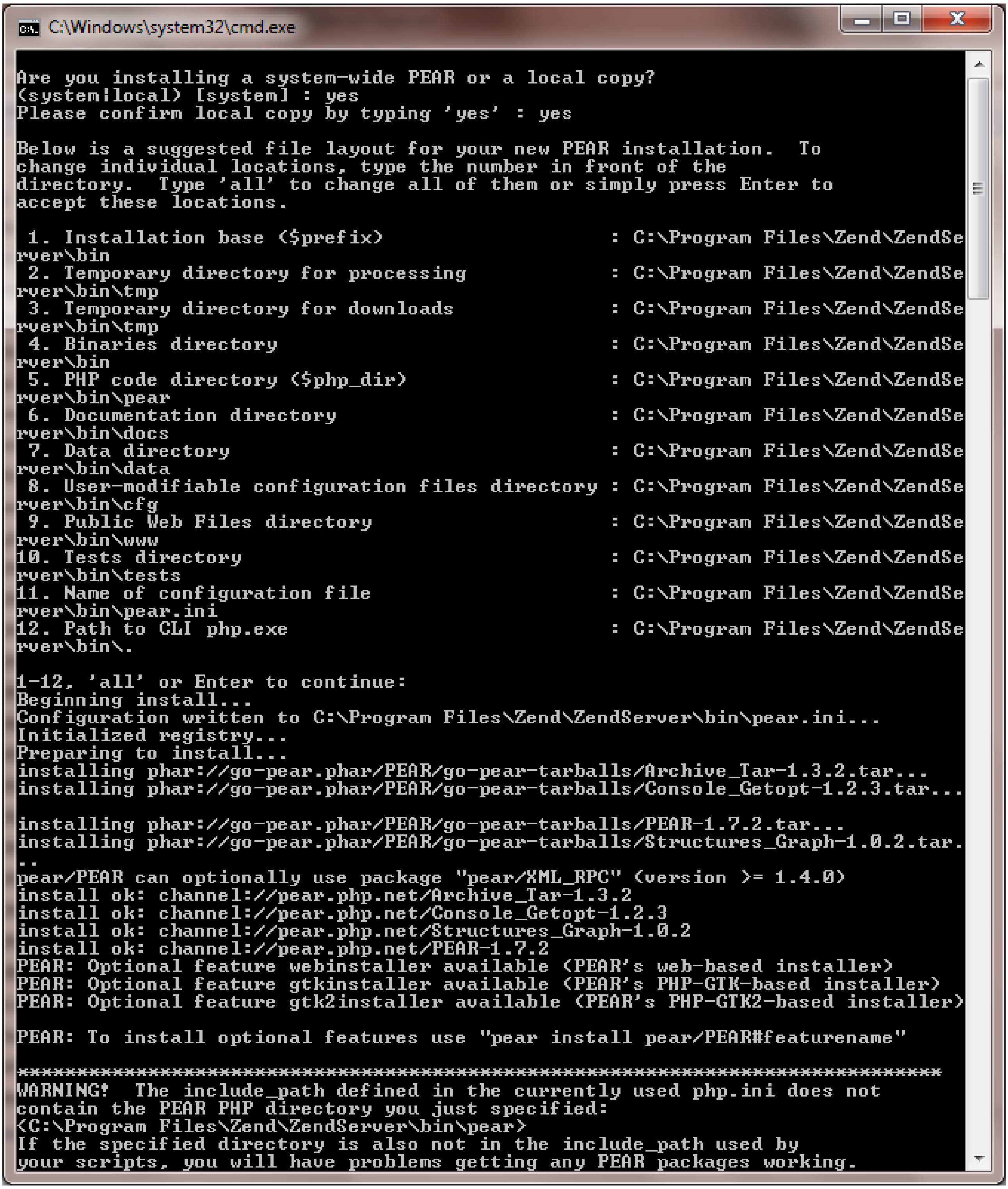
Lab 6-2. Advanced Database Techniques

Prepared: TrangNTT

6.1. Install PEAR DB

- Goes to http://pear.php.net/manual/en/installation.getting.php to get the installation guide of PEAR DB.

