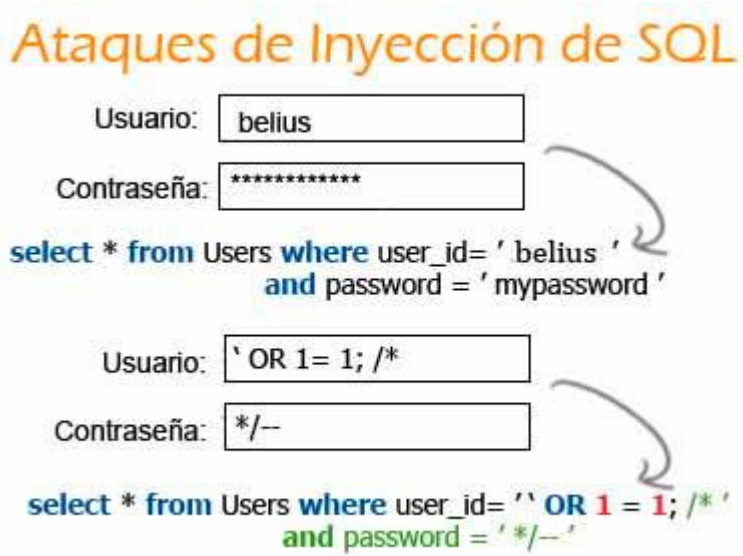
A05:2025 Injection

TOP 10 Vulnerabilidades OWASP

Álvaro Allén

¿Qué es?

- Una vulnerabilidad de inyección es un fallo de la aplicación que permite que datos de entrada no confiables proporcionados por el usuario se envíen a un intérprete y éste ejecute partes de esa entrada.



Vulnerabilidades

- Los datos proporcionados por el usuario no se valida, filtran ni sanean.
- Se utilizan consultas dinámicas o llamadas no parametrizadas sin un escapado adecuado.
- Se usan datos no saneados en parámetros de búsqueda.
- Datos potencialmente maliciosos se usan o concatenan directamente.

¿Cómo prevenirlo?

- La mejor opción es utilizar una API segura que evite por completo el uso directo del interprete.
- En caso de no usar API, podemos usar validación positiva de entradas en el servidor o, en caso de consultas dinámicas residuales, escapar los caracteres especiales.

Prevención utilizada

La prevención utilizada es la utilización de sentencias preparadas con las cuales podemos evitar dichas inyecciones.

java Copiar código

```java
String sql = "SELECT * FROM usuarios WHERE usuario = ? AND password = ?";

PreparedStatement ps = connection.prepareStatement(sql);
ps.setString(1, usuario);
ps.setString(2, password);

ResultSet rs = ps.executeQuery();
```

¿En qué afecta a nuestra Aplicación Final?

- Principalmente en el login, el cual es un punto débil donde se suele hacer una inyección de código SQL. Nuestra solución es utilizar consultas preparadas en nuestro código para evitar posibles inyecciones.
- Otro punto de "conflicto" es el mantenimiento de departamentos donde también se trabaja directamente con la base de datos. En este caso el hacker podría intentar confundir a la base de datos y modificar su tipo de perfil obteniendo privilegios de administrador.