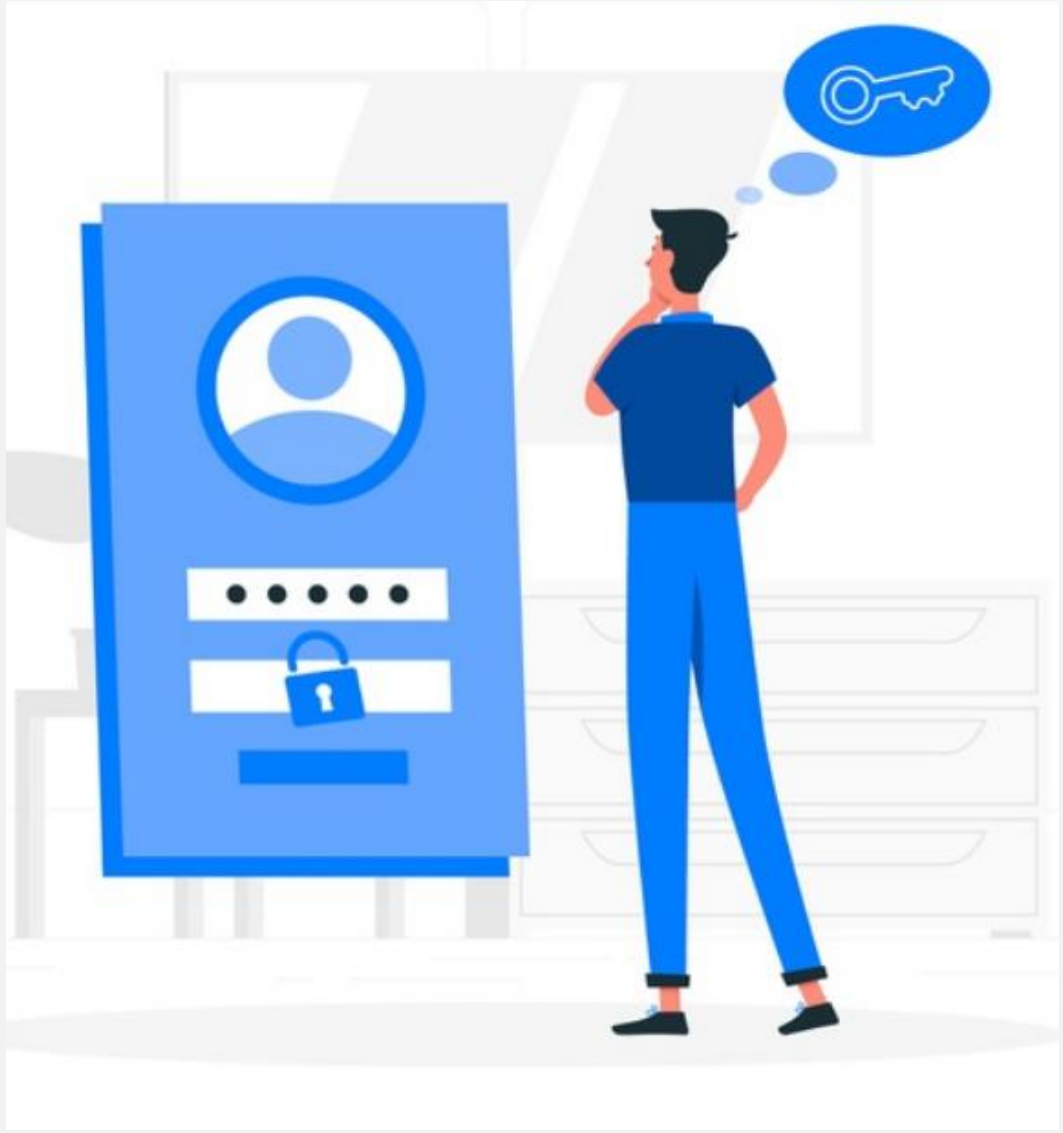
Principales Amenazas

- Ausencia de contraseñas
- Privilegios excesivos
- Vulnerabilidades de la plataforma
- Inyección de sql
- Auditoría débil
- Denegación de servicio
- La Exposición De Los Datos De Backup
- Desbordamiento de búfer
- Bases de datos sin actualizar

Ausencia de contraseñas

- Nombre de usuario/password en blanco o bien hacer uso de uno débil Hoy en día no es raro encontrarnos pares de datos usuario/password del tipo admin/12345 o similar.
- Esta es la primera línea de defensa de entrada a nuestra información y debemos optar por el uso de algo más complejo que sea complicado de conseguir por parte de cualquier atacante.