- Follow the guide to install PEAR DB to your Apache server and check if PEAR works.



```
Are you installing a system-wide PEAR or a local copy?
(system|local) [system] : yes
Please confirm local copy by typing 'yes' : yes

Below is a suggested file layout for your new PEAR installation.  To
change individual locations, type the number in front of the
directory.  Type 'all' to change all of them or simply press Enter to
accept these locations.

 1. Installation base ($prefix)                   : C:\Program Files\Zend\ZendSe
rver\bin
 2. Temporary directory for processing            : C:\Program Files\Zend\ZendSe
rver\bin\tmp
 3. Temporary directory for downloads             : C:\Program Files\Zend\ZendSe
rver\bin\tmp
 4. Binaries directory                            : C:\Program Files\Zend\ZendSe
rver\bin
 5. PHP code directory ($php_dir)                 : C:\Program Files\Zend\ZendSe
rver\bin\pear
 6. Documentation directory                       : C:\Program Files\Zend\ZendSe
rver\bin\docs
 7. Data directory                                : C:\Program Files\Zend\ZendSe
rver\bin\data
 8. User-modifiable configuration files directory : C:\Program Files\Zend\ZendSe
rver\bin\cfg
 9. Public Web Files directory                    : C:\Program Files\Zend\ZendSe
rver\bin\www
10. Tests directory                               : C:\Program Files\Zend\ZendSe
rver\bin\tests
11. Name of configuration file                    : C:\Program Files\Zend\ZendSe
rver\bin\pear.ini
12. Path to CLI php.exe                           : C:\Program Files\Zend\ZendSe
rver\bin\.

1-12, 'all' or Enter to continue:
Beginning install...
Configuration written to C:\Program Files\Zend\ZendServer\bin\pear.ini...
Initialized registry...
Preparing to install...
installing phar://go-pear.phar/PEAR/go-pear-tarballs/Archive_Tar-1.3.2.tar...
installing phar://go-pear.phar/PEAR/go-pear-tarballs/Console_Getopt-1.2.3.tar...

installing phar://go-pear.phar/PEAR/go-pear-tarballs/PEAR-1.7.2.tar...
installing phar://go-pear.phar/PEAR/go-pear-tarballs/Structures_Graph-1.0.2.tar.
..
pear/PEAR can optionally use package "pear/XML_RPC" (version >= 1.4.0)
install ok: channel://pear.php.net/Archive_Tar-1.3.2
install ok: channel://pear.php.net/Console_Getopt-1.2.3
install ok: channel://pear.php.net/Structures_Graph-1.0.2
install ok: channel://pear.php.net/PEAR-1.7.2
PEAR: Optional feature webinstaller available (PEAR's web-based installer)
PEAR: Optional feature gtkinstaller available (PEAR's PHP-GTK-based installer)
PEAR: Optional feature gtk2installer available (PEAR's PHP-GTK2-based installer)

PEAR: To install optional features use "pear install pear/PEAR#featurename"

******************************************************************************
WARNING!  The include_path defined in the currently used php.ini does not
contain the PEAR PHP directory you just specified:
<C:\Program Files\Zend\ZendServer\bin\pear>
If the specified directory is also not in the include_path used by
your scripts, you will have problems getting any PEAR packages working.
```

6.2. Authentication and SQL Injection

Get the login form in the exercise 9.4 of Lab 09 to do the followings:

Step 1. Enter the following case for username or password and see what happens

- ' or 1=1; #
- ' UNION ALL SELECT * FROM users #
- '; DROP TABLE Users (Be careful with that input)
- '; INSERT INTO Users…

Step 2. Modify Authentication to prevent SQL injection

Use the following techniques to ensure that the Login form will not be SQL Injection attacker (Ex.)

- Using mysql_real_escape_string()
- Using parameterized/prepared SQL of mysqli
- Using parameterized/prepared SQL of PEAR DB

6.3. Modify the business listing service from previous class

Modify the business listing service from previous class to ensure all the pages will not be attacked by SQL Injection.

