

Exercise models for web Pen-Test system

MODEL A step by step installation

Resources	Sender(attacker)	Receiver(victim)	Homepage
OS	Ubuntu	Windows	
IP address			
URL			http://localhost:8080/
Web browser	Ubuntu	Chrome	
CSS language			
Web server			Apache
Web application			PHP
DB server script			MySQL

Install web server (if necessary) => screen shot and explain in detail

```

1 <?php
2
3 define('ROOTDIR', realpath(dirname(__DIR__)).DIRECTORY_SEPARATOR);
4 define('APPNAME', 'My Phonebook');
5
6 // Turn off error display in production
7 ini_set('display_errors', 1);
8 ini_set('display_startup_errors', 1);
9 error_reporting(E_ALL);
10
11 require_once ROOTDIR.'vendor/autoload.php';
12 require_once ROOTDIR.'db.php';
13
14 session_start();
15
16 use \App\Router;
17
18 if (! ob_get_level()) {
19     ob_start();
20 }
21
22 // Auth routes
23 Router::post('/logout', '\App\Controllers\Auth\LoginController@logout');
24 Router::get('/register', '\App\Controllers\Auth\RegisterController@showRegisterForm');
25 Router::post('/register', '\App\Controllers\Auth\RegisterController@register');
26 Router::get('/login', '\App\Controllers\Auth\LoginController@showLoginForm');
27 Router::post('/login', '\App\Controllers\Auth\LoginController@login');
28
29 // Contact routes
30 Router::get('/', '\App\Controllers\ContactsController@index');
31 Router::get('/home', '\App\Controllers\ContactsController@index');
32
33 Router::get('/contacts/add', '\App\Controllers\ContactsController@add');
34 Router::post('/contacts', '\App\Controllers\ContactsController@create');
35
36 Router::get('/contacts/edit/{:num}', '\App\Controllers\ContactsController@edit');
37 Router::post('/contacts/{:num}', '\App\Controllers\ContactsController@update');
38 Router::post('/contacts/delete/{:num}',
39     '\App\Controllers\ContactsController@delete');
40
41
42 Router::error('\App\Controllers\Controller@notFound');
43
44 Router::dispatch();
45
46 ob_end_flush();
47
  
```

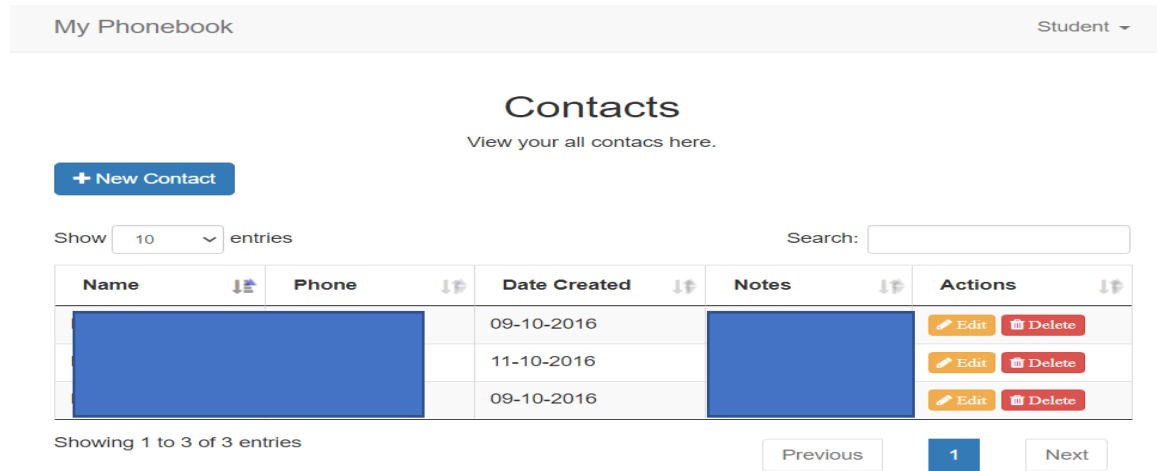
Figure 1: File index.php inside web server setup folder

① **Install web application => screen shot and explain in detail**

The web application is a Phonebook. Each user will have their own list of contacts and

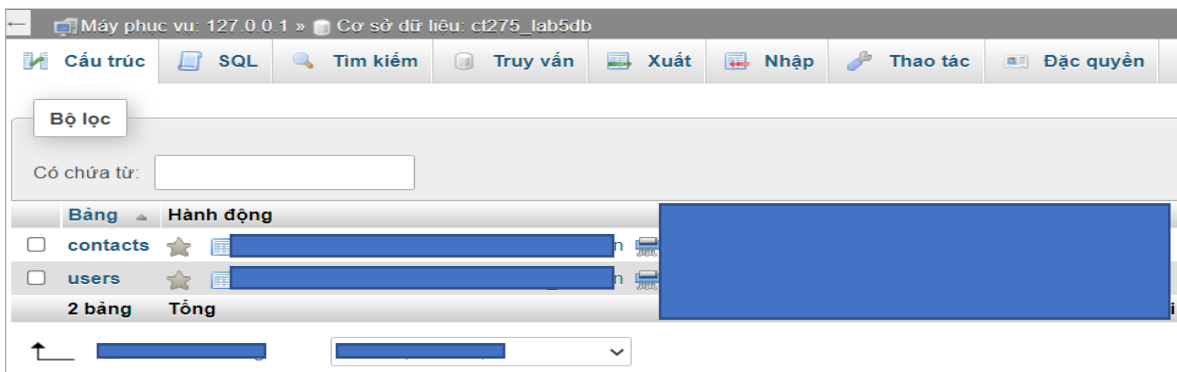
information.

When user log in to the system, they can create, edit, delete their list and manage their contacts easily.



② Install SQL DB server => screen shot and explain in detail

Inside database, there are two table, one for users information, other for contacts informations.



③ Develop client log in screen (if necessary) => screen shot and explain in detail

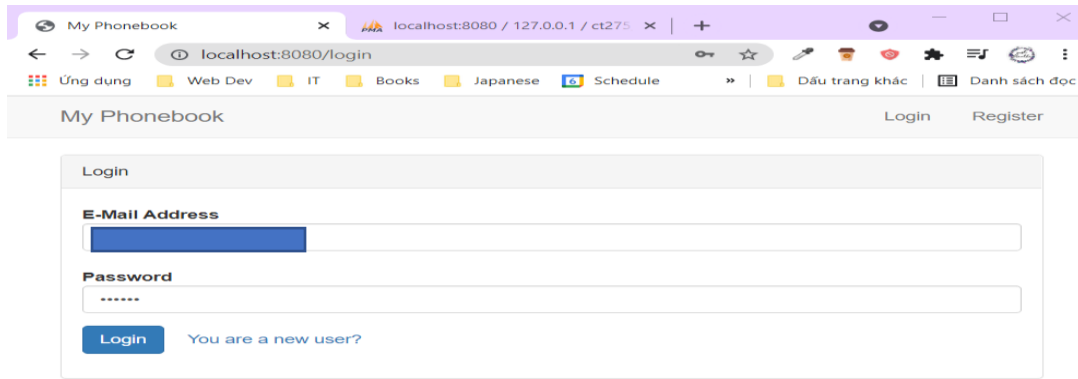


Figure 2: Client login screen

If user is already login then it won't show this login form. Otherwise, it collect data such as message, form, errors.

