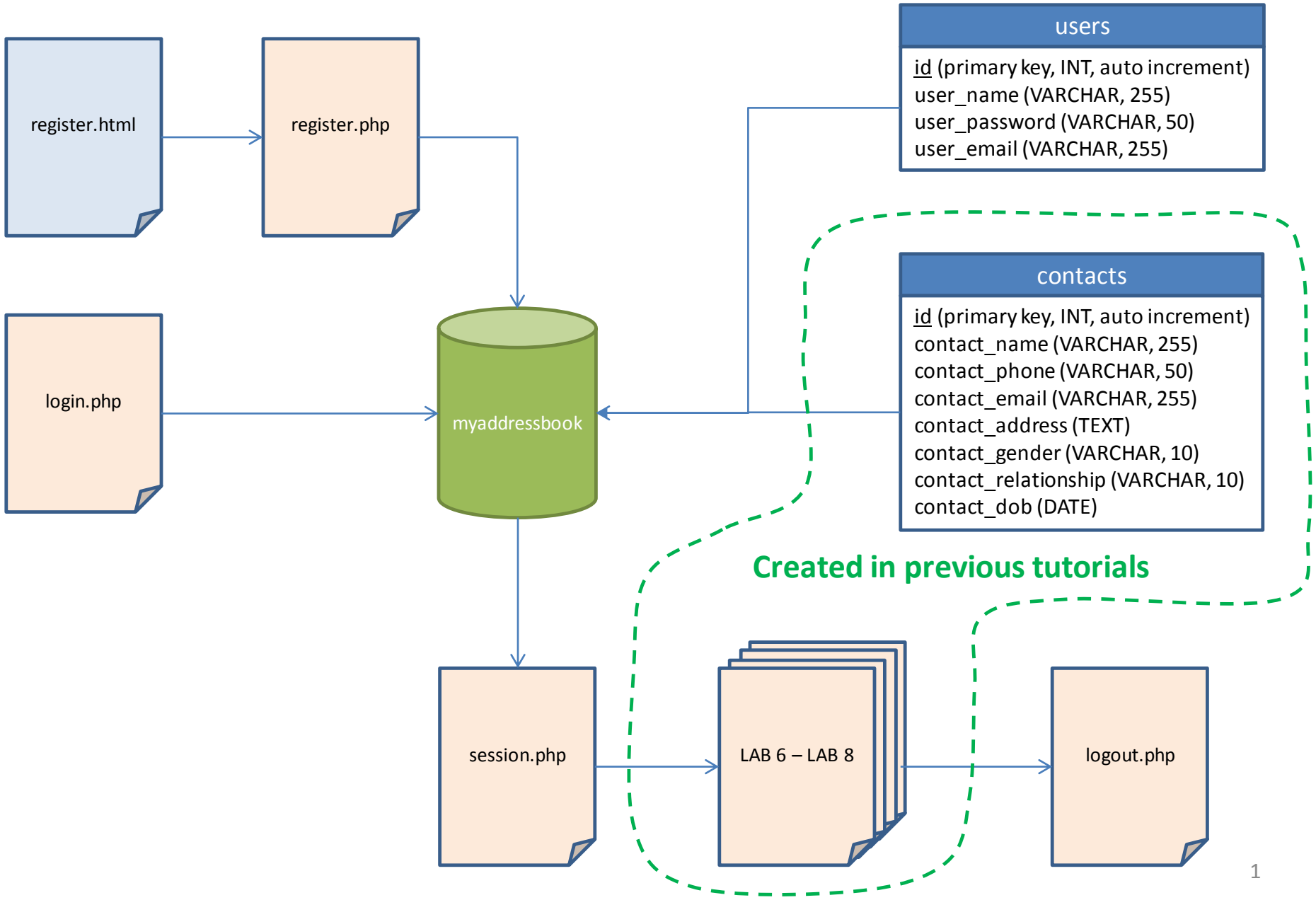
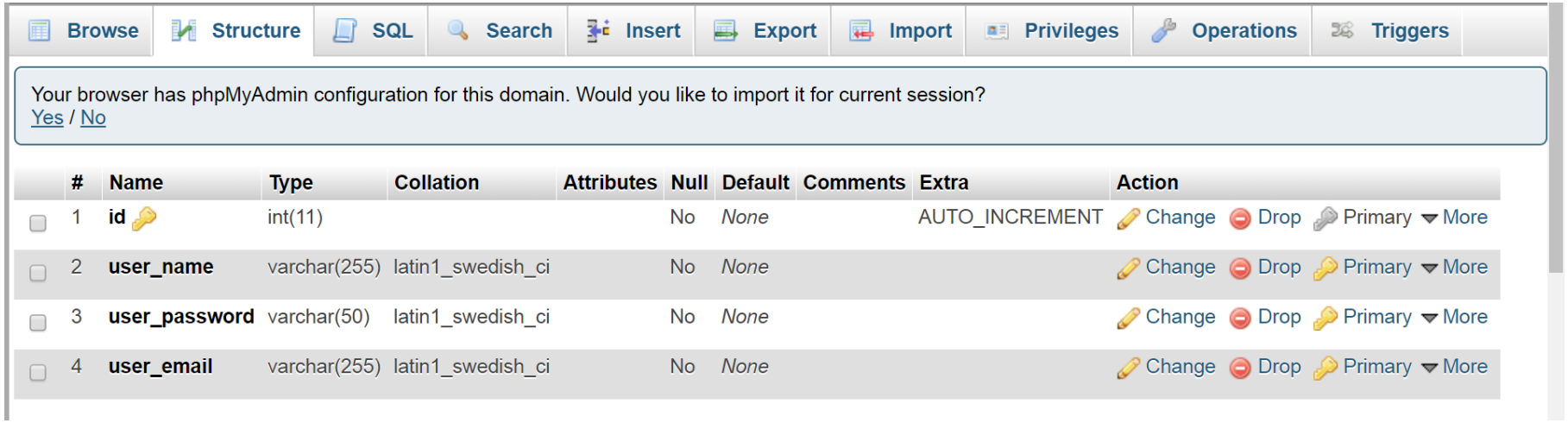