- Using mysql_real_escape_string()
- Using parameterized/prepared SQL of mysqli
- Using parameterized/prepared SQL of PEAR DB
- Using parameterized/prepared SQL of PDO

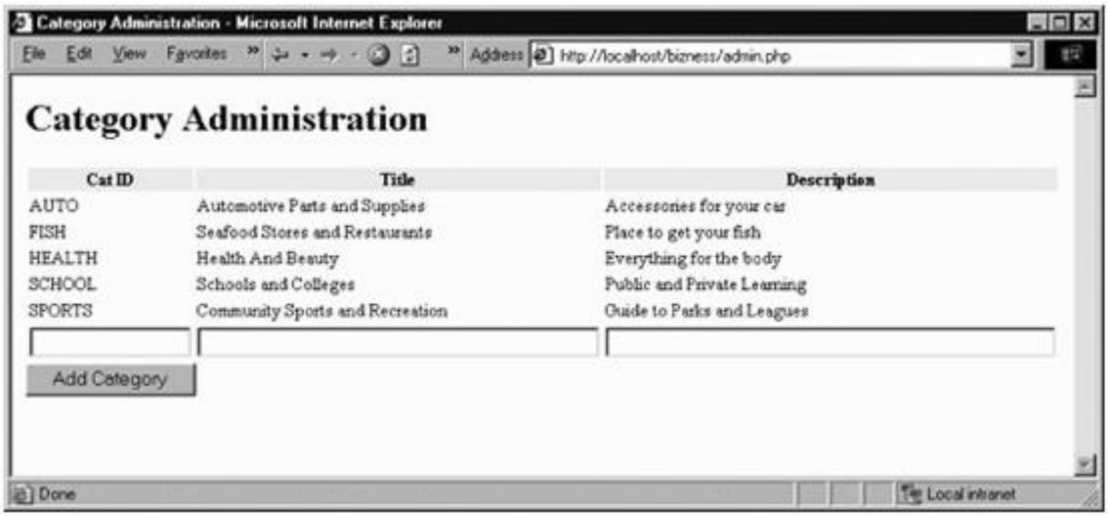
The suggestion is for PEAR DB. This is only suggestion, there can be some errors or omited, you have to complete them. Good luck!

Step 1. Create *db_login.php* includes all DB parameters

```
<?php
  # parameters for connecting to the "business_service"
  $username = "root"; $password = "12345";
  $hostspec = "localhost"; $database = "business_service";
  // $dbtype = 'pgsql';
  // $dbtype = 'oci8';
  $dbtype = 'mysqli';

  # DSN constructed from parameters
  $dsn = "$dbtype://$username:$password@$hostspec/$database";

  # Establish the connection
  $db = DB::connect($dsn);
  if (DB::isError($db)) {
     die ($db->getMessage());
  }
?>
```

Step 2. Create Category Administration page

This page that allows administrators to add categories to the listing service. The input fields for adding a new record appear after a dump of the current data. The administrator fills in the form and presses the Add Category button, and the page redisplays with the new record. If any of the three fields are not filled in, the page displays an error message.


Category Administration - Microsoft Internet Explorer
File Edit View Favorites
Address http://localhost/bizness/admin.php
Done
Local intranet