Then it will echo these data to show in client login screen.

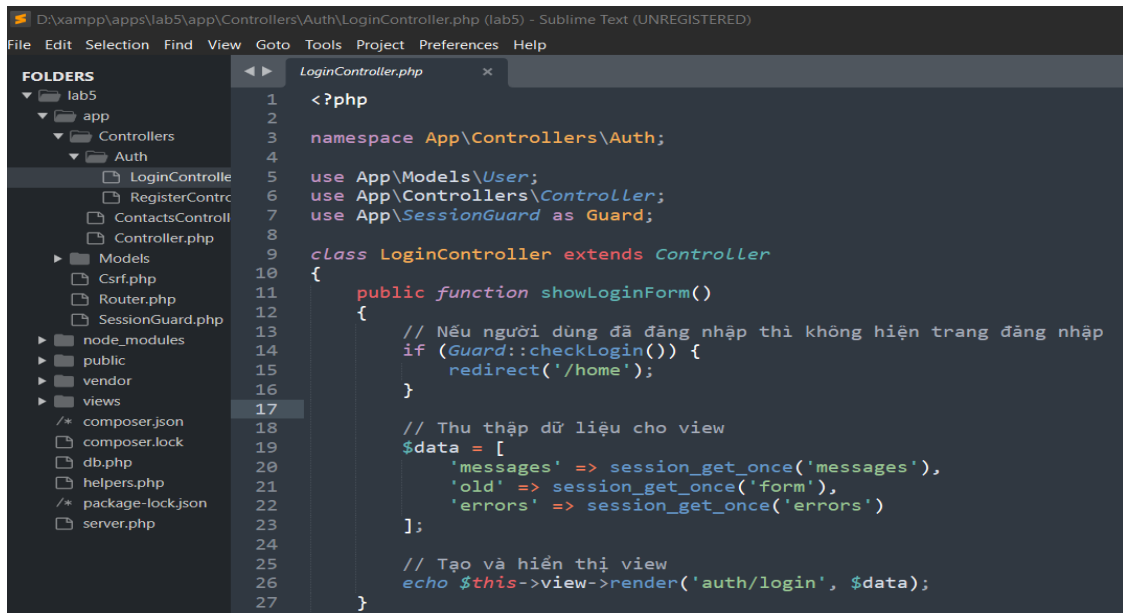


Figure 3: Function to show login form

Login function will collect information that user entered login form and check if it has been in User table of database.

It will print an error in the screen if it can't find matching email or password. If all the information matching, it will direct to home page.

```
D:\xampp\apps\lab5\app\Controllers\Auth\LoginController.php (lab5) - Sublime Text (UNREGISTERED)
File Edit Selection Find View Goto Tools Project Preferences Help

FOLDERS
└─ lab5
  └─ app
    └─ Controllers
      └─ Auth
        └─ LoginController.php
          └─ RegisterContr...
            └─ ContactsControll...
              └─ Controller.php
                └─ Models
                  └─ Csrf.php
                    └─ Router.php
                      └─ SessionGuard.php
                        └─ node_modules
                          └─ public
                            └─ vendor
                              └─ views
                                └─ /* composer.json
                                  └─ composer.lock
                                    └─ db.php
                                      └─ helpers.php
                                        └─ /* package-lock.json
                                          └─ server.php

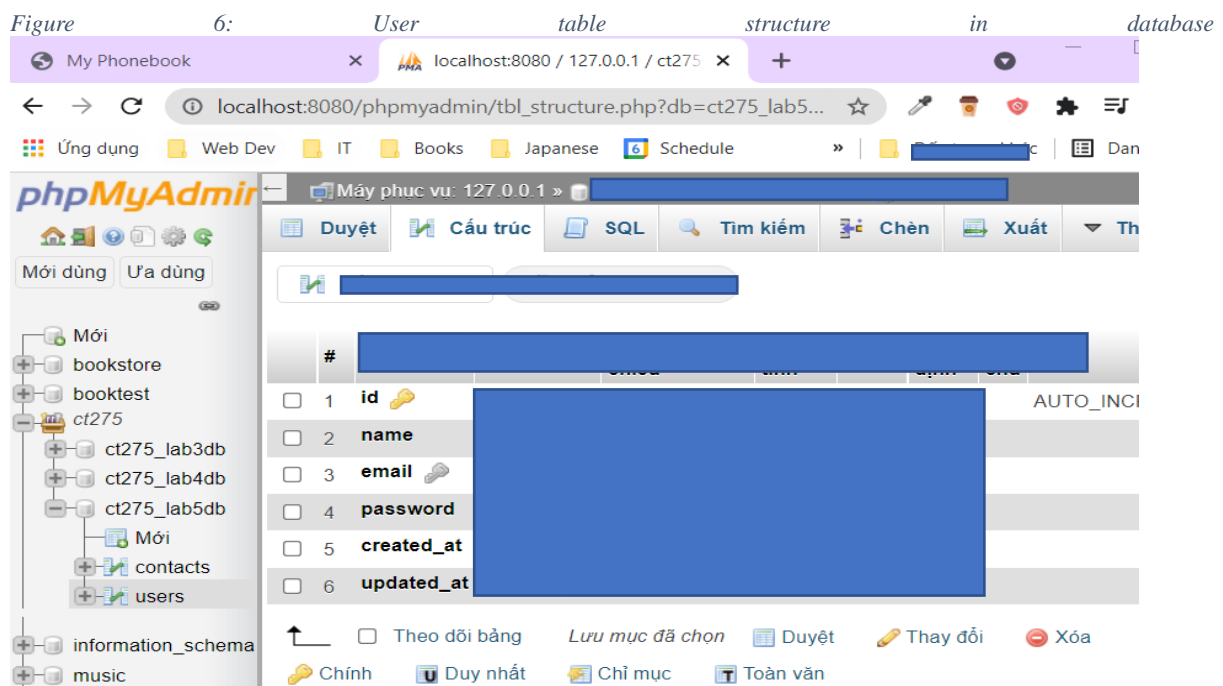
LoginController.php
28
29
30 public function login()
31 {
32     // Ngăn ngừa tấn công CSRF
33     $this->invokeCsrfGuard();
34
35     // Đọc giá trị của form
36     $userCredentials = $this->getUserCredentials();
37
38     $errors = [];
39     $user = User::where('email', $userCredentials['email'])->first();
40     if ($user === null) {
41         // Người dùng không tồn tại...
42         $errors['email'] = 'Unknown email.';
43     } else if (Guard::login($user, $userCredentials)) {
44         // Đăng nhập thành công...
45         redirect('/home');
46     } else {
47         // Sai mật khẩu...
48         $errors['password'] = 'Incorrect password.';
49     }
50
51     // Đăng nhập không thành công...
52     $this->saveFormValues(['password']);
53     redirect('/login', ['errors' => $errors]);
54 }
55
56 public function logout()
57 {
58     Guard::logout();
59     redirect('/login');
60 }
61
62 protected function getUserCredentials()
63 {
64     return [
65         'email' => filter_var($_POST['email'], FILTER_VALIDATE_EMAIL),
66         'password' => $_POST['password']
67     ];
68 }
69 }
```

