

Security & Development Standards

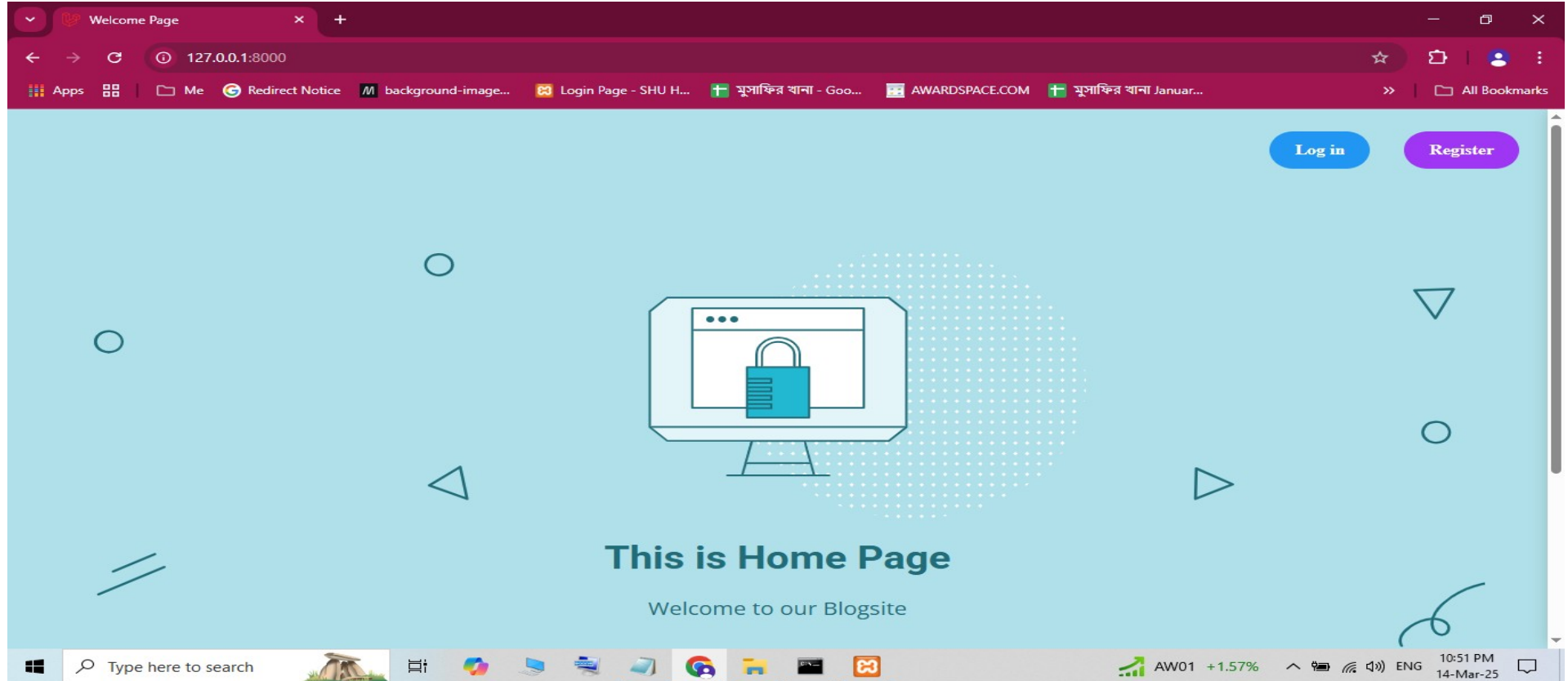
Assignment: 17

Submitted by Asaduzzaman khan(15)

