EDUCACIÓN
SECRETARÍA DE EDUCACIÓN PÚBLICA

TECNOLÓGICO NACIONAL DE MÉXICO
Instituto Tecnológico de Tlaxiaco

TECNOLÓGICO NACIONAL DE MÉXICO
INSTITUTO TECNOLÓGICO DE TLAXIACO

SEGURIDAD Y VIRTUALIZACIÓN

Práctica 3 - Bases de datos seguras

CARRERA:
INGENIERIA EN SISTEMAS COMPUTACIONALES

INTEGRANTES:
SANDRA YOLOTZIN REYES GARCÍA – 19620079
LUZ KARINA REYES LÓPEZ – 21620184
JERONIMA ROQUE CABALLERO – 21620206

DOCENTE
OSORIO SALINAS EDWARD

Tlaxiaco, Oax., OCTUBRE de 2024.

MENU

TABLA DE ILUSTRACIONES

PRACTICA

Primero instalamos MySQL, después ingresamos con nuestra contraseña que asignamos durante el proceso de instalación.

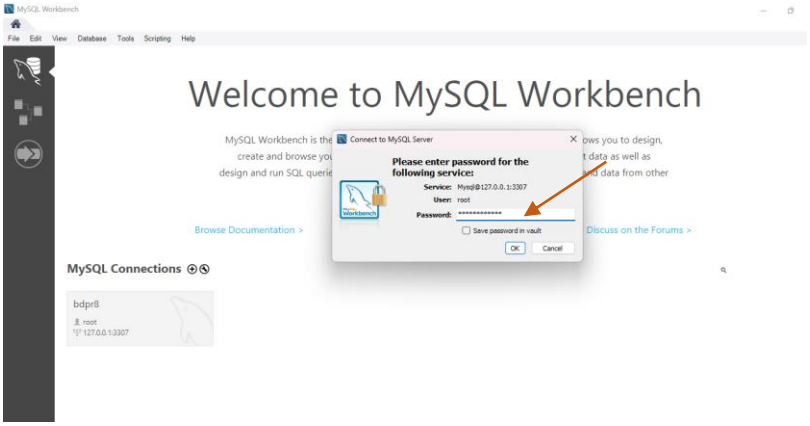

Ilustración 1

Luego en la parte de Schemas damos clic derecho y seleccionamos la opción que dice Create Schema para crear una base de datos con las siguientes tres tablas diferentes: users, address y customers.

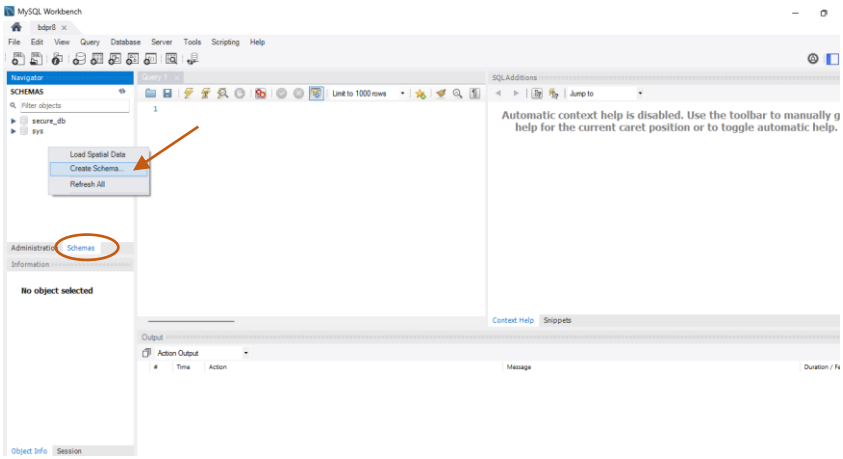

Ilustración 2

En esta parte le asignamos el nombre a la base de datos y damos clic en apply para que se cree la base de datos.

