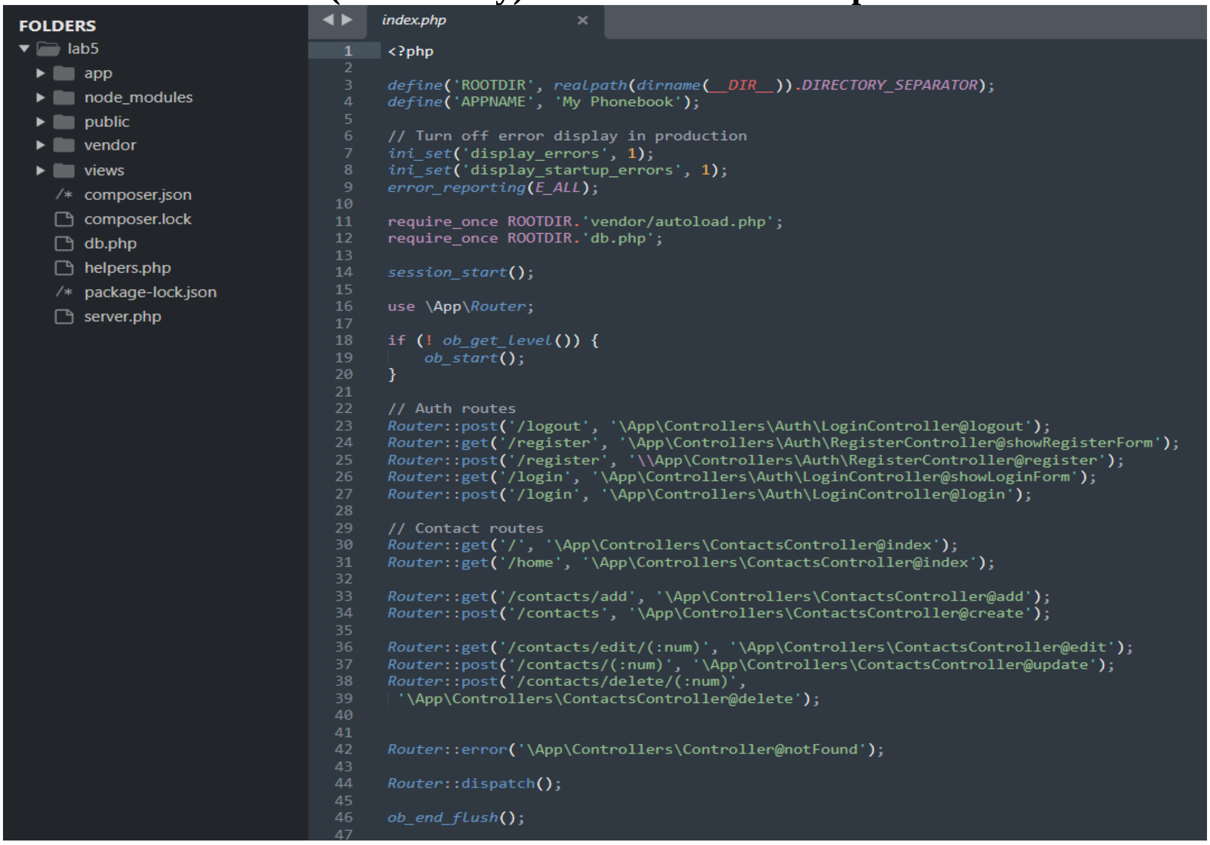
Exercise models for web Pen-Test system

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



```php
<?php

define('ROOTDIR', realpath(dirname(__DIR__)).DIRECTORY_SEPARATOR);
define('APPNAME', 'My Phonebook');

// Turn off error display in production
ini_set('display_errors', 1);
ini_set('display_startup_errors', 1);
error_reporting(E_ALL);

require_once ROOTDIR.'vendor/autoload.php';
require_once ROOTDIR.'db.php';

session_start();

use \App\Router;

if (! ob_get_level()) {
    ob_start();
}

// Auth routes
Router::post('/logout', '\App\Controllers\Auth\LoginController@logout');
Router::get('/register', '\App\Controllers\Auth\RegisterController@showRegisterForm');
Router::post('/register', '\\App\Controllers\Auth\RegisterController@register');
Router::get('/login', '\App\Controllers\Auth\LoginController@showLoginForm');
Router::post('/login', '\App\Controllers\Auth\LoginController@login');

// Contact routes
Router::get('/', '\App\Controllers\ContactsController@index');
Router::get('/home', '\App\Controllers\ContactsController@index');

Router::get('/contacts/add', '\App\Controllers\ContactsController@add');
Router::post('/contacts', '\App\Controllers\ContactsController@create');

Router::get('/contacts/edit/(:num)', '\App\Controllers\ContactsController@edit');
Router::post('/contacts/(:num)', '\App\Controllers\ContactsController@update');
Router::post('/contacts/delete/(:num)',
 '\App\Controllers\ContactsController@delete');


Router::error('\App\Controllers\Controller@notFound');

Router::dispatch();

ob_end_flush();

