Security & Development Standards