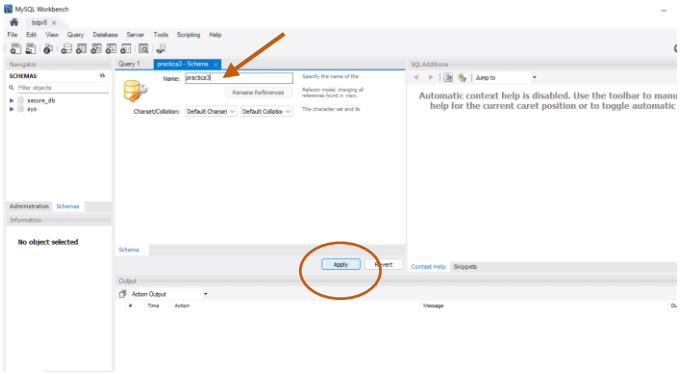

Ilustración 3

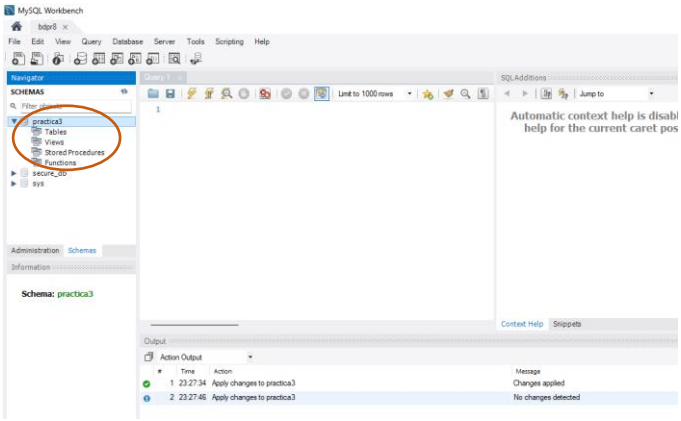

Ilustración 4

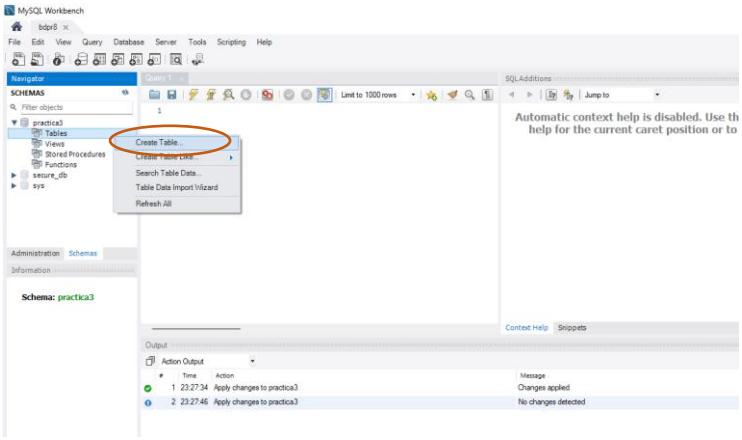

Ilustración 5

En esta parte se muestra la creación de las 3 tablas, cada una con sus columnas correspondientes.

