Développer un site web dynamique en PHP

Module 5 : L'accès aux données

Objectifs

- Se connecter à une base de données avec PDO
- Récupérer des informations stockées sur une base de données
- Manipuler les données stockées en base
- Savoir préserver la sécurité des données

L'accès aux données

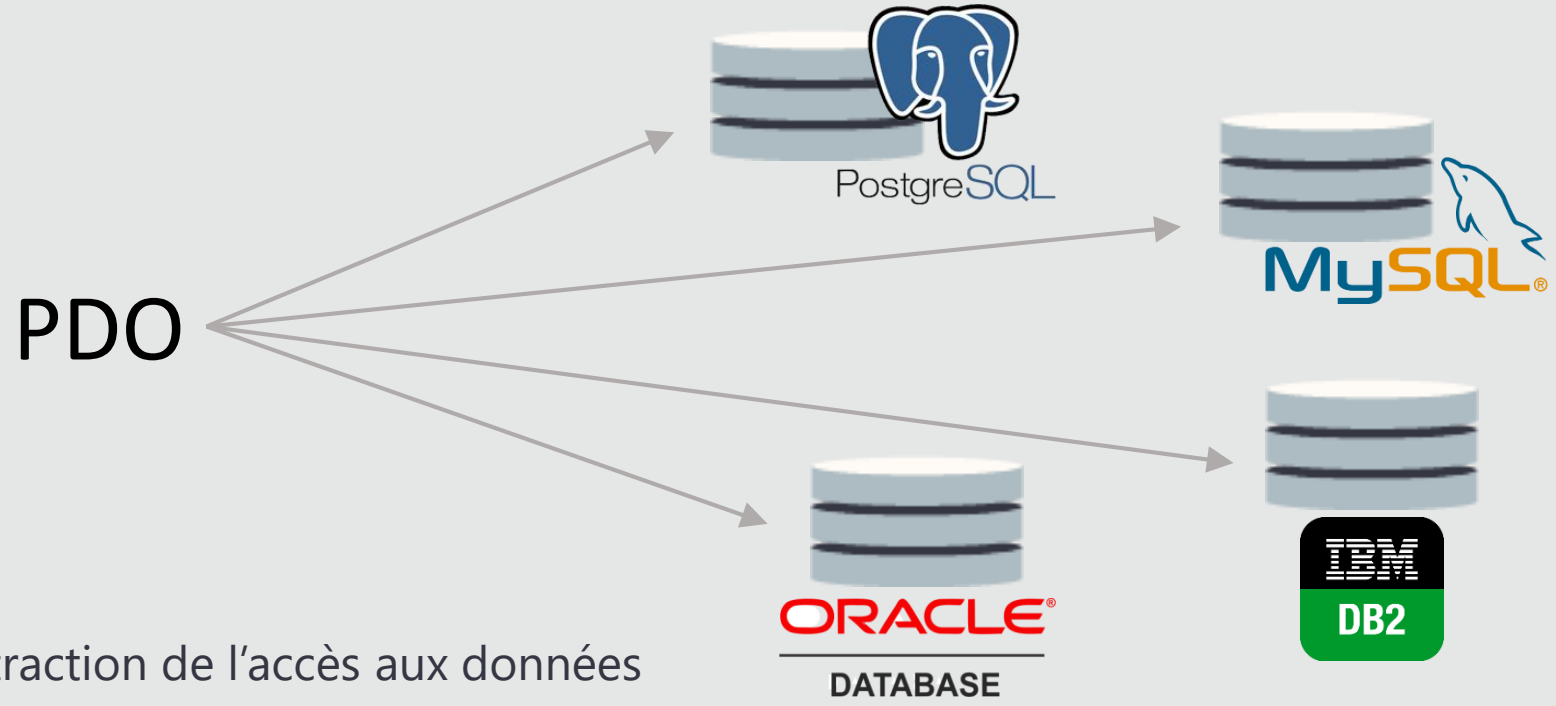
Utilisation de phpMyAdmin

Démonstration

L'accès aux données

PDO

- PDO : Php Data Object
  - Capable de se connecter à différents système de gestion de bases de données