```

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

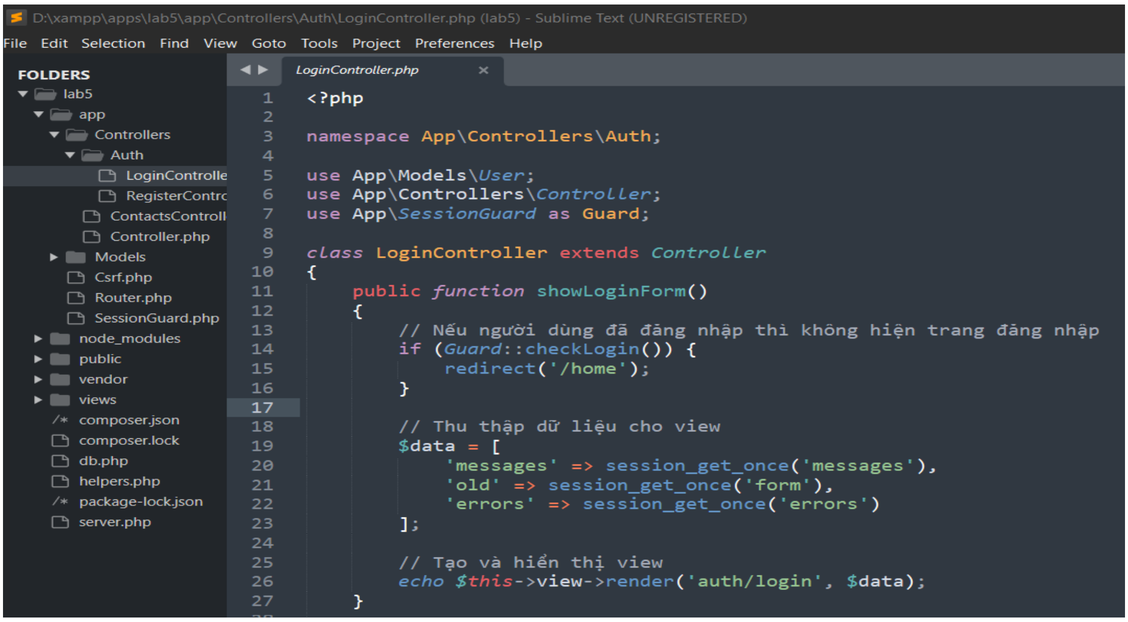
Inside database, there are two table, one for users information, other for contacts informations.

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.

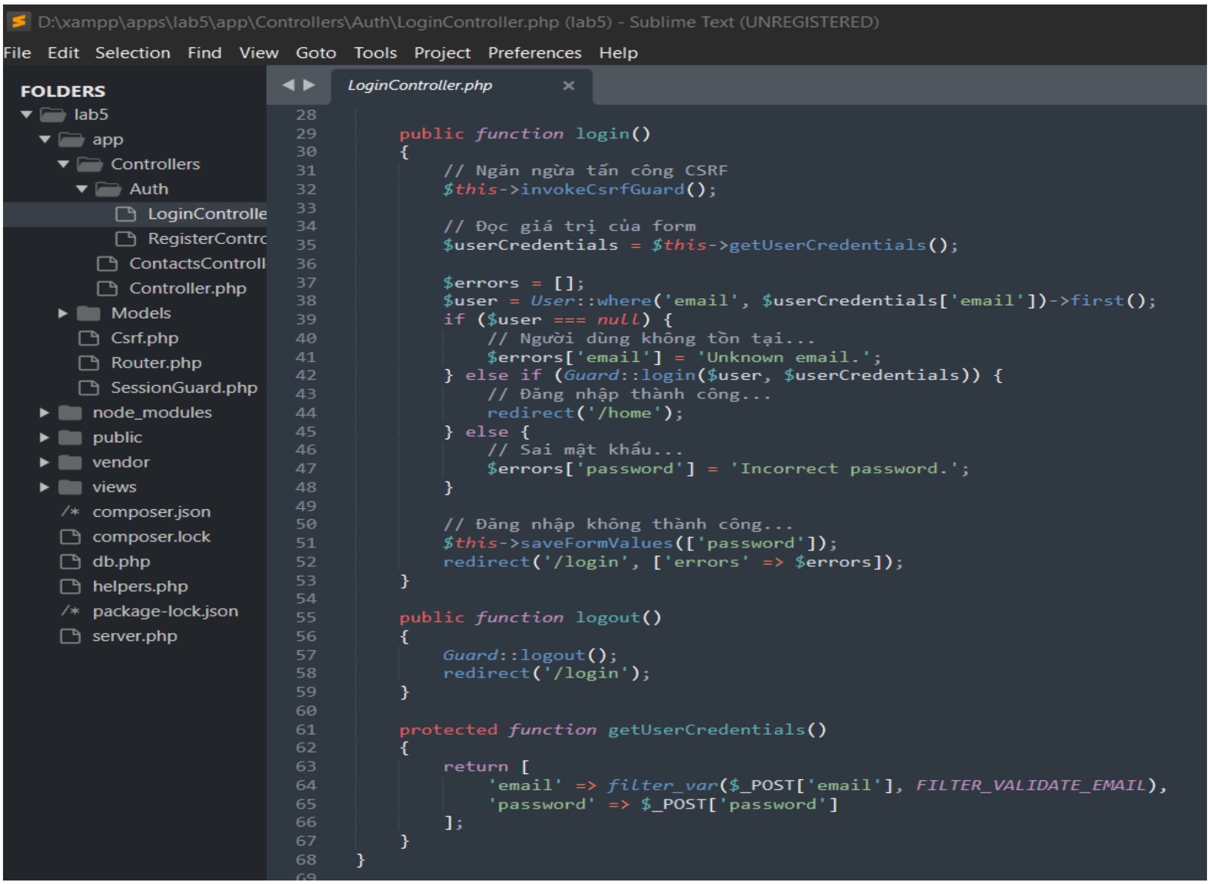


```php
<?php

namespace App\Controllers\Auth;

use App\Models\User;
use App\Controllers\Controller;
use App\SessionGuard as Guard;

class LoginController extends Controller
{
    public function showLoginForm()
    {
        // Nếu người dùng đã đăng nhập thì không hiện trang đăng nhập
        if (Guard::checkLogin()) {
            redirect('/home');
        }

        // Thu thập dữ liệu cho view
        $data = [
            'messages' => session_get_once('messages'),
            'old' => session_get_once('form'),
            'errors' => session_get_once('errors')
        ];

        // Tạo và hiển thị view
        echo $this->view->render('auth/login', $data);
    }
```

