WEB PROGRAMMING SCV1223

PHP : Authentication Example

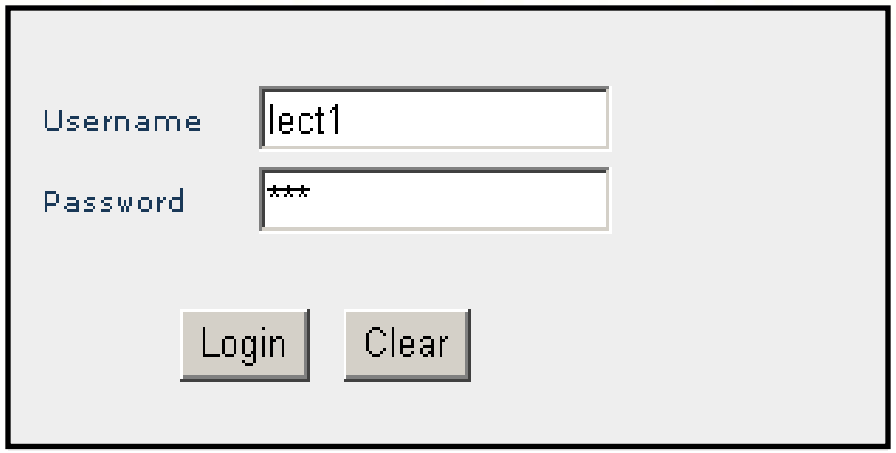
Dr. Md Sah bin Hj Salam

En. Jumail bin Taliba

Topics

- Form Handling
- Redirection
- Connecting to Database
- User Authentication
- Session Authentication

Case study: Login

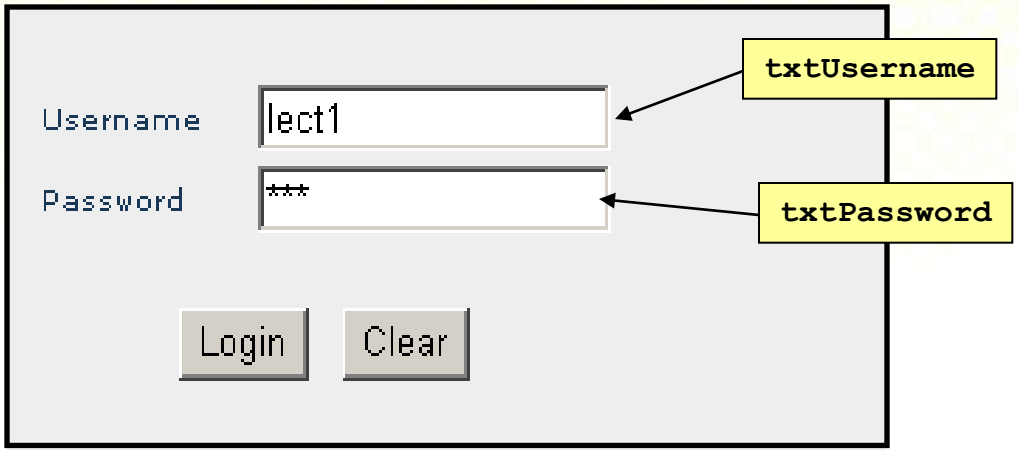


Form Handling Basics

login.html

```
<html>
<head>
  <title>Login</title>
  <link rel="stylesheet" href="styles.css">
</head>
<body>
  </b><br><br><br>

<form name='frmLogin' method='get' action='login.php'>

<table border='0' cellspacing='0' cellpadding='0'>
<tr height='30'>
   <td>Username</td>
</form>
```

Form Handling Basics (cont.)



login.php

```
<?php

  $username = $_GET["txtUsername"];
  $password = $_GET["txtPassword"];



?>
```

Redirection

Example: redirect to elearning website

```
<?php

require_once ('HTTP.php');
HTTP::redirect("http://elearning.utm.my");

?>
```

Connecting to Database

The steps:

- Connect to mysql server `mysql_connect()`
- select and open database `mysql_select_db()`
- submit query using sql statement `mysql_query()`
- read or get the query result `mysql_fetch_row()`
- Disconnect or close the database `mysql_close()`

