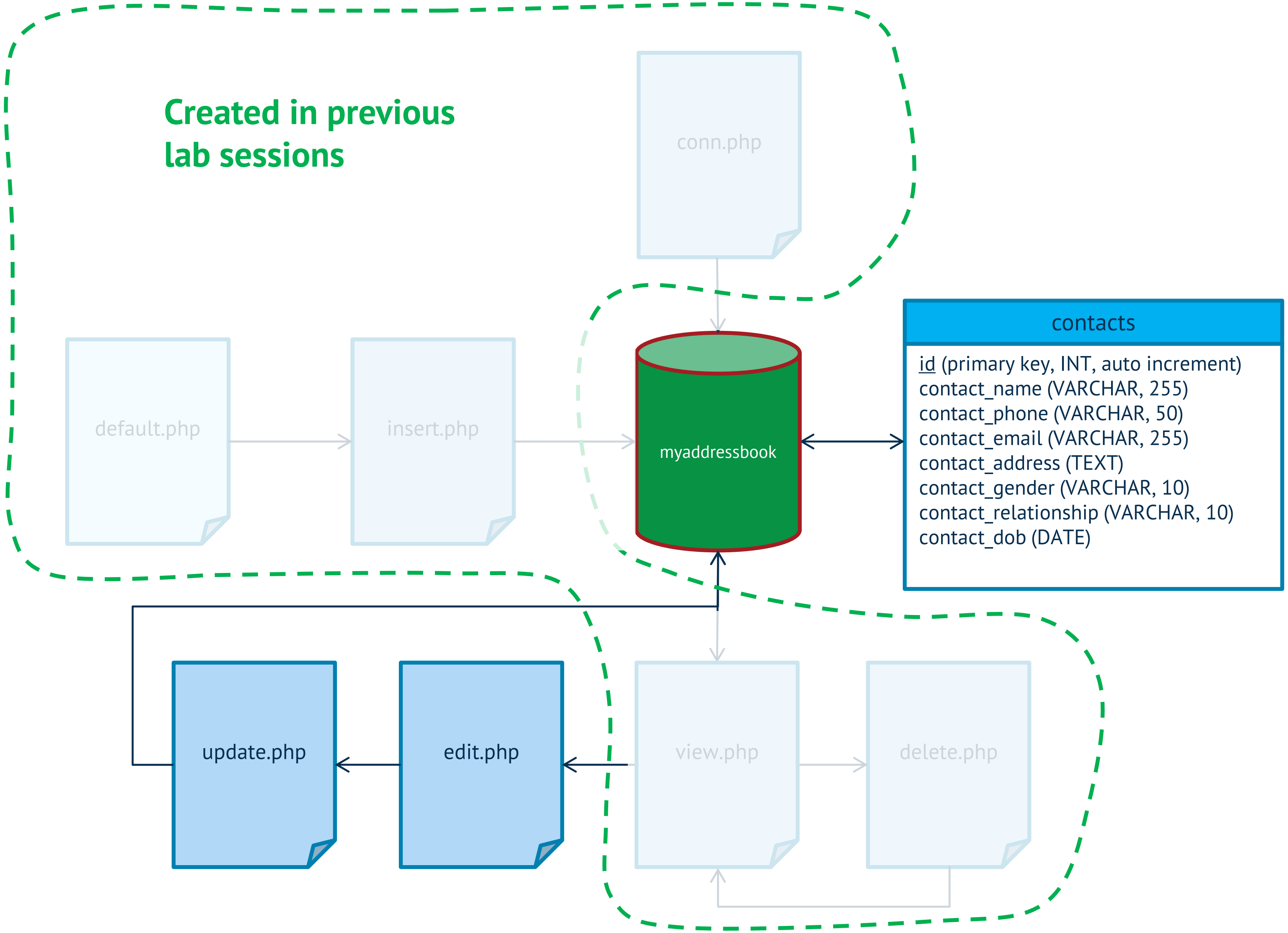
AAPP009-4-2 Web Development

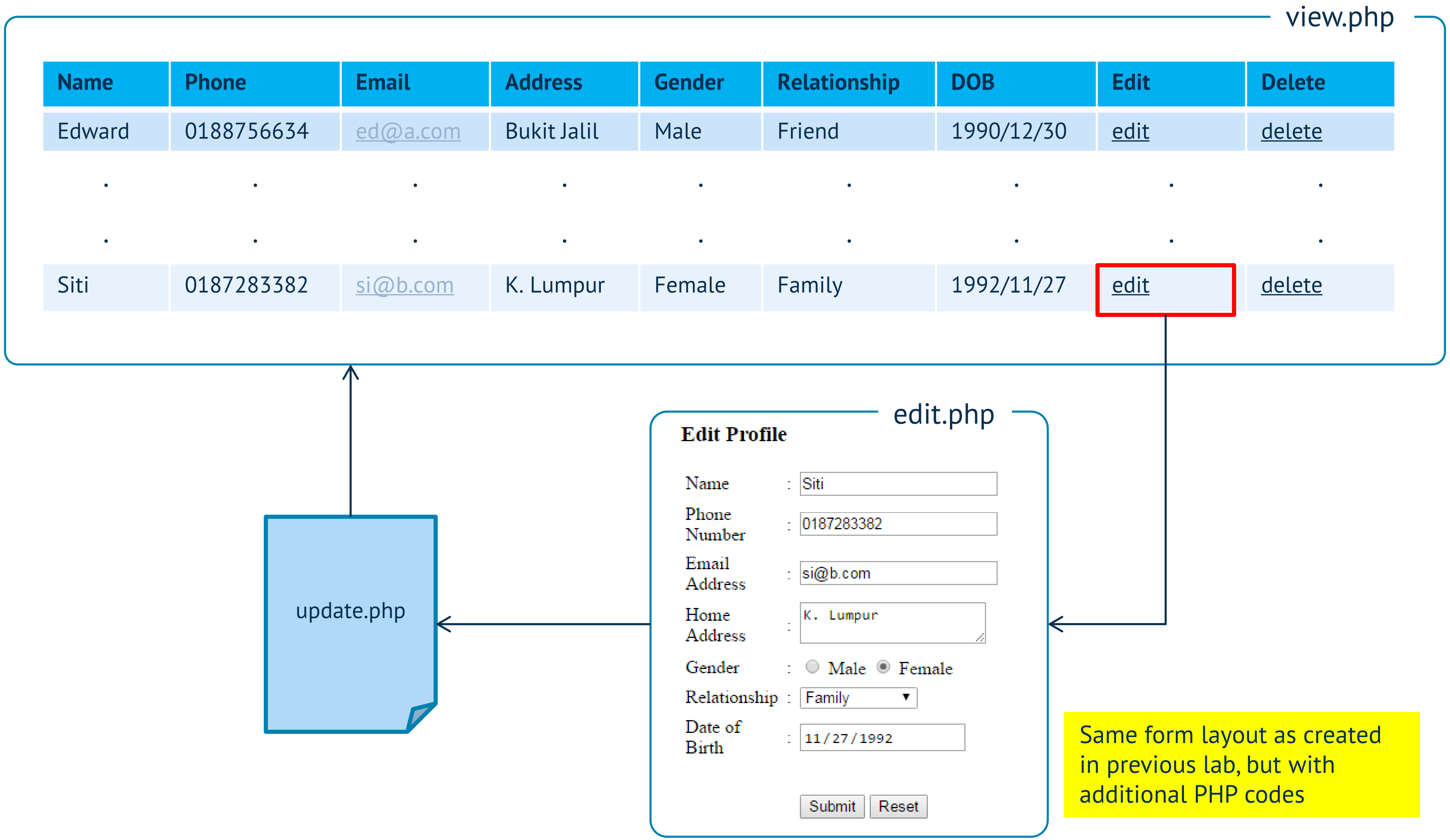
PHP & MYSQL PART 3: UPDATE QUERY, USER AUTHENTICATION & AUTHORIZATION



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)

Edit the data based on the row selection (edit.php)