Category Administration

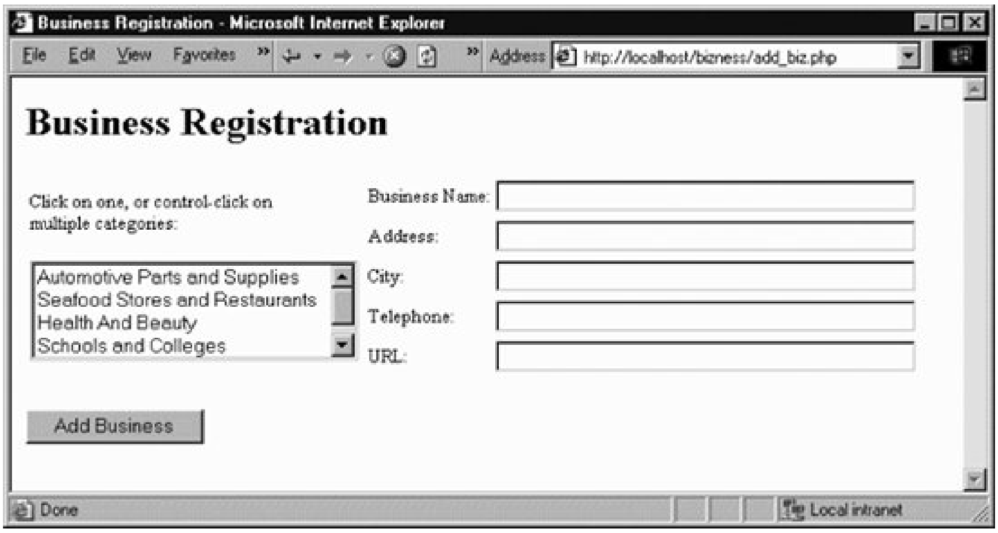
Cat ID	Title	Description
AUTO	Automotive Parts and Supplies	Accessories for your car
FISH	Seafood Stores and Restaurants	Place to get your fish
HEALTH	Health And Beauty	Everything for the body
SCHOOL	Schools and Colleges	Public and Private Learning
SPORTS	Community Sports and Recreation	Guide to Parks and Leagues

Add Category

```
<html>
<head>
<?php
 require_once('db_login.php');
?>

<title>
<?php
 // print the window title and the topmost body heading
 $doc_title = 'Category Administration';
 echo "$doc_title\n";
?>
</title>
</head>
<body>
<h1>
<?php
 echo "$doc_title\n";
?>
</h1>

<?php
 // add category record input section

 // extract values from $_REQUEST
 $Cat_ID = $_REQUEST['Cat_ID'];
 $Cat_Title = $_REQUEST['Cat_Title'];
 $Cat_Desc = $_REQUEST['Cat_Desc'];
 $add_record = $_REQUEST['add_record'];

 // determine the length of each input field
 $len_cat_id = strlen($_REQUEST['Cat_ID']);
 $len_cat_tl = strlen($_REQUEST['Cat_Title']);
 $len_cat_de = strlen($_REQUEST['Cat_Desc']);

 // validate and insert if the form script has been
 // called by the Add Category button
 if ($add_record == 1) {
     if (($len_cat_id > 0) and ($len_cat_tl > 0) and ($len_cat_de > 0)){
         $sql  = "insert into categories (category_id, title, description)";
         $sql .= " values ('$Cat_ID', '$Cat_Title', '$Cat_Desc')";
         $result = $db->query($sql);
         $db->commit(  );
     } else {
     echo "<p>Please make sure all fields are filled in ";
     echo "and try again.</p>\n";
     }
 }

 // list categories reporting section

 // query all records in the table after any
 // insertion that may have occurred above
 $sql = "select * from categories";
 $result = $db->query($sql);
?>

<form method="post" action="<?= $PHP_SELF ?>">

<table>
<tr><th bgcolor="#eeeeee">Cat ID</th>
    <th bgcolor="#eeeeee">Title</th>
    <th bgcolor="#eeeeee">Description</th>
</tr>

<?php
 // display any records fetched from the database
 // plus an input line for a new category
 while ($row = $result->fetchRow(  )){
     echo "<tr><td>$row[0]</td><td>$row[1]</td><td>$row[2]</td></tr>\n";
 }
?>
<tr><td><input type="text" name="Cat_ID"    size="15" maxlength="10" /></td>
    <td><input type="text" name="Cat_Title" size="40" maxlength="128" /></td>
    <td><input type="text" name="Cat_Desc"  size="45" maxlength="255" /></td>
</tr>
</table>
<input type="hidden" name="add_record" value="1" />
<input type="submit" name="submit" value="Add Category" />
</body>
</html>
```

Step 3. Adding a Business

This page that lets a business insert data into the `business` and `biz_categories` tables.