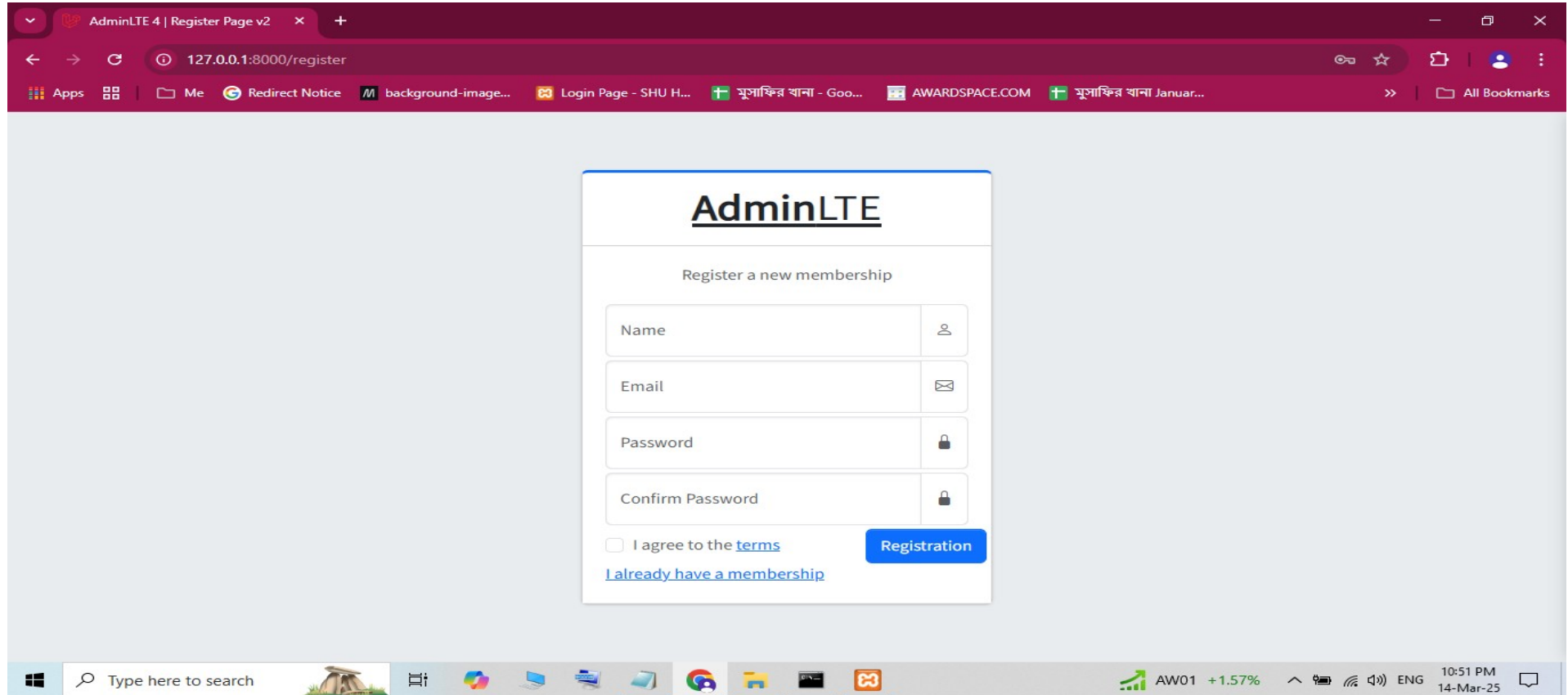
Objectives

- We have implemented a **blog site** and secured it against OWASP Top 10 vulnerabilities .
- **What we have do for our system:**
- Authentication & Password Hashing
- Prevent SQL Injection (Eloquent ORM)
- Prevent XSS (htmlspecialchars())
- Prevent CSRF (@csrf)
- Restrict Access (Middleware & Policies)
- Use UUIDs Instead of IDs (Str::uuid())

Blog site Home page



Registration page



The screenshot shows a web browser window with the title "AdminLTE 4 | Register Page v2". The address bar shows the URL "127.0.0.1:8000/register". The browser's bookmark bar contains several entries, including "Apps", "Me", "Redirect Notice", "background-image...", "Login Page - SHU H...", "মুসাফির খানা - Goo...", "AWARDSPACE.COM", and "মুসাফির খানা Januar...".

The main content area displays a registration form titled "AdminLTE" with the subtitle "Register a new membership". The form includes the following fields and elements:

- Name**: A text input field with a person icon on the right.
- Email**: A text input field with an envelope icon on the right.
- Password**: A text input field with a lock icon on the right.
- Confirm Password**: A text input field with a lock icon on the right.
- ☐ I agree to the [terms](#)
- [I already have a membership](#)
- Registration**: A blue button to submit the form.

The Windows taskbar at the bottom shows the search bar with the text "Type here to search", several application icons, and system status information including "AW01 +1.57%", "ENG", and the date/time "10:51 PM 14-Mar-25".

After login

The screenshot shows a web browser window displaying the AdminLTE v4 dashboard. The browser's address bar shows the URL `127.0.0.1:8000/dashboard`. The dashboard has a dark sidebar on the left with the 'AdminLTE 4' logo and navigation links for 'Dashboard' and 'Blog'. The main content area has a top navigation bar with 'Home' and 'Contact' links, a search icon, and a user profile 'Rifat'. Below this, the 'Dashboard' title is followed by four colored cards: '150 New Orders' (blue), '53% Bounce Rate' (green), '44 User Registrations' (yellow), and '65 Unique Visitors' (red). Each card includes a 'More info' link. The footer contains the copyright notice 'Copyright © 2014-2024 AdminLTE.io. All rights reserved.' and the slogan 'Anything you want'. The Windows taskbar at the bottom shows the search bar and several application icons.

AdminLTE v4 | Dashboard

127.0.0.1:8000/dashboard

Apps | Me | Redirect Notice | background-image... | Login Page - SHU H... | মুসাফির খানা - Goo... | AWARDSPACE.COM | মুসাফির খানা Januar...

