**Práctica Inyección SQL**

****

**Qué es**

**Definición:**

*Sql Injection ó Inyección SQL es una vulnerabilidad que permite al atacante enviar o “inyectar” instrucciones SQL de forma maliciosa y malintencionada dentro del código SQL programado para la manipulación de bases de datos, de esta forma todos los datos almacenados estarían en peligro. La finalidad de este ataque es poder modificar del comportamiento de nuestras consultas a través de parámetros no deseados, pudiendo así falsificar identidades, obtener y divulgar información de la base de datos (contraseñas, correos, información relevante, entre otros), borrar la base de datos, cambiar el nombre a las tablas, anular transacciones, el atacante puede convertirse en administrador de la misma.*

*Esto ocurre normalmente a la mala filtración de las variables en un programa que tiene o crea SQL, generalmente cuando solicitas a un usuario entradas de cualquier tipo y no se encuentran validadas, como por ejemplo su nombre y contraseña, pero a cambio de esta información el atacante envía una sentencia SQL invasora que se ejecutará en la base de datos.*

(Fuente: OpenWebinars, https://openwebinars.net/blog/que-es-sql-injection/)

**Qué se necesita**

**Víctima:**

\* Máquina virtual con Windows o Linux (Ip estática)

\* Servidor WEB con PHP y MySQL

**Cómo es el proceso (Trabajo)**

- Instalar 1 máquina en VirtualBox en red "Puente"

- Instalar un servidor WEB con PHP y MySQL en Windows (WAMP) o Linux (LAMP) - (Opcional) en Linux instalar el paquete PHPMyAdmin para gestionar el acceso a la Base de Datos - Crear una Base de Datos con una tabla de Usuarios (Nombre y Contraseña)

- Crear 2 páginas en el servidor WEB

\* Página inicial (index.htm) con un formulario que pida Nombre y Contraseña y los envíe al servidor.

\* Página en PHP (login.php) que conecte con la base de datos y realice una consulta para comprobar y mostrar si se permite el acceso según los datos enviados.

- Atacar el servidor insertando en el campo Contraseña códigos de inyección SQL \* Ej. ' or '1=1

**Ayuda**

**Páginas:**

\* index.htm

<form action="login.php" method="post">

Nombre: <input type="text" name="nombre"> <br>

Clave: <input type="password" name="clave"> <br>

<input type="submit" value="Login">

</form>

\* login.php

<?php

$nombre=$\_POST['nombre'];

$clave=$\_POST['clave'];

$conexion=mysqli\_connect('localhost','root');

mysqli\_select\_db($conexion,"usuarios");

$cadenaSQL="SELECT \* FROM usuarios WHERE nombre='$nombre' AND contrasena='$clave'";

$fila=mysqli\_query($conexion,$cadenaSQL);

if(mysqli\_num\_rows($fila)!=0)

{

echo("<html><body>Acceso Concedido</body></html>");

}

else

{

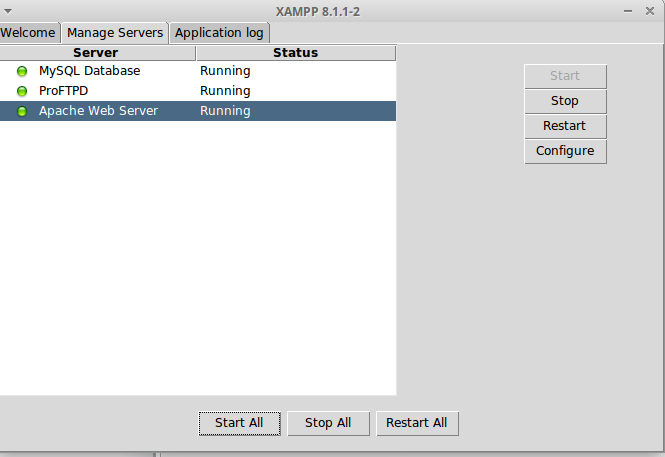
echo("<html><body>Acceso Denegado</body></html>");