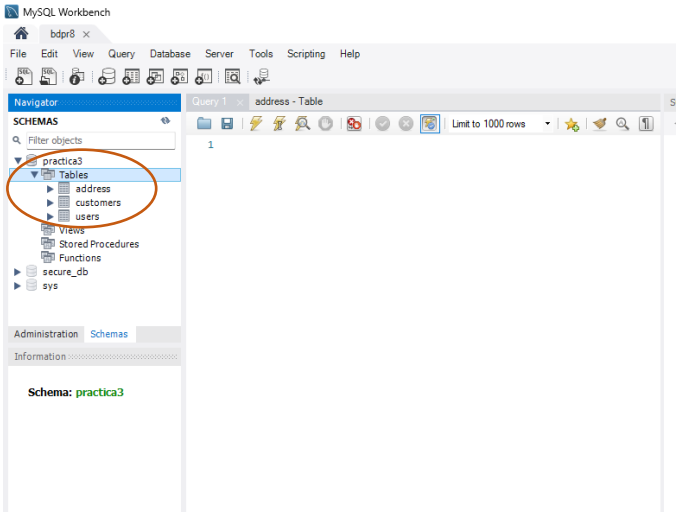

Ilustración 6

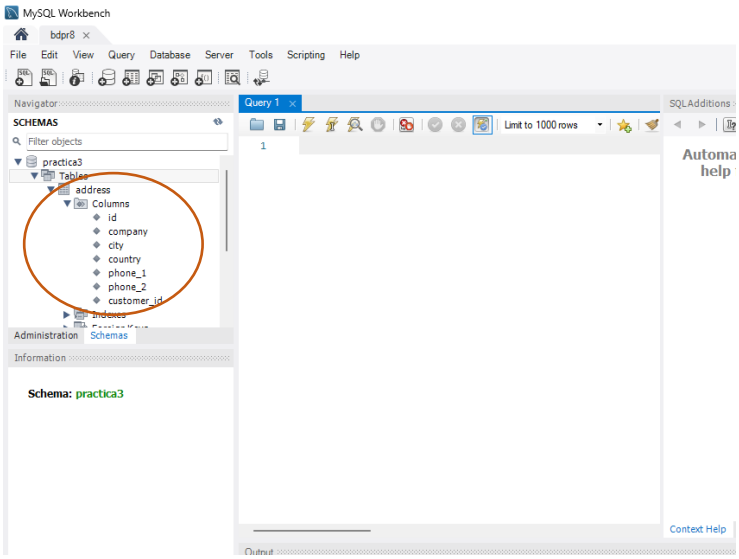

Ilustración 7

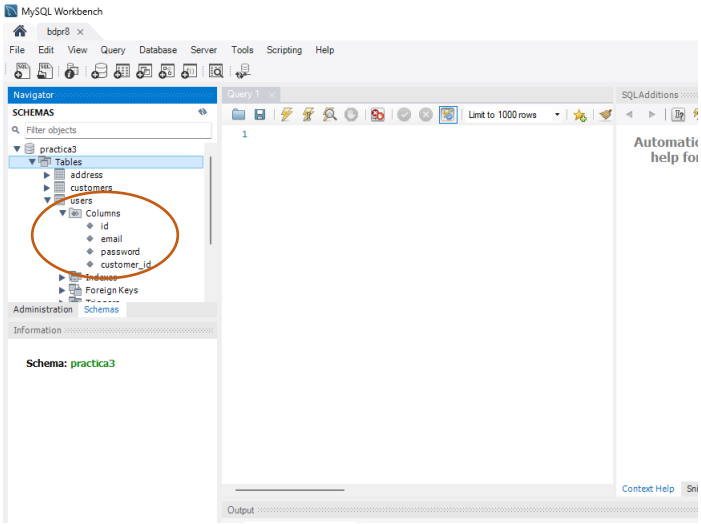

Ilustración 8

Luego creamos tres usuarios en MySQL con los siguientes permisos:

- Usuario 1: Permisos de lectura en la tabla `customers`
- Usuario 2: Permisos de lectura y escritura en la tabla `address`
- Usuario 3: Permisos de lectura, escritura y eliminación en la tabla `users`

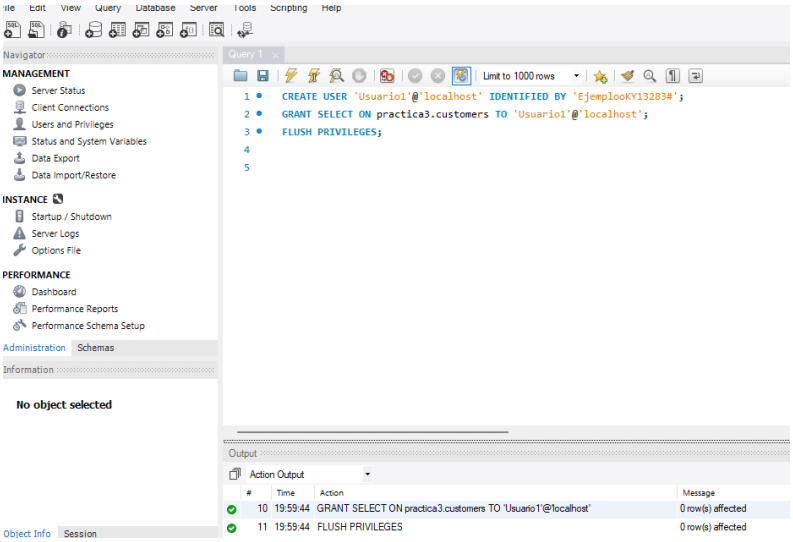

Ilustración 9

Primero hay que asignar el nombre para el usuario y una contraseña segura que desees asignar.