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.

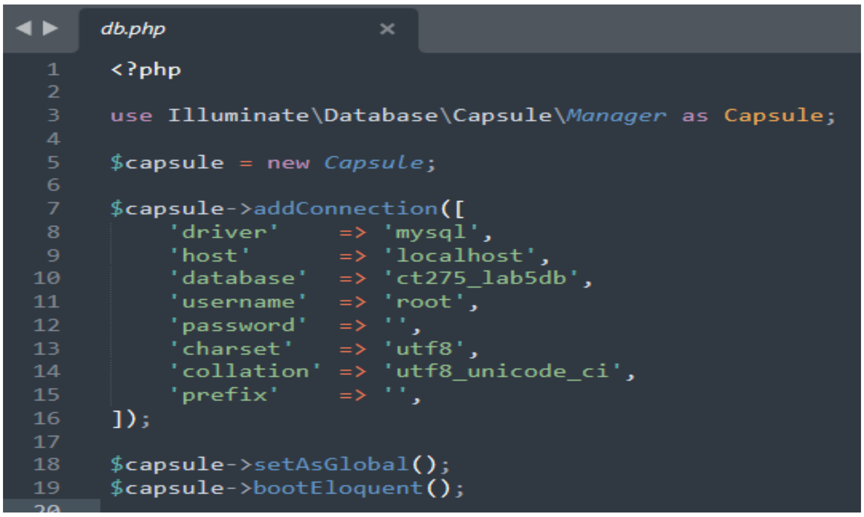
It will print an error in the screen if it can’t find matching email or password. If all the information matching, it will direct to home page.



```php

    public function login()
    {
        // Ngăn ngừa tấn công CSRF
        $this->invokeCsrfGuard();

        // Đọc giá trị của form
        $userCredentials = $this->getUserCredentials();

        $errors = [];
        $user = User::where('email', $userCredentials['email'])->first();
        if ($user === null) {
            // Người dùng không tồn tại...
            $errors['email'] = 'Unknown email.';
        } else if (Guard::login($user, $userCredentials)) {
            // Đăng nhập thành công...
            redirect('/home');
        } else {
            // Sai mật khẩu...
            $errors['password'] = 'Incorrect password.';
        }

        // Đăng nhập không thành công...
        $this->saveFormValues(['password']);
        redirect('/login', ['errors' => $errors]);
    }

    public function logout()
    {
        Guard::logout();
        redirect('/login');
    }

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

Figure 4: login function and getUserCredentials function

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



```php
<?php

use Illuminate\Database\Capsule\Manager as Capsule;

$capsule = new Capsule;

$capsule->addConnection([
    'driver'    => 'mysql',
    'host'      => 'localhost',
    'database'  => 'ct275_lab5db',
    'username'  => 'root',
    'password'  => '',
    'charset'   => 'utf8',
    'collation' => 'utf8_unicode_ci',
    'prefix'    => '',
]);