register.html
register.php
users
id (primary key, INT, auto increment)
user_name (VARCHAR, 255)
user_password (VARCHAR, 50)
user_email (VARCHAR, 255)
login.php
myaddressbook
contacts
id (primary key, INT, auto increment)
contact_name (VARCHAR, 255)
contact_phone (VARCHAR, 50)
contact_email (VARCHAR, 255)
contact_address (TEXT)
contact_gender (VARCHAR, 10)
contact_relationship (VARCHAR, 10)
contact_dob (DATE)
Created in previous tutorials
session.php
LAB 6 – LAB 8
logout.php

Add new table ‘users’

Part 1 – add new table to myaddressbook database

users
id (primary key, INT, auto increment) user_name (VARCHAR, 255) user_password (VARCHAR, 50) user_email (VARCHAR, 255)

1. Run WAMP server.
2. Open PHPMyAdmin page from the browser.
3. Access the existing database “myadddressbook”.
4. Under “myaddressbook” database, create a table named “users” as per structure below.



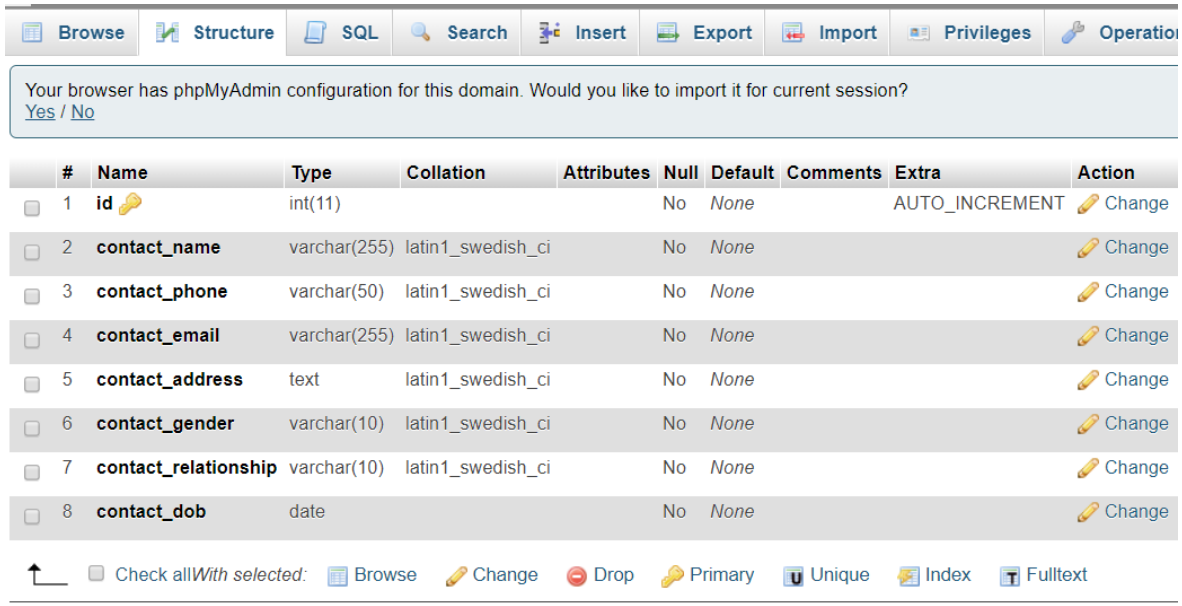
Alter ‘contacts’ table

Part 2 – add ‘user_id’ in table ‘contacts’

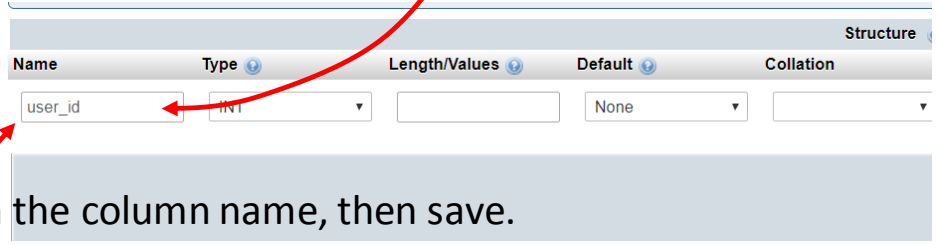
1. Access ‘contacts’ table in PHPMyAdmin

contacts
id (primary key, INT, auto increment)
contact_name (VARCHAR, 255)
contact_phone (VARCHAR, 50)
contact_email (VARCHAR, 255)
contact_address (TEXT)
contact_gender (VARCHAR, 10)
contact_relationship (VARCHAR, 10)
contact_dob (DATE)
user_id (INT)

This user_id is to identify the contact information is belong to which user in ‘users’ table. It’ll contain the id from table ‘users’



