# Sem3 – Dia3

**■ Objetivo**
Proteger el sistema de inyecciones SQL.

```
<?php
$conexion = new mysqli('localhost','root','','bootcamp');
$nombre = $conexion->real_escape_string($_POST['nombre']);
$rango = $conexion->real_escape_string($_POST['rango']);
$conexion->query("INSERT INTO soldados (nombre, rango) VALUES ('$nombre','$rango')");
?>
```

**■ Mini reto**
Investiga qué pasa si intentas ingresar como nombre: ' OR '1'='1 y observa el efecto sin la protección.

**■■ Cierre épico**
Hoy reforzaste tu fortaleza: ninguna inyección enemiga penetrará tu base de datos.