Cristina Margaret Calvario Serrano

Módulo 9. Seguridad en el desarrollo con IA.

Caso práctico 9. Realizar un escaneo y análisis de vulnerabilidades del proyecto

Permite gestionar productos (guardarlos y visualizarlos), integrando **machine learning (ML)** para detectar contenido sospechoso y **SQLite** para almacenamiento persistente.

Librerías usadas, figura 1:

* kivy: Para la interfaz gráfica (ventanas, botones, campos de texto).
* sqlite3: Para la base de datos local.
* pandas: Para mostrar datos en formato de tabla en la consola.
* sklearn: Para el modelo de ML que detecta contenido sospechoso.

Escala de tiempo

El contenido generado por IA puede ser incorrecto.

Figura 1. Librerias

Machine Learning (Detección de contenido sospechoso), véase figura 2.

* Datos de entrenamiento:
  + ejemplos\_logs: Lista de mensajes de ejemplo (como "Intrusion from unknown IP").
  + etiquetas: 1 (sospechoso) o 0 (normal).
* Modelo:
* Usa TfidfVectorizer para convertir texto en vectores numéricos.
* Entrena un LogisticRegression para clasificar si un texto es sospechoso o no.
* Uso en la app:
  + Cuando el usuario guarda un producto, el modelo analiza el nombre y descripción. Si predice 1, bloquea el guardado.

Texto

El contenido generado por IA puede ser incorrecto.

Figura 2. Detección de contenido sospechoso

Base de Datos (SQLite), véase figura3.

* Tabla productos:
  + Campos: id, nombre, descripcion, precio.
* Funciones clave:
  + init\_db(): Crea la tabla si no existe.
  + obtener\_productos(): Devuelve todos los productos registrados.

Texto

El contenido generado por IA puede ser incorrecto.

Figura 3. Base de datos

Interfaz Gráfica (Kivy)

* Clase ProductPanel:
  + Contiene campos para ingresar nombre, descripción y precio.

Texto

El contenido generado por IA puede ser incorrecto.

* + Botones:
    - Guardar Producto: Valida los datos, aplica el modelo ML y guarda en SQLite.

Interfaz de usuario gráfica, Texto

El contenido generado por IA puede ser incorrecto.

* + - Ver Productos: Muestra los productos en la consola usando pandas.

Pantalla de computadora con letras

El contenido generado por IA puede ser incorrecto.

* + Validaciones:
    - Nombre solo permite caracteres alfanuméricos y signos de puntuación comunes.
    - Precio debe ser un número positivo.

Texto

El contenido generado por IA puede ser incorrecto.

* Clase ProductApp:
  + Inicia la aplicación y carga ProductPanel.

Imagen que contiene nombre de la empresa

El contenido generado por IA puede ser incorrecto.

Flujo de la Aplicación

1. Al iniciar:
   * Se crea la base de datos (si no existe).
   * Se entrena el modelo de ML con los datos simulados.
2. Al guardar un producto:
   * Valida el formato del nombre y precio.

Una captura de pantalla de una red social

El contenido generado por IA puede ser incorrecto.

Interfaz de usuario gráfica, Texto

El contenido generado por IA puede ser incorrecto.

* + Usa el modelo para detectar si el texto es sospechoso.

Interfaz de usuario gráfica, Aplicación

El contenido generado por IA puede ser incorrecto.

* + Si pasa las validaciones, guarda en SQLite.

Interfaz de usuario gráfica

El contenido generado por IA puede ser incorrecto.

1. Al ver productos:
   * Recupera los datos de SQLite y los muestra en la consola con pandas.

Una captura de pantalla de un celular

El contenido generado por IA puede ser incorrecto.