Figure 4: login function and getUserCredentials function

- ④ Creat SQL DB table(sharing with group table or not?) => screen shot and explain in detail

```
db.php
1  <?php
2
3  use Illuminate\Database\Capsule\Manager as Capsule;
4
5  $capsule = new Capsule;
6
7  $capsule->addConnection([
8      'driver' => 'mysql',
9      'host' => 'localhost',
10     'database' => 'ct275_lab5db',
11     'username' => 'root',
12     'password' => '',
13     'charset' => 'utf8',
14     'collation' => 'utf8_unicode_ci',
15     'prefix' => '',
16 ]);
17
18 $capsule->setAsGlobal();
19 $capsule->bootEloquent();
20
```

Figure 5: Database configuration file



- ⑤ Creat test data(ID,PW data,sharing with group table or not?) => screen shot and explain in detail

The screenshot shows a web browser window with the address bar displaying 'localhost:8080/register'. The page title is 'My Phonebook'. The registration form is titled 'Register' and contains the following fields:

- Name:** A text input field containing the value 'meimei'.
- E-Mail Address:** A text input field with a blue placeholder or redacted content.
- Password:** A password input field with six dots indicating masked characters.
- Confirm Password:** A password input field with six dots indicating masked characters.

A blue 'Register' button is located at the bottom of the form.

Figure 7: Client register form

⑥ Connection test from client to web application

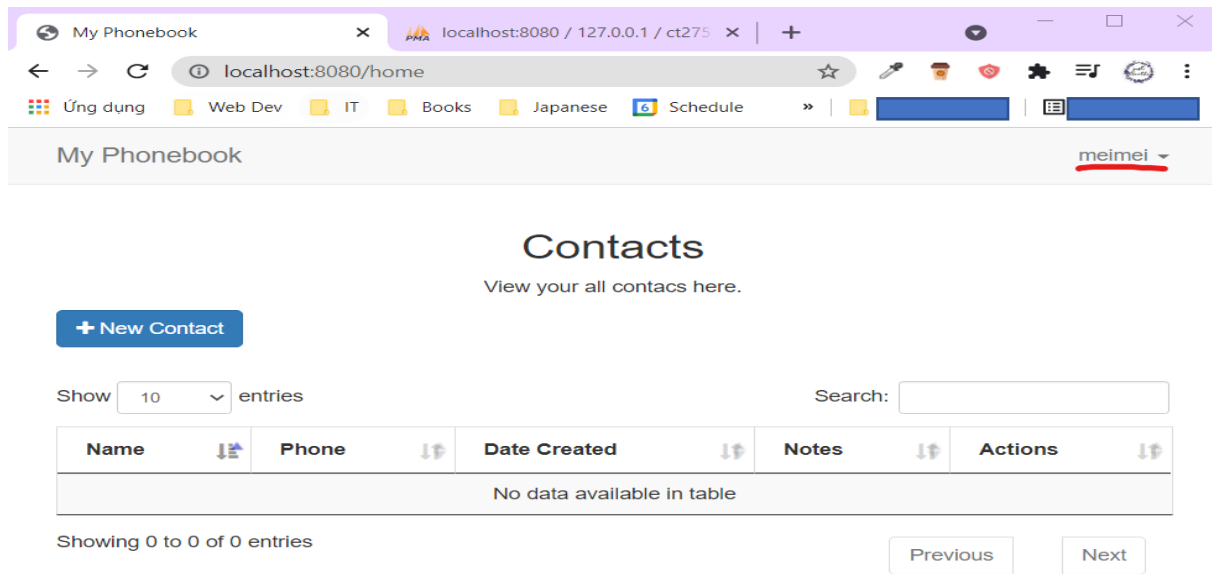
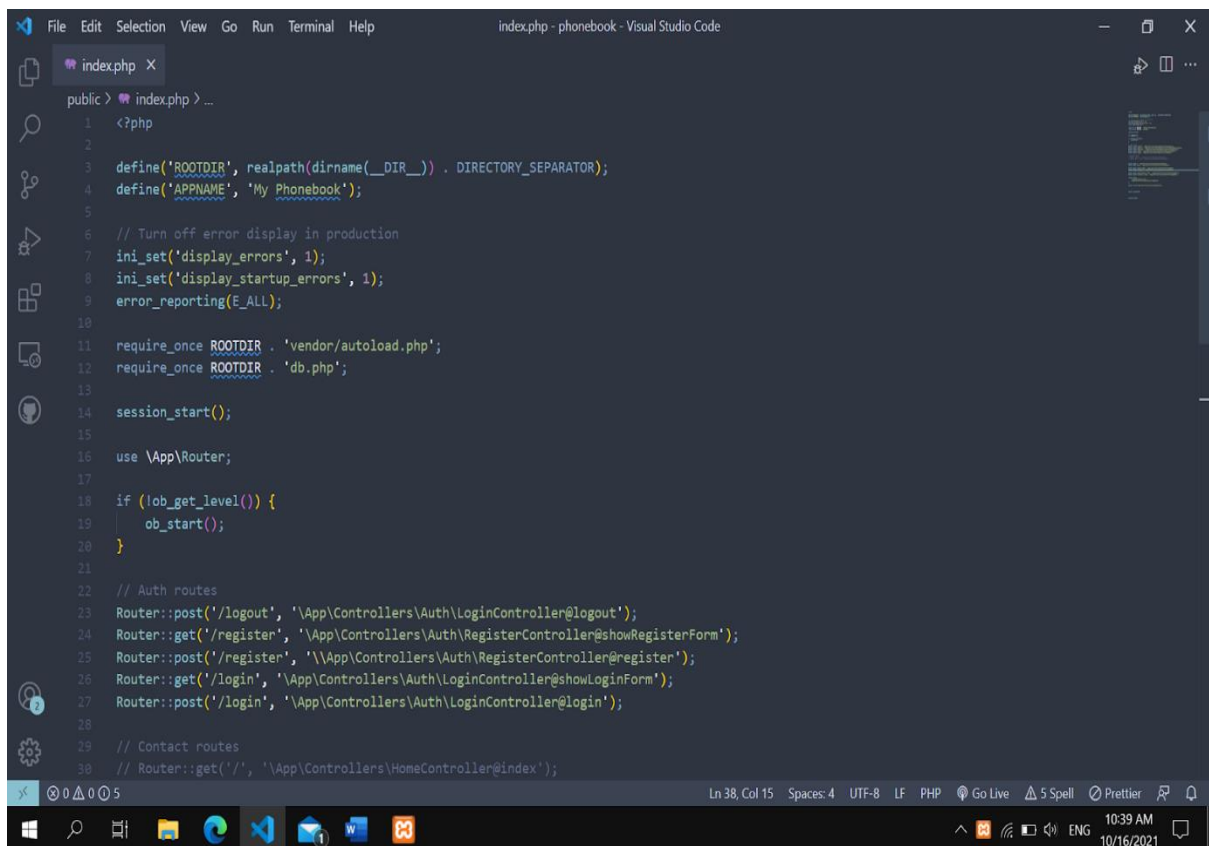