.



PRIVILEGIOS EXCESIVOS

Cuando a un usuario se le entregan privilegios de la base de datos que excedan los requerimientos de su puesto de trabajo, el riesgo que se crea puede ser innecesario

La solución a este problema (además de buenas políticas de contratación) es el control de acceso a nivel de consulta

El control de acceso a nivel de consulta restringe los privilegios de las operaciones a solo utilizar los datos mínimos requeridos.

La plataformas de seguridad de bases de datos nativas ofrecen estas capacidades (triggers, RLS, y así sucesivamente), pero el diseño de estas herramientas manuales las hacen impracticables en todo excepto en las implementaciones más limitados según experiencia de expertos de seguridad web.

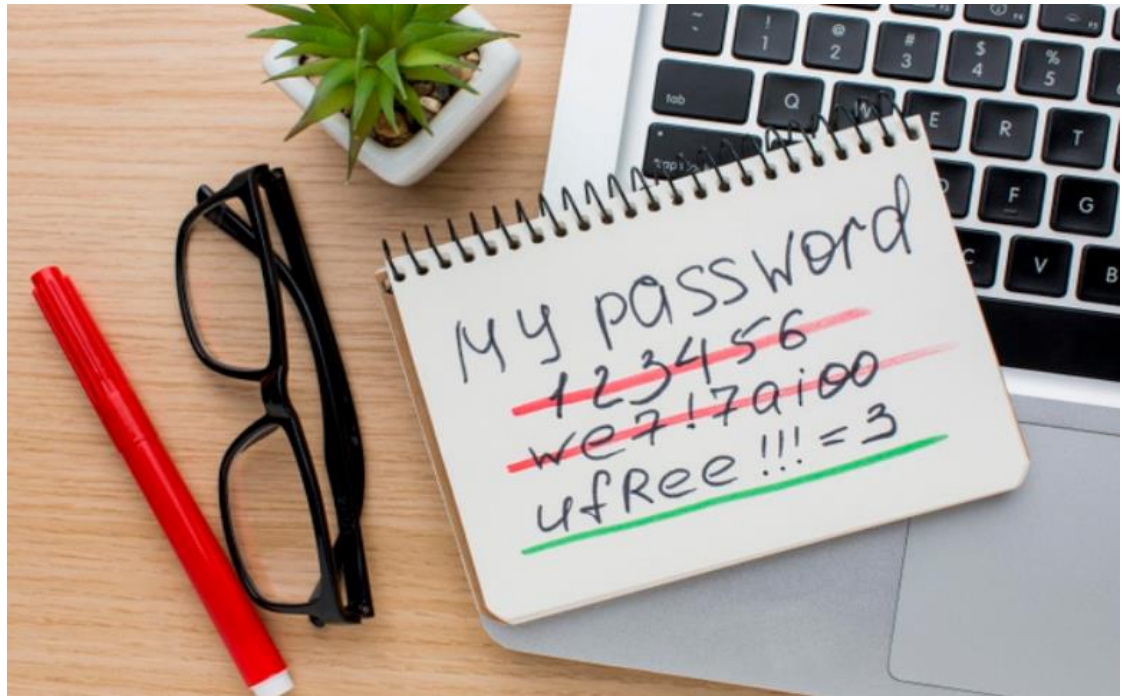
Características de bases de datos innecesariamente habilitadas

Cada instalación de base de datos viene con una serie de paquetes o módulos adicionales de distintas formas y tamaños que en muy pocas ocasiones todos ellos son utilizadas por las compañías, lo que las convierten en una posible puerta de entrada para sufrir algún tipo de ataque si en esos paquetes se descubre cualquier problema de seguridad.

Para reducir riesgos, es recomendable que los usuarios detecten esos paquetes que no se utilizan y se desactiven del servidor donde estén instalados.

Esto no sólo reduce los riesgos de ataques, sino que también simplifica la gestión de parches ya que únicamente será de máxima urgencia actualizar aquellos que hagan referencia a un módulo que estemos utilizando.