  - Abstraction de l'accès aux données

La connexion avec PDO

```php
<?php
try {
    // chaine de connexion à la base de données
    $dsn = 'mysql:host=localhost;dbname=legumes';
    // option de connexion : encodage UTF8 pour MySQL
    $options = [PDO::MYSQL_ATTR_INIT_COMMAND => "SET NAMES utf8"];
    // création d'une instance de connexion à la base de données et ouverture de
    // la connexion
    $pdo = new PDO($dsn, 'userCodePHP', 'YMRwhDxHQunQ9h7M', $options);
    // choix de la méthode d'information en cas d'erreur : levée d'exception
    $pdo->setAttribute(PDO::ATTR_ERRMODE, PDO::ERRMODE_EXCEPTION);
    echo 'connexion effectuée avec le driver ' .
       $pdo->getAttribute(PDO::ATTR_DRIVER_NAME) . '<br>';
} catch (PDOException $e) {
    $msg = 'ERREUR PDO dans ' . $e->getFile() . ' : ' .
       $e->getLine() . ' : ' . $e->getMessage();
    die($msg);
}
```

connexion effectuée avec le driver mysql

Les requêtes non préparées

- Ordre de type SELECT
  - Récupération d'une ligne

```php
<?php
require_once '../connexion/connexion.php';

$id = 1;
$query = 'SELECT * FROM articles where identifiant = ' . $id . ';';
$arr = $pdo->query($query)->fetch();
var_dump($arr);

echo 'Article : ' . $arr['libelle'] . ' à ' . $arr[2] . ' €<br>';
```

```
array (size=6)
          'identifiant' => string '1' (length=1)
          0 => string '1' (length=1)
          'libelle' => string 'Abricots' (length=8)
          1 => string 'Abricots' (length=8)
          'prix' => string '35.50' (length=5)
          2 => string '35.50' (length=5)

Article : Abricots à 35.50 €
```

Les requêtes non préparées

- Ordre de type SELECT
  - Récupération de plusieurs lignes

```php
<?php
require_once '../connexion/connexion.php';

$prixMax = 40;
$query = 'SELECT * FROM articles where prix < ' .
     $prixMax . ';';
$stmt = $pdo->query($query);
$arrAll = $stmt->fetchAll();
var_dump($arrAll);

for ($i = 0; $i < count($arrAll); $i++) {
    echo 'Article : ' . $arrAll[$i]['libelle'] . ' à ' .
     $arrAll[$i][2] . ' €<br>';
}
```

```
array (size=3)
  0 => array (size=6)
         'identifiant' => string '1' (length=1)
         0 => string '1' (length=1)
         'libelle' => string 'Abricots' (length=8)
         1 => string 'Abricots' (length=8)
         'prix' => string '35.50' (length=5)
         2 => string '35.50' (length=5)
  1 => array (size=6)
         'identifiant' => string '3' (length=1)
         0 => string '3' (length=1)
         'libelle' => string 'Fraises' (length=7)
         1 => string 'Fraises' (length=7)
         'prix' => string '29.95' (length=5)
         2 => string '29.95' (length=5)
  2 => array (size=6)
         'identifiant' => string '4' (length=1)
         0 => string '4' (length=1)
         'libelle' => string 'Peches' (length=6)
         1 => string 'Peches' (length=6)
         'prix' => string '37.20' (length=5)
         2 => string '37.20' (length=5)
Article : Abricots à 35.50 €
Article : Fraises à 29.95 €
Article : Peches à 37.20 €
```

Les requêtes non préparées

- Ordre de type INSERT, UPDATE ou DELETE
  - Insertion

```php
<?php
require_once '../connexion/connexion.php';

$id = 9;
$libelle = 'Artichauts';
$prix = 7.2;
$query = 'INSERT INTO articles(identifiant, libelle, prix) VALUES(' . $id . ', \'' .
        $libelle . '\', ' . $prix . ');';
$rowcount = $pdo->exec($query);
echo "Nombre de lignes insérées : " . $rowcount . '<br>';

require '../afficheTousLesArticles.php';
```

```
Nombre de lignes insérées : 1
Article : Abricots à 35.50 €
Article : Cerises à 48.90 €
Article : Fraises à 29.95 €
Article : Peches à 37.20 €
Article : Artichauts à 7.20 €
```