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

Figure 5: Database configuration file

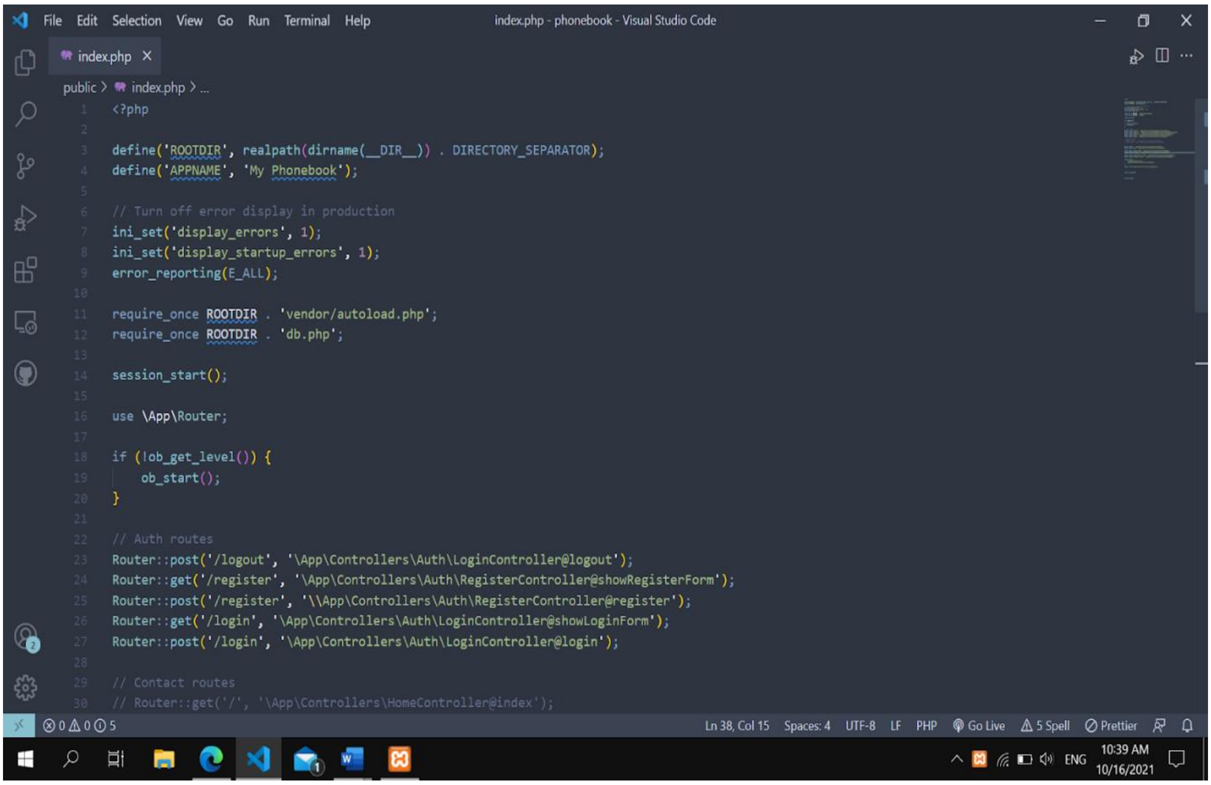
⑤ Connection test from client to web application

