5.4 Control de formularis

L'entrada de dades a través de formularis per part dels usuaris pot provocar problemes a l'aplicació web si no es filtren prèviament aquestes dades.
Per aconseguir-ho, haurem d'aplicar alguna de les següents polítiques:

1. Data validation (Validació de dades)

- Es quan ens hem d'assegurar que les dades que agafem siguin del tipus que esperem.
- Per exemple:
  - Si demanem un número enter a l'usuari, assegurar-nos que és enter
  - Si demanem un telèfon, no pot tenir lletres.
  - Si és una matrícula de cotxe ha de ser de 4 números i 3 lletres
  - Si és un NIF...
  - ... en definitiva hem de revisar el format

- Per assegurar això, tenim diverses funcions:
  is_integer(...) —> per saber si és un número enter (i totes les variants amb els altres tipus)
  strlen(...) —> per controlar la mida
  preg_match('expresió_regular', $variable) —> per controlar el format d'una variable
  filter_var(..) —> per a comprovar si una variable compleix amb algun format. Hi ha molts tipus de filtres. Per exemple —> FILTER_VALIDATE_EMAIL

  Exemple matrícula de cotxe

```
if (preg_match('/^\d{4}[A-Za-z]{3}$/', $matricula)) {
            echo "La matrícula $matricula es válida";
      } else {
            echo "La matrícula $matricula NO es válida";
      }
```

  - /^ → inici del string
  - \d{4} → 4 digits
  - [A-Za-z]{3} → 3 lletres majúscules o minúscules
  - $/ → final de l'string

  Exemple correu electrònic

```
$email = "ejemplo@dominio.com";
if (filter_var($email, FILTER_VALIDATE_EMAIL)) {
      echo "CORREU OK";
}else{
      echo "CORREU INCORRECTE";
}
```

2. Data sanitization

- És quan hem d'editar i manipular les dades per assegurar-nos que són segures, fins i tot és possible que haguem d'esborrar certes parts
- La funció més habitual és —> strip_tags(...) que permet eliminar les etiquetes HTML que conté un string

Exemple:

```
<?php
        if(isset($_POST["boto"])){
                $dadaFiltrada=strip_tags($_POST["dada"]);
                echo "DADA FILTRADA: ".$dadaFiltrada;
        }
?>
<form method="POST">
        <input type="text" name="dada">
        <input type="submit" name="boto">
</form>
```

—> Si ara l'usuari posa etiquetes HTML en la caixa de text, aquestes queden eliminades.

Exemple: strip_tags(HTML) + preg_match(MATRICULA)

```
<?php
    if(isset($_POST["boto1"])){
        $dadaFiltrada=strip_tags($_POST["dada"]);
        echo "DADA FILTRADA amb strip_tags: ".$dadaFiltrada;
        echo "<br>";

        $matricula=$_POST["matricula"];
        if (preg_match('/^\d{4}[A-Za-z]{3}$/', $matricula)) {
            echo "Matricula OK: $matricula";
        }else{
            echo "Matricula INCORRECTA: $matricula";
        }
    }
?>
<form method="POST">
    <input type="text" name="dada" placeholder="HTML">
    <input type="text" name="matricula" placeholder="1234ABC">
    <input type="submit" name="boto1">
</form>
```