Figure 8: Login successfully with new created account

Model B step by step installation

Resources	Sender(attacker)	Receiver(victim)	Homepage
OS			Windows
IP address			127.0.0.1
URL			Localhost:80/
Web browser			Microsoft Edge
CSS language			Bootstrap
Web server			Apache
Web application			PHP
DB server script			PHPMyAdmin
Others			

1. Install web server (if necessary) => screenshot and explain in detail



```

File Edit Selection View Go Run Terminal Help
index.php - phonebook - Visual Studio Code

index.php X
public > index.php > ...
1 <?php
2
3 define('ROOTDIR', realpath(dirname(__DIR__)) . DIRECTORY_SEPARATOR);
4 define('APPNAME', 'My Phonebook');
5
6 // Turn off error display in production
7 ini_set('display_errors', 1);
8 ini_set('display_startup_errors', 1);
9 error_reporting(E_ALL);
10
11 require_once ROOTDIR . 'vendor/autoload.php';
12 require_once ROOTDIR . 'db.php';
13
14 session_start();
15
16 use \App\Router;
17
18 if (ob_get_level()) {
19     ob_start();
20 }
21
22 // Auth routes
23 Router::post('/logout', '\App\Controllers\Auth\LoginController@logout');
24 Router::get('/register', '\App\Controllers\Auth\RegisterController@showRegisterForm');
25 Router::post('/register', '\App\Controllers\Auth\RegisterController@register');
26 Router::get('/login', '\App\Controllers\Auth\LoginController@showLoginForm');
27 Router::post('/login', '\App\Controllers\Auth\LoginController@login');
28
29 // Contact routes
30 Router::get('/', '\App\Controllers\HomeController@index');
  
```

Figure 1: My Web Server

2. Install web application => screenshot and explain in detail

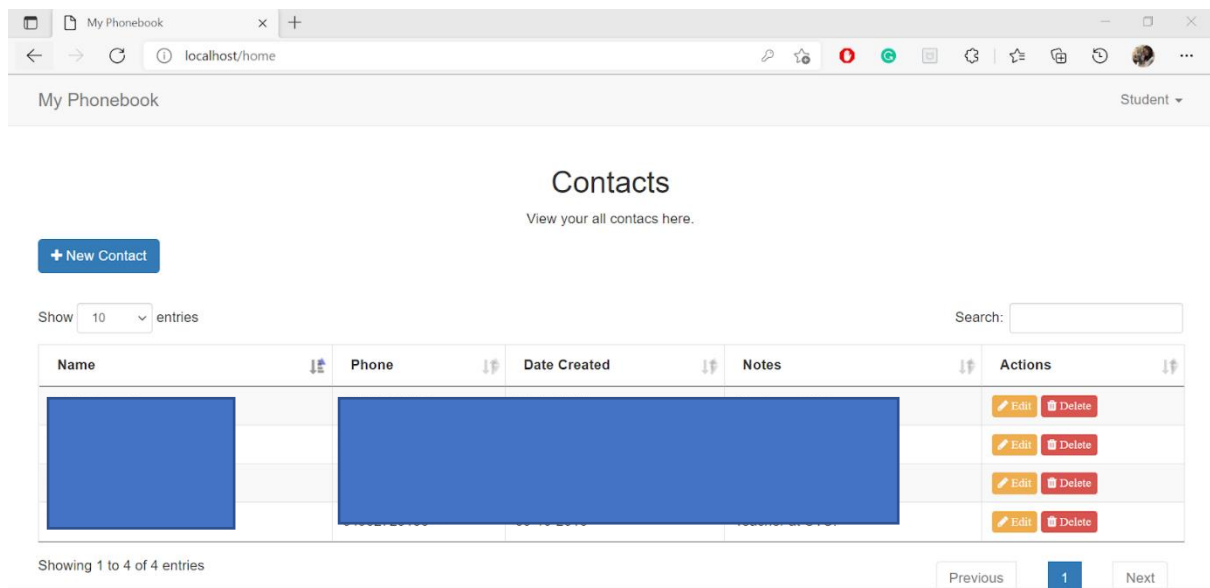


Figure 2: My Web Application PhoneBook

3. Install SQL DB server => screenshot and explain in detail

I use phpMyAdmin with SQL language to store the database of web application PhoneBook.