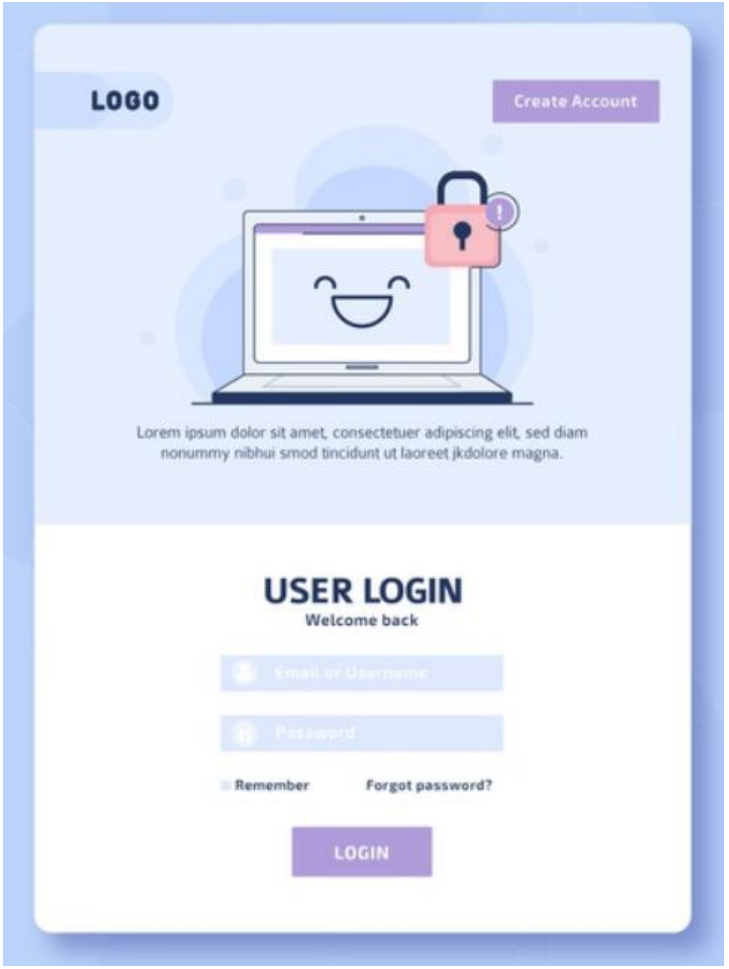
Elevación de privilegios no autorizados



Los atacantes pueden aprovechar las vulnerabilidades en el software de gestión en la base de datos para convertir los privilegios de acceso de bajo nivel de privilegios de acceso de alto nivel. Por ejemplo, sin seguridad de bases de datos, un atacante podría aprovechar una vulnerabilidad de desbordamiento de búfer de base de datos para obtener privilegios administrativos.

Exploits de elevación de privilegios pueden ser derrotados con una combinación de control de acceso a nivel de consulta, auditoría de base de datos y los sistemas de prevención de intrusiones (IPS) tradicionales. Control de acceso a nivel de consulta puede detectar un usuario que de repente utiliza una operación de SQL inusual, mientras que un IPS puede identificar una amenaza específica de seguridad web documentada dentro de la operación.

Vulnerabilidades de la plataforma



Las vulnerabilidades en los sistemas operativos pueden conducir al acceso no autorizado a datos y la corrupción.

Las herramientas de IPS son una buena manera de identificar y / o bloquear ataques diseñados para aprovechar las vulnerabilidades de la plataforma de base de datos.

Inyección de sql

La mayoría de las aplicaciones web desarrolladas hoy en día hacen uso de una base de datos para ofrecer páginas dinámicas y almacenar información tanto de los usuarios como de la propia herramienta, el uso de este tipo de lenguaje ha traido consigo la aparición de numerosas vulnerabilidades. Los Ataques de inyección SQL implican a un usuario que se aprovecha de vulnerabilidades en aplicaciones web y procedimientos almacenados para proceder a enviar consultas de bases de datos no autorizadas, a menudo con privilegios elevados.

Soluciones de seguridad de bases de datos, auditoría de base de datos, control de acceso a nivel de consulta detecta consultas no autorizadas inyectadas a través de aplicaciones web y / o procedimientos almacenados.

Auditoría débil

En los últimos años, las redes empresariales han evolucionado considerablemente. Todo, desde el computo móvil hasta la nube, todos los sistemas están haciendo que las redes actuales sean más complejas que nunca, incluso las mismas herramientas que son utilizadas para administrar la seguridad de red pueden expandir el ataque y crear vulnerabilidades.

