**Taller de Inyección SQL**

Actividades a desarrollar:

* Crear una aplicación web en PHP y PostgreSQL con un módulo de inicio de sesión y un módulo de consulta de productos.
* Aplicar los métodos básicos de inyección SQL para sobrepasar el inicio de sesión, recuperar la estructura de la base de datos y obtener datos de las tablas.

**Configurando el entorno**

Primero verificamos que tenemos instalada la última versión de php(7.2) con el comando *php -v*



En caso de no tener la última versión, actualizar con el comando *apt install php7-\**



Iniciar Apache 2



Iniciar PostgreSQL



Crear un archivo *info.php*, y guardarlo en la ruta /var/www/html con el siguiente código



Abrir el navegador e ingresar a *localhost/info.php,* y luego verificar la versión de PHP



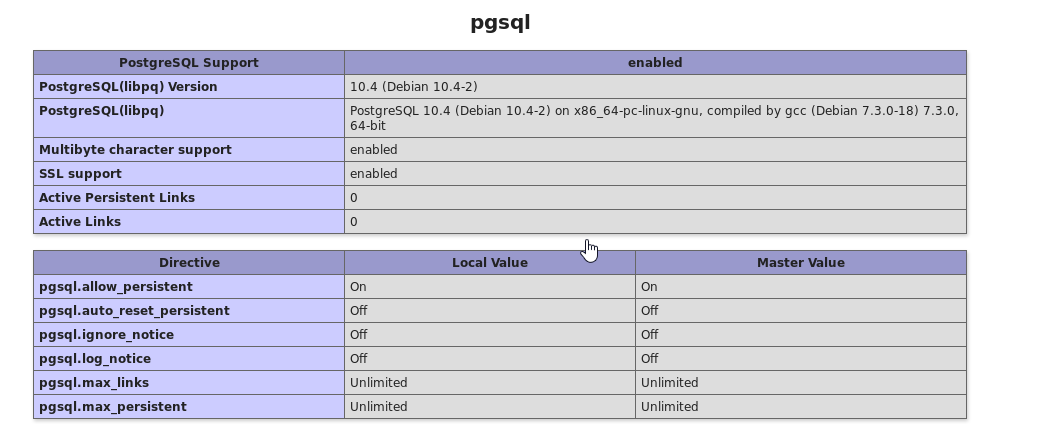
En caso de no tener la última versión activada, en una terminal encribir *a2dismod php5 (o la versión actual),* y luego *a2enmod php7.2*



Y luego reiniciar apache 2

**

Nuevamente en la información de PHP verificar que el módulo psql está activo



En caso de no tenerla, instalar la extensión de PostgreSQL para PHP con el comando *apt install php7.2-psql* o bien,  *apt install php-psql*



Y luego reiniciar apache2.

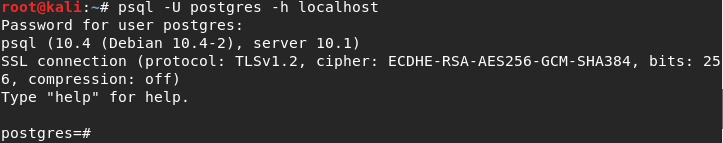
**Configurando la base de datos**

Vamos a crear una base de datos con las siguientes tablas:

|  |  |  |  |
| --- | --- | --- | --- |
| Id | Nombre | Contraseña | Descripcion |
| 1 | admin | passadmin | Administrador |
| 2 | usuario1 | password1 | Primer Usuario |
| 3 | usuario2 | password2 | Segundo Usuario |
| 4 | leet | P@55w0rd | Amigo Friki |

|  |  |  |  |
| --- | --- | --- | --- |
| Id | Referencia | Nombre | Precio |
| 1 | AAA | tornillo | 1 |
| 2 | BBB | tuerca | 2 |
| 3 | CCC | bombilla | 4 |
| 4 | DDD | arandela | 3 |
| 5 | EEE | destornillador | 10 |