Figure 6: 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			

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
public > index.php > ...
⊗ 0 ⚠ 0 ⓘ 5
Ln 38, Col 15 Spaces: 4 UTF-8 LF PHP Go Live ⚠ 5 Spell ⊘ Prettier
ENG
10:39 AM
10/16/2021

```php
<?php

define('ROOTDIR', realpath(dirname(__DIR__)) . DIRECTORY_SEPARATOR);
define('APPNAME', 'My Phonebook');

// Turn off error display in production
ini_set('display_errors', 1);
ini_set('display_startup_errors', 1);
error_reporting(E_ALL);

require_once ROOTDIR . 'vendor/autoload.php';
require_once ROOTDIR . 'db.php';

session_start();

use \App\Router;

if (!ob_get_level()) {
    ob_start();
}

// Auth routes
Router::post('/logout', '\App\Controllers\Auth\LoginController@logout');
Router::get('/register', '\App\Controllers\Auth\RegisterController@showRegisterForm');
Router::post('/register', '\\App\Controllers\Auth\RegisterController@register');
Router::get('/login', '\App\Controllers\Auth\LoginController@showLoginForm');
Router::post('/login', '\App\Controllers\Auth\LoginController@login');

// Contact routes
// 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

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,..

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 comfirm password in order to login to Web Application

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

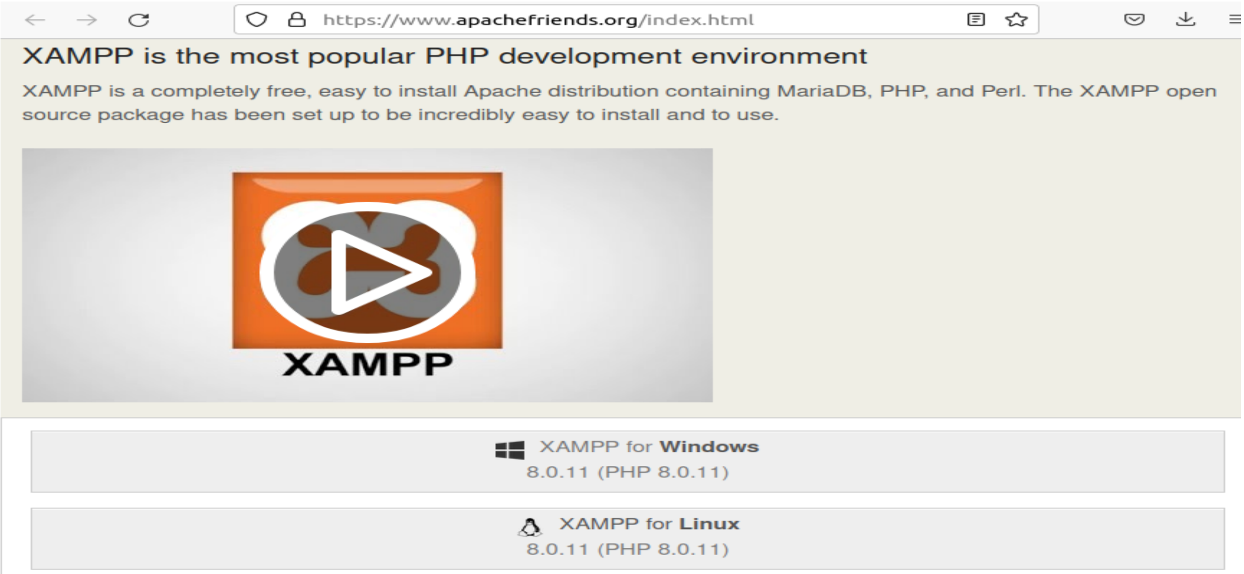
When the input values which I entered are both true, so I can move on to the Home Page (Contacts) of the web application

MODEL C XAMPP framework

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

Install XAMPP framework

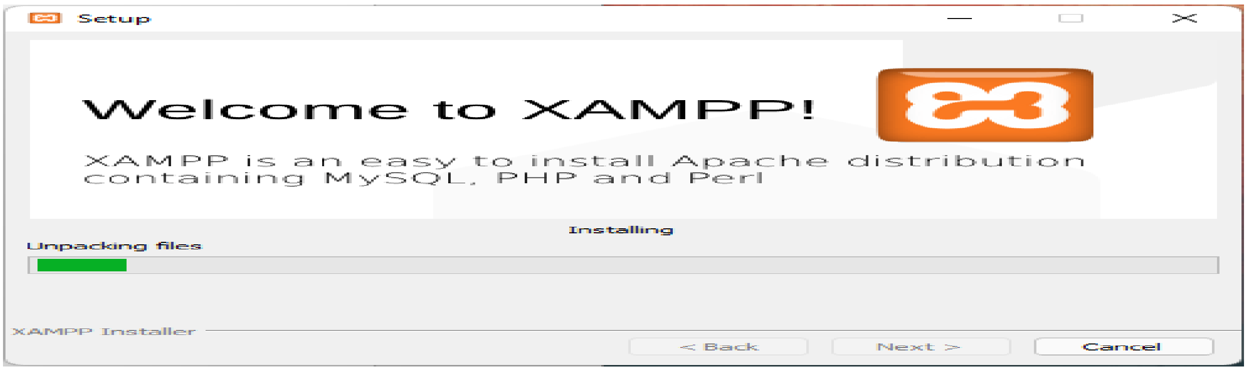
Visit the website https://www.apachefriends.org/index.html to download:



XAMPP is the most popular PHP development environment

XAMPP is a completely free, easy to install Apache distribution containing MariaDB, PHP, and Perl. The XAMPP open source package has been set up to be incredibly easy to install and to use.

After downloading, we proceed to install:



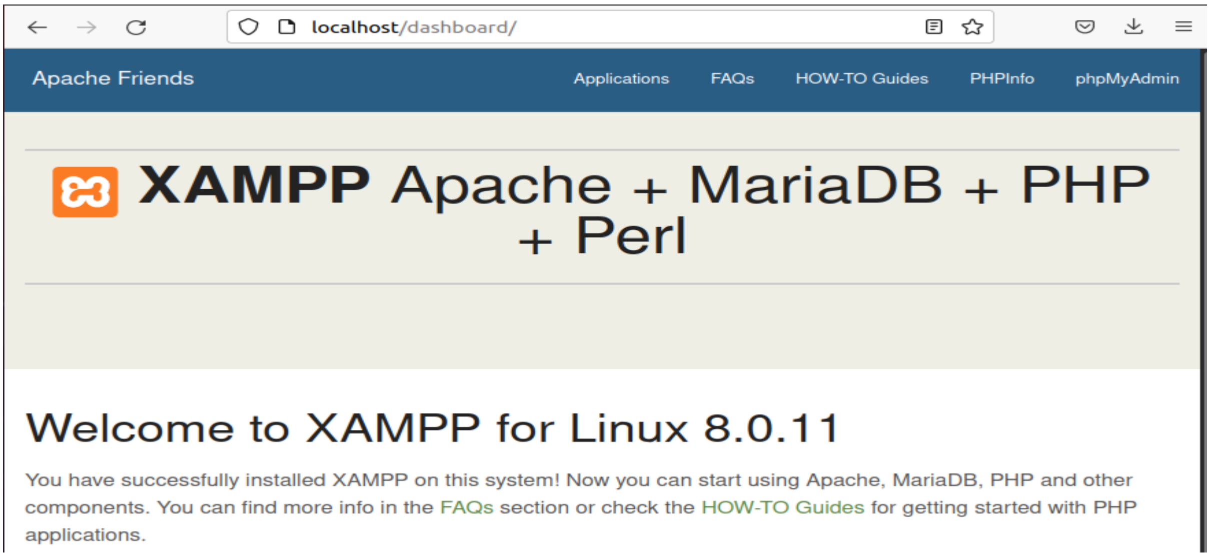
