



upcomillas *es*

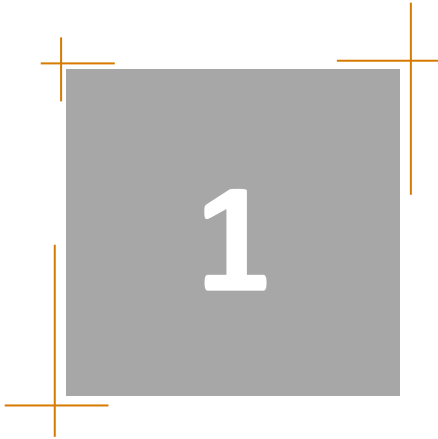
upcomillas *es*

## 7-PHP and MySQL queries

**Course: Developing web-based applications**

Cristina Puente, Rafael Palacios

2010-2011



# Introduction

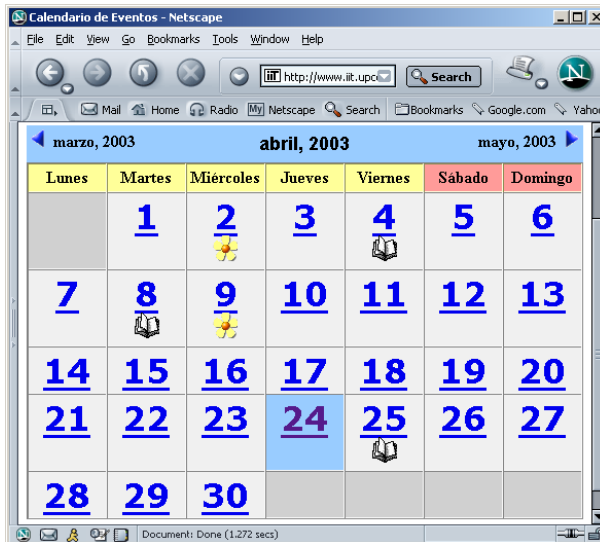


# Introduction

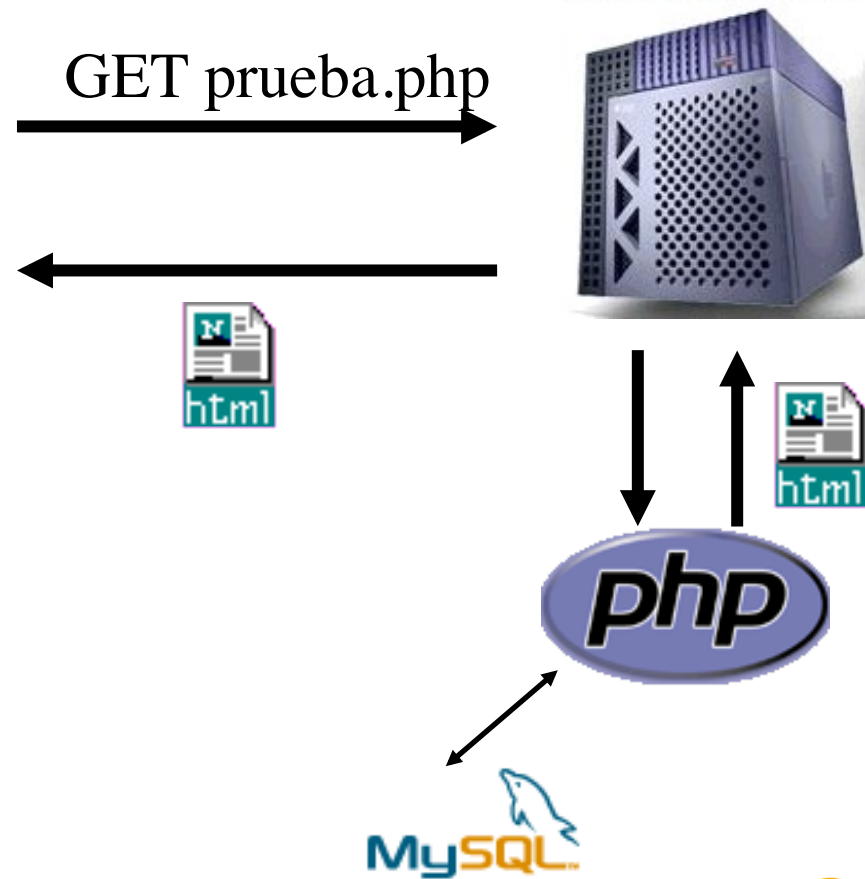
- PHP includes libraries for communicating with several databases:
  - **MySQL** (OpenSource, the use selected for this course)
  - DBM (Berkeley)
  - Informix
  - MS SQL (Microsoft)
  - Oracle 8
  - PostgreSQL (Berkeley—open source)
  - Sybase

# Introduction

- ¿Who does it work?

