TAREA 4

Esta tarea debe entregarse mediante la plataforma virtual del curso (Metics) a más tardar el **lunes 25 de julio a las 8 p.m.**. La tarea debe realizarse en los equipos del proyecto, de manera que se realice una sola entrega por equipo.

Cada miembro del equipo debe:

1. Estudiar esta presentación sobre SQL Injection:
   https://drive.google.com/file/d/1cti5SXyCwZ22t1wb2r_YVpysRFhGzM5i/view?usp=sharing
2. Realizar este tutorial sobre SQL Injection:
   https://www.hacksplaining.com/exercises/sql-injection#/
3. Revisar este material:
   https://www.aspneto.com/sql-injections-what-is-sql-injection-and-how-to-prevent-it.html

   https://developsecure.com/2016/03/12/sql-injection-use-parameterisation/

   https://dotnetcoretutorials.com/2017/10/11/owasp-top-10-asp-net-core-sql-injection/

Una vez estudiado el material, los miembros del equipo deben trabajar lo siguiente:

1. Seleccionar al menos dos entradas de datos de su proyecto para blindar contra inyecciones SQL (sanear los datos). Recuerden que la seguridad debe estar presente en todas las capas de la aplicación, no solo la interfaz de usuario, por lo que deben asegurar que la sanidad de los datos hasta que llegan a la BD.
2. Para las entradas seleccionadas, indicar a cuál historia de usuario pertenecen, y completar estas historias con las tareas técnicas asociadas a la implementación del blindaje.
3. Implementar los controles necesarios (tareas técnicas) para validar y blindar las entradas seleccionadas.
4. Realizar pruebas para comprobar que las entradas no permitan inyección SQL ni entradas de datos inválidas.
5. Elaborar un reporte donde expliquen y muestren evidencia de cómo abordaron los puntos anteriores.