Con el comando concede los privilegios SELECT, que permiten al usuario leer la tabla.

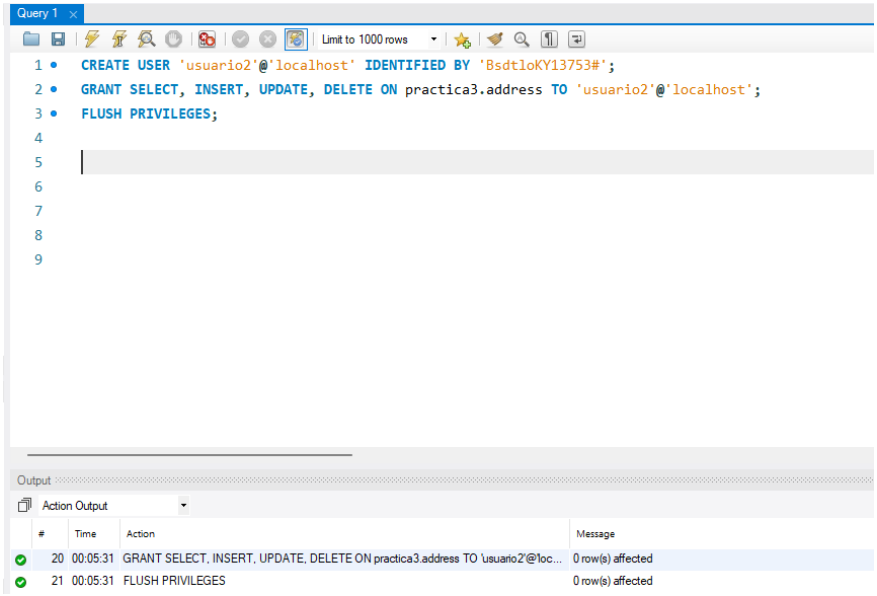

Ilustración 10

Con los comandos SELECT, INSERT, UPDATE concede los Permisos de lectura y escritura en la tabla `address`.

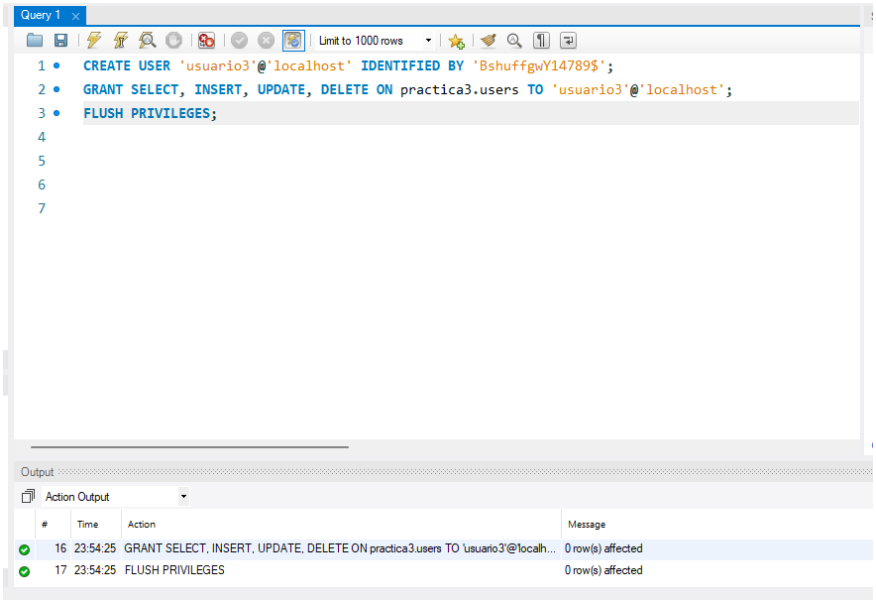

Ilustración 11

Con los comandos SELECT, INSERT, UPDATE, DELETE ON se concede los permisos de lectura, escritura y eliminación en la tabla `users`

Posteriormente creamos un backup de la base de datos `secure_db` para restaurar la base de datos en un servidor diferente.

Para crear un backup de la base de datos `secure_db` primero la seleccionamos y también seleccionamos donde queremos que se guarde.