Business Registration - Microsoft Internet Explorer
File
Edit
View
Favorites
Address
http://localhost/bizness/add_biz.php
Done
Local intranet

Business Registration

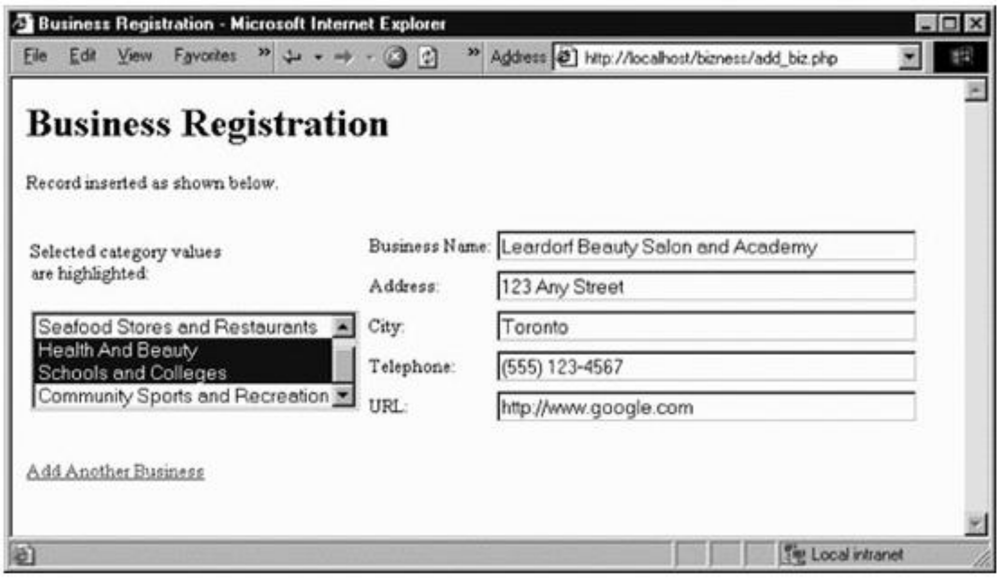
Click on one, or control-click on multiple categories:

Automotive Parts and Supplies
Seafood Stores and Restaurants
Health And Beauty
Schools and Colleges

Business Name:
Address:
City:
Telephone:
URL:

Add Business

When the user enters data and clicks on the Add Business button, the script calls itself to display a confirmation page. The following figure shows a confirmation page for a company listing assigned to two categories.


Business Registration - Microsoft Internet Explorer
File Edit View Favorites
Address http://localhost/bizness/add_biz.php
Local intranet

Business Registration

Record inserted as shown below.

Selected category values
are highlighted:

Seafood Stores and Restaurants
Health And Beauty
Schools and Colleges
Community Sports and Recreation