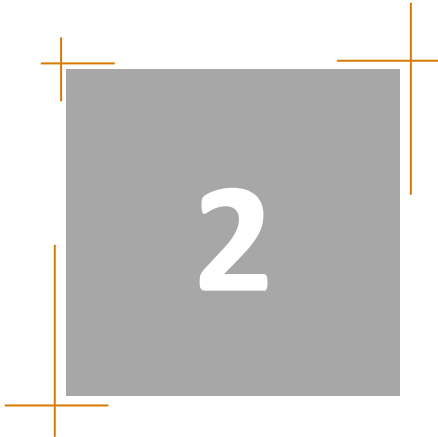


GET prueba.php



## Example of PHP program

1. Open connection with database server
2. Select database
3. Build the query
4. Execute the query
5. Loop to display results row by row
6. Close connection



Open database connection



# Database connection

- `mysql_connect()`, sentence including three parameters: host name, user name, and password.
- In local modo use "localhost" (localhost = 127.0.0.1)

```
<?php
$conn = mysql_connect("localhost","mysql_user","mysql_pwd");
if (!$conn) {
    die('Error connecting to database server');
}

/* Code goes here*/

mysql_close($conn);
?>
```

# Database connection

- It is possible to use variables and develop functions

```
<?php
function connect()
{
    $host="localhost";
    $user="mysql_user";
    $pass="shhh";
    $conn = mysql_connect($host,$user,$pass);
    if (!$conn) {
        die('Connection Error');
    }
    return $conn;
}
```

Access.php



# Selección de la base de datos

- Los ficheros que accedan a la base de datos incluyen la función.

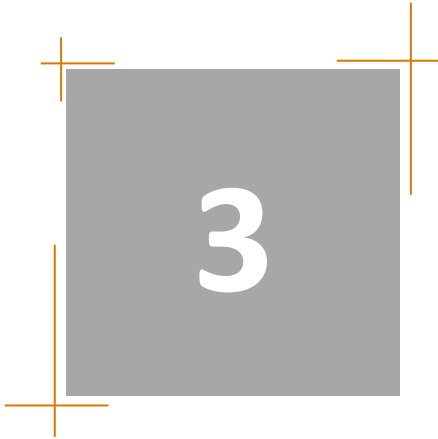
```
<?php
include("access.php");

$conn=Connect();

if (!mysql_select_db("testing",$conn)) {
    printf("ERROR: %s\n",mysql_error());
    mysql_close($conn);
    die("Error selecting database.\n");
}

/* Code goes here*/

mysql_close($conn);
```



Queries



## Query example

- Queries are executed with `mysql_query`. It is recommended to check the error

```
$query="SELECT name, lastname  
      FROM users  
      WHERE salary<10000;"
```

```
$result=mysql_query($query,$conn);  
if (!$result) {  
    printf("Error in query: ".mysql_error());  
    mysql_close($conn);  
    exit;  
}
```

## Query example

- `mysql_fetch_array` stores the result of the query into one array containing all the information of one row.
- Array elements use the same names as the tables.

```
$row=mysql_fetch_array($result);  
while ($row) {  
    printf("Name: {$row['name']} {$row['lastname']}<br>");  
    $row=mysql_fetch_array($result);  
}  
mysql_free_result($result);
```

## Summary of PHP functions to access MySQL

- `mysql_connect()` :Connects to database server.
- `mysql_select_db()` :Selects database.
- `mysql_query()` : Excutes SQL query.
- `mysql_num_rows($result)` : Number of resulting registers
- `mysql_fetch_array($result)` : Convert result into array variable
- `mysql_free_result($result)` : Free memory
- `mysql_close()` : Closes connection.
- `mysql_error()` : Displays latest error message
- `mysql_real_escape_string()` : Obtain secure string (see below)