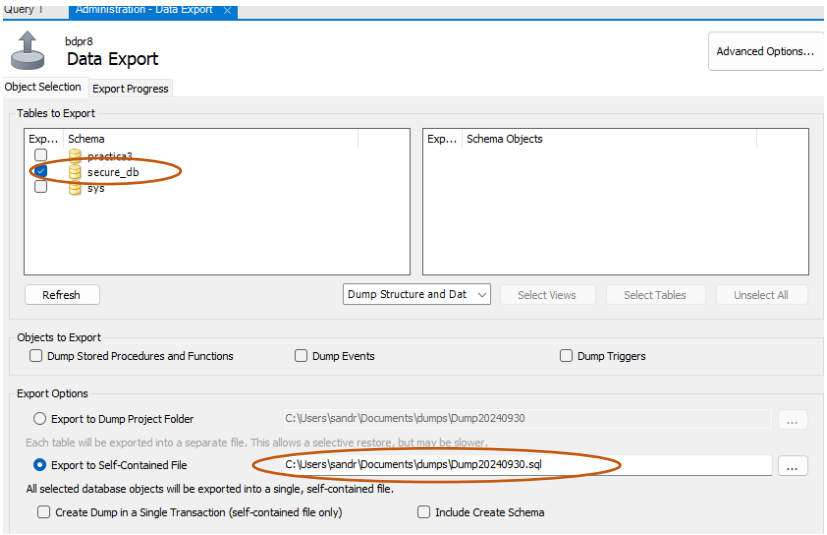

Ilustración 12

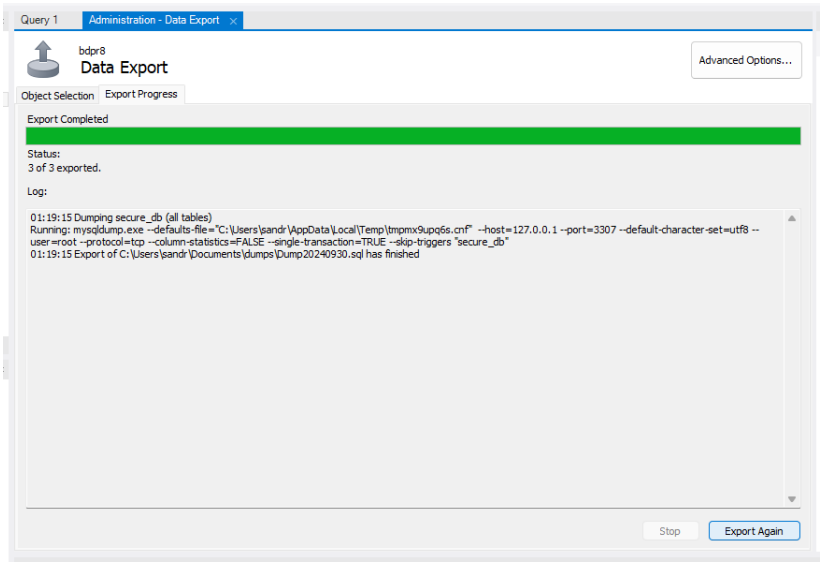

Ilustración 13

Ya que se creo exitosamente el backup, nos dirigimos a la ubicación que asignamos y se puede observar que ya se encuentra el backup.

Luego lo compartimos a otra integrante del equipo para que lo restaure en su servidor.