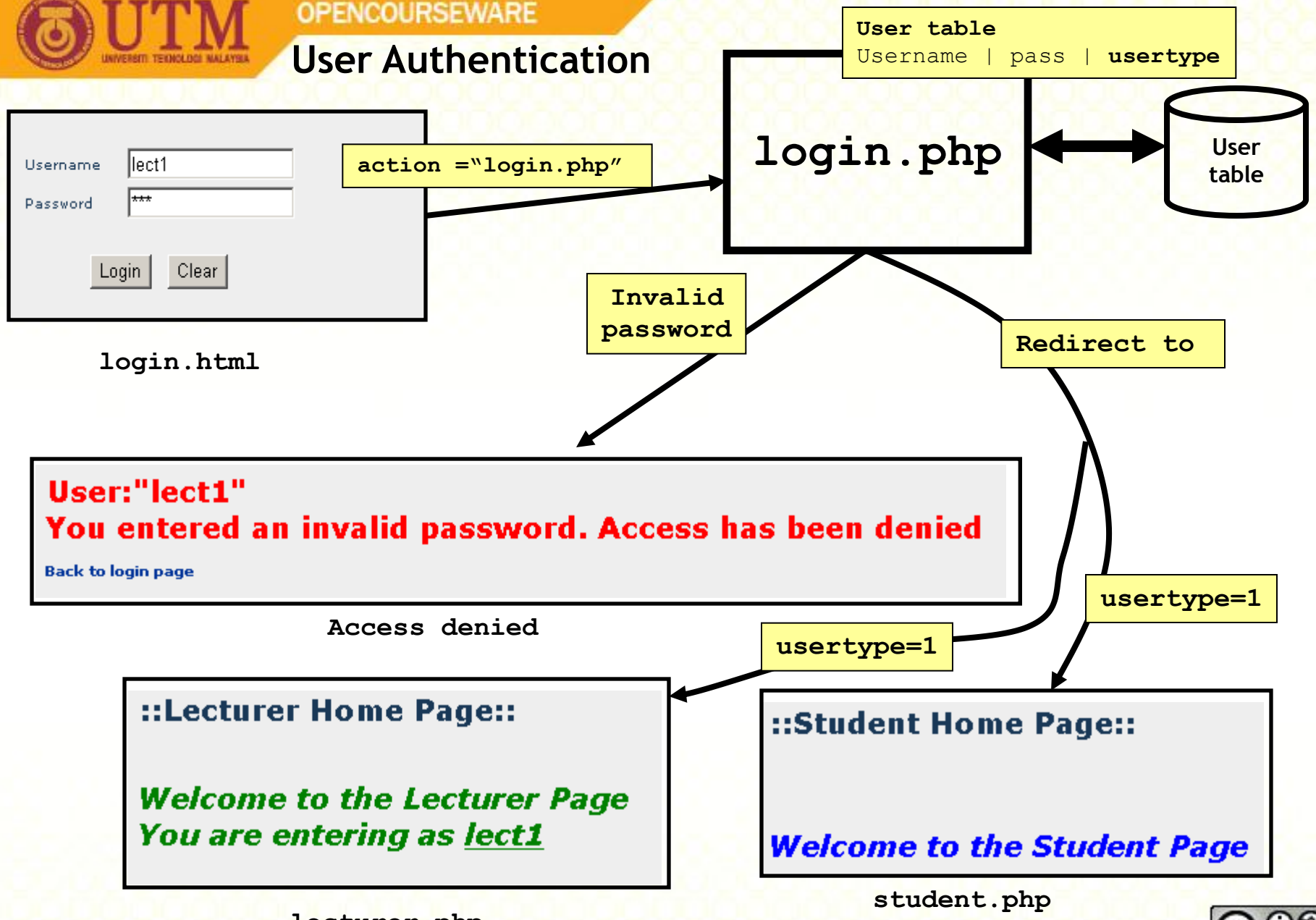
Connecting to Database (cont.)

Example: verifying username and password

```
<?php
function VerifyUser($username,$password)
{
  $conn = mysql_connect("localhost","your_login","password");
  mysql_select_db("your_db", $conn);
  $query_result = mysql_query("select * from user where
                  username='$username' and pass = Password('$password')"
                 );

  if ($query_result!=NULL)
       $row = mysql_fetch_row($query_result);

  if ($row==NULL) $usertype=0;
   else
     $usertype = $row[2];

  mysql_close($conn);

  return $usertype;
}
?>
```

```
// $usertype=1: student
// $usertype=2: lecturer
// $usertype=0: unauthorized
```

