



Université Sidi Mohamed Ben Abdllah

Faculté des sciences Dhar El Mahraz  
Licence professionnelle SIGL

# **WEB DYNAMIQUE: PHP**

Réalisé par: Pr. Mahraz Med Adnane  
Année universitaire:2017/2018

# SGBD?

- Les **SGBD** (Systèmes de Gestion de Bases de Données) permettent d'organiser le stockage d'informations.
- Plusieurs SGRB existe:
  - Oracle,
  - Sybase,
  - Microsoft SQL Server,
  - PostgreSQL,
  - MySQL ...

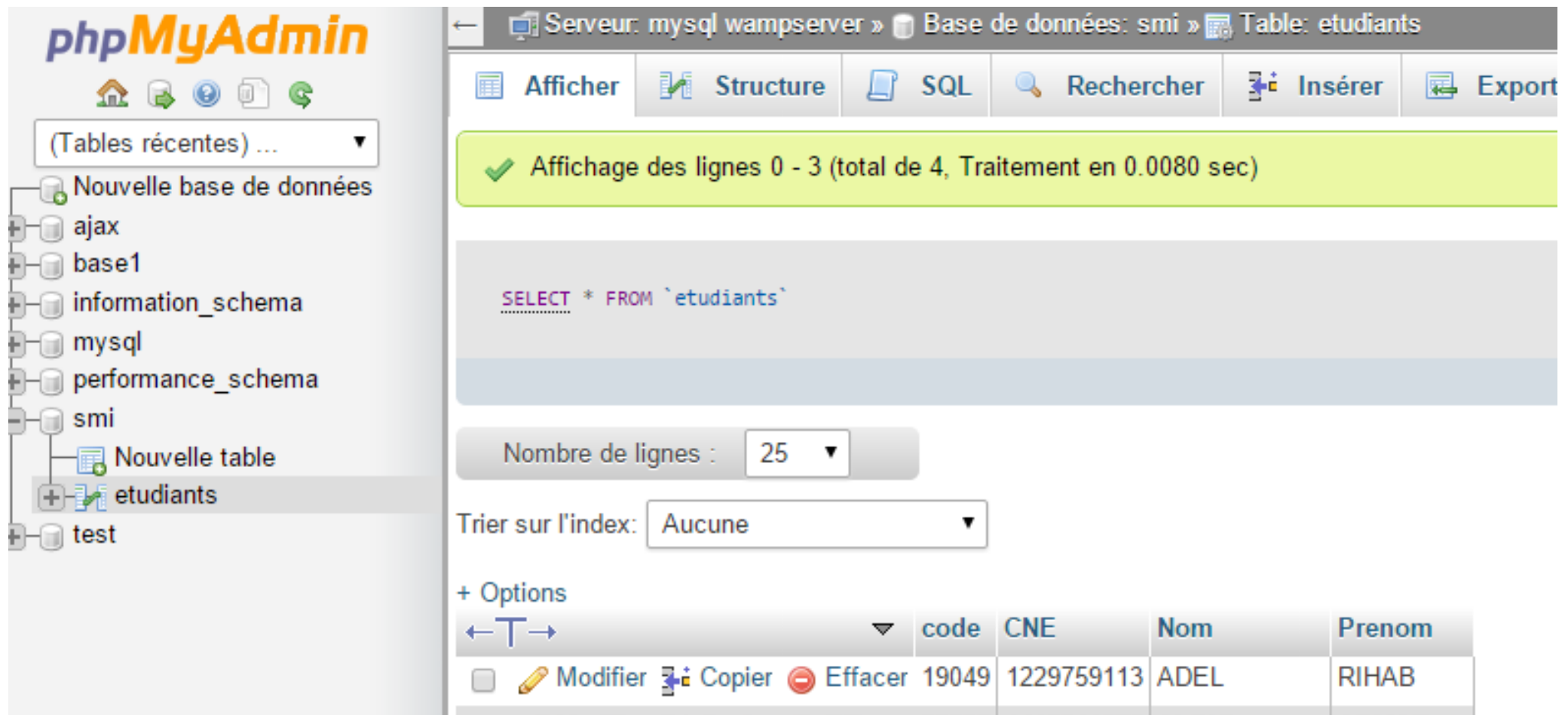
# SQL?