1. Diagram below summarize the edit process



Name	Phone	Email	Address	Gender	Relationship	DOB	Edit	Delete
Edward	0188756634	ed@a.com	Bukit Jalil	Male	Friend	1990/12/30	edit	delete
.	.	.	.	.	.	.	.	.
.	.	.	.	.	.	.	.	.
Siti	0187283382	si@b.com	K. Lumpur	Female	Family	1992/11/27	edit	delete

Edit Profile

Name	:	Siti
Phone Number	:	0187283382
Email Address	:	si@b.com
Home Address	:	K. Lumpur
Gender	:	○ Male ● Female
Relationship	:	Family ▾
Date of Birth	:	11/27/1992

Same form layout as created in previous lab, but with additional PHP codes

edit.php

1. You may duplicate the form layout that has been created in previous lab and save it as a php file.
2. Add this codes before and after <form> tag.

```
<?php
include("conn.php");
$id = intval($_GET['id']); //intval – Get the integer value of a variable
$result = mysqli_query($con,"SELECT * FROM contacts WHERE id=$id");
while($row = mysqli_fetch_array($result))
  {
?>

<form action="update.php" method="post">
.
.
.
</form>

<?php
}
mysqli_close($con);
?>
```

edit.php – cont.

3. Add one hidden input within the <form> tag. This hidden input will be carrying id (primary key) value.

```
<input type="hidden" name="id" value="<?php echo $row['id'] ?>">
```

4. Add value attribute within the input element for the following fields:

Fields	Value
Name	value="<?php echo $row['contact_name'] ?>"
Phone number	value="<?php echo $row['contact_phone'] ?>"
Email Address	value="<?php echo $row['contact_email'] ?>"
Date of Birth	value="<?php echo $row['contact_dob'] ?>"

i.e.
```
<input type="text" name="name" required="required"   value="<?php echo $row['contact_name']  ?>" >
```

5. Add this code to display the value of the address within the textarea field.

```
<textarea required="required" name="address">   <?php echo $row['contact_address'] ?>   </textarea>
```

edit.php – cont.

6. Add this code within the ‘gender’ field radio button input to show the checked based on the value from the database. Do the same for ‘Female’ radio button.

```
<input type="radio" name="gender"          value="Male" required="required" >
```

```
<?php if ($row['contact_gender'] == "Male") {  ?>
  checked="checked"
<?php } ?>
```

7. Add this code within the ‘relationship’ field dropdown list option to show the selected list based on the value from the database. Do the same for ‘Friend’, ‘Colleague’ and ‘Other’ option.

```
<option value="Family"     >Family</option>
```

```
<?php if ($row['contact_relationship'] == "Family") { ?>
   selected="selected"
<?php } ?>
```