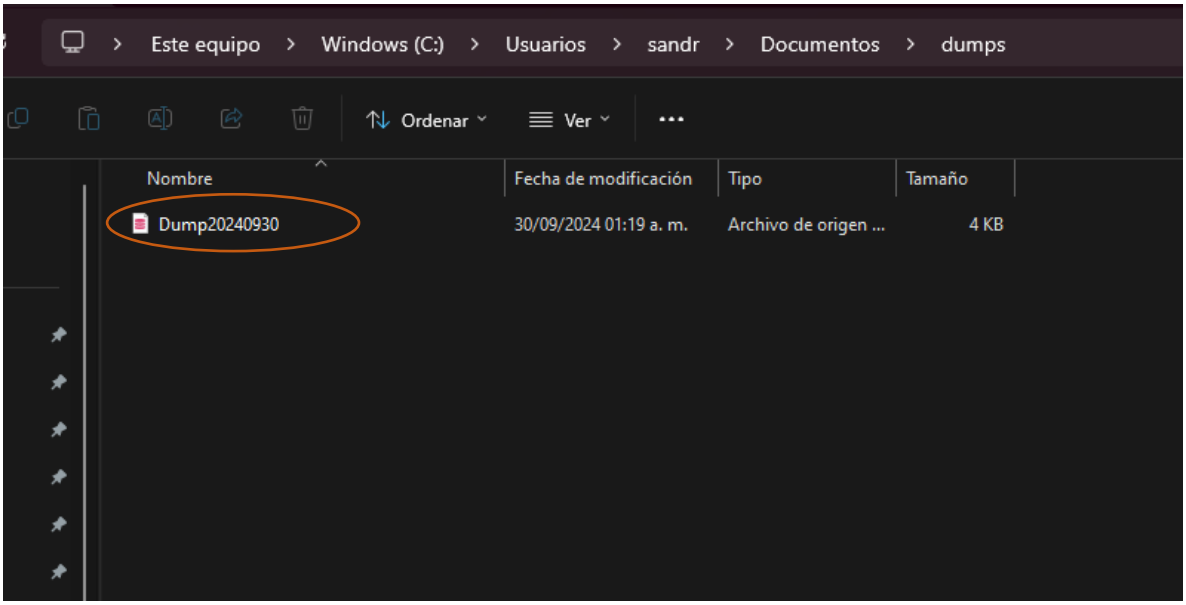

Ilustración 14

Primero se tuvo que crear una base de datos vacía para realizar el respaldo, en nuestro caso con el mismo nombre.

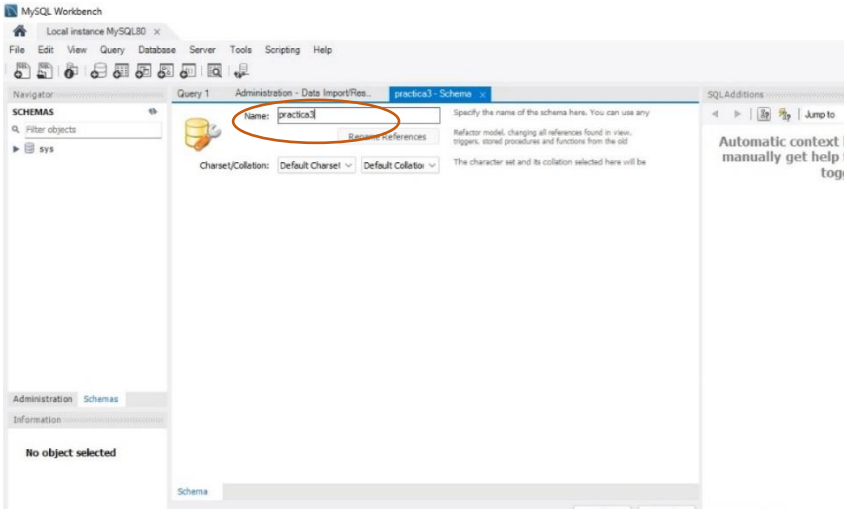

Ilustración 15

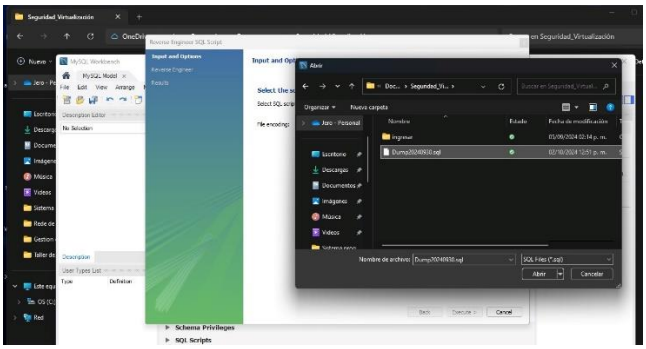

Ilustración 16

Luego importamos el archivo anterior, también seleccionamos en que base de datos queremos que se importe y seleccionamos la base de datos vacia creada que se llama practica3.