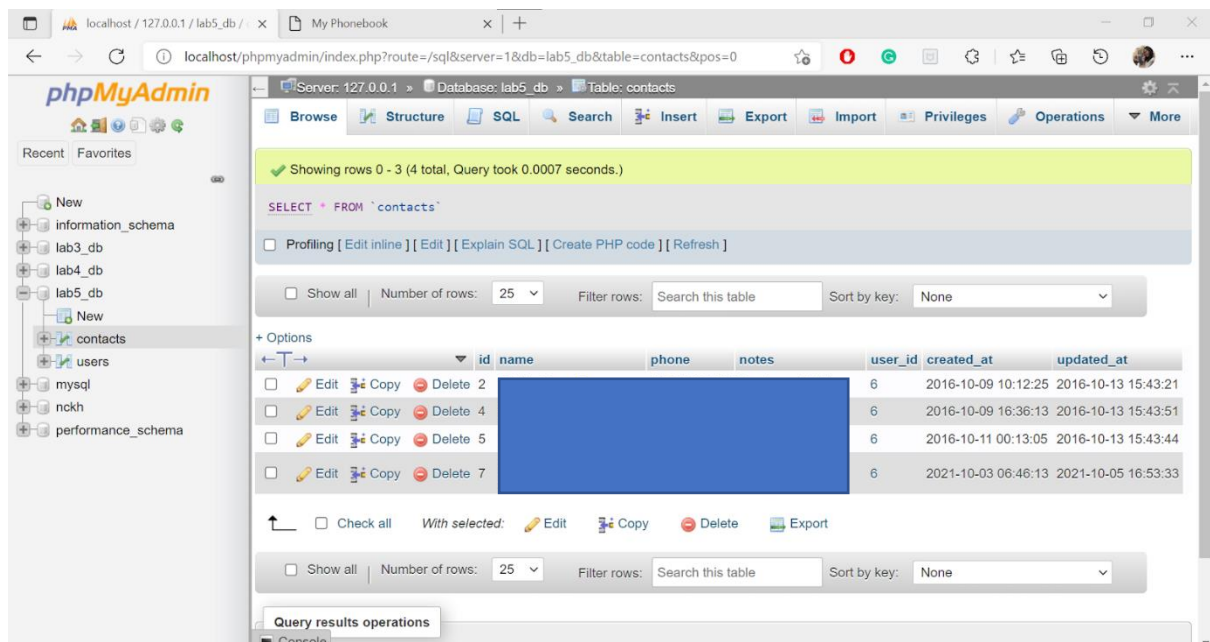


Figure 3: SQL Database Server – PHPMYAdmin

4. Develop client login screen (if necessary) => screenshot and explain in detail

Login Page allows users to login to the web application PhoneBook using email address and password

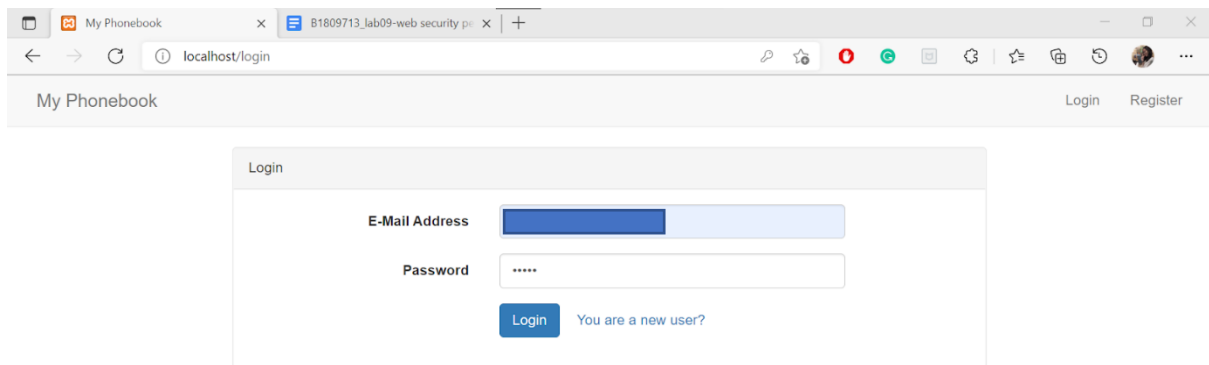


Figure 4: Login Page

5. Create SQL DB table(sharing with group table or not?) => screenshot and explain in detail

My PhoneBook created 2 table:

+ contacts: store users information includes name, phone, notes,...

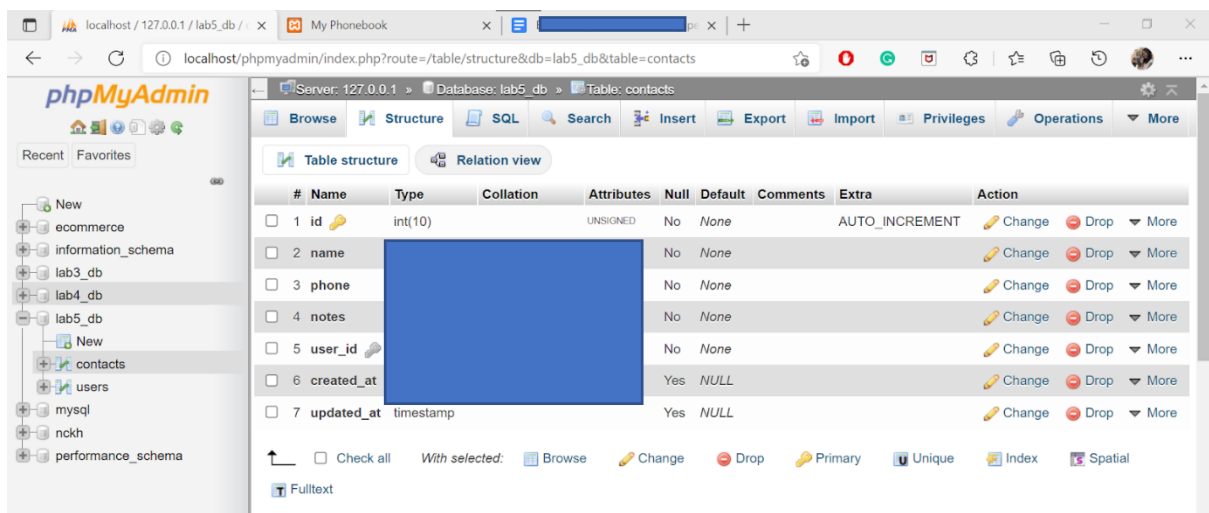
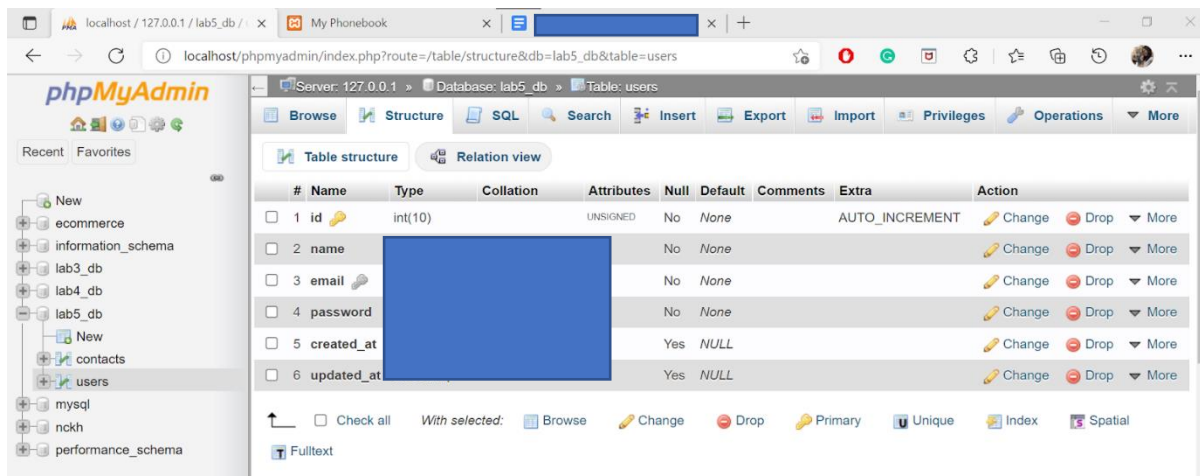