Click ‘Go’

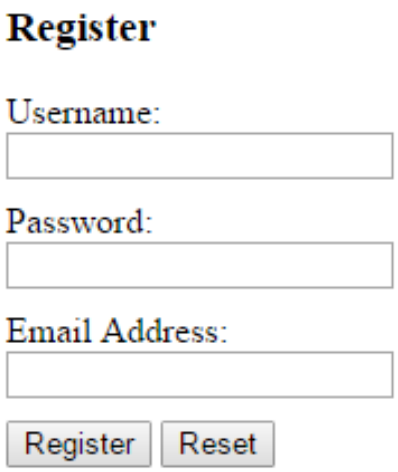


Fill in the column name, then save.

Securing you Web Application with Authorization & Authentication

Part 3 – Creating a registration page (to store user data to log in to web application)

1. Create a table named ‘users’ in ‘myaddressbook’ database with the fields as in page 1.
2. Create ‘register.html’ page with the UI as below:

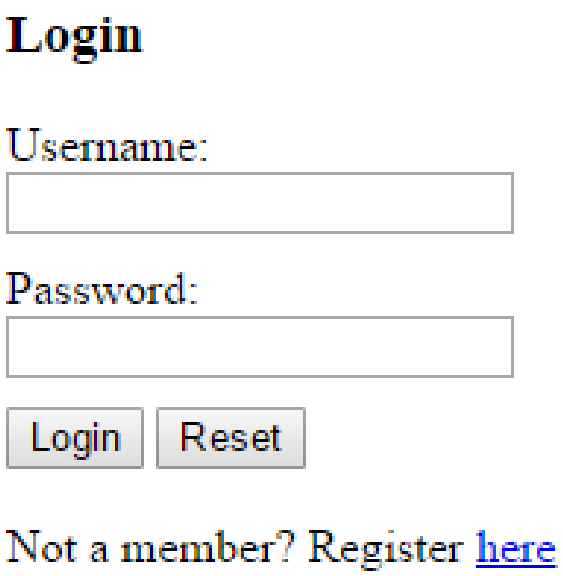


3. Create ‘register.php’ to process the registration form in Step 2. (note: for the code, you may refer to insert.php)

Securing you Web Application with Authorization & Authentication

Part 4 – Login & Session

1. Create ‘login.php’ page with the UI as below:



Securing you Web Application with Authorization & Authentication

Part 4 – Login & Session

3. Start the session **session_start();** before <html> tag
4. Include these codes right after <body> tag of '**login.php**'

login.php

```php
<?php
include("conn.php");
if($_SERVER["REQUEST_METHOD"] == "POST")
{
// username and password sent from Form
$username=mysqli_real_escape_string($con,$_POST['username']);
$password=mysqli_real_escape_string($con,$_POST['password']);

$sql="SELECT id FROM admin WHERE username='$username' and
password='$password'";
```

The **mysqli_real_escape_string()** function escapes special characters in a string for use in an SQL statement.