Les requêtes non préparées

- Ordre de type INSERT, UPDATE ou DELETE
  - Modification

```php
<?php
require_once '../connexion/connexion.php';

$libelle = 'Artichauts';

$query = 'UPDATE articles SET prix = prix/2 WHERE libelle=\'' . $libelle . '\';';
$rowcount = $pdo->exec($query);
echo "Nombre de lignes modifiées : " . $rowcount . '<br>';

require '../afficheTousLesArticles.php';
```

```
Nombre de lignes modifiées : 1
Article : Abricots à 35.50 €
Article : Cerises à 48.90 €
Article : Fraises à 29.95 €
Article : Peches à 37.20 €
Article : Artichauts à 3.60 €
```

Les requêtes non préparées

- Ordre de type INSERT, UPDATE ou DELETE
  - Suppression

```php
<?php
require_once '../connexion/connexion.php';

$prix = 10;
$query = 'DELETE FROM articles WHERE prix < ' . $prix . ';';
$rowcount = $pdo->exec($query);
echo "Nombre de lignes supprimées : " . $rowcount . '<br>';

require '../afficheTousLesArticles.php';
```

```
Nombre de lignes supprimées : 1
Article : Abricots à 35.50 €
Article : Cerises à 48.90 €
Article : Fraises à 29.95 €
Article : Peches à 37.20 €
```

Les requêtes préparées

- Résolvent le problème de l'injection de code SQL
  - Les caractères saisis par un utilisateur ne doivent pas être interprétés comme du code SQL


```
$req = "SELECT COUNT(*) FROM Comptes WHERE login='' OR '1'='1';-- AND mdp='';"
```

Les requêtes préparées

- Avec paramètre non nommé

```php
<?php
require_once '../connexion/connexion.php';

$id = 1;
// Préparer la requête
$query = 'SELECT * FROM articles where identifiant = ?;';
$prep = $pdo->prepare($query);
// Associer des valeurs aux "trous"
$prep->bindValue(1, $id);
// Exécuter la requête
$prep->execute();
// Récupérer les données retournées.
$arr = $prep->fetch();
var_dump($arr);

echo 'Article : ' . $arr['libelle'] . ' à ' . $arr[2] . ' €<br>';
```

```
array (size=6)
  'identifiant' => string '1' (length=1)
  0 => string '1' (length=1)
  'libelle' => string 'Abricots' (length=8)
  1 => string 'Abricots' (length=8)
  'prix' => string '35.50' (length=5)
  2 => string '35.50' (length=5)
```

Article : Abricots à 35.50 €

L'accès aux données

Les requêtes préparées

- Avec paramètre nommé

```php
<?php
require_once '../connexion/connexion.php';

$prixMax = 40;
$query = 'SELECT * FROM articles where prix < :prixMax;';
$prep = $pdo->prepare($query);
$prep->bindValue(':prixMax', $prixMax);
$prep->execute();
$arrAll = $prep->fetchAll();
var_dump($arrAll);

for ($i = 0; $i < count($arrAll); $i++) {
    echo 'Article : ' . $arrAll[$i]['libelle'] . ' à ' .
$arrAll[$i][2] . ' €<br>';
}
```

```
array (size=3)
  0 => array (size=6)
         'identifiant' => string '1' (length=1)
         0 => string '1' (length=1)
         'libelle' => string 'Abricots' (length=8)
         1 => string 'Abricots' (length=8)
         'prix' => string '35.50' (length=5)
         2 => string '35.50' (length=5)
  1 => array (size=6)
         'identifiant' => string '3' (length=1)
         0 => string '3' (length=1)
         'libelle' => string 'Fraises' (length=7)
         1 => string 'Fraises' (length=7)
         'prix' => string '29.95' (length=5)
         2 => string '29.95' (length=5)
  2 => array (size=6)
         'identifiant' => string '4' (length=1)
         0 => string '4' (length=1)
         'libelle' => string 'Peches' (length=6)
         1 => string 'Peches' (length=6)
         'prix' => string '37.20' (length=5)
         2 => string '37.20' (length=5)
```