AdminLTE 4

Dashboard

Blog

Home Contact

Dashboard

Home / Dashboard

150 New Orders More info

53% Bounce Rate More info

44 User Registrations More info

65 Unique Visitors More info

Copyright © 2014-2024 AdminLTE.io. All rights reserved. Anything you want

Type here to search

Result 10:53 PM 14-Mar-25

Blogs

AdminLTE v4 | Blogs

127.0.0.1:8000/blogs

Apps | Me | Redirect Notice | background-image... | Login Page - SHU H... | মুসাফির খানা - Goo... | AWARDSPACE.COM | মুসাফির খানা Januar...

All Bookmarks

AdminLTE 4

Dashboard

Blog

Home | Contact

Search | Messages 3 | Notifications 15 | Full Screen | User Image Rifat

Blogs

Home / Blogs

Blog List

Add New Blog

Show 10 entries

Search:

#	Title	Author	Category	Created At	Action
1	Ramadan	Asaduzzaman khan	news	2025-03-14T13:54:46.000000Z	<div>View Edit Delete</div>

Showing 1 to 1 of 1 entries

Previous 1 Next

127.0.0.1:8000/blogs

Copyright © 2014-2024 AdminLTE.io. All rights reserved.

Anything you want

Windows Taskbar

System Tray

Problem(the id was visible on url)

The screenshot displays a web browser window with the following elements:

- Address Bar:** Shows the URL `127.0.0.1:8000/blogs/1`, indicating the blog ID is visible in the URL.
- Browser Tabs:** The active tab is labeled "AdminLTE v4 | View Blog".
- Browser Bookmarks:** Includes "Apps", "Me", "Redirect Notice", "background-image...", "Login Page - SHU H...", "মুসাফির খানা - Goo...", "AWARDSPACE.COM", and "মুসাফির খানা Januar...".
- Page Header:** Features the "AdminLTE 4" logo, navigation links for "Home" and "Contact", a search icon, notification icons (3 and 15), a "User Image" placeholder, and the username "Asaduzzaman".
- Sidebar:** Contains links for "Dashboard" and "Blog".
- Main Content Area:**
 - View Blog:** The page title, with a breadcrumb trail "Home / View Blog".
 - Ramadan:** The title of the blog post.
 - Author:** Asaduzzaman khan
 - Summary:** As the crescent moon graces the night sky, Muslims around the world prepare to welcome the holy month of Ramadan. This sacred time, observed during the ninth month of the Islamic lunar calendar, is much more than abstaining from food and drink from dawn to sunset. It is a profound spiritual journey that invites us to reflect, renew, and reconnect with our faith, ourselves, and our communities.
 - Category:** news
 - Content:** As the crescent moon graces the night sky, Muslims around the world prepare to welcome the holy month of Ramadan. This sacred time, observed during the ninth month of the Islamic lunar calendar, is much more than abstaining from food and drink from dawn to sunset. It is a profound spiritual journey that invites us to reflect, renew, and reconnect with our faith, ourselves, and our communities. What is Ramadan? Ramadan commemorates the month when the Quran, the holy book of Islam, was first revealed to the Prophet Muhammad (peace be upon him). It is one of the Five Pillars of Islam and is observed by fasting (sawm), prayer, charity, and self-discipline. The fast begins at dawn (Fajr) and ends at sunset (Maghrib), with dates and water traditionally used to break the fast, followed by a meal known as Iftar. The Essence of Fasting Fasting during Ramadan is not just about physical

Solution using UUID

The screenshot displays a web browser window with the AdminLTE v4 dashboard. The address bar shows the URL `127.0.0.1:8000/blogs/91cb178b-31c5-45d9-8709-311fe0b39407`. The dashboard includes a sidebar with 'Dashboard' and 'Blog' links. The main content area shows a 'View Blog' page for a post titled 'Ramadan'. The post details include the author 'Asaduzzaman khan', a summary of Ramadan, the category 'news', and a detailed content section.

AdminLTE v4 | View Blog

127.0.0.1:8000/blogs/91cb178b-31c5-45d9-8709-311fe0b39407

Apps | Me | Redirect Notice | background-image... | Login Page - SHU H... | মুসাফির খানা - Goo... | AWARDSPACE.COM | মুসাফির খানা Januar...

Home | Contact

Search | 3 | 15 | User Image Rifat

View Blog

[Home](#) / [View Blog](#)

Ramadan

Author: Asaduzzaman khan

Summary: As the crescent moon graces the night sky, Muslims around the world prepare to welcome the holy month of Ramadan. This sacred time, observed during the ninth month of the Islamic lunar calendar, is much more than abstaining from food and drink from dawn to sunset. It is a profound spiritual journey that invites us to reflect, renew, and reconnect with our faith, ourselves, and our communities.