Business Name: Leardorf Beauty Salon and Academy

Address: 123 Any Street

City: Toronto

Telephone: (555) 123-4567

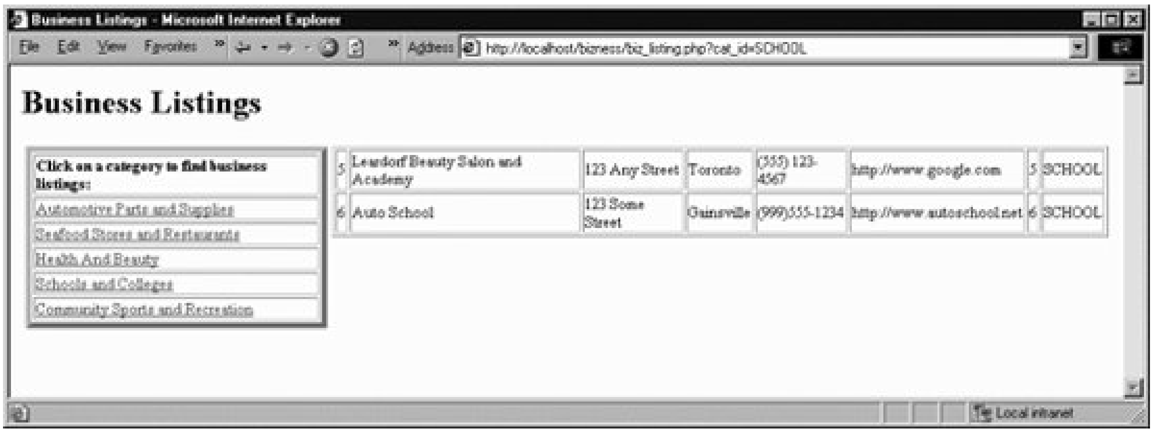
URL: http://www.google.com

Add Another Business

```
<html>
<head>
<title>
<?php
 $doc_title = 'Business Registration';
 echo "$doc_title\n";
?>
</title>
</head>
<body>
<h1>
<?= $doc_title ?>
</h1>

<?php
 require_once('db_login.php');

 // fetch query parameters
 $add_record = $_REQUEST['add_record'];
 $Biz_Name = $_REQUEST['Biz_Name'];
 $Biz_Address = $_REQUEST['Biz_Address'];
 $Biz_City = $_REQUEST['Biz_City'];
 $Biz_Telephone = $_REQUEST['Biz_Telephone'];
 $Biz_URL = $_REQUEST['Biz_URL'];
 $Biz_Categories = $_REQUEST['Biz_Categories'];

 $pick_message = 'Click on one, or control-click on<BR>multiple ';
 $pick_message .= 'categories:';

 // add new business
 if ($add_record == 1) {
     $pick_message = 'Selected category values<br />are highlighted:';
     $sql  = 'INSERT INTO businesses (name, address, city, telephone, ';
     $sql .= ' url) VALUES (?, ?, ?, ?, ?)';
     $params = array($Biz_Name, $Biz_Address, $Biz_City, $Biz_Telephone,
$Biz_URL);
     $query = $db->prepare($sql);
     if (DB::isError($query)) die($query->getMessage(  ));
     $resp = $db->execute($query, $params);
     if (DB::isError($resp)) die($resp->getMessage(  ));
     $resp = $db->commit(  );
     if (DB::isError($resp)) die($resp->getMessage(  ));
     echo '<p class="message">Record inserted as shown below.</p>';
     $biz_id = $db->getOne('SELECT max(business_id) FROM businesses');
 }
?>

<form method="post" action="<?= $PHP_SELF ?>">
<table>
<tr><td class="picklist"><?= $pick_message ?>
    <p>
    <select name="Biz_Categories[]" size="4" multiple>
    <?php
     // build the scrolling pick list for the categories
     $sql = "SELECT * FROM categories";
     $result = $db->query($sql);
     if (DB::isError($result)) die($result->getMessage(  ));
     while ($row = $result->fetchRow(  )){
         if (DB::isError($row)) die($row->getMessage(  ));
         if ($add_record == 1){
             $selected = false;
             // if this category was selected, add a new biz_categories row
             if (in_array($row[1], $Biz_Categories)) {
                 $sql  = 'INSERT INTO biz_categories';
                 $sql .= ' (business_id, category_id)';
                 $sql .= ' VALUES (?, ?)';
                 $params = array($biz_id, $row[0]);
                 $query = $db->prepare($sql);
                 if (DB::isError($query)) die($query->getMessage(  ));
                 $resp = $db->execute($query, $params);
                 if (DB::isError($resp)) die($resp->getMessage(  ));
                 $resp = $db->commit(  );
                 if (DB::isError($resp)) die($resp->getMessage(  ));
                 echo "<option selected=\"selected\">$row[1]</option>\n";
                 $selected = true;
             }
             if ($selected == false) {
                 echo "<option>$row[1]</option>\n";
             }
         } else {
             echo "<option>$row[1]</option>\n";
         }
     }
    ?>

    </select>
    </td>
    <td class="picklist">
        <table>
        <tr><td class="FormLabel">Business Name:</td>
            <td><input type="text" name="Biz_Name" size="40" maxlength="255"
                value="<?= $Biz_Name ?>" /></td>
        </tr>
        <tr><td class="FormLabel">Address:</td>
         <td><input type="text" name="Biz_Address" size="40" maxlength="255"
                value="<?= $Biz_Address ?>" /></td>
        </tr>
        <tr><td class="FormLabel">City:</td>
            <td><input type="text" name="Biz_City" size="40" maxlength="128"
                value="<?= $Biz_City ?>" /></td>
        </tr>
        <tr><td class="FormLabel">Telephone:</td>
        <td><input type="text" name="Biz_Telephone" size="40" maxlength="64"
                value="<?= $Biz_Telephone ?>" /></td>
        </tr>
        <tr><td class="FormLabel">URL:</TD>
            <td><input type="text" name="Biz_URL" size="40" maxlength="255"
                value="<?= $Biz_URL ?>" /></td>
        </tr>
        </table>
    </td>
</tr>
</table>
<p>
<input type="hidden" name="add_record" value="1" />

<?php
 // display the submit button on new forms; link to a fresh registration
 // page on confirmations
 if ($add_record == 1){
     echo '<p><a href="'.$PHP_SELF.'">Add Another Business</a></p>';
 } else {
     echo '<input type="submit" name="submit" value="Add Business" />';
 }
?>

</p>
</body>
</html>
```