Iniciamos el cliente PostgreSQL



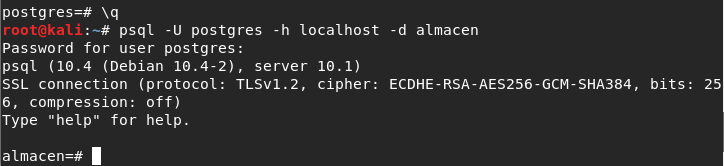
Cambiamos la contraseña al usuario postgres



Creamos la base de datos *almacen*.



Salimos del cliente con el comando *\q* y entramos a la nueva base de datos



Creamos la tabla *usuarios*



Creamos la tabla *productos*



Insertamos los datos en la tabla usuarios









Insertamos los datos en la tabla productos





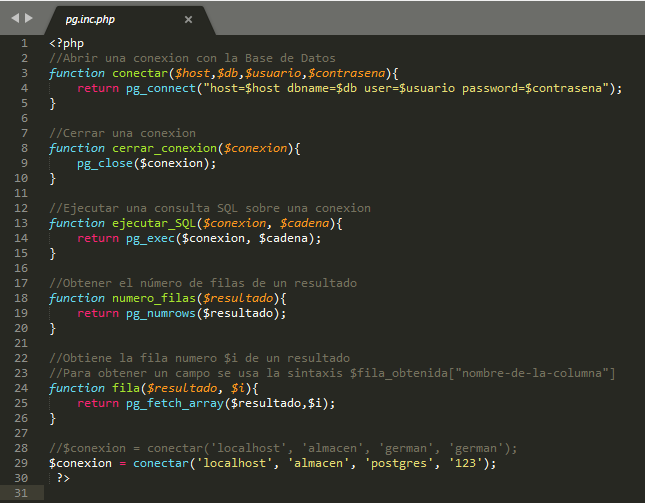




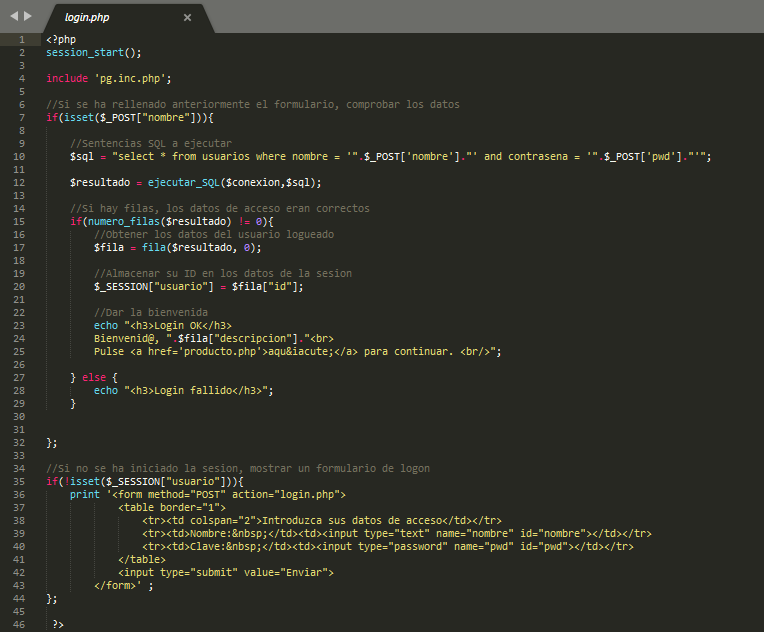


**Despliegue de la aplicación**

Primero creamos una nueva carpeta llamada Inyeccion\_SQL en la ruta /var/www/html, y dentro de esta carpeta creamos el archivo *pg.inc.php* con el siguiente código:



Ahora creamos el archivo *login.php* con el siguiente código:



Probamos la aplicación en nuestro navegador

