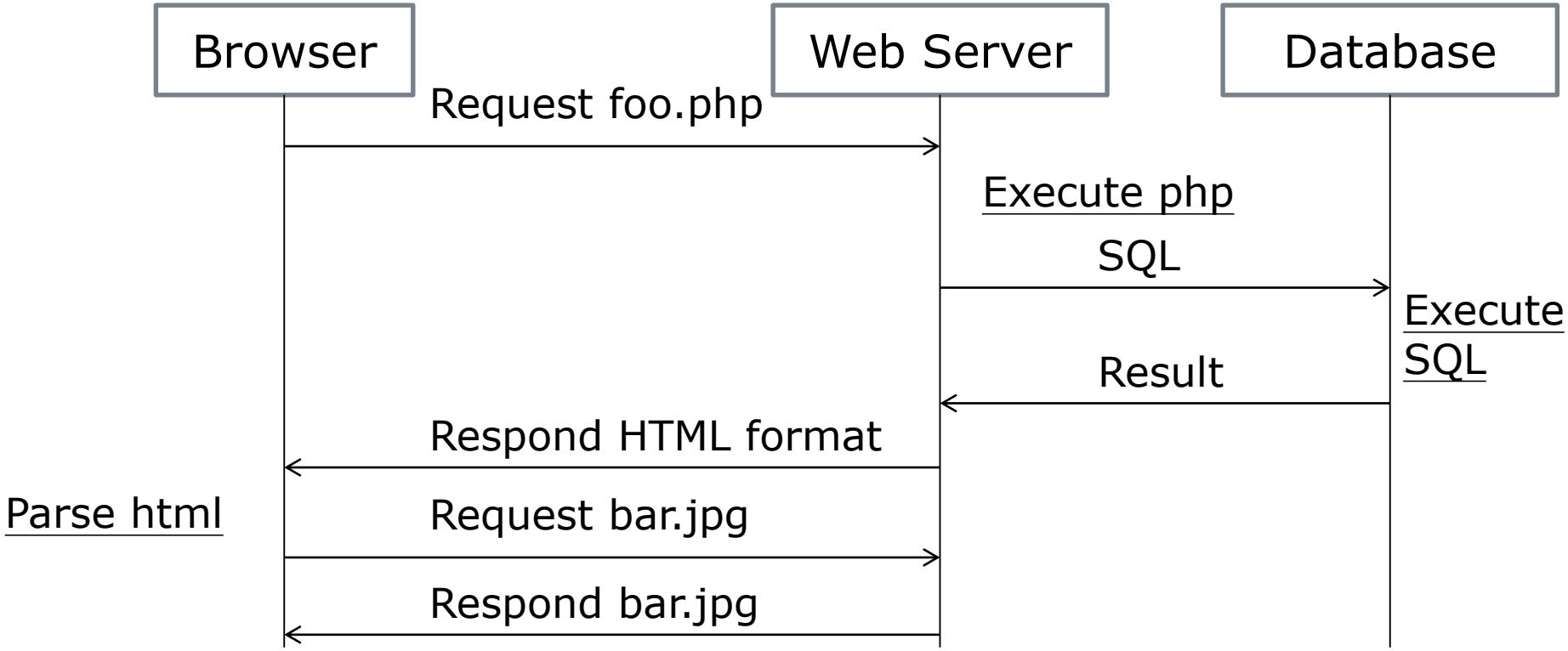
A Very Brief Introduction to Web Application Development (II)

Jiun-Long Huang (黃俊龍)
Department of Computer Science
National Chiao Tung University

Dynamic Web Application 1.0: Back End Approach

Control Flow



- Data transfer between php files
  - GET
  - POST
  - Session
- SQL
  - Prepared statement