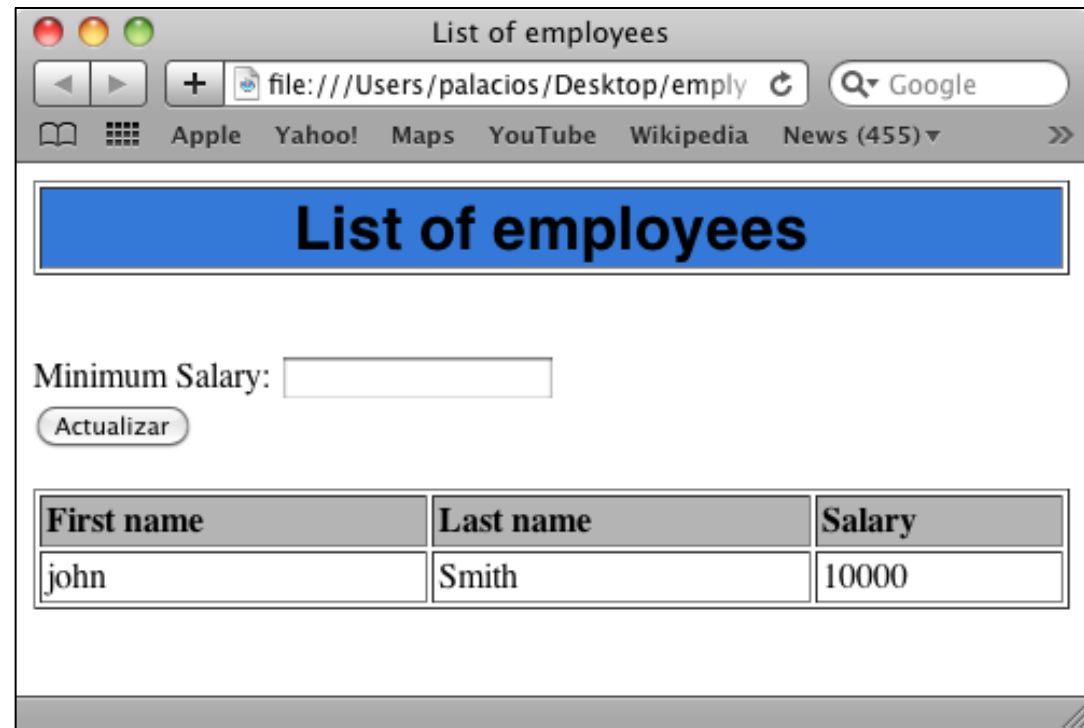


## Forms and security aspects



# Form-based query

1. Design your page using any HTML editor
2. Convert into PHP and insert database code
3. Obtain and protect form data
4. Build the query
5. Create output



The screenshot shows a web browser window with the title "List of employees". The address bar contains the file path "file:///Users/palacios/Desktop/emply". The browser's search bar is set to "Google". The browser's menu bar includes "Apple", "Yahoo!", "Maps", "YouTube", "Wikipedia", and "News (455)".

The main content area features a blue header with the text "List of employees". Below the header, there is a form with the label "Minimum Salary:" followed by an empty text input field. Below the input field is a button labeled "Actualizar".

Below the form is a table with three columns: "First name", "Last name", and "Salary". The table contains one row of data:

First name	Last name	Salary
john	Smith	10000

# Structure of PHP file

The screenshot shows a web browser window titled "List of employees" with the address bar set to "file:///Users/palacios/Desktop/emply". The page content includes a blue header with the text "List of employees", a form for "Minimum Salary" with an "Actualizar" button, and a table with the following data:

First name	Last name	Salary
john	Smith	10000

Annotations on the right side of the browser window indicate the structure of the PHP file:

- Initial HTML code (points to the blue header)
- PHP Query (points to the table)
- final HTML code (points to the bottom of the browser window)



# Building the query

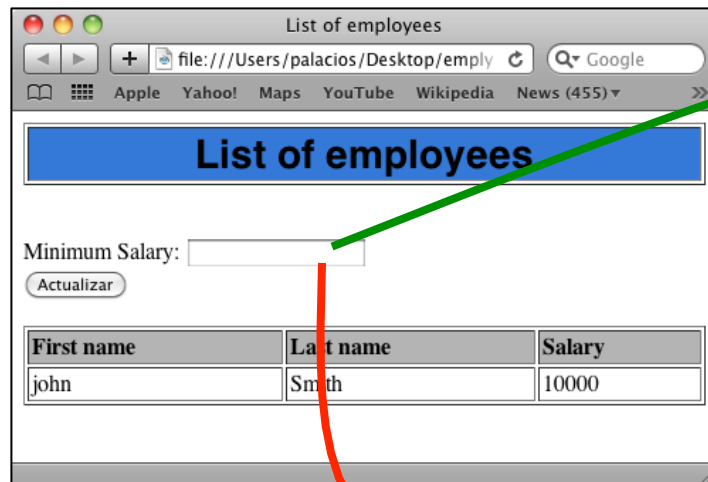
```
if (isset($_GET['salary'])) {
    $salary=mysql_real_escape_string($_GET['salary']); //important
    $query='SELECT firstname, lastname, salary FROM users
           WHERE salary>={ $salary}';
} else {
    /* No filter */
    $query='SELECT firstname, lastname, salary FROM users;';
}

$result=mysql_query($query,$conn);
if (!$result) {
    die('Query error '.mysql_error());
}

$row=mysql_fetch_array($result);
while ($row) {
    printf("<tr>\n");
    printf("<td>{$row['firstname']}</td><td>{$row['lastname']}</td>");
    printf("<td>{$row['salary']}</td></tr>");
    $row=mysql_fetch_array($result);
}
mysql_free_result($result);
```

# Security aspects

- ¿Why is `mysql_real_escape_string` important?



10000

```
query='SELECT name FROM users  
WHERE salary<=10000;'
```

10000; drop table users;

```
query='SELECT name FROM users  
WHERE salary<=10000; drop table users'
```



**Escuela Técnica Superior de Ingeniería ICAI**

Alberto Aguilera 25  
28015 Madrid  
Tel +34 91 542 28 00  
Fax + 34 91 542 31 76  
lwww.icaí.upcomillas.es

[www.upcomillas.es](http://www.upcomillas.es)