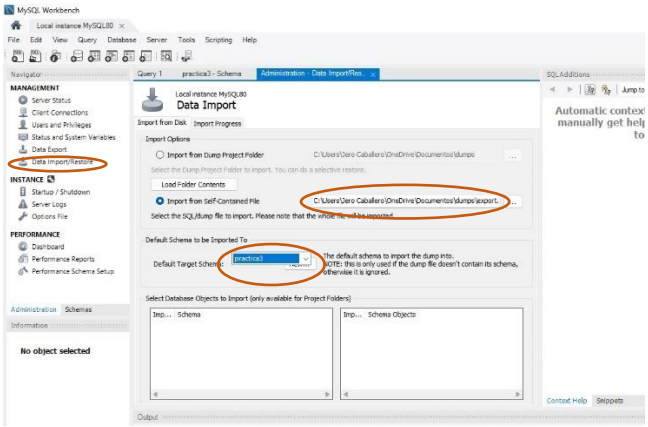

Ilustración 17

Finalmente se puede observar que se a importado y restaurado con éxito el backup a la base de datos.

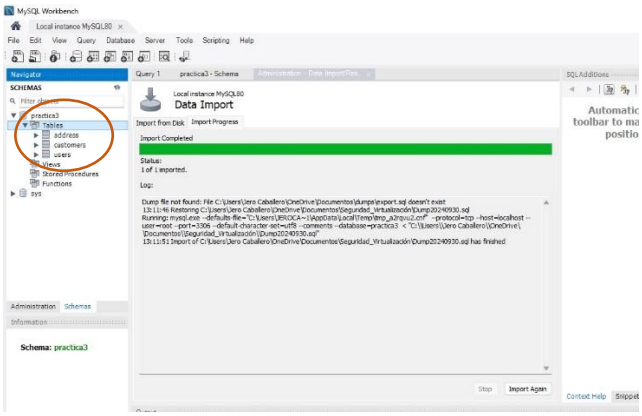

Ilustración 18

INVESTIGA Y DESCRIBE LOS CONCEPTOS DE SQL INJECTION Y CÓMO SE PUEDEN PREVENIR

¿Qué es la inyección de SQLy cómo funciona?

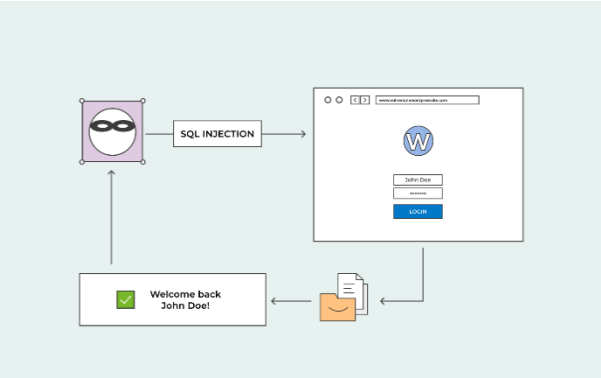

Ilustración 19

La inyección de SQL es un tipo de ciberataque encubierto en el cual un hacker inserta código propio en un sitio web con el fin de quebrantar las medidas de seguridad y acceder a datos protegidos. Una vez dentro, puede controlar la base de datos del sitio web y secuestrar la información de los usuarios.

Cómo prevenir la inyección de código SQL

Ilustración 20

Aunque la inyección de código SQL es una de las amenazas más frecuentes de API, puede evitarse eficazmente con las estrategias de prevención adecuadas. Algunos métodos útiles para evitar la inyección de código SQL incluyen restringir los procedimientos de la base de datos, sanear las entradas de la base de datos y aplicar el acceso con menos privilegios.

Restringir los procedimientos y código de la base de datos

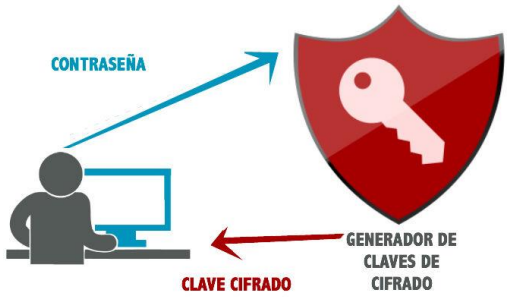

Ilustración 21

La inyección de código SQL depende en gran medida de la capacidad de un atacante para manipular las entradas de datos y funciones de la base de datos. Al restringir estas entradas y limitar el tipo de procedimientos de base de datos que se pueden realizar, las organizaciones pueden minimizar el riesgo de consultas no autorizadas o maliciosas. Las formas de hacerlo incluyen:

Aplicación de declaraciones preparadas y consultas parametrizadas: las declaraciones preparadas definen el código SQL aceptable, y luego establecen parámetros específicos para las consultas entrantes. Las declaraciones de SQL maliciosas se clasifican como entradas de datos no válidas y no como comandos ejecutables.