Las políticas débiles de auditoría de base de datos representan riesgos en términos de cumplimiento, la disuasión, detección, análisis forense y recuperación

Auditoría débil

Por desgracia, el sistema de gestión de base de datos nativa (DBMS) audita las capacidades que dan lugar a una degradación del rendimiento inaceptable y son vulnerables a los ataques relacionados con el privilegio– es decir, los desarrolladores o administradores de bases (DBA) puede desactivar la auditoría de base de datos.

La mayoría de las soluciones de auditoría de base de datos también carecen del detalle necesario. Por ejemplo, los productos DBMS rara vez se registran qué aplicación se utiliza para acceder a la base de datos, las direcciones IP de origen y falló de consultas.

Auditoría débil

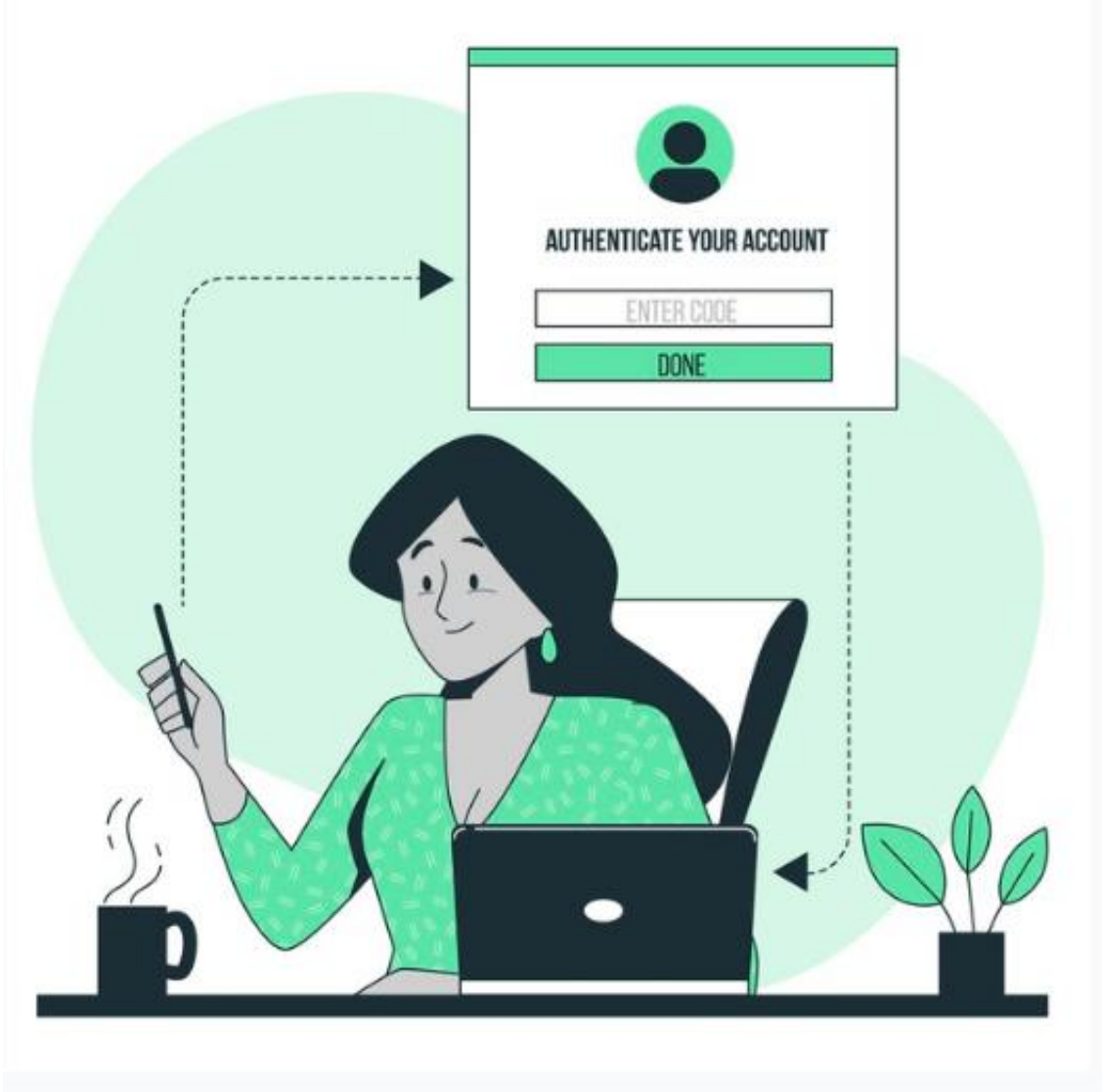
Las soluciones de auditoría de base de datos basados en la red son una buena opción. Tales soluciones de auditoría de base de datos no deben tener ningún impacto en el rendimiento de base de datos, operan de forma independiente de todos los usuarios y ofrecen la recopilación de datos a detalle.