Characters encoded are NUL (ASCII 0), \n, \r, \, ', ", and Control-Z.

```php
if ($result=mysqli_query($con,$sql))
{
        $rowcount=mysqli_num_rows($result);  // Return the number of rows in result set
        while($row = mysqli_fetch_array($result))  // Fetch the data row
        {
                $user_id  = $row['id']; // Fetch the data row
        }
        if($rowcount==1)
        {
                $_SESSION['mySession']=$username;  // session creation
                $_SESSION['user_id'] = $user_id; // session creation
                header("location:  view.php");
        }
        else
        {
                $error=printf("Your  Login Name or Password is invalid. Please re login<br/><br/>");
        }
}
mysqli_close($con);
}
```

login.php

Securing you Web Application with Authorization & Authentication

Part 4 – Login & Session

1. Include these codes in a new file named '**session.php**'

session.php

```
session_start();
if (!isset($_SESSION['mySession'])) // to check if session is set
{
    echo '<script>alert("Please  Login!");window.location.href="login.php";</script>';
}
else {
    $user_id = $_SESSION['user_id']; // to assign session value to a variable, so it can be used throughout the pages
}
```

2. To include 'session.php' in any pages that required user to login (i.e. view.php, edit.php, update.php, delete.php, insert.php etc.)

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

Securing you Web Application with Authorization & Authentication

Part 5 – Logout

1. Include these codes in a new file named '**logout.php**'

```
<?php
session_start();
header("location: login.php");
session_destroy();
?>
```

logout.php

2. To link 'logout.php' in any pages that allow user to logout (i.e. view.php, edit.php, delete.php etc.)

Securing you Web Application with Authorization & Authentication

Part 6 – Filter view.php, insert.php, edit.php update.php and delete.php to only show, insert, edit, update and delete contacts who are belongs to the login user.

1. Open view.php page and amend SQL Query to this

```
SELECT * FROM contacts WHERE user_id = $user_id
```

2. Open insert.php page and amend SQL Query to this

```
INSERT INTO contacts (contact_name, contact_phone, contact_email, contact_address,
contact_gender, contact_relationship, contact_dob, user_id)

VALUES

('$_POST[name]','$_POST[phone_num]','$_POST[email_address]','$_POST[home_address]','$_POST[
gender]', '$_POST[relationship]','$_POST[dob]', $user_id)
```

Securing you Web Application with Authorization & Authentication

3. Open edit.php page and amend SQL Query to this

```
SELECT * FROM contacts WHERE id=$id AND user_id=$user_id
```

4. Open insert.php page and amend SQL Query to this

```
UPDATE contacts SET
        contact_name='$_POST[name]',
        contact_phone='$_POST[phone_num]',
        contact_email='$_POST[email_address]',
        contact_address='$_POST[address]',
        contact_gender='$_POST[gender]',
        contact_relationship='$_POST[relationship]',
        contact_dob='$_POST[dob]'
WHERE
        id=$_POST[id] AND user_id=$user_id
```

5. Open insert.php page and amend SQL Query to this

```
DELETE FROM contacts WHERE id=$id AND user_id=$user_id
```

Lab 9 Submission

Please provide the URL of Lab 9 that has been hosted in free web hosting server.

Make sure the URL is pointing to the login page of your website.

For example:
https://tp830830.000webhostapp.com/myaddressbook/**login.php**

Please submit by **Sunday, 26 April 2020, 11:59 PM** via this Moodle:

https://lms2.apiit.edu.my/mod/questionnaire/view.php?id=17392

External Resources

PHP Variables
http://www.w3schools.com/php/php_variables.asp

PHP MySQL Database
http://www.w3schools.com/php/php_mysql_intro.asp

PHP 5 MySQLi Functions
http://www.w3schools.com/php/php_ref_mysqli.asp

PHP 5 Include files
http://www.w3schools.com/php/php_includes.asp

JavaScript
http://www.w3schools.com/js/