8. Add action="update.php" within <form> tag.

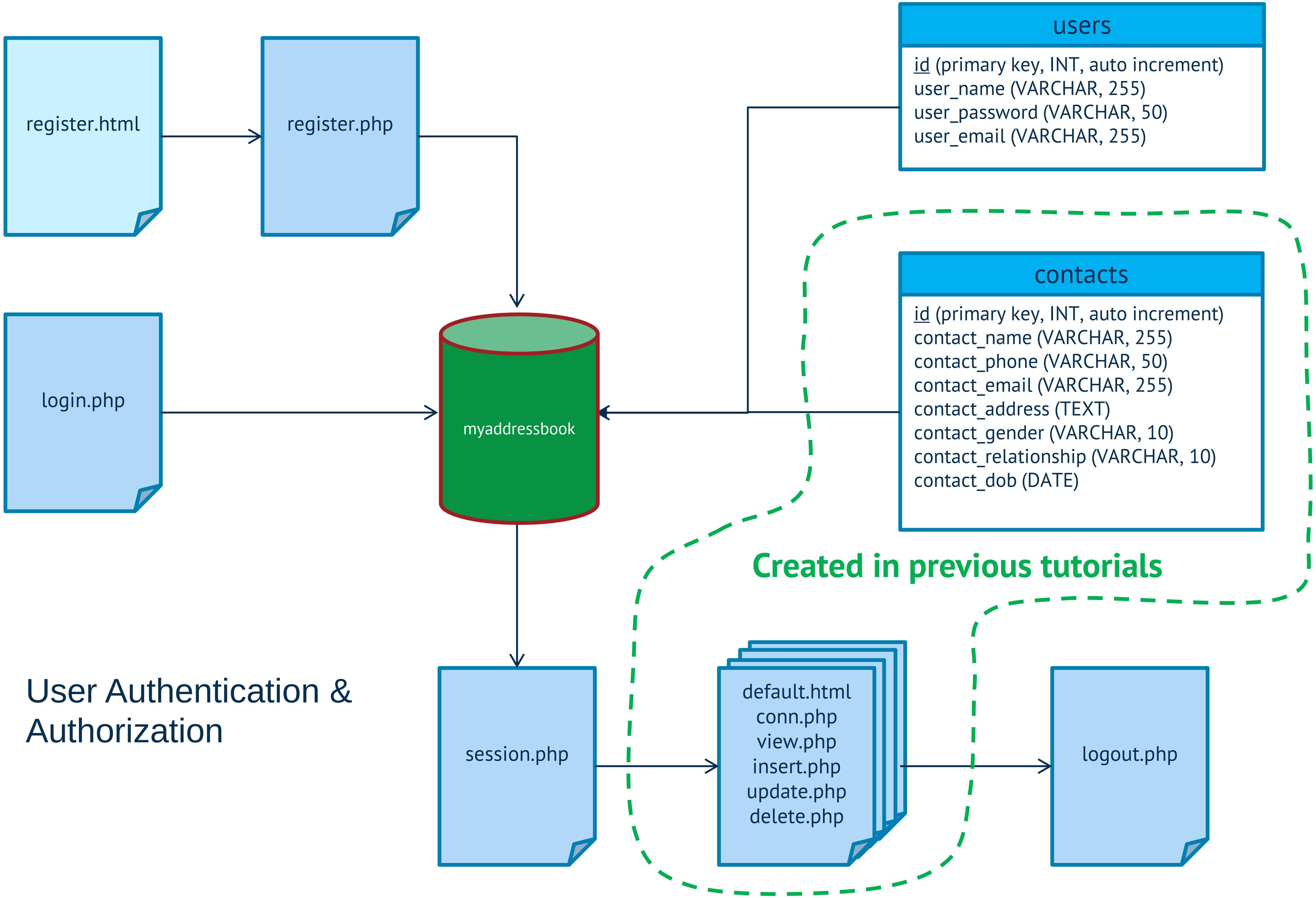
Update the edited data from the form (update.php)

1. Create a php file in Web Authoring Tool and name it as “update.php”.

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

$sql = "UPDATE contacts SET
contact_name='$_POST[name]',
contact_phone='$_POST[phone_num]',
contact_email='$_POST[email_address]',
contact_address='$_POST[home_address]',
contact_gender='$_POST[gender]',
contact_relationship='$_POST[relationship]',
contact_dob='$_POST[dob]'

WHERE id=$_POST[id];";