Article : Abricots à 35.50 €
Article : Fraises à 29.95 €
Article : Peches à 37.20 €

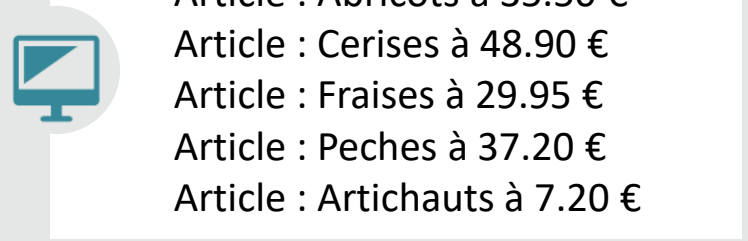
Les requêtes préparées

- Les ordres de type INSERT, UPDATE ou DELETE
  - Insertion

```php
<?php
require_once '../connexion/connexion.php';

$id = 9;
$libelle = 'Artichauts';
$prix = 7.2;
$query = 'INSERT INTO articles(libelle, prix) VALUES(:libelle, :prix);';
$prep = $pdo->prepare($query);
$prep->bindValue(':libelle', $libelle);
$prep->bindValue(':prix', $prix);
$prep->execute();
echo "Nombre de lignes insérées : " . $prep->rowCount() . '<br>';

require '../afficheTousLesArticles.php';
```



Les requêtes préparées

- Les ordres de type INSERT, UPDATE ou DELETE
  - Modification

```php
<?php
require_once '../connexion/connexion.php';

$libelle = 'Artichauts';

$query = 'UPDATE articles SET prix = prix/2 WHERE libelle=:libelle;';
$prep = $pdo->prepare($query);
$prep->bindValue(':libelle', $libelle);
$prep->execute();
echo "Nombre de lignes modifiées : " . $prep->rowCount() . '<br>';

require '../afficheTousLesArticles.php';
```

```
Nombre de lignes modifiées : 1
Article : Abricots à 35.50 €
Article : Cerises à 48.90 €
Article : Fraises à 29.95 €
Article : Peches à 37.20 €
Article : Artichauts à 3.60 €
```

Les requêtes préparées

- Les ordres de type INSERT, UPDATE ou DELETE
  - Suppression

```php
<?php
require_once '../connexion/connexion.php';

$prix = 10;
$query = 'DELETE FROM articles WHERE prix < :prix;';
$prep = $pdo->prepare($query);
$prep->bindValue(':prix', $prix);
$prep->execute();
echo "Nombre de lignes supprimées : " . $prep->rowCount() . '<br>';

require '../afficheTousLesArticles.php';
```

Nombre de lignes supprimées : 1
Article : Abricots à 35.50 €
Article : Cerises à 48.90 €
Article : Fraises à 29.95 €
Article : Peches à 37.20 €

Les requêtes préparées

- La réutilisation de requêtes

```php
<?php
require_once '../connexion/connexion.php';

$query = 'INSERT INTO articles(libelle, prix) VALUES(:libelle, :prix);';
$prep = $pdo->prepare($query);
$prep->bindParam(':libelle', $libelle);
$prep->bindParam(':prix', $prix);

$libelle = 'Chou-fleur';
$prix = 23.1;
$prep->execute();

$libelle = 'Poireau';
$prix = 15.7;
$prep->execute();

require '../afficheTousLesArticles.php';
```

Article : Abricots à 35.50 €
Article : Cerises à 48.90 €
Article : Fraises à 29.95 €
Article : Peches à 37.20 €
Article : Chou-fleur à 23.10 €
Article : Poireau à 15.70 €