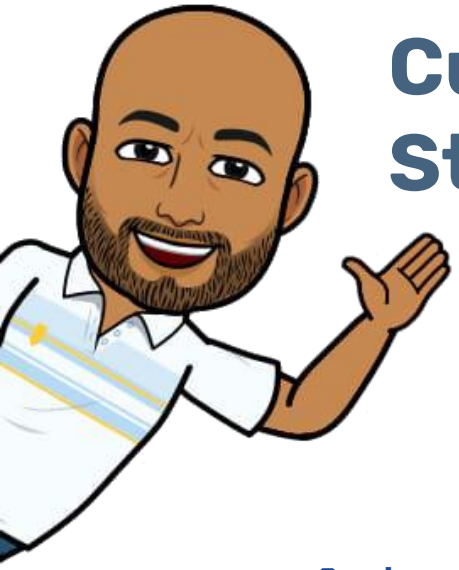


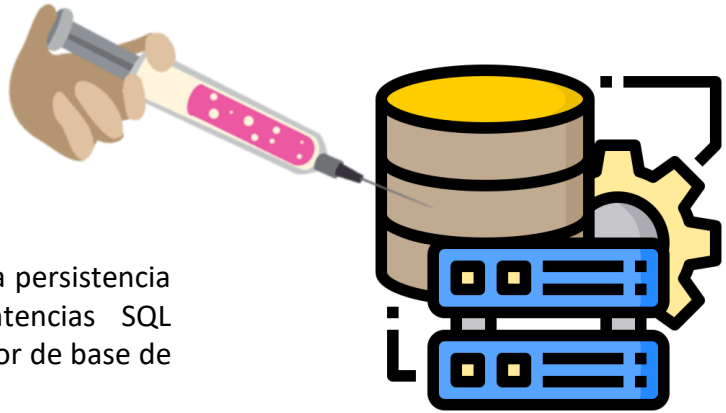
Curso de Java Standard

Ing. Octavio Robleto

octavio.robleto@gmail.com

https://octaviorobleto.com

Introducción



Al comenzar en el mundo del desarrollo y dar nuestros primeros pasos en la persistencia de información con una base de datos relacional, ejecutamos sentencias SQL concatenando los valores y así poder enviar la información pertinente al gestor de base de datos.

Esto sucede por lo general cuando tenemos que generar sentencias dinámicas y enviar un valor en el SQL que se le pide al usuario que lo introduzca, por ejemplo: correo, contraseña, filtros y/o datos en general.

```
String filtroCampo1 = "VALOR";
String seleccionar = " SELECT Campo1, Campo2 FROM TABLA WHERE Campo1 = '" + filtroCampo1 + "';";
```

El problema es que concatenando la información sin validar qué contiene puede venir con lo que se llama **Inyección SQL**, que no es mas que la técnica de introducir código malicioso en las declaraciones SQL que puede perjudicar completamente nuestros datos.

Inyección SQL

A pesar que parece una tontería que nuestro código sea así de vulnerable sigue siendo según la fundación OWASP el primero de los riesgos de seguridad en sitios WEB y aplicaciones https://owasp.org/www-project-top-ten.

Aunque existen otros tipos de vulnerabilidades que tienen que ver con la inyección de código nosotros en este modulo aprenderemos a evitar las de tipo SQL a través de herramientas que nos ofrecen los gestores de base de datos y Java.