Utilizar procedimientos almacenados: al igual que las declaraciones preparadas, los procedimientos almacenados son declaraciones de SQL preparadas y reutilizables que pueden recuperarse de una base de datos y evitan que las partes maliciosas ejecuten código directamente en la base de datos.

¿Qué efecto tienen los ataques de inyección de SQL?

Los hackers recurren a los ataques de inyección de SQL con el fin de introducirse en la base de datos de un sitio web. A veces solo quieren eliminar datos para provocar el caos y, en otras ocasiones, lo que buscan es editar la base de datos, especialmente en el caso de sitios web financieros. En el momento en que el hacker ha logrado el control de la base de datos, ya es fácil interferir en los saldos de las cuentas de los clientes y mandarse dinero a su propia cuenta.

INVESTIGA Y DESCRIBE LOS CONCEPTOS DE BASES DE DATOS SEGURAS Y CÓMO SE PUEDEN IMPLEMENTAR.

¿Qué es la seguridad de las bases de datos?

Ilustración 22

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

La seguridad de las bases de datos es una iniciativa compleja que implica todos los aspectos de las tecnologías y las prácticas de seguridad de la información. Además, se enfrenta a la usabilidad de la base de datos. Cuanto más accesible y utilizable sea la base de datos, más vulnerable será ante las amenazas de seguridad; cuanto más protegida esté la base de datos ante las amenazas, más difícil será acceder a ella y utilizarla. En ocasiones, esta paradoja se denomina regla de Anderson (enlace externo a IBM).

¿Por qué es importante?

Ilustración 23

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:

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.

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.

AMENAZAS Y DIFICULTADES HABITUALES

Ilustración 24

Son muchas las configuraciones erróneas de software, vulnerabilidades o patrones de descuido o mal uso que pueden dar lugar a una infracción. Los siguientes son los tipos o causas más habituales de los ataques de seguridad de base de datos y sus causas.

Amenazas internas

Las amenazas internas son amenazas de seguridad de una de las tres fuentes que tienen acceso con privilegios a la base de datos:

Un usuario interno malicioso que tiene la intención de hacer daño.

Un usuario interno negligente que comete errores que provocan que la base de datos sea vulnerable a los ataques.

Un infiltrado un usuario externo que, de alguna manera, obtiene las credenciales a través de una estrategia de phishing u obtiene acceso a la propia base de datos de credenciales.

CONCLUSIÓN

Garantizar la seguridad de las bases de datos es crucial para proteger la información sensible de una organización. Las bases de datos seguras deben implementar mecanismos que aseguren la confidencialidad, integridad y disponibilidad de los datos, mediante técnicas como el cifrado, control de accesos, auditorías y políticas de privilegios mínimos. Además, se debe mantener una gestión proactiva de actualizaciones y parches para mitigar vulnerabilidades conocidas.

Un aspecto fundamental es la prevención de SQL Injection, uno de los ataques más comunes que explota consultas SQL mal construidas. Para prevenir estos ataques, se recomienda el uso de consultas preparadas, la validación y saneamiento de entradas, y la limitación de permisos en la base de datos. Estas prácticas no solo protegen los sistemas, sino que también refuerzan la confiabilidad y disponibilidad de los servicios.

REFERENCIAS

https://www.avast.com/es-es/c-sql-injection#:~:text=La%20inyecci%C3%B3n%20de%20SQL%20es,la%20informaci%C3%B3n%20de%20los%20usuarios.

https://www.ibm.com/es-es/topics/database-security#:~:text=%C2%BFQu%C3%A9%20es%20la%20seguridad%20de,de%20las%20bases%20de%20datos.

https://www.one.com/es/seguridad-de-su-web/que-es-sql-injection#:~:text=SQL%20injection%20es%20un%20tipo,que%20la%20expone%20a%20ataques.