Figure 5: SQL DB – contacts table

+ users: store users' identification using for login includes name, email, passwords,..

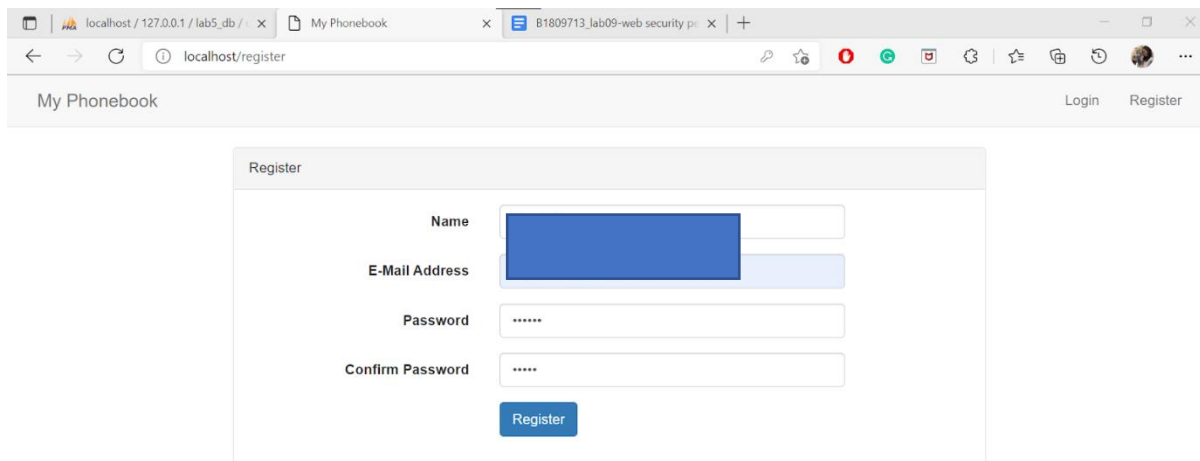


#	Name	Type	Collation	Attributes	Null	Default	Comments	Extra	Action
1	id	int(10)		UNSIGNED	No	None		AUTO_INCREMENT	Change Drop More
2	name				No	None			Change Drop More
3	email				No	None			Change Drop More
4	password				No	None			Change Drop More
5	created_at				Yes	NULL			Change Drop More
6	updated_at				Yes	NULL			Change Drop More

Figure 6: SQL DB – users table

Create test data(ID,PW data,sharing with group table or not?) => screenshot and explain in detail

I used the Register Page to test data, this page allows users to register a new account, which includes name, email address, password and confirm password in order to login to Web Application



My Phonebook

Login Register

Register

Name

E-Mail Address

Password

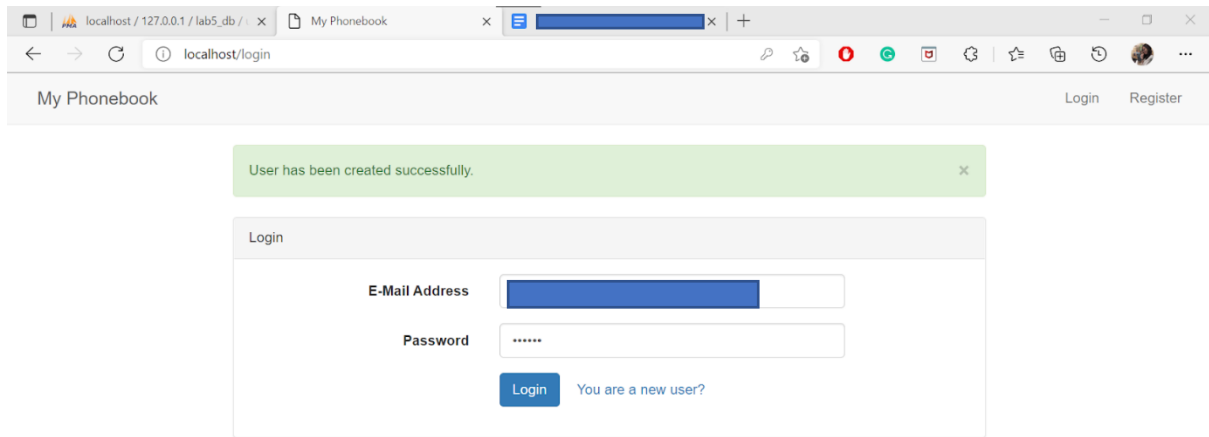
Confirm Password

Register

Figure 7: Register Page

7. Connection test from client to web application

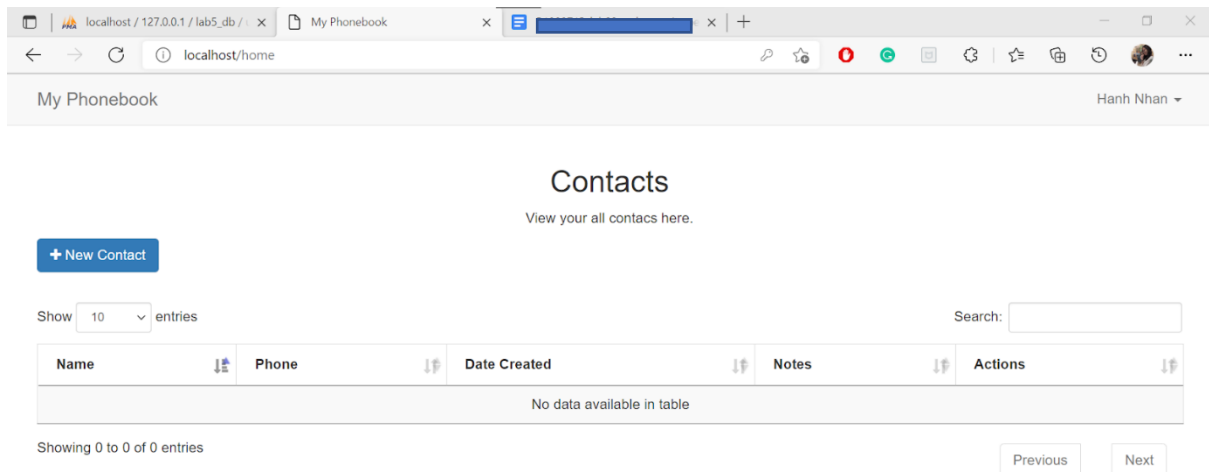
I used the Login Page to connect web application from client, I entered email address and password which I registered to login to PhoneBook