Welcome to XAMPP!

XAMPP is an easy to install Apache distribution containing MySQL, PHP and Perl

Installing

Unpacking files

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



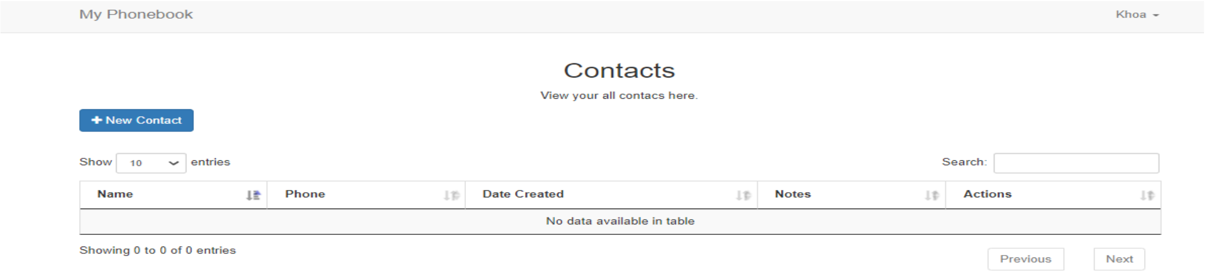
XAMPP Apache + MariaDB + PHP + Perl

Welcome to XAMPP for Linux 8.0.11

You have successfully installed XAMPP on this system! Now you can start using Apache, MariaDB, PHP and other components. You can find more info in the FAQs section or check the HOW-TO Guides for getting started with PHP applications.

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/.



Contacts

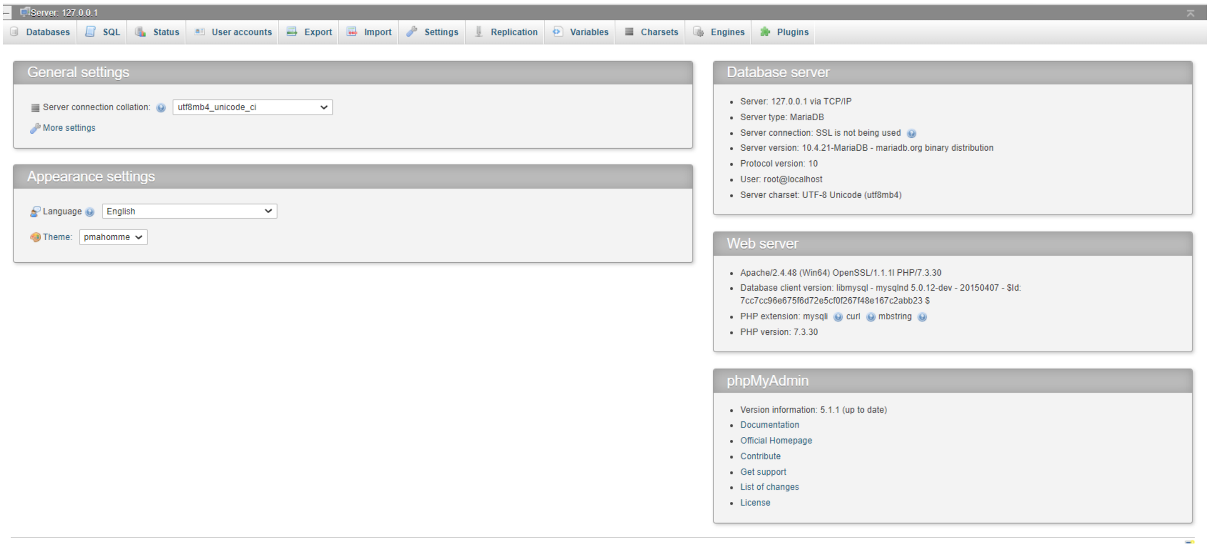
View your all contacs here.

Name	Phone	Date Created	Notes	Actions
No data available in table				

Showing 0 to 0 of 0 entries

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

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



General settings

- Server connection collation: utf8mb4_unicode_ci
- More settings

Appearance settings

- Language: English
- Theme: pmahomme

Database server

- Server: 127.0.0.1 via TCP/IP
- Server type: MariaDB
- Server connection: SSL is not being used
- Server version: 10.4.21-MariaDB - mariadb.org binary distribution
- Protocol version: 10
- User: root@localhost
- Server charset: UTF-8 Unicode (utf8mb4)

Web server

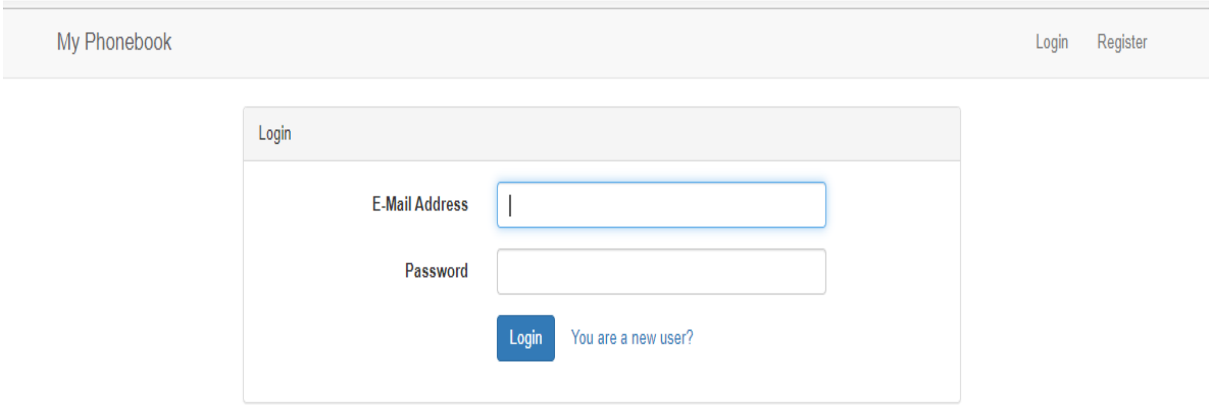
- Apache/2.4.48 (Win64) OpenSSL/1.1.1l PHP/7.3.30
- Database client version: libmysql - mysqlnd 5.0.12-dev - 20150407 - $Id: 7cc7cc96e675f6d72e5cf0f267f48e167c2abb23 $
- PHP extension: mysqli curl mbstring
- PHP version: 7.3.30

phpMyAdmin

- Version information: 5.1.1 (up to date)
- Documentation
- Official Homepage
- Contribute
- Get support
- List of changes
- License

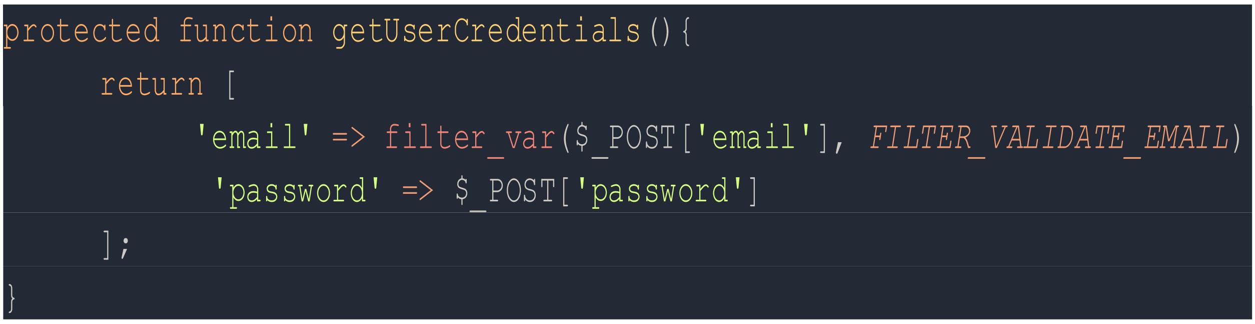
④ Develop client log in screen (if necessary) => screen shot and explain in detail

Create the login interface as follows:



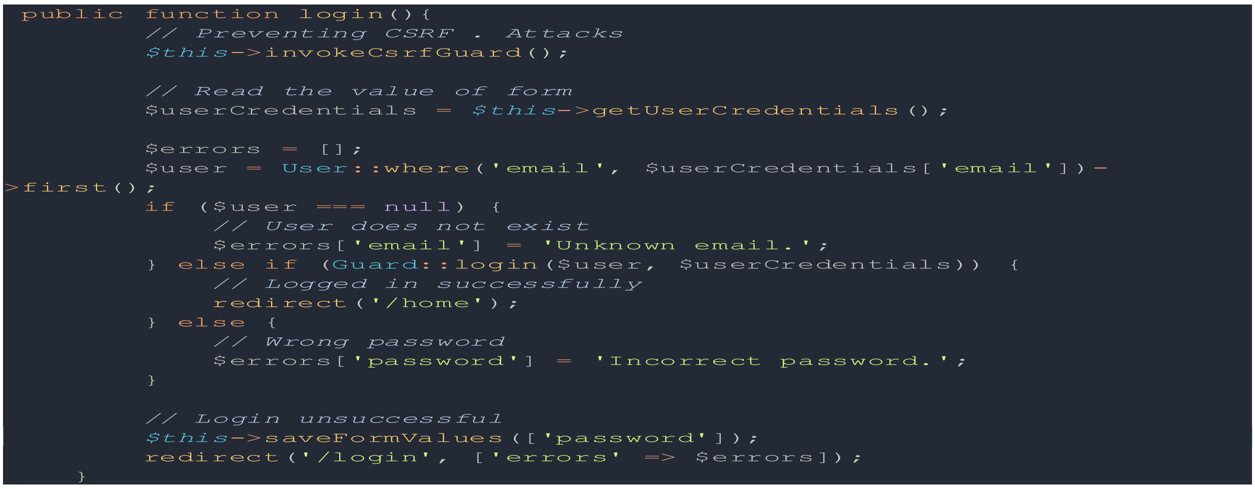
The logic code part, I handle á follows

- 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]);
    }
```