Denegación de servicio

Recomendaciones sobre las bases de datos incluyen el despliegue de un IPS y controles de la velocidad de conexión. Al abrir rápidamente un gran número de conexiones, los controles de velocidad de conexión pueden impedir que los usuarios individuales usan los recursos del servidor de base de datos.

Las contraseñas deben cumplir:

Por qué las contraseñas deben ser secretas



Aunque parezca una perogrullada, la primera recomendación para que nuestra contraseña sea segura es mantenerla en secreto. Una clave compartida por dos o más personas no es segura.

Es muy importante transmitir esta recomendación especialmente a los menores, acostumbrados a compartir las claves con amigos o parejas. Si esa relación se rompe o se produce una enemistad, la otra persona tendrá acceso a toda su información.

Cómo crear contraseñas robustas

Debemos asegurarnos que la contraseña tenga una:

- longitud mínima de ocho caracteres,
- que combine mayúsculas,
- minúsculas,
- números y
- **símbolos**.

No debemos utilizar como claves:

- palabras sencillas en cualquier idioma,
- nombres propios,
- lugares,
- combinaciones excesivamente cortas,
- fechas de nacimiento,
- etc.

Concatenacion

- Tampoco debemos usar claves formadas únicamente a partir de la concatenación de varios elementos. Por ejemplo: “Juan1985” (nombre + fecha de nacimiento).

EJEMPLOS DE CONTRASEÑAS QUE NO DEBEMOS UTILIZAR

Cambiar contraseñas periodicamente

- Uno de los problemas de utilizar claves demasiado simples es que existen programas diseñados para probar millones de contraseñas por minuto.
- La tabla siguiente muestra el tiempo que tarda un programa de este tipo en averiguar una contraseña en función de su longitud y los caracteres que utilicemos

Longitud	Todos los caracteres	Sólo minúsculas
3 caracteres	0,86 segundos	0,02 segundos
4 caracteres	1,36 minutos	0,46 segundos
5 caracteres	2,15 horas	11,9 segundos
6 caracteres	8,51 días	5,15 minutos
7 caracteres	2,21 años	2,23 horas
8 caracteres	2,10 siglos	2,42 días
9 caracteres	20 milenios	2,07 meses
10 caracteres	1.899 milenios	4,48 años
11 caracteres	180.365 milenios	1,16 siglos
12 caracteres	17.184.705 milenios	3,03 milenios
13 caracteres	1.627.797.068 milenios	78,7 milenios
14 caracteres	154.640.721.434 milenios	2.046 milenios

“Tempor sociis euismod quisque montes iaculis. Nisi eu arcu sagittis velit cursus, vivemos est tincidunt”