An Example

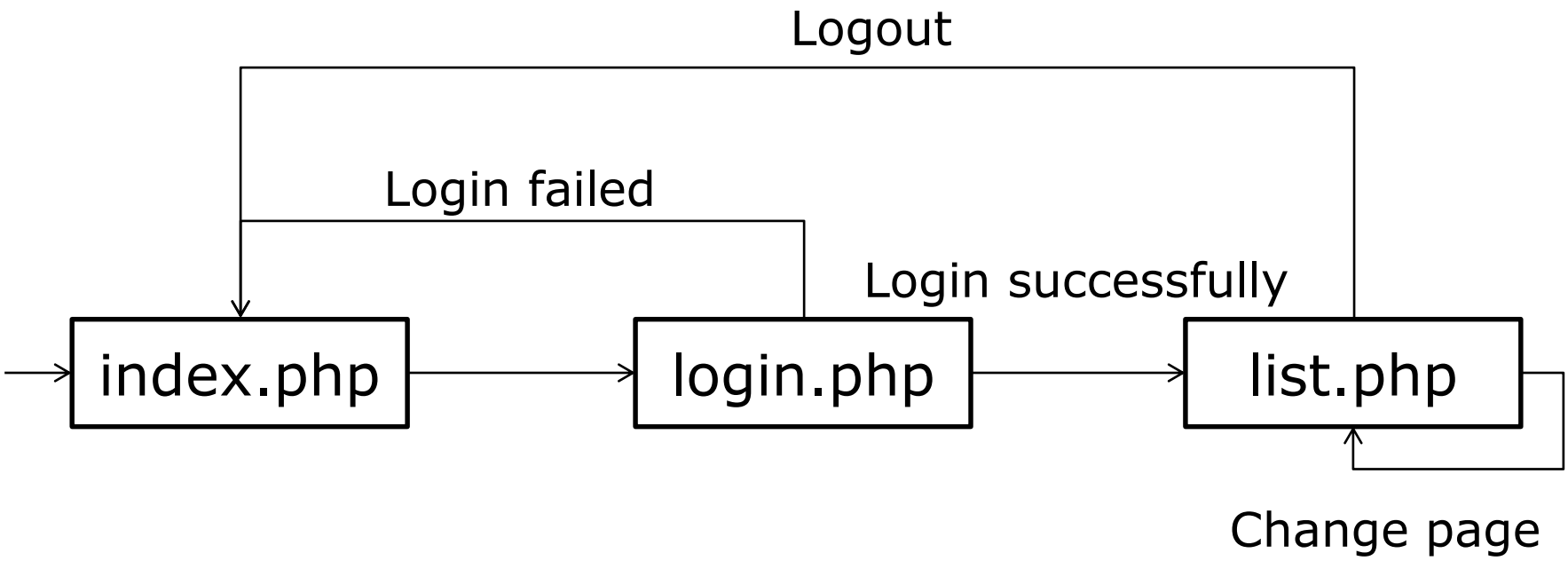

Logout
Login failed
Login successfully
index.php
login.php
list.php
Change page

Table users

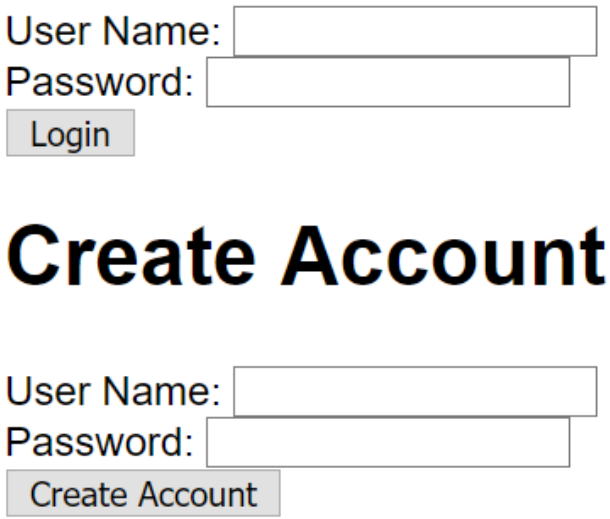
- Column
  - user_id: int(11), AUTO_INCREMENT, Primary Key
  - username: char(40), Unique
  - password: char(64), Not null
    - The length of the result of shar256 is 32 bytes (64 characters in hex mode)
  - salt: char(4)
- Index
  - user_id, username