The screenshot shows a web browser window with the URL `localhost/login`. The page title is "My Phonebook". A green success message at the top states "User has been created successfully." Below this is a "Login" form with two input fields: "E-Mail Address" and "Password". The "Password" field contains six dots. A blue "Login" button is positioned below the password field, followed by a link that says "You are a new user?". In the top right corner of the page, there are links for "Login" and "Register".

Figure 8: Login Page

When the input values which I entered are both true, so I can move on to the Home Page (Contacts) of the web application



The screenshot shows the "Contacts" page of the PhoneBook application. The page title is "Contacts" with the subtitle "View your all contacts here." A blue button labeled "+ New Contact" is located on the left. Below this is a "Show" dropdown menu set to "10" and the text "entries". To the right is a "Search:" input field. A table with the following columns is displayed: "Name", "Phone", "Date Created", "Notes", and "Actions". Each column has a small icon for sorting. The table is currently empty, with a message "No data available in table" centered below it. At the bottom left, it says "Showing 0 to 0 of 0 entries". At the bottom right, there are "Previous" and "Next" buttons. The top right of the page shows the user's name "Hanh Nhan" with a dropdown arrow.

Figure 9: Home Page

MODEL C XAMPP framework

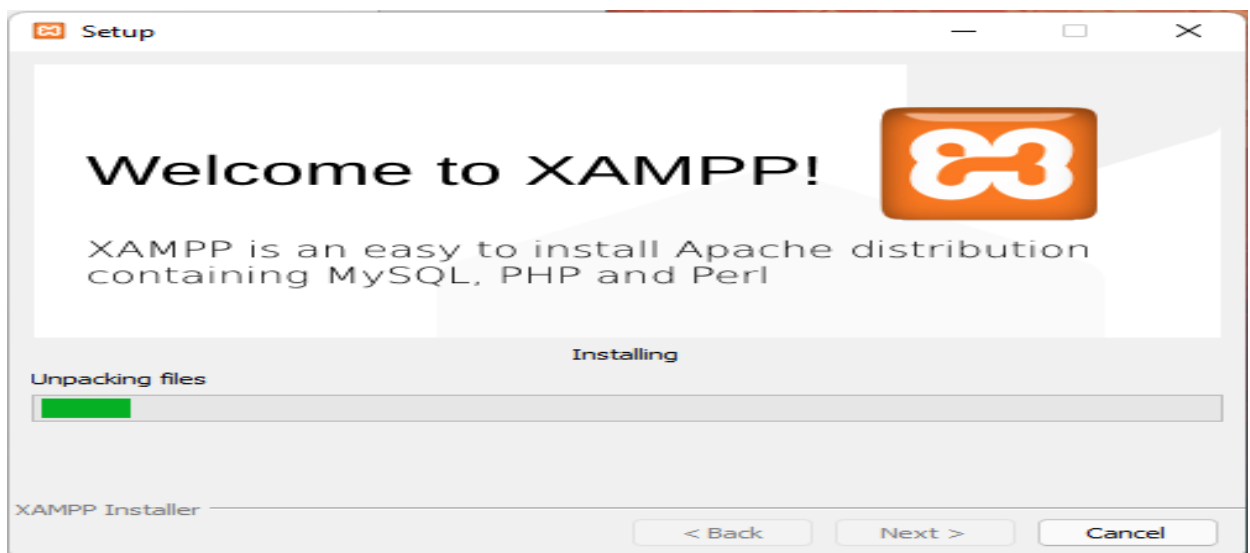
① Install web server (if necessary) => screen shot and explain in detail:

Install XAMPP framework

Visit the website <https://www.apachefriends.org/index.html> to download:



After downloading, we proceed to install:

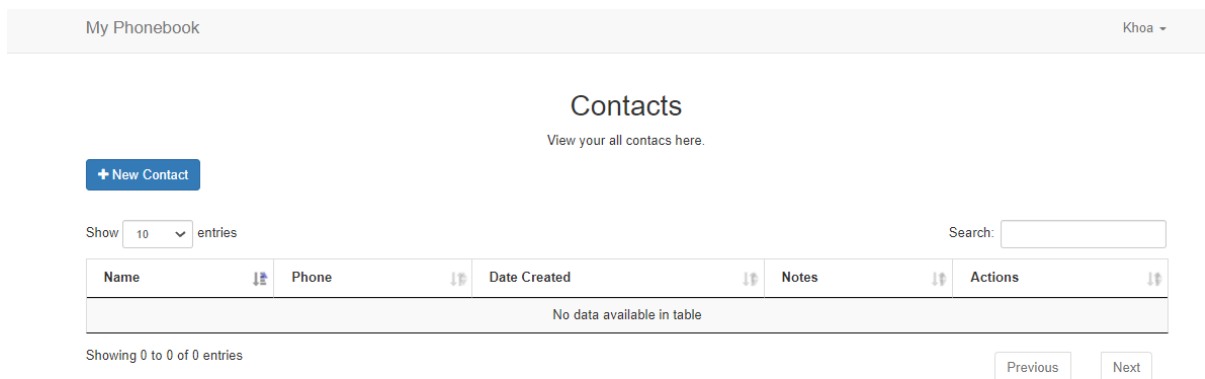


After it is installed, we restart Xampp and go to <http://localhost> to open the Xampp Web Server interface on Windows