Nombre apellido
Autor de cien años de soledad

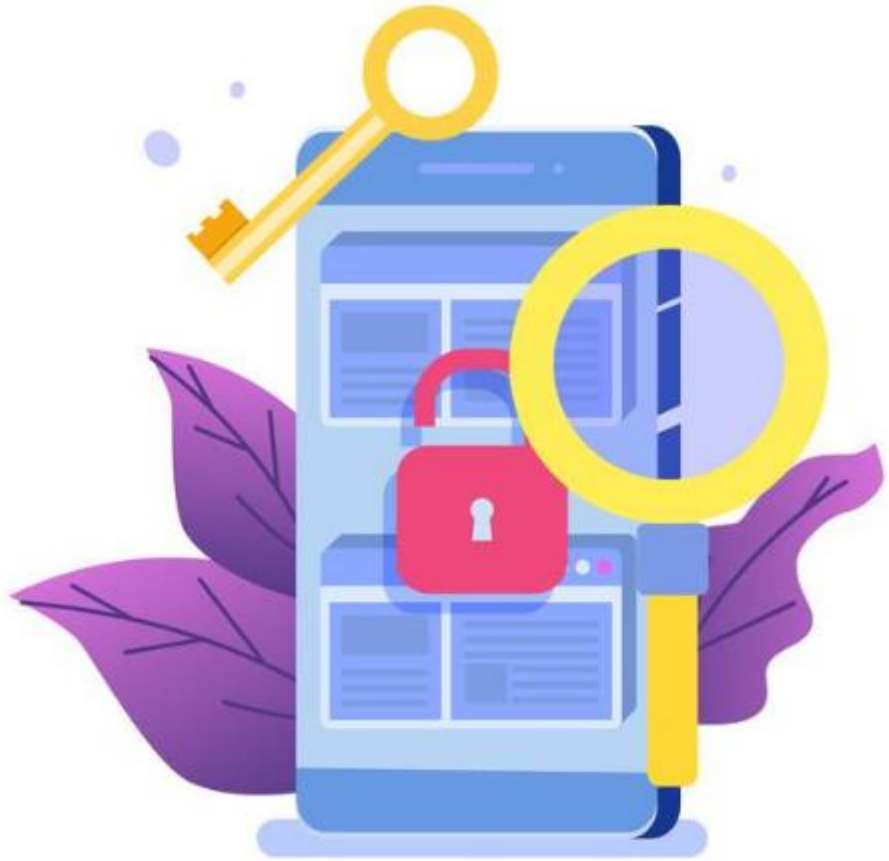
UNIVERSIDAD GERARDO BARRIOS
Líderes en Gestión del Conocimiento

Comisión de Acreditación de la Calidad de la Educación Superior
UNIVERSIDAD GERARDO BARRIOS (UGB)
ACREDITADA
2019- 2024

Vulnerabilidades en los protocolos de las Bases de Datos

Existe una constante preocupación por la seguridad de la base de datos: Muchas veces la seguridad se ve afectada por la configuración de los procesos de conexión. Las vulnerabilidades en los protocolos de bases de datos pueden permitir el acceso no autorizado a datos, la corrupción o la disponibilidad. Por ejemplo, SQL Slammer worm se aprovechó de una vulnerabilidad de protocolo de Microsoft SQL Server para ejecutar código de ataque en los servidores de base de datos destino.

Los protocolos de ataques pueden ser derrotados mediante el análisis y validación de las comunicaciones de SQL para asegurarse de que no están malformados. Pueden aprender más sobre este ataque durante cursos de seguridad suministrados por Ona Systems,



La Exposición de los datos de Backup

El robo de información y la filtración de datos confidenciales son noticias del día a día, Algunos ataques recientes de alto perfil han involucrado el robo de cintas de backup de base de datos y discos duros.

Es importante que todas las copias de seguridad deben ser cifradas. De hecho, algunos proveedores han sugerido que los futuros productos DBMS no deberían admitir la creación de copias de seguridad sin cifrar. El cifrado de base de datos en línea es un pobre sustituto de controles granulares de privilegios acuerdo a expertos de seguridad de base de datos.

Desbordamiento de búfer

Se trata de otro de los medios favoritos utilizados por los piratas y que se dan por el exceso de información que se puede llegar a enviar por medio del ingreso de información mediante el uso de formularios, es decir, se recibe mucha más información de lo que la aplicación espera.

Por poner un ejemplo, si se espera la entrada de una cuenta bancaria que puede ocupar unos 25 caracteres y se permite la entrada de muchos más caracteres desde ese campo, se podría dar este problema.