Table posts

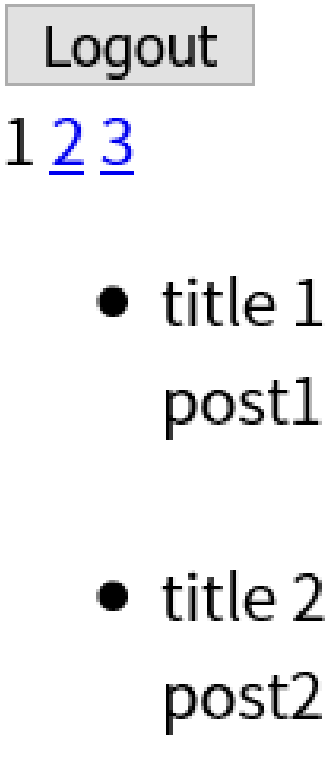
- Column
  - post_id: int(11), AUTO_INCREMENT, Primary Key
  - title: char(30), Not null
  - content: char(100), Not null
- Index
  - post_id

Screenshots

- Login/Create Account



- Browse



index.php

```php
<?php
  session_start();
  # remove all session variables
  session_unset();
  # destroy the session
  session_destroy();
  $_SESSION['Authenticated']=false;
?>

<!DOCTYPE html>
<html>
<body>
<h1>Login</h1>
<form action="login.php" method="post">
  User Name:
  <input type="text" name="uname"><br>
  Password:
  <input type="password" name="pwd"><br>
  <input type="submit" value="Login">
</form>
```

```
<h1>Create Account</h1>
<form action="register.php" method="post">
  User Name:
  <input type="text" name="uname"><br>
  Password:
  <input type="password" name="pwd"><br>
  <input type="submit" value="Create Account">
</form>

</body>
</html>
```

register.php

```
<?php
session_start();
$_SESSION['Authenticated']=false;

$dbservername='localhost';
$dbname='examdb';
$dbusername='examdb';
$dbpassword='examdb';

try {
  if (!isset($_POST['uname']) || !isset($_POST['pwd']))
  {
    header("Location: index.php");
    exit();
  }
  if (empty($_POST['uname']) || empty($_POST['pwd']))
    throw new Exception('Please input user name and
password.');
```

```
  $uname=$_POST['uname'];
  $pwd=$_POST['pwd'];
  $conn = new
PDO("mysql:host=$dbservername;dbname=$dbname",
$dbusername, $dbpassword);
  # set the PDO error mode to exception
  $conn->setAttribute(PDO::ATTR_ERRMODE,
PDO::ERRMODE_EXCEPTION);

  $stmt=$conn->prepare("select username from users where
username=:username");
  $stmt->execute(array('username' => $uname));

  if ($stmt->rowCount()==0)
  {
    $salt=strval(rand(1000,9999));

    $hashvalue=hash('sha256', $salt.$pwd);
```

```
    $stmt=$conn->prepare("insert into users (username,
password, salt) values (:username, :password, :salt)");
    $stmt->execute(array('username' => $uname,
'password' => $hashvalue, 'salt' => $salt));
    echo <<<EOT
        <!DOCTYPE html>
      <html>
        <body>
            <script>
            alert("Create an account successfully.
Please log in.");
            window.location.replace("index.php");
          </script>
        </body>
      </html>
EOT;
    exit();
  }
  else
    throw new Exception("Login failed.");
}
```

```
catch(Exception $e)
{
  $msg=$e->getMessage();
  session_unset();
  session_destroy();

  echo <<<EOT
    <!DOCTYPE html>
    <html>
      <body>
          <script>
          alert("$msg");
               window.location.replace("index.php");
        </script>
      </body>
       </html>
EOT;
}
?>
</body>
</html>
```