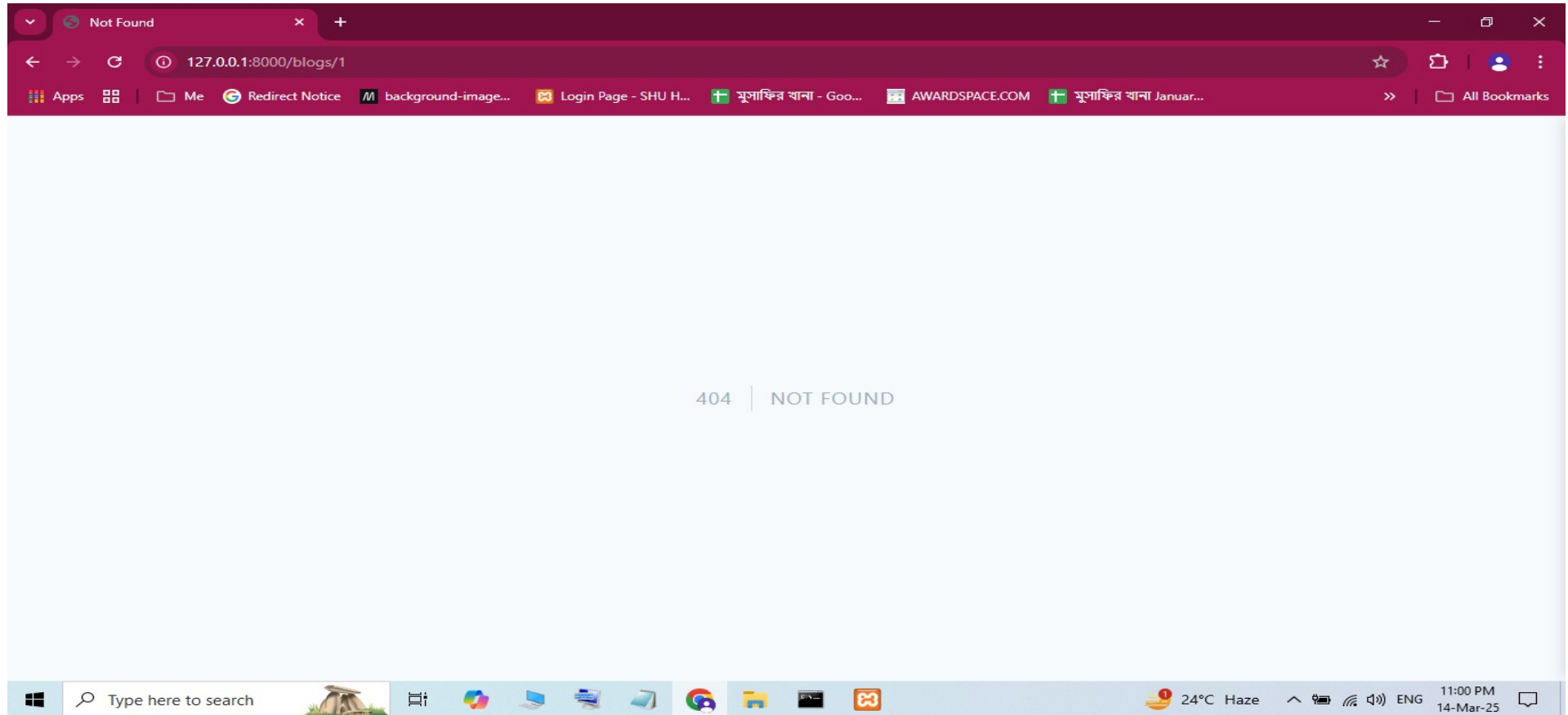
Category: news

Content:

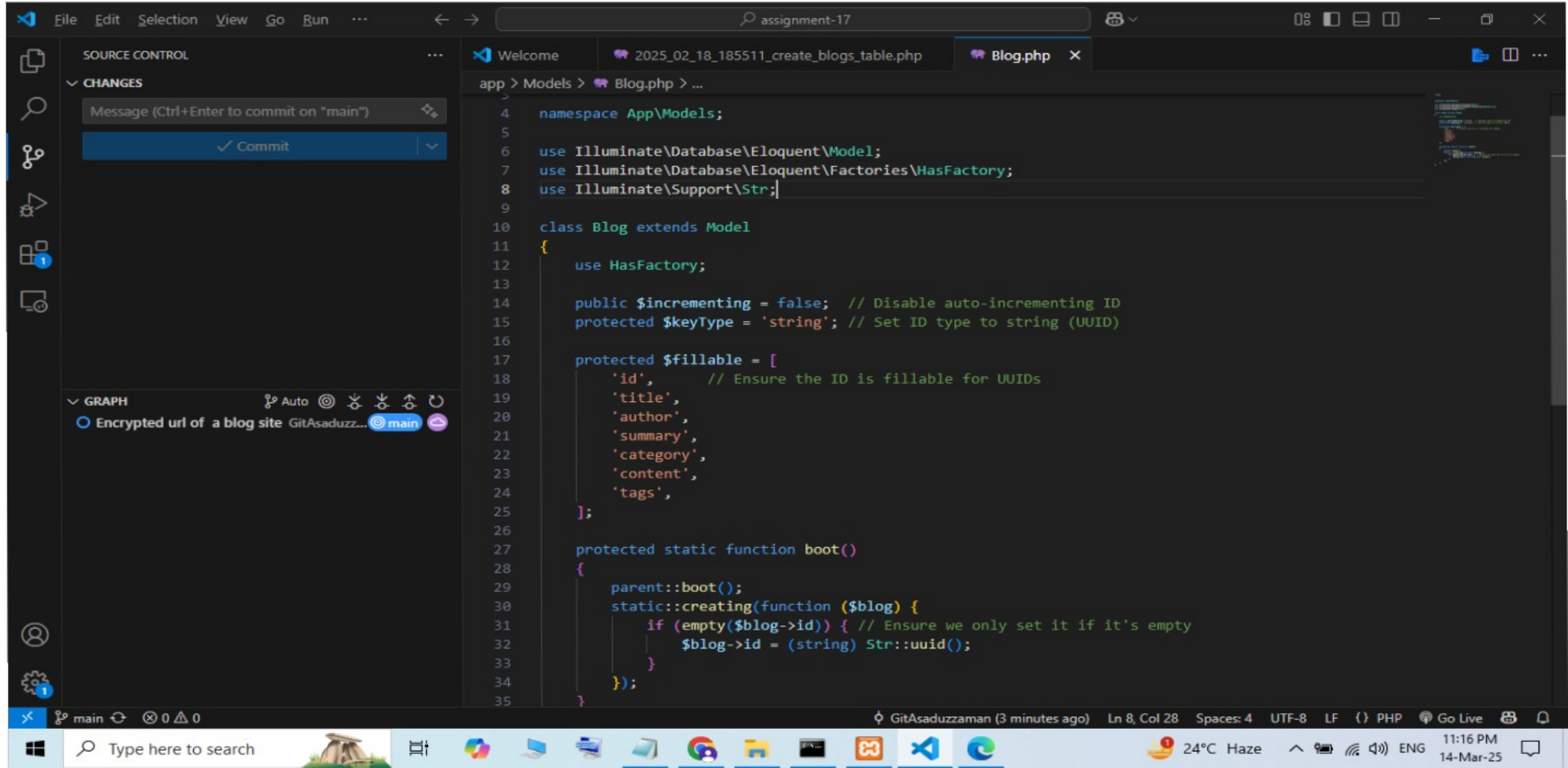
What is Ramadan? Ramadan commemorates the month when the Quran, the holy book of Islam, was first revealed to the Prophet Muhammad (peace be upon him). It is one of the Five Pillars of Islam and is observed by fasting (sawm), prayer, charity, and self-discipline. The fast begins at dawn (Fajr) and ends at sunset (Maghrib), with dates and water traditionally used to break the fast, followed by a meal known as Iftar. The Essence of Fasting Fasting during Ramadan is not just about physical abstinence; it is a holistic practice that nurtures the soul. By refraining from food, drink, and other worldly distractions, we are reminded of the blessings we often take for granted. It teaches us patience, gratitude, and empathy for those who face hunger and hardship every day. Fasting is also a means of purifying the heart and mind, allowing us to focus on our spiritual growth and strengthen our relationship with Allah (God).

Windows taskbar: Type here to search | 24°C Haze | 10:58 PM 14-Mar-25

sql injection will not work



uuid implementation



The screenshot shows the Visual Studio Code editor interface. The left sidebar contains the 'SOURCE CONTROL' panel with a 'Commit' button and a 'GRAPH' panel showing a commit history. The main editor area displays a PHP file named 'Blog.php' with the following code:

```
4 namespace App\Models;
5
6 use Illuminate\Database\Eloquent\Model;
7 use Illuminate\Database\Eloquent\Factories\HasFactory;
8 use Illuminate\Support\Str;
9
10 class Blog extends Model
11 {
12     use HasFactory;
13
14     public $incrementing = false; // Disable auto-incrementing ID
15     protected $keyType = 'string'; // Set ID type to string (UUID)
16
17     protected $fillable = [
18         'id', // Ensure the ID is fillable for UUIDs
19         'title',
20         'author',
21         'summary',
22         'category',
23         'content',
24         'tags',
25     ];
26
27     protected static function boot()
28     {
29         parent::boot();
30         static::creating(function ($blog) {
31             if (empty($blog->id)) { // Ensure we only set it if it's empty
32                 $blog->id = (string) Str::uuid();
33             }
34         });
35     }
```

The bottom status bar shows the current file is 'main', the commit message is 'Encrypted url of a blog site', and the commit is on the 'main' branch. The bottom right corner displays the system tray with the date and time: 11:16 PM, 14-Mar-25.

