

# PHP

## exemple de code de formulaire

```
<form action="listeFilms.php" method="post"> <!-- post : champs saisis -> transaction HTTP POST -->
  <p>
    <input type="hidden" name="nomForm" value="formRecherche"/>
    <label for="titre">Titre:</label> <input type="text" size="20" name="titre" id="titre"/>
    <label for="annee">Année:</label> <input type="number" min="1900" step="1" name="annee"
id="annee"/>
  </p>
  <p> <!-- checkbox = choix multiples, radio = choix exclusif -->
  Comédie: <input type="checkbox" name="genre" value="c"/>
  Drame: <input type="checkbox" name="genre" value="d"/>
  Histoire: <input type="checkbox" name="genre" value="h"/>
  </p>
  <p>
  Résumé: <textarea name="resume" cols="30" rows="3">mots clés du résumé</textarea>
  </p>
  Metteur en scène:
  <select name="realisateur">
    <option value="1">Alfred Hitchcock</option>
    <option value="2">Francois Truffaut</option>
    <option value="3" selected="selected">Quentin Tarantino</option>
  </select>
  <br/>
  <p>Votre choix ?</p>
  <button type="submit">Rechercher</button>
</form>
```

## PHP en vrac

- portée des variables : `script`; `global` pour utiliser variable non locale dans fonction
- variables superglobales : `$_GET` et `$_POST` pour valeurs de formulaire, `$_SERVER`, `$_SESSION`
- chaînes de caractères : guillemets simples  $\neq$  guillemets doubles (interprétation)
- tableaux associatifs : `$real["alien"] = "Scott";`
- parcours de tableau : `foreach ($stab as $key => $value){...}`
- fonctions : passage des arguments par valeur
- objets : `$s = new SimpleClass(); $s->displayVar();`
- inclusion : `include_once`

## PHP et les bases de données

PDO : interface d'abstraction de l'accès aux données

- classe PDO = connexion entre PHP et SGBD
- PDO Statement = requête préparée et, une fois exécutée, le jeu de résultats associé
- généralement utilisation de préparation de requête : `prepare()` puis `execute()`
- `fetch()` ou `fetchAll()` pour récupérer les tuples

## Architecture MVC

- Modèle : accès aux données
- Vue : affichage
- Contrôleur : traitement des données

## Sécurité web

Ne jamais faire confiance aux données envoyées par le client

- contrôler les données reçues (par GET ou par POST) : présence des informations attendues et contrôle de validité de ces informations (type, bornes..)
- contrôler les données affichées

Exemples de failles : injection SQL, injection HTML (XSS)