- Le langage **SQL** (Structured Query Language) permet d'interroger les bases de données relationnelles :



```
SELECT cl_nom, cl_prenom FROM clients WHERE cl_ville = "FES";
```

- Les données sont récupérées sous forme de tables (n lignes \* m colonnes)

# UTILISATION DE L'OUTIL PHPMYADMIN



The screenshot displays the phpMyAdmin web interface. On the left, a sidebar shows a tree of databases, with 'smi' selected and its tables listed, including 'etudiants'. The main panel at the top shows the breadcrumb path: 'Serveur: mysql wampserver » Base de données: smi » Table: etudiants'. Below this is a toolbar with buttons for 'Afficher', 'Structure', 'SQL', 'Rechercher', 'Insérer', and 'Export'. A green status bar indicates 'Affichage des lignes 0 - 3 (total de 4, Traitement en 0.0080 sec)'. The SQL query editor contains the query 'SELECT \* FROM `etudiants`'. Below the editor, there are controls for 'Nombre de lignes' (set to 25) and 'Trier sur l'index' (set to 'Aucune'). A '+ Options' section is partially visible. At the bottom, a table displays the first three rows of data from the 'etudiants' table.

	code	CNE	Nom	Prenom
<input type="checkbox"/> 	19049	1229759113	ADEL	RIHAB
<input type="checkbox"/> 	22225	1112211272	ALOU	ALMAE

# DROITS D'ACCÈS À LA BASE DE DONNÉES

**Admin**

tes) ... ▼

ise de données

\_schema

e\_schema

e table

s

← Serveur: mysql wampserver

Bases de données SQL État Utilisateurs Exporter Importer Paramètres

## Survol des utilisateurs

	Utilisateur	Client	Mot de passe	Privilèges globaux ?	«Grant»	Action
<input type="checkbox"/>	N'importe quel	%	—	USAGE	Non	<a href="#">Changer les privilèges</a> <a href="#">Exporter</a>
<input type="checkbox"/>	N'importe quel	localhost	Non	USAGE	Non	<a href="#">Changer les privilèges</a> <a href="#">Exporter</a>
<input type="checkbox"/>	adnane	localhost	Oui	ALL PRIVILEGES	Oui	<a href="#">Changer les privilèges</a> <a href="#">Exporter</a>
<input type="checkbox"/>	root	::1	Non	ALL PRIVILEGES	Oui	<a href="#">Changer les privilèges</a> <a href="#">Exporter</a>
<input type="checkbox"/>	root	localhost	Non	ALL PRIVILEGES	Oui	<a href="#">Changer les privilèges</a> <a href="#">Exporter</a>

↑ ☐ Tout cocher Pour la sélection : Exporter

# SGBD ET TRAITEMENT DE DONNÉES?

- Un certain nombre de traitements ne peuvent pas être réalisés en SQL.
- Pour pouvoir les réaliser, il faut faire appel à un langage (autre que SQL) qui est capable d'interagir avec un SGBD
- Parmi les langages susceptibles d'être utilisés on trouve :
  - Perl
  - Python
  - PHP
- Il s'agit de langages de script (interprétés)



# SGBD ET PHP

- PHP 5 propose plusieurs connecteurs capables de se connecter à une base de données MySQL.
- Le premier et le plus courant est le driver MySQL => extension MySQLi (MySQL improved)
  - MySQLi a la particularité d'être orienté objet ou procédurale.
- Le deuxième connecteur est l'extension PDO qui signifie PHP Data Objects.
  - Pouvoir se connecter à de multiples bases de données à condition que les pilotes pour chaque SGBD soient installés sur le serveur Web.
  - Interface orientée objet

# SGBD ET PHP?

L'objet MySQLi fournit un grand choix de fonctions permettant de manipuler les bases de données.

Trois fonctions sont essentielles:

- La fonction de connexion à la base de données
- La fonction de requête
- La fonction de déconnexion



# LA CONNEXION À UNE BD

- Ce sont les paramètres (optionnels généralement) des fonctions de connexion à la base. Ces variables sont:
  - \$user : Le nom d'utilisateur
  - \$passwd : Le mot de passe
  - \$host : L'hôte (ordinateur sur lequel le SGBD est installé)
    - par défaut le nom d'hôte est **localhost**
  - \$bd : Le nom de la base de données

```
$access = new mysqli($host, $user, $passwd, $bd);
```

# GESTION DES ERREURS D'OUVERTURE D'UNE BD

```
$errnum=$access->connect_errno;
```

```
if ($errnum) {
```

```
$errmsg=$access->connect_error;
```

```
echo "Connexion impossible:$errmsg";
```

```
exit();
```

```
}
```

```
if ($errnum) {
```

```
$errmsg=$access->connect_error;
```

```
Die("Connexion impossible:$errmsg");
```

```
}
```