Changing on database

The screenshot displays the Visual Studio Code interface with a PHP migration file open. The left sidebar shows the 'SOURCE CONTROL' panel with a 'Commit' button and a 'GRAPH' panel showing the 'main' branch. The main editor area shows the file '2025_02_18_185511_create_blogs_table.php' with the following code:

```
1 <?php
2 use Illuminate\Database\Migrations\Migration;
3 use Illuminate\Database\Schema\Blueprint;
4 use Illuminate\Support\Facades\Schema;
5
6 return new class extends Migration
7 {
8     /**
9      * Run the migrations.
10     */
11     public function up(): void
12     {
13         Schema::create('blogs', function (Blueprint $table) {
14             $table->uuid('id')->primary(); // Change from auto-increment to UUID
15             $table->string('title');
16             $table->string('author')->nullable();
17             $table->text('summary')->nullable();
18             $table->string('category')->nullable();
19             $table->longText('content');
20             $table->string('tags')->nullable();
21             $table->timestamps();
22         });
23     }
24
25     /**
26      * Reverse the migrations.
27     */
28     public function down(): void
29     {
30         Schema::dropIfExists('blogs');
31     }
32
33 }
```

The status bar at the bottom indicates the file is on the 'main' branch, 4 minutes ago, at line 9, column 27. The system tray shows the date and time as 11:17 PM on 14-Mar-25.

uuid at database

localhost / 127.0.0.1 / assignment x +

localhost/phpmyadmin/index.php?route=/sql&db=assignment17&table=blogs&pos=0

Server: 127.0.0.1 » Database: assignment17 » Table: blogs

Browse Structure SQL Search Insert Export Import Privileges Operations Tracking Triggers

✓ Showing rows 0 - 1 (2 total, Query took 0.0004 seconds.)

`SELECT * FROM `blogs``

☐ Profiling [[Edit inline](#)] [[Edit](#)] [[Explain SQL](#)] [[Create PHP code](#)] [[Refresh](#)]

☐ Show all | Number of rows: 25 | Filter rows: Search this table | Sort by key: None

Extra options

		id	title	author	summary	category	content	tags	created_at	updated_at
<input type="checkbox"/>	Edit	Copy	Delete	91cb178b-31c5-45d9-8709-311fe0b39407	Ramadan	Asaduzzaman khan	As the crescent moon graces the night sky, Muslims...	news	What is Ramadan? Ramadan commemorates the month w...	festival culture 2025-03-14 13:54:46 2025-03-14 13:54:46
<input type="checkbox"/>	Edit	Copy	Delete	9605581d-efa2-4199-8e4a-756161f1013d	Eid Ul Fitar	Rifat Khan	Eid ul-Fitr, also known as the "Festival of Breaki...	opinion	Eid ul-Fitr: A Celebration of Gratitude and Unity	festival culture 2025-03-14 16:58:19 2025-03-14 16:58:19

☐ Check all | With selected: [Edit](#) [Copy](#) [Delete](#) [Export](#)

☐ Show all | Number of rows: 25 | Filter rows: Search this table | Sort by key: None