}

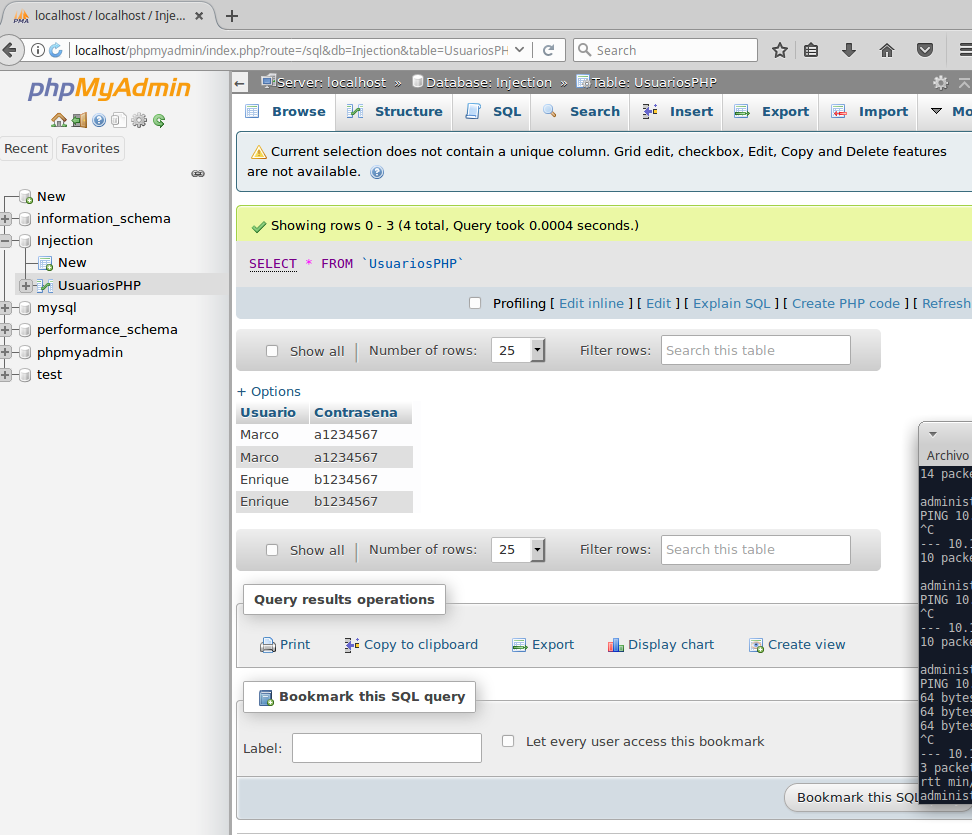
mysqli\_close($conexion);

?>

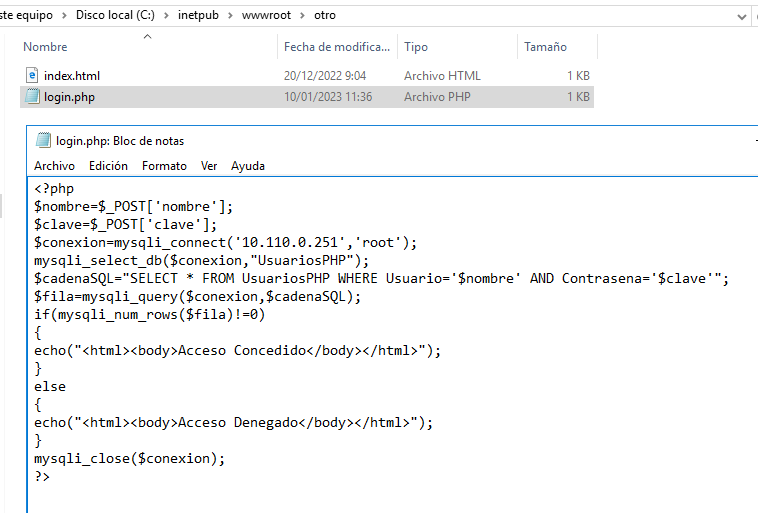
**Iniciamos XAMPP e iniciamos MySQL Server**

****

**Creamos la Base de Datos Injection**

****

**Modificamos el fichero con los datos solicitados**

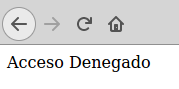
****

****



Iniciamos sesión con alguno de los usuarios de la Bases de Batos y probamos que no deja otro

****

****

A la hora de introducir ciertas expresiones,accedemos a la bases de datos. Esto es Injection