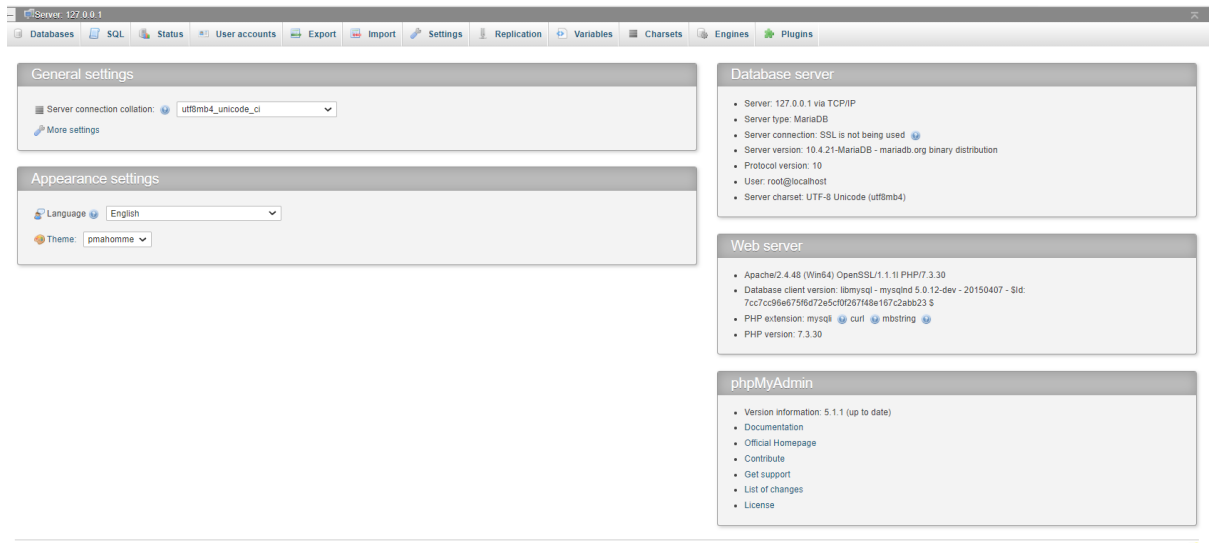
② Install web application => screen shot and explain in detail

To deploy my phonebook website to Webserver (XAMPP), I need to move the phonebook folder to xampp/htdocs. Go to localhost/.



③ Install SQL DB server => screen shot and explain in detail:

Here I use Mysql (MariaDB) which is installed with XAMPP:



④ Develop client log in screen (if necessary) => screen shot and explain in detail

Create the login interface as follows:

The screenshot shows a login interface for a web application titled 'My Phonebook'. The interface includes a header with the title and links for 'Login' and 'Register'. The main content area is a 'Login' form with the following elements:

- E-Mail Address:** A text input field with a blue border and a cursor.
- Password:** A text input field with a white border.
- Login button:** A blue button with the text 'Login'.
- Link:** A link that says 'You are a new user?'.

The logic code part, I handle á follows

- Read the value of form


```
protected function getUserCredentials() {
    return [
        'email' => filter_var($_POST['email'], FILTER_VALIDATE_EMAIL)
        'password' => $_POST['password']
    ];
}
```

Log in handling:

```
public function login() {
    // Preventing CSRF . Attacks
    $this->invokeCsrfGuard();


    // Read the value of form
    $userCredentials = $this->getUserCredentials();

    $errors = [];
    $user = User::where('email', $userCredentials['email'])->
>first();
    if ($user == null) {
        // User does not exist
        $errors['email'] = 'Unknown email.';
    } else if (Guard::login($user, $userCredentials)) {
        // Logged in successfully
        redirect('/home');
    } else {
        // Wrong password
        $errors['password'] = 'Incorrect password.';
    }

    // Login unsuccessful
    $this->saveFormValues(['password']);
    redirect('/login', ['errors' => $errors]);
}
```

⑤ Create SQL DB table (sharing with group table or not?) => screen shot and explain in detail

Here, I create a database named users(id, username, password, email).

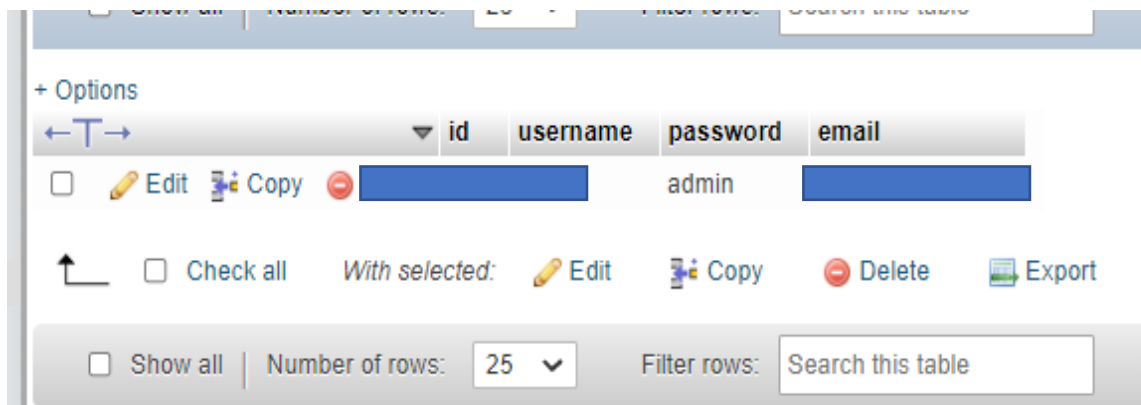


#	Name	Type	Collation	Attributes	Null	Default	Comments	Extra	Action
1	id	int(11)			No	None			Change Drop More
2	username				No	None			Change Drop More
3	password				No	None			Change Drop More
4	email				No	None			Change Drop More

☐ Check all
 With selected: ☐ Browse ☐ Change ☐ Drop ☐ Primary ☐ Unique ☐ Index ☐ Spatial

- ⑥ Create test data (ID, PW data, sharing with group table or not?) => screen shot and explain in detail

I create data like this: id: [redacted] email: [redacted]



- ⑦ Connection test from client to web application

```
<?php
use Illuminate\Database\Capsule\Manager as Capsule;

$capsule = new Capsule;

$capsule->addConnection([
    'driver' => 'mysql',
    'host' => 'localhost',
    'database' => 'phonebook',
    'username' => 'root',
    'password' => '',
    'charset' => 'utf8',
    'collation' => 'utf8_unicode_ci',
    'prefix' => '',
]);

$capsule->setAsGlobal();
$capsule->bootEloquent();
```

▼ **General**

Request URL: http://localhost:8080/login

Request Method: POST

Status Code: 🟡 302 Found

Remote Address: [::1]:8080

Referrer Policy: strict-origin-when-cross-origin

▼ **Response Headers** [View source](#)

Cache-Control: no-store, no-cache, must-revalidate

Connection: Keep-Alive

Content-Length: 0

Content-Type: text/html; charset=UTF-8

Date: Fri, 08 Oct 2021 07:07:24 GMT

Expires: Thu, 19 Nov 1981 08:52:00 GMT

Keep-Alive: timeout=5, max=100

Location: /home

Pragma: no-cache

Server: Apache/2.4.48 (Win64) OpenSSL/1.1.11 PHP/7.3.30