Query results operations

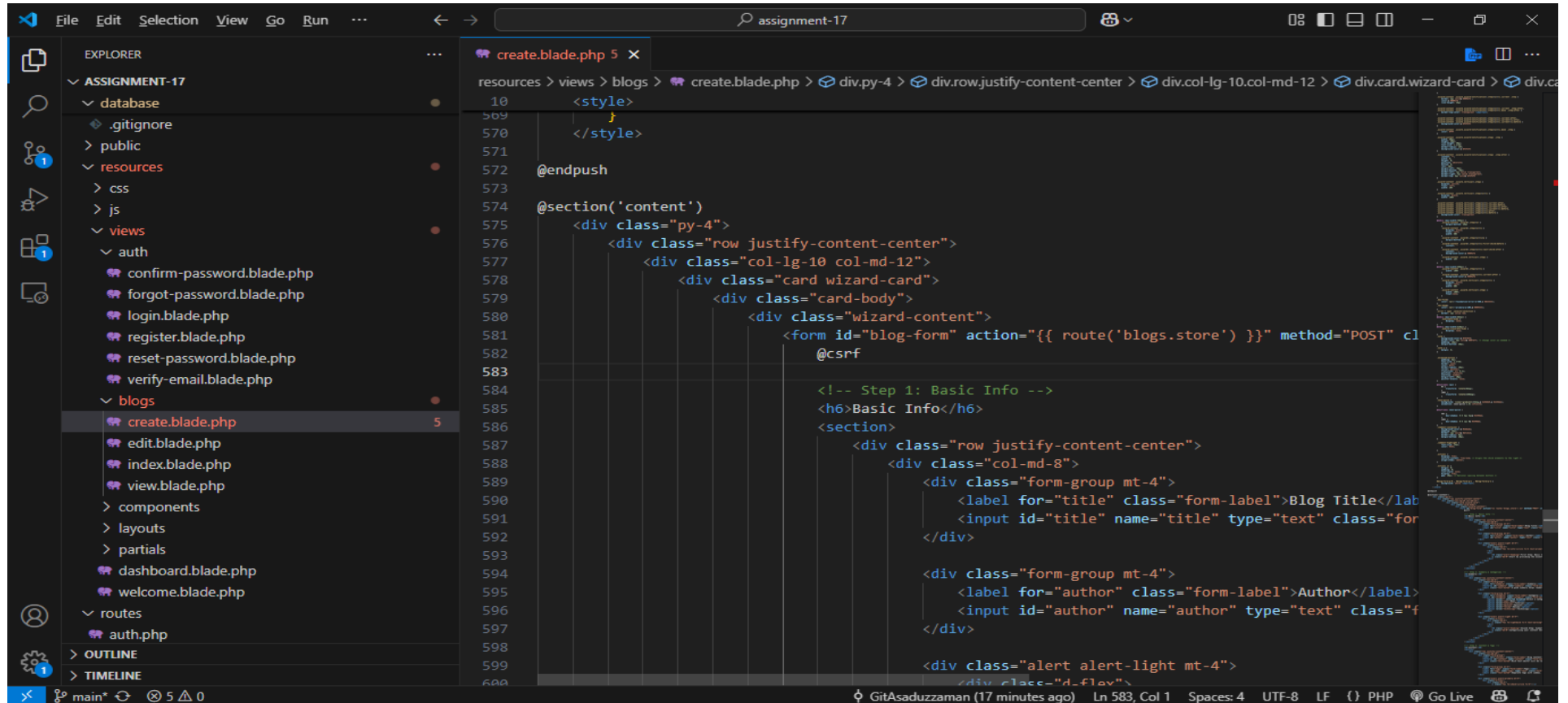
[Print](#) [Copy to clipboard](#) [Export](#) [Display chart](#) [Create view](#)