if (mysqli_query($con, $sql)) {
        mysqli_close($con);
        header('Location: view.php');
}
?>
```

View the outcome in the browser

User Authentication & Authorization



users

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

contacts

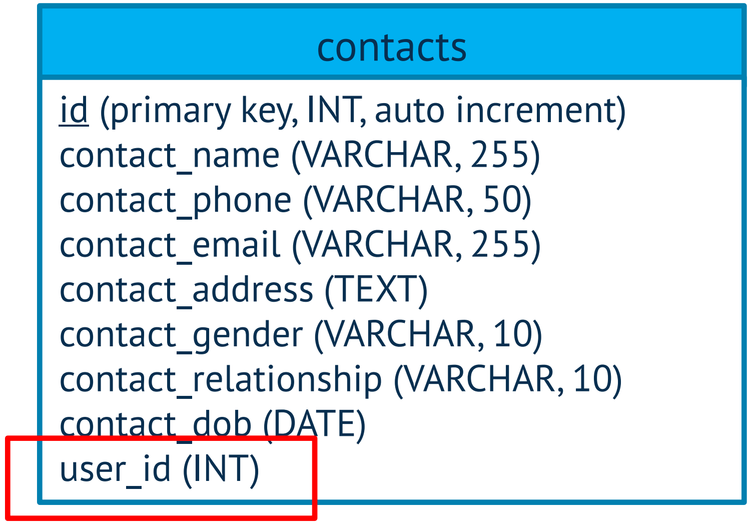
id (primary key, INT, auto increment)
contact_name (VARCHAR, 255)
contact_phone (VARCHAR, 50)
contact_email (VARCHAR, 255)
contact_address (TEXT)
contact_gender (VARCHAR, 10)
contact_relationship (VARCHAR, 10)
contact_dob (DATE)

Created in previous tutorials

Amend ‘contacts’ table

Part 1 – add Foreign Key ‘user_id’ in table ‘contacts’

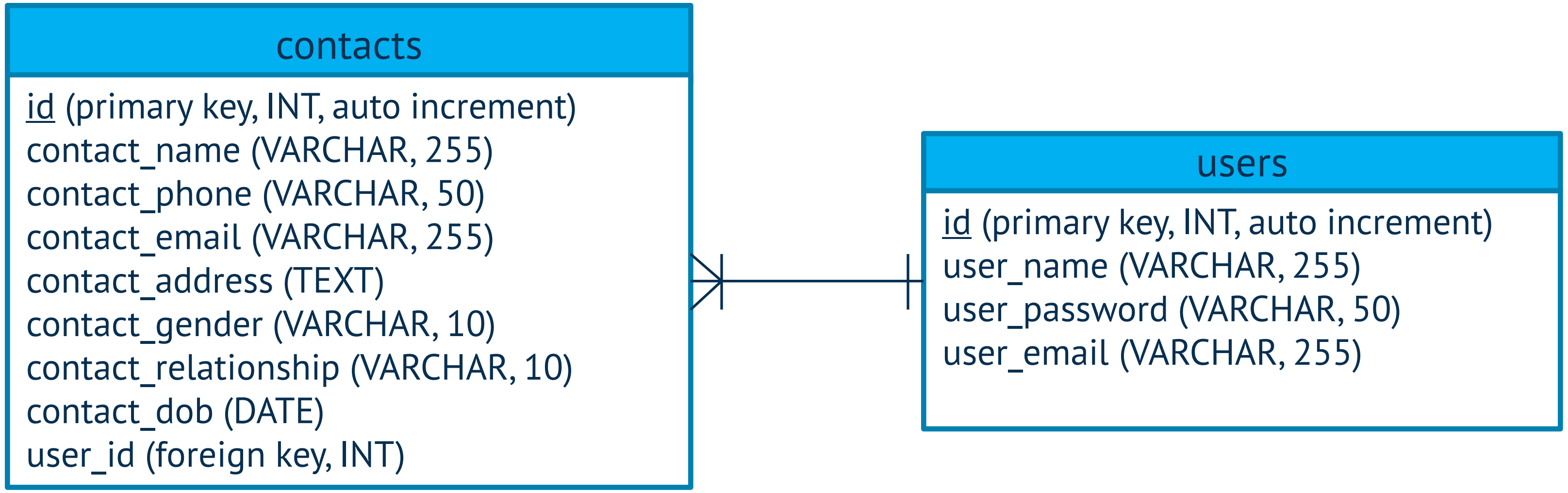
1. Access ‘contacts’ table in PHPMyAdmin



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)

Entity Relationship Diagram (ERD)



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 (foreign key, INT)

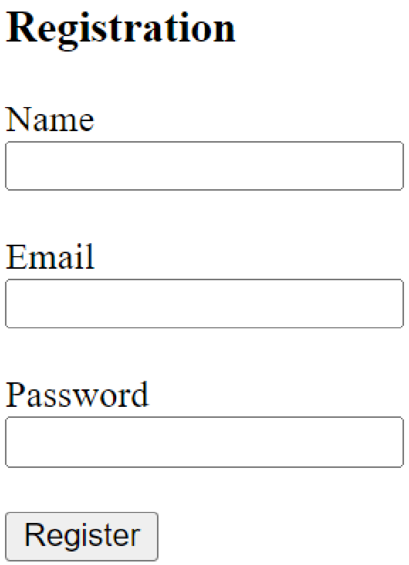
users

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

Securing you Web Application with Authorization & Authentication

Part 1 – 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:

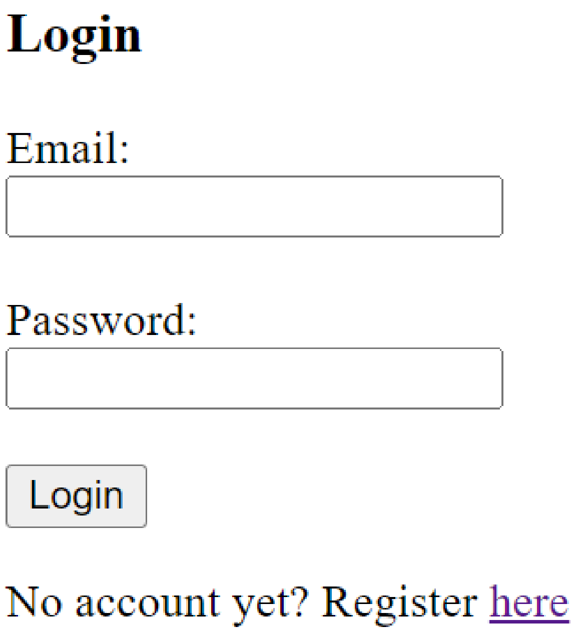


3. Create 'register.php' to process the registration form in Step 2. (note: for the code, you may refer to insert.php)

Securing you Web Application with Authorization & Authentication

Part 2 – Login

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



Login

Email:

Password:

No account yet? Register here

Securing you Web Application with Authorization & Authentication

Part 2 – Login & Session

login.php

2. Include these codes right after <body> tag of ‘**login.php**’