# CRÉATION ET L'EXÉCUTION D'UNE REQUÊTE

```
$access = new mysqli($host, $user, $passwd, $bd);  
$req="SELECT * FROM Etudiants WHERE code=22985";
```

```
$stmt=$access->query($req) or die ($access->error); // afficher l'erreur  
et quitter
```

Mieux:

```
$stmt=$access->query($req) or die($access->error. "à la ligne" .  
(__LINE__) ); //afficher la ligne de l'erreur
```

# MANIPULATION DES DONNÉES

## ISSUES D'UNE REQUÊTE

```
$stmt=$access->query('select * from Etudiants');
```

```
$count=$stmt->num_rows;
```

```
if ($count>0){  
    while($donnees = $stmt->fetch_row()){  
        echo $donnees[2];  
        echo " : ";  
        echo $donnees[3];  
        echo "<br/>";  
    }  
}
```

```
if ($count>0){  
    while($donnees = $stmt->fetch_assoc()){  
        echo $donnees['nom'];  
        echo " : ";  
        echo $donnees['prenom'];  
        echo "<br/>";  
    }  
}
```

# MANIPULATION DES DONNÉES ET AFFICHAGE VISUEL

```
$stmt= $mysqli->query("SELECT * FROM Etudiants");
$nbcol = $stmt->field_count;
echo "<table style='border-color:red' border=2> <tr>";
for ($i=0; $i < $nbcol; $i++) {
    $colonne = $stmt->fetch_field();
    echo "<th style='color:red'> " . $colonne->name . "</th>";
}
echo "</tr>";
while ($ligne = $stmt->fetch_assoc()) {
    echo '<tr>';
    foreach ($ligne as $indice => $information) {
        echo "<td style='color:purple'>" . $information . "</td>";
    }
    echo '</tr>';
}
echo '</table>';
```

code	CNE	Nom	Prenom
19049	1229759113	ADEL	RIHAB
22985	1412811976	ALOUI	ASMAE
25033	1412755481	ANDALOUSSI	ISMAIL
25103	1412744400	AKKA	OTHMANE

# REQUÊTES PRÉPARÉE

Une requête préparée peut être exécutée à plusieurs reprises.

A chaque exécution, la valeur courante de la variable liée est évaluée, et envoyée au serveur. La requête n'est pas analysée de nouveau. Le Template de la requête n'est pas une nouvelle fois envoyée au serveur non plus.

```
$stmt=$access->prepare("insert into users  
values(?,?,?)");
```

```
$x=1;
```

```
$y="toto";
```

```
$z="momo";
```

```
$stmt->bind_param('iss',$x,$y,$z);
```

```
$stmt->execute();
```

```
for ($x = 2; $x < 5; $x++) {
```

```
    $stmt->execute();
```

```
}
```

# FAILLE DE SÉCURITÉ INJECTION SQL

votre nom :

Mot de passe:

```
$sql = "SELECT * FROM password where login='$login' and pass='$pass' ";
```

```
$sql = "SELECT * FROM password where login=' ' or 1=1' and pass=' ' or 1=1' ";
```



# FAILLE DE SÉCURITÉ INJECTION SQL

## addslashes

Permet d'échapper les caractères(' , « ,\, NULL).  
Il faut vérifier si magic\_quotes\_gpc() est activée.

```
$login= addslashes($_POST['nom']);  
$pass= addslashes($_POST['passwd']);  
$sql = "SELECT * FROM password  
where login='$login' and  
pass='$pass'";
```

## Mysqli::real\_escape\_string

Cette fonction est utilisée pour créer une chaîne SQL valide qui pourra être utilisée dans une requête SQL.

```
$login=$mysqli->real_escape_string(  
$_POST['nom']);  
$pass=$mysqli->real_escape_string(  
$_POST['passwd']);  
$sql = "SELECT * FROM password where  
login='$login' and pass='$pass'";
```

# LA SÉCURITÉ MD5

- Lors de l'enregistrement du mot de passe, il est judicieux de l'hasher avant de l'insérer à la base de données.
- Cela permet aux ceux qui ont le droit d'accéder à la bd de reconnaître facilement le mot de passe.
- Les algorithmes de hashage comme MD5 ([\*Message-Digest Algorithm\*](#)), SHA1 (*Secure Hash Algorithm*) sont destinés à être rapides et efficaces.

## **enregistrement**

```
$login=$_POST['nom']; $pass=MD5($_POST['passwd']);  
$sql = "insert into password values('$login','$pass')";
```

## **authentification**

```
$login=$_POST['nom']; $pass=MD5($_POST['passwd']);  
$sql = "SELECT * FROM password where login='$login' and pass='$pass'";
```