User Authentication



Sample data of `user` table

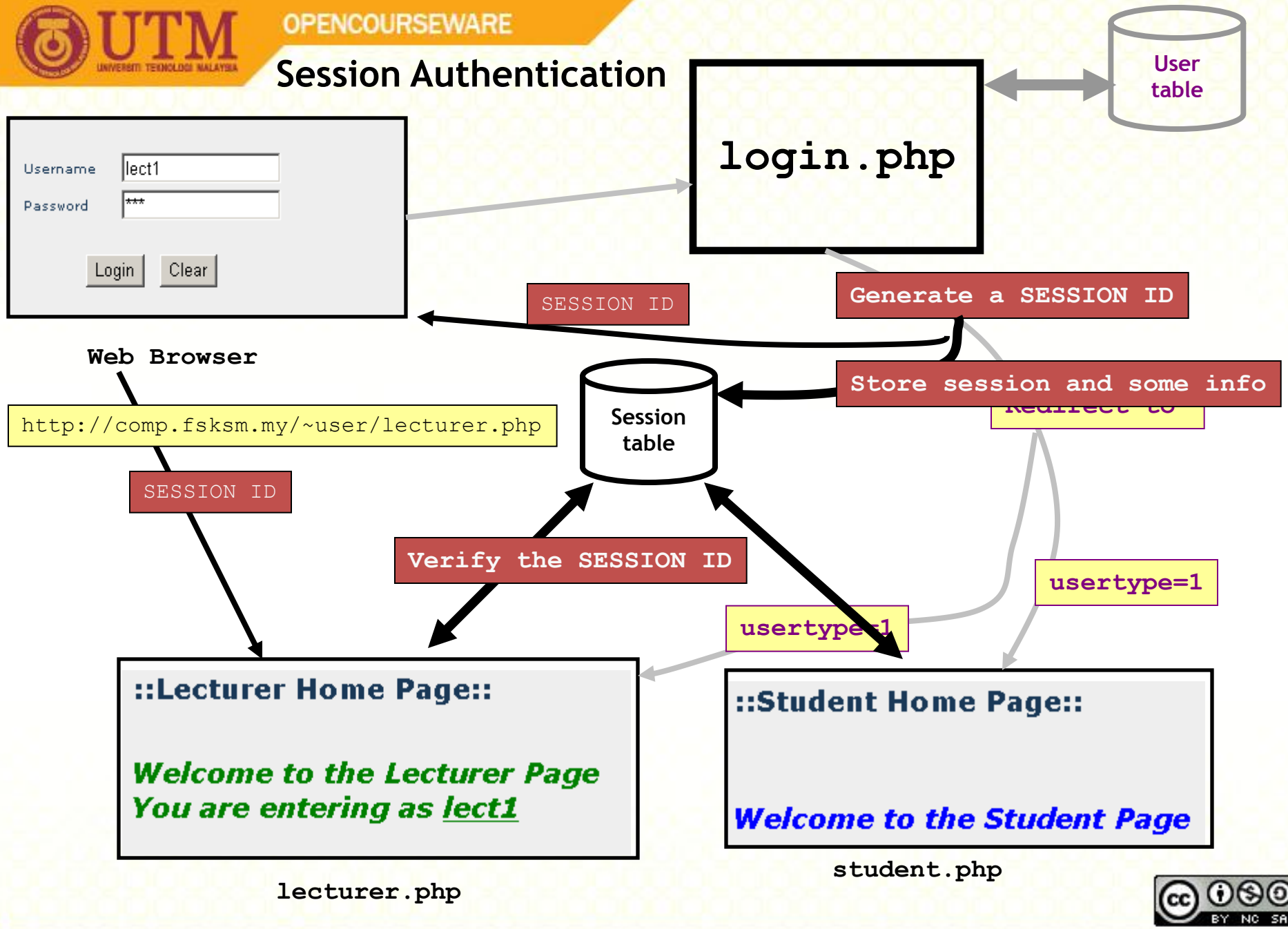
```
mysql> select * from user;
+----------+-------------------+------+
| username | pass              | type |
+----------+-------------------+------+
| stud1    | 773359240eb9a1d9 |    1 |
| lect1    | 7cd2b5942be28759 |    2 |
+----------+-------------------+------+
```

```
create table user
(
  username varchar(30),
  pass varchar(50),
  type int default 1,

  primary key (username)
);

insert into user values('stud1', Password('123'), 1);
insert into user values('lect1', Password('abc'), 2);
```

User Authentication (cont.)

```
<?php
$username = $_GET["txtUsername"];
$password = $_GET["txtPassword"];

$usertype = VerifyUser ($username,$password);

if ($usertype==0)
{ require_once ("access_denied.php");
}
else{
     require_once ('HTTP.php');

     if ($usertype==1) HTTP::redirect("student.php");
       else
          if ($usertype==2)
             HTTP::redirect("lecturer.php?username=$username");
}
```

