REPORTE DE VULNERABILIDADES SQLi

Resumen del análisis

archivos analizados: 4

lineas afectadas: 4

tiempo de analisis: 0.09

Archivo: src/com/miapp/datos/UsuarioDAO.java

Linea: 11

```
// Forma segura (sin vulnerabilidad):
    String query = "SELECT * FROM usuarios WHERE id = ?";
    PreparedStatement ps = conn.prepareStatement(query);
```

Detalles:

- [CRITICO] SQLi por uso de parametro no validado: Se usa la variable 'id' directamente en una sentencia SQL en la capa 'DATOS'. Esto puede permitir inyeccion SQL si no se valida correctamente.

Linea: 19

```
// Mala practica incluso en la capa DAO:
    String query = "SELECT * FROM usuarios WHERE id = " + id;
    conn.createStatement().executeQuery(query);
```

Detalles:

- [CRITICO] SQLi por uso de parametro no validado: Se usa la variable 'id' directamente en una sentencia SQL en la capa 'DATOS'. Esto puede permitir inyeccion SQL si no se valida correctamente.

Archivo: src/com/miapp/logica/UsuarioService.java

Linea: 7

```
// Este metodo deberia validar la entrada antes de usarla
    return "SELECT * FROM usuarios WHERE id = " + id;
}
```

Detalles:

- [CRITICO] SQLi por uso de parametro no validado: Se usa la variable 'id' directamente en una sentencia SQL en la capa 'LOGICA'. Esto puede permitir inyeccion SQL si no se valida correctamente.
- [CRITICO] SQLi por concatenacion: La variable 'id' contaminada se concatena en una sentencia SQL en la capa 'LOGICA'. Esto puede permitir inyeccion SQL.

Archivo: src/com/miapp/presentacion/UsuarioController.java

Linea: 12

```
try {
        Statement stmt = conn.createStatement(); // Mala practica fuera de DAO
```

Detalles:

- [CRITICO] SQLi por uso de parametro no validado: Se usa la variable 'conn' directamente en una sentencia SQL en la capa 'PRESENTACION'. Esto puede permitir inyeccion SQL si no se valida correctamente.

- [CRITICO] SQLi por concatenacion: La variable 'conn' contaminada se concatena en una sentencia SQL en la capa 'PRESENTACION'. Esto puede permitir inyeccion SQL.

- [CRITICO] Violacion de arquitectura N-capas: En la capa 'PRESENTACION' no esta permitido ejecutar sentencias SQL directamente. Las operaciones SQL deben realizarse solo en la capa de datos.