Investigación sobre ataques a las API SOAP

1. Ataque de Inyección SQL

Definición: Inserción de código SQL malicioso a través de parámetros de entrada.

Afectación:

Posible en consultas directas a la base de datos en AppDbContext

Podría permitir robo, modificación o eliminación de datos

Solución:

Usar Entity Framework Core con consultas parametrizadas

Implementar el patrón Repository

Validar y sanear todas las entradas de usuario

2. Ataque de Fuerza Bruta

Definición: Intentos repetitivos de autenticación con diferentes credenciales.

Afectación:

LoginController podría ser vulnerable a múltiples intentos de inicio de sesión

Podría permitir el acceso no autorizado

Solución:

Implementar bloqueo de cuentas después de varios intentos fallidos

Agregar CAPTCHA

Usar autenticación de múltiples factores (MFA)

3. Ataque de Manipulación de Tokens JWT

Definición: Modificación o falsificación de tokens JWT.

Afectación:

El controlador de login genera tokens JWT

Tokens podrían ser robados o manipulados

Solución:

Usar HTTPS en todas las comunicaciones

Implementar renovación de tokens de refresco

Firmar tokens con algoritmos seguros (como RS256)

Establecer tiempos de expiración cortos

4. Ataque de Denegación de Servicio (DoS)

Definición: Sobrecarga del sistema con solicitudes masivas.

Afectación:

Podría afectar el rendimiento del servicio

Consumo excesivo de recursos

Solución:

Implementar limitación de tasa (Rate Limiting)

Usar MetricasMiddleware para monitoreo

Configurar balanceo de carga

5. Exposición de Datos Sensibles

Definición: Filtración de información confidencial.

Afectación:

Posible en logs, respuestas de error o mensajes de depuración

Solución:

Revisar el LogMiddleware para asegurar que no se registren datos sensibles

Implementar enmascaramiento de datos sensibles en logs

6. Ataque de Manipulación de XML (XXE)

Definición: Inyección de entidades XML maliciosas.

Afectación:

Las APIs SOAP son particularmente vulnerables a este tipo de ataque

Solución:

Deshabilitar el procesamiento de entidades externas XML

Validar estrictamente los esquemas XML

Usar versiones seguras de analizadores XML

7. Ataque de Replay

Definición: Captura y reenvío de solicitudes autenticadas

Afectación:

Posible con los tokens JWT si son interceptados

Solución:

Implementar nonces (números usados una sola vez)

Usar timestamps en las solicitudes

Rotación frecuente de claves de firma