Step 4. Business listing page

The page that displays the information in the database. The links on the left side of the page are created from the categories table and link back to the script, adding a category ID. The category ID forms the basis for a query on the businesses table and the biz_categories table.



Business Listings - Microsoft Internet Explorer
File
Edit
View
Favorites
Address
http://localhost/bizness/biz_listing.php?cat_id=SCHOOL
Local intranet

Business Listings

Click on a category to find business listings:

Automotive Parts and Supplies

Seafood Stores and Restaurants

Health And Beauty

Schools and Colleges

Community Sports and Recreation

5	Leardorf Beauty Salon and Academy	123 Any Street	Toronto	(555) 123-4567	http://www.google.com	5	SCHOOL
6	Auto School	123 Some Street	Gainsville	(999)555-1234	http://www.autoschool.net	6	SCHOOL

```
<html>
<head>
<title>
<?php
 $doc_title = 'Business Listings';
 echo "$doc_title\n";
?>
</title>
</head>
<body>
<h1>
<?= $doc_title ?>
</h1>

<?php
 // establish the database connection
 require_once('db_login.php');

 $pick_message = 'Click on a category to find business listings:';
?>

<table border=0>
<tr><td valign="top">
    <table border=5>
    <tr><td class="picklist"><strong><?= $pick_message ?></strong></td></tr>
    <p>
    <?php
     // build the scrolling pick list for the categories
     $sql = "SELECT * FROM categories";
     $result = $db->query($sql);
     if (DB::isError($result)) die($result->getMessage(  ));
     while ($row = $result->fetchRow(  )){
         if (DB::isError($row)) die($row->getMessage(  ));
         echo '<tr><td class="formlabel">';
         echo "<a href=\"$PHP_SELF?cat_id=$row[0]\">";
         echo "$row[1]</a></td></tr>\n";
     }
    ?>
    </table>
</td>
<td valign="top">
     <table border=1>
     <?php
      if ($cat_id) {
        $sql = "SELECT * FROM businesses b, biz_categories bc where";
        $sql .= " category_id = '$cat_id'";
        $sql .= " and b.business_id = bc.business_id";
        $result = $db->query($sql);
        if (DB::isError($result)) die($result->getMessage(  ));
        while ($row = $result->fetchRow(  )){
          if (DB::isError($row)) die($row->getMessage(  ));
          if ($color == 1) {
            $bg_shade = 'dark';
            $color = 0;
          } else {
            $bg_shade = 'light';
            $color = 1;
          }
          echo "<tr>\n";
          for($i = 0; $i < count($row); $i++) {
            echo "<td class=\"$bg_shade\">$row[$i]</td>\n";
          }
          echo "</tr>\n";
        }
      }
     ?>
     </table>
</td></tr>
</table>
</body>
</html>
```