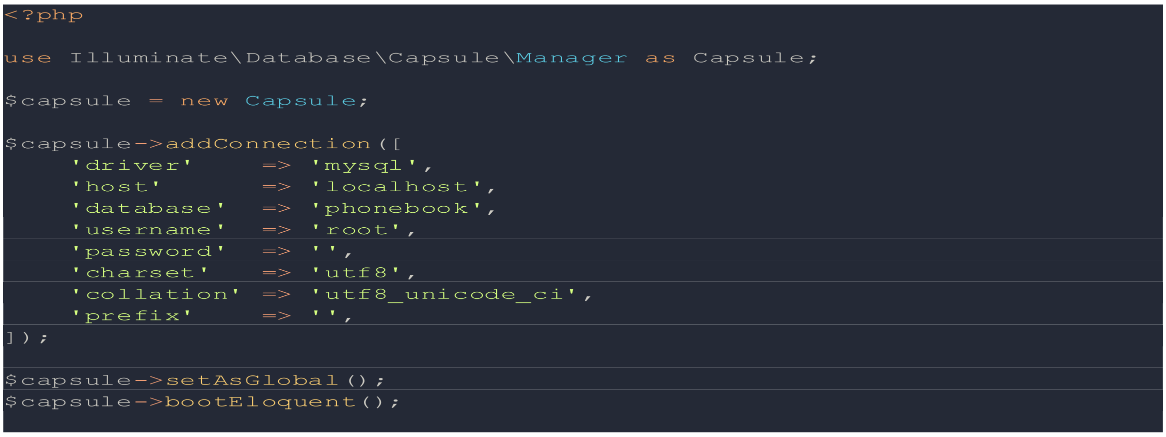
Create SQL DB table (sharing with group table or not?) => screen shot and explain in detail