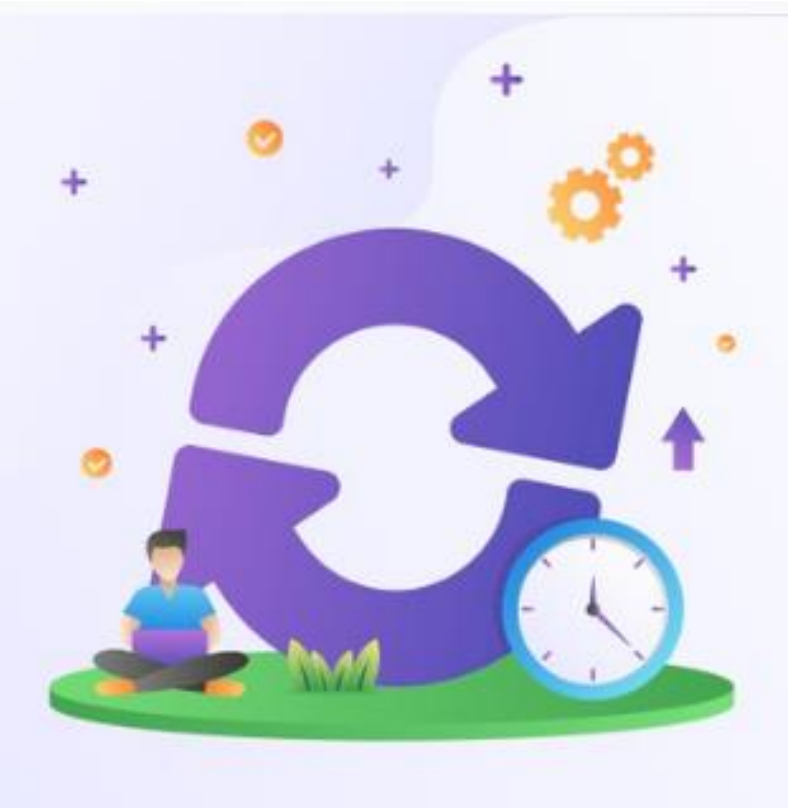
Bases de datos sin actualizar

Como ocurre con cualquier tipo de aplicación que tengamos instalada en nuestra máquina, es necesario ir actualizando la versión de nuestra base de datos con las últimas versiones lanzadas al mercado, ya que en ellas se solucionan aquellos problemas de seguridad detectados, por lo que pondremos más barreras a los posibles atacantes.

Bases de datos sin actualizar

Bases de datos sin actualizar

Para ello es muy importante estar informados de todos las noticias relacionadas con la base de datos que estemos utilizando para saber en todo momento si algo nuevo ha sido lanzado al mercado que pueda solucionar cualquier brecha de seguridad.



Datos sensibles sin cifrar

Aunque pueda ser algo obvio, a la hora de la verdad no todo el mundo cifra la información más importante que se almacena en base de datos.

Esto es una buena práctica para que en caso de hackeo, sea complicado para el atacante poder recuperar esa información. Por poner un ejemplo, las contraseñas de acceso a un sitio por parte de los usuarios podrían ser cifradas utilizando el algoritmo MD5.

De esta forma una contraseña del tipo “YUghd73j%” en base de datos se almacenaría con el siguiente valor “993e65b24451e0241617d6810849c824”. Como podéis ver, se trata de un valor que poco o nada tiene que ver con el original.

Tabla de actividades	
Nombre de la actividad	Analisis de Amenazas Amenazas, riesgos y vulnerabilidades de las bases de datos
Tipo de actividad	Microgrupos
Competencias especifica de la asignatura	Manipular bases de datos para asegurar la disponibilidad y seguridad de los datos, utilizando entornos web o locales, implementando datawarehouse y mineria de datos, trabajando de manera individual o colaborativa.
Instrucciones	1. Identifica problemas de amenazas, riesgos y vulnerabilidades de bases de datos SQL y NoSQL. 2. Investiga como solucionar y aporta nuevas ideas sobre como solucionas los problemas identificados en el punto 1. 3. Una vez realizados los puntos 1 y 2, elaborar un documento formal en donde incluya: • Portada • Introducción • Desarrollo del contenido (Problemas identificados, soluciones (de la investigacion y aportes)). • Conclusiones 4. Finalmente, un integrante del equipo Debera compartir el documento creado en el espacio de tarea en canvas
Fecha de entrega	Domingo, al final de la semana
Instrumento de evaluación	Lista de cotejo
Ponderación	50% Laboratorio I

Recursos Complementarios		
Recurso	Título	Cita Referencial
Web	Las 10 principales amenazas a la seguridad de los datos de las PyMEs	https://www.watchguard.com/docs/whitepaper/wg_top10-summary_wp_es.pdf
Web	Vulnerabilidades y amenazas de seguridad informática	https://casandrasoft.com/vulnerabilidades-y-amenazas-de-seguridad-informatica/

¿Preguntas?

¡Muchas gracias!

UNIVERSIDAD GERARDO BARRIOS
Líderes en Gestión del Conocimiento

Comisión de Acreditación de la Calidad de la Educación Superior
UNIVERSIDAD GERARDO BARRIOS (UGB)
ACREDITADA
2019- 2024