Práctica 2.1: Ataque en Login

<Incluye en un documento Word capturas de pantalla de todo el proceso>

1) Realiza una inyección SQL sobre tu aplicación Login.

2) Modifica el código para evitar una posible inyección SQL en la aplicación:

Debes cambiar la forma en que se realiza la consulta a la base de datos y en su lugar usar una sentencia preparada. Para ello usa las funciones:

- mysqli_prepare: crea una sentencia preparada.
- mysqli_stmt_bind_param: liga los parámetros a la sentencia.
- mysqli_stmt_execute: ejecuta la sentencia.
- mysqli_stmt_store_result: guarda el resultado de la consulta.
- mysqli_stmt_num_rows: devuelve el número de filas de resultado.

Ayuda:

https://www.php.net/manual/es/mysqli.prepare.php

https://www.php.net/manual/es/mysqli-stmt.num-rows.php

Por último, no olvides comprobar que la inyección SQL ya no es posible en tu aplicación.