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

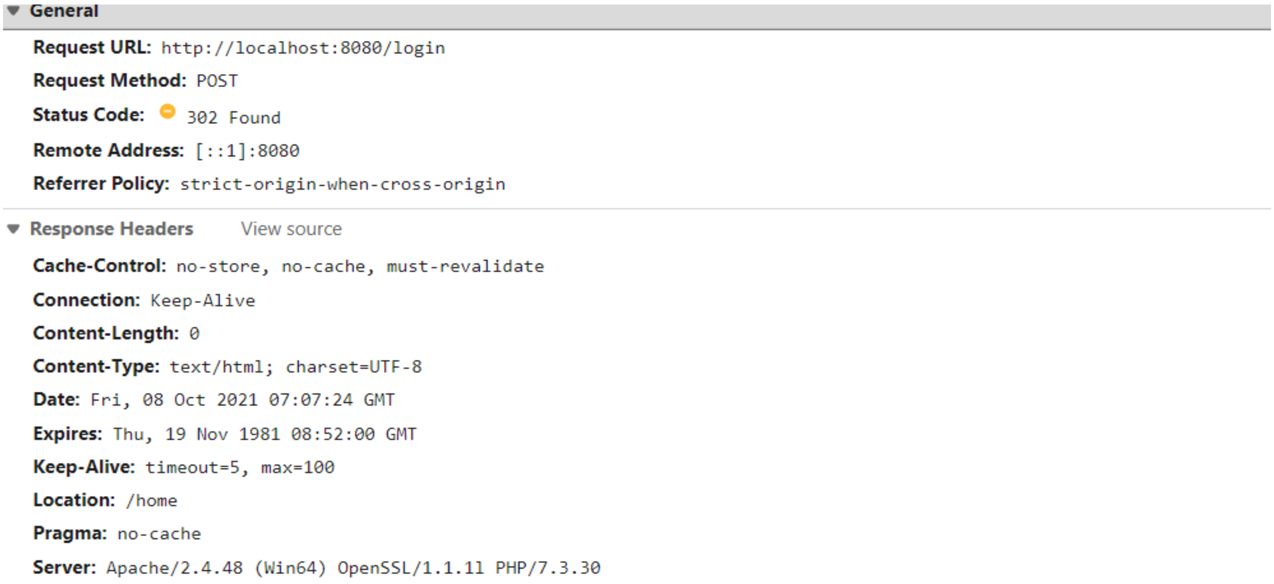
⑤ Create test data (ID, PW data, sharing with group table or not?) => screen shot and explain in detail

I create data like this: id:1234; username: admin; password: admin; email: admin@gmail.com

⑥ Connection test from client to web application



```php
<?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/1.1.1l PHP/7.3.30