login.php

```
<?php
session_start();

$_SESSION['Authenticated']=false;

$dbservername='localhost';
$dbname='examdb';
$dbusername='examdb';
$dbpassword='examdb';

try
{
  if (!isset($_POST['uname']) || !isset($_POST['pwd']))
  {
    header("Location: index.php");
    exit();
  }
  if (empty($_POST['uname']) || empty($_POST['pwd']))
    throw new Exception('Please input user name and
password.');
```

```
  $uname=$_POST['uname'];
  $pwd=$_POST['pwd'];
  $conn = new PDO("mysql:host=$dbservername;dbname=$dbname",
$dbusername, $dbpassword);
  # set the PDO error mode to exception
  $conn->setAttribute(PDO::ATTR_ERRMODE,
PDO::ERRMODE_EXCEPTION);
  $stmt=$conn->prepare("select username, password, salt
from users where username=:username");
  $stmt->execute(array('username' => $uname));

  if ($stmt->rowCount()==1)
  {
    $row = $stmt->fetch();
```

```
  if
($row['password']==hash('sha256',$row['salt'].$_POST['pwd']
))
    {
      $_SESSION['Authenticated']=true;
      $_SESSION['Username']=$row[0];
      header("Location: list.php?page=1");
      exit();
       }
       else
         throw new Exception('Login failed.');
  }
  else
     throw new Exception('Login failed.');
}
```

```
catch(Exception $e)
{
  $msg=$e->getMessage();
  session_unset();
  session_destroy();
  echo <<<EOT
    <!DOCTYPE html>
    <html>
      <body>
          <script>
          alert("$msg");
               window.location.replace("index.php");
        </script>
         </body>
       </html>
EOT;
}
?>
```

list.php

```
<?php
  session_start();

  $dbservername='localhost';
  $dbname='examdb';
  $dbusername='examdb';
  $dbpassword='examdb';

try
{
  if (!isset($_SESSION['Authenticated']) ||
$_SESSION['Authenticated']!=true)
  {
    header("Location: index.php");
    exit();
  }

  if (isset($_GET['page']))
    $page=$_GET['page'];
  else
    $page=1;
```

```
  $postperpage=2;
  $conn = new
PDO("mysql:host=$dbservername;dbname=$dbname", $dbusername,
$dbpassword);
  $conn->setAttribute(PDO::ATTR_ERRMODE,
PDO::ERRMODE_EXCEPTION);
  $stmt=$conn->prepare("select count(*) from posts");
  $stmt->execute();
  $row=$stmt->fetch();
  $totalpage=ceil($row[0]/$postperpage);

  echo <<<EOT
    <!DOCTYPE html>
      <html>
      <body>
        <button type="button"
onClick="window.location.replace('index.php');">Logout</bu
tton><br>
EOT;
```

```
  echo <<<EOT
    <!DOCTYPE html>
      <html>
      <body>
        <button type="button"
onClick="window.location.replace('index.php');">Logout</bu
tton><br>
EOT;

  if ($totalpage>0)
  {
    for($i=1;$i<=$totalpage;$i++)
    {
      if ($i==$page)
        echo "$i ";
      else
        echo "<a href='list.php?page=$i'>$i</a> ";
    }
    echo '<br>';
    $startrow=($page-1)*$postperpage;
```

```
  $stmt=$conn->prepare("select title, content from posts
limit $startrow,2");
    $stmt->execute();
    echo '<ul>';
    while($row=$stmt->fetch())
      echo '<li> ' . $row['title'] . '<br>' .
$row['content'] . '<br><br> </li>';
  }
  echo '</ul></body></html>';
}
```

```
catch (PDOException $e)
{
  session_unset();
  session_destroy();

  echo <<<EOT
    <!DOCTYPE html>
      <html>
        <body><script>
          alert("Internal Error. $msg");
            window.location.replace("index.php");
        </script></body>
      </html>
EOT;
}
?>
```

PHP Database Access

- PDO
- MySQLi
  - 'i' means improvement
- MySQL (deprecated in PHP 5.5.0)
  - mysql_connect, mysql_select_db
- PDO is better

Hash

- Do not use MD5 and SHA-1 for authentication
  - MD5 has been broken by Tao Xie and Dengguo Feng in 2009
  - SHA-1 has been broken by Google in 2017
- SHA-2 is preferred
  - SHA-224、SHA-256、SHA-384、SHA-512、SHA-512/224、SHA-512/256
- salt

Web Development Framework

- Framework
  - CodeIngiter
  - Laravel