### **DevSkim: Seguridad en Código en Tiempo Real**

**DevSkim** es una herramienta de análisis de seguridad en el código fuente desarrollada por Microsoft. Está diseñada para ayudar a los desarrolladores a detectar y corregir problemas de seguridad en tiempo real dentro de su entorno de desarrollo.

## **1. Concepto de DevSkim**

* Es una herramienta de análisis estático de código fuente centrada en la seguridad.
* Proporciona reglas predefinidas para detectar vulnerabilidades comunes (como inyecciones SQL, manejo inseguro de datos, etc.).
* Se integra con editores de código como **Visual Studio Code, Visual Studio y JetBrains**.
* Funciona en **Windows, Linux y macOS**.

## **2. Tutorial Básico: Instalación y Uso**

### **2.1 Instalación en VS Code**

1. Abre **Visual Studio Code**.
2. Ve a la pestaña **Extensiones** (Ctrl+Shift+X).
3. Busca "**DevSkim**" y haz clic en **Instalar**.
4. Una vez instalado, DevSkim comenzará a analizar tu código automáticamente.

### **2.2 Instalación con CLI (Command Line Interface)**

Si quieres usar DevSkim en la línea de comandos:

Instala DevSkim desde su repositorio en GitHub:

git clone https://github.com/microsoft/devskim.git

cd devskim

dotnet build

Ejecuta el escaneo de seguridad en un archivo: dotnet run -- analyze --source archivo.js

## **3. Configuración de DevSkim**

### **3.1 Configuración con Archivo JSON**

Puedes personalizar DevSkim usando un archivo de configuración en formato JSON, llamado devskim.rules.json.

Ejemplo de un archivo de reglas personalizadas:

{

"rules": [

{

"id": "DS100001",

"name": "Uso inseguro de eval() en JavaScript",

"severity": "high",

"patterns": [

{

"pattern": "eval\\(.\*\\)",

"type": "regex"

}

],

"fixes": [

{

"description": "Evita el uso de eval(). Usa JSON.parse() o funciones seguras en su lugar."

}

]

}

]

}

Puedes colocar este archivo en tu directorio de trabajo o en la configuración de DevSkim para que se aplique automáticamente.

## **4. Ejemplo de Uso en Código**

### **Ejemplo de Código con Advertencia de DevSkim**

Si DevSkim detecta una vulnerabilidad, mostrará advertencias en el editor.

Ejemplo en **JavaScript**:

// 🚨 DevSkim detectará esto como inseguro

let userInput = "alert('Hackeado')";

eval(userInput); // ⚠️ No se recomienda el uso de eval()

DevSkim te sugerirá reemplazar eval() con una alternativa más segura, como JSON.parse().

### **Conclusión**

DevSkim es una excelente herramienta para ayudar a los desarrolladores a mantener buenas prácticas de seguridad en su código. Se integra fácilmente con editores y puede configurarse con reglas personalizadas para adaptarse a diferentes entornos de desarrollo.

### **¿Necesitas ayuda con una configuración específica? 😊**