Console Bookmarks Options History Clear

Type here to search

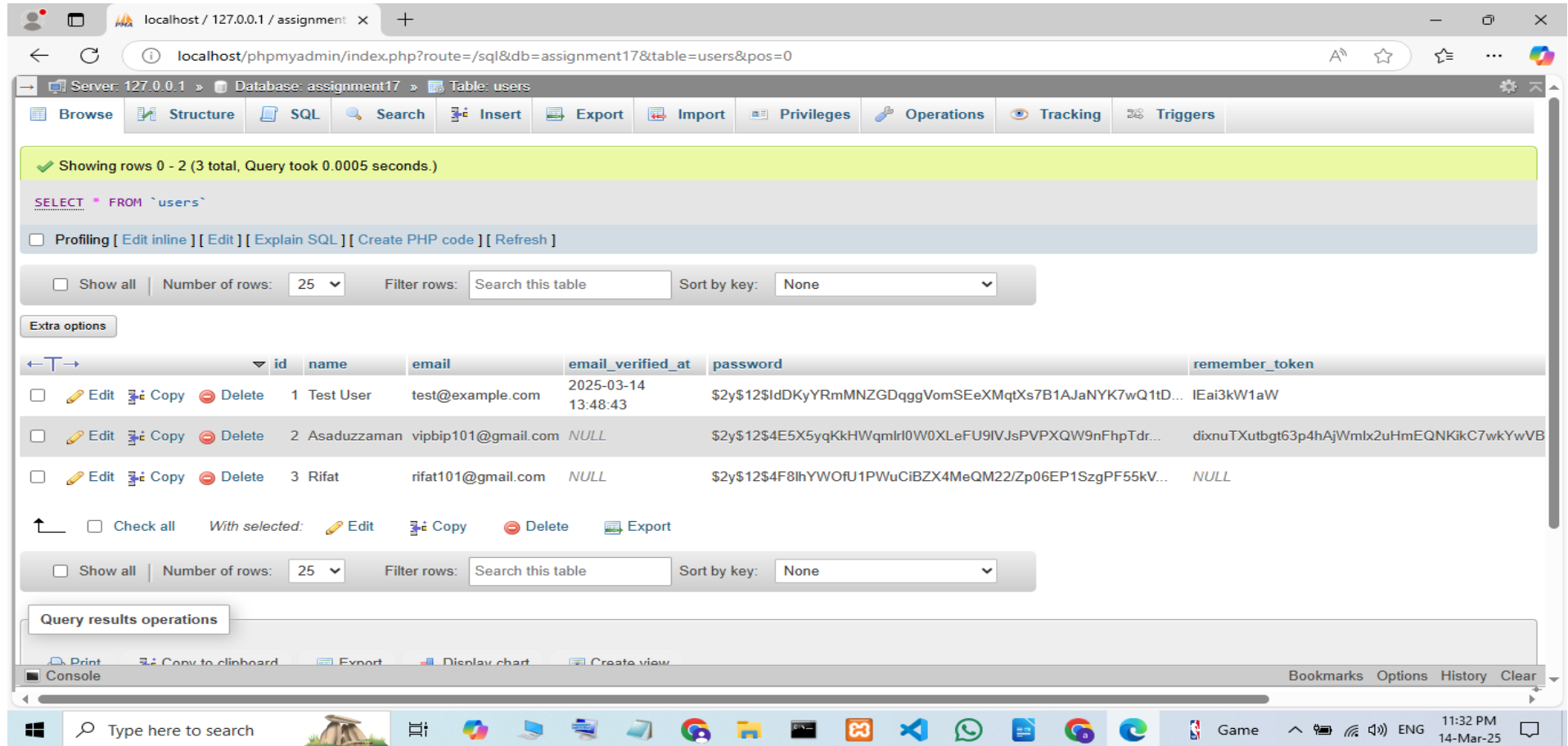
News for you 11:22 PM 14-Mar-25

CSRF



```
10      <style>
569
570    </style>
571
572    @endpush
573
574    @section('content')
575      <div class="py-4">
576        <div class="row justify-content-center">
577          <div class="col-lg-10 col-md-12">
578            <div class="card wizard-card">
579              <div class="card-body">
580                <div class="wizard-content">
581                  <form id="blog-form" action="{{ route('blogs.store') }}" method="POST" class="form">
582                    @csrf
583
584                    <!-- Step 1: Basic Info -->
585                    <h6>Basic Info</h6>
586                    <section>
587                      <div class="row justify-content-center">
588                        <div class="col-md-8">
589                          <div class="form-group mt-4">
590                            <label for="title" class="form-label">Blog Title</label>
591                            <input id="title" name="title" type="text" class="form-control">
592                          </div>
593
594                          <div class="form-group mt-4">
595                            <label for="author" class="form-label">Author</label>
596                            <input id="author" name="author" type="text" class="form-control">
597                          </div>
598
599                          <div class="alert alert-light mt-4">
600                            <div class="d-flex">
```

Password Hashing



The screenshot shows the phpMyAdmin interface for a database named 'assignment17'. The 'users' table is selected, and the SQL query `SELECT * FROM `users`` has been executed. The results show three users, each with a hashed password. The interface includes a top navigation bar with tabs for Browse, Structure, SQL, Search, Insert, Export, Import, Privileges, Operations, Tracking, and Triggers. A status bar at the top indicates 'Showing rows 0 - 2 (3 total, Query took 0.0005 seconds.)'. Below the query, there are options for Profiling, Edit inline, Edit, Explain SQL, Create PHP code, and Refresh. A filter section allows showing all rows, with a dropdown for the number of rows (25) and a search filter. The table data is displayed with columns: id, name, email, email_verified_at, password, and remember_token. Each row has edit, copy, and delete actions. At the bottom, there are options for Query results operations, including Print, Copy to clipboard, Export, Display chart, and Create view. The Windows taskbar is visible at the bottom of the screen.

Showing rows 0 - 2 (3 total, Query took 0.0005 seconds.)

```
SELECT * FROM `users`
```

☐ Profiling [Edit inline] [Edit] [Explain SQL] [Create PHP code] [Refresh]

☐ Show all | Number of rows: 25 | Filter rows: Search this table | Sort by key: None

Extra options

		id	name	email	email_verified_at	password	remember_token
<input type="checkbox"/>	Edit Copy Delete	1	Test User	test@example.com	2025-03-14 13:48:43	\$2y\$12\$dKyYRmMNZGDqggVomSEeXMqTxs7B1AJaNYK7wQ1tD...	IEai3kW1aW
<input type="checkbox"/>	Edit Copy Delete	2	Asaduzzaman	vipbip101@gmail.com	NULL	\$2y\$12\$4E5X5yqKkHWqmlr0W0XLeFU9IVJsPVPXQW9nFhpTdr...	dixnuTXutbgt63p4hAjWmlx2uHmEQNKikC7wkYwVB
<input type="checkbox"/>	Edit Copy Delete	3	Rifat	rifat101@gmail.com	NULL	\$2y\$12\$4F8lhYWOfu1PWuCiBZX4MeQM22/Zp06EP1SzgPF55kV...	NULL

☐ Check all | With selected: Edit Copy Delete Export

☐ Show all | Number of rows: 25 | Filter rows: Search this table | Sort by key: None

Query results operations

Print Copy to clipboard Export Display chart Create view

Console Bookmarks Options History Clear

My Laravel web is now secure against OWASP Top 10 vulnerabilities!

I have ensured:

- Authentication & Password Hashing
- Prevent SQL Injection (Eloquent ORM)
- Prevent XSS (htmlspecialchars())
- Prevent CSRF (@csrf)
- Restrict Access (Middleware & Policies)
- Use UUIDs Instead of IDs (Str::uuid())

Thank You