```
<?php
include(”conn.php”);
session_start();
if($_SERVER["REQUEST_METHOD"] == "POST")
{
// username and password sent from Form
$useremail=$_POST['useremail'];
$userpassword=$_POST[‘userpassword'];

$sql="SELECT * FROM users WHERE user_email='$useremail' and user_password=‘$userpassword'";
$result=mysqli_query($con,$sql);
//fetching a result row from the result object returned by mysqli_query()
$row = mysqli_fetch_array($result);
 // Return the number of rows in result set
$rowcount=mysqli_num_rows($result);

if($rowcount==1)  {
        $_SESSION['mySession’]=$row[‘id’];
        header("location: view.php");
}
else  {
       echo ‘<p style="color:red">Your Email or Password is invalid. Please re login</p>’;
}
mysqli_close($con);
}
?>
```

login.php

Securing you Web Application with Authorization & Authentication

Part 3 – Session

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

```
<?php
session_start();
if (!isset($_SESSION['mySession']))
{
echo '<script>alert("Please Login!"); window.location.href="login.php";</script>';
}
?>
```

session.php

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

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

Securing you Web Application with Authorization & Authentication

Part 4 – Logout

logout.php

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

```
<?php
session_start();
session_destroy();
echo '<script>alert("Successfully Logout!"); window.location.href="login.php";</script>';
?>
```

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 5 – Amend the SQL Query in insert.php, view.php and new_view.php

insert.php

```
$sql = "INSERT INTO contacts (contact_name, contact_phone, contact_email,
contact_address, contact_gender, contact_relationship, contact_dob, user_id)
VALUES
('$_POST[name]','$_POST[phone_num]','$_POST[email_address]','$_POST[home_address]',
'$_POST[gender]','$_POST[relationship]','$_POST[dob]','$_SESSION[mySession]')";
```

view.php new_view.php

```
$sql = "SELECT * FROM contacts WHERE contact_name LIKE '%".$search_key."%' AND
user_id=".$_SESSION['mySession'];
```

The purpose of including the user_id in the SQL query:

1. To **filter the contact list** so that it displays only the contacts associated with the currently logged-in user.
2. To **assign ownership** of any new contacts added to the database to the user who is currently logged in.