Session Authentication



Sample data of `session` table

```
mysql> select * from session;
+--------------+------------+------------+----------+----------+
| id           | log_time   | log_from   | username | usertype |
+--------------+------------+------------+----------+----------+
| 114248433179 | 1142484331 | 10.1.0.124 | stud1    |        1 |
+--------------+------------+------------+----------+----------+
```

```
create table session
(
  id varchar(30) not null,
  log_time integer,
  log_from varchar(50),
  username varchar(30),
  usertype integer,

  primary key (id)
);
```

Generating SESSION ID

In file: session.php

```
function GenerateSessionID()
{
  $current_time = time();
  $a_number = rand(1,1000);
  $id = $current_time.$a_number;
  return $id;
}
```

Storing session and its info into database

In file: session.php

```
function StoreSession($session_id,$username,$usertype)
{
  $log_time=time();
  $log_from=$_SERVER['REMOTE_ADDR'];

  $conn = mysql_connect("localhost",“user",“pass");
  mysql_select_db(“dbase_name");
  $query_result = mysql_query("insert into session
                  values('$session_id',$log_time,
                  '$log_from', '$username', '$usertype')");
  mysql_close($conn);
}
```

Sending a copy of SESSION ID to the client

In file: login.php

```
require_once("session.php");

$session_id = GenerateSessionID();
SetCookie('SESSION_ID', $session_id);
```

Session authentication: Putting all together

In file: login.php (original)

```
<?php
$username = $_GET["txtUsername"];
$password = $_GET["txtPassword"];

$usertype = VerifyUser ($username,$password);

if ($usertype==0)
{ require_once ("access_denied.php");
}
else{
     require_once ('HTTP.php');
     if ($usertype==1) HTTP::redirect("student.php");
       else
          if ($usertype==2)
             HTTP::redirect("lecturer.php?username=$username");
}
```

Putting all together

In file: login.php (added with session features)

```
<?php
$username = $_GET["txtUsername"];
$password = $_GET["txtPassword"];

$usertype = VerifyUser ($username,$password);

if ($usertype==0)
{ require_once ("access_denied.php");
}
else{
      require_once("session.php");

      $session_id = GenerateSessionID();
      StoreSession($session_id, $username, $usertype);
      SetCookie('SESSION_ID', $session_id);

    require_once ('HTTP.php');
    if ($usertype==1) HTTP::redirect("student.php");
      else
         if ($usertype==2)
            HTTP::redirect("lecturer.php?username=$username");
}
```

Session authentication for each page

In file: lecturer.php (original)

```
<html>
<head>
  <title>Lecturer</title>
  <link rel="stylesheet" href="styles.css">
</head>
<body>
<b style='font-size:20px;'>::Lecturer Home Page::</b><br><br><br>
<br>


<b style='font-size:20px; font-style:italic; color: green'>Welcome to the
Lecturer Page <br>

You are entering as
<u>
<?php
  print( $_GET['username'] );
?>
</u> </b><br><br><br><hr>
<b>Notes: </b><i>This is only a dummy page. It's just to show you the
redirection process is working.</i>

</body>
</html>
```

Session authentication for each page

In file: lecturer.php (added with session authentication)

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

  $page_type=2;
  $session_id = $_COOKIE['SESSION_ID'];

  if (!VerifySession($session_id, $page_type) )
  {
    include ("access_denied.php");
    die();
  }
?>

<html>
<head>
  <title>Lecturer</title>
  <link rel="stylesheet" href="styles.css">
</head>
<body>
<b style='font-size:20px;'>::Lecturer Home Page::</b><br><br><br>
<br>
```

Verifying a session

In file: session.php

```
function VerifySession($session_id, $page_type)
{
  global $username, $usertype;

  $conn = mysql_connect("localhost","user","pass");
  mysql_select_db("dbase_name");
  $query_result = mysql_query("select * from session where
                  id='$session_id' and usertype=$page_type");
  if ($query_result!=NULL)
          $row= mysql_fetch_row($query_result);

  if ($row==NULL) $result=false;
   else{
        $result=true;
        $username=$row[3];
        $usertype=$row[4];
  }

  mysql_close($conn);

  return $result;
}
```

Signing Out

In file: logout.php

```
<?php
  include ("session.php");
  include ("HTTP.php");

  $session_id = $_COOKIE['SESSION_ID'];
  if ($session_id)
  {
    DeleteSession($session_id);
  }

  HTTP::redirect("login.html");
?>
```

In file: session.php

```
<?php
 function DeleteSession($session_id)
 {
   $conn = mysql_connect("localhost",“user",“pass");
   mysql_select_db(“dbase_name");
   $query_result = mysql_query("delete from session where id='$session_id'");
   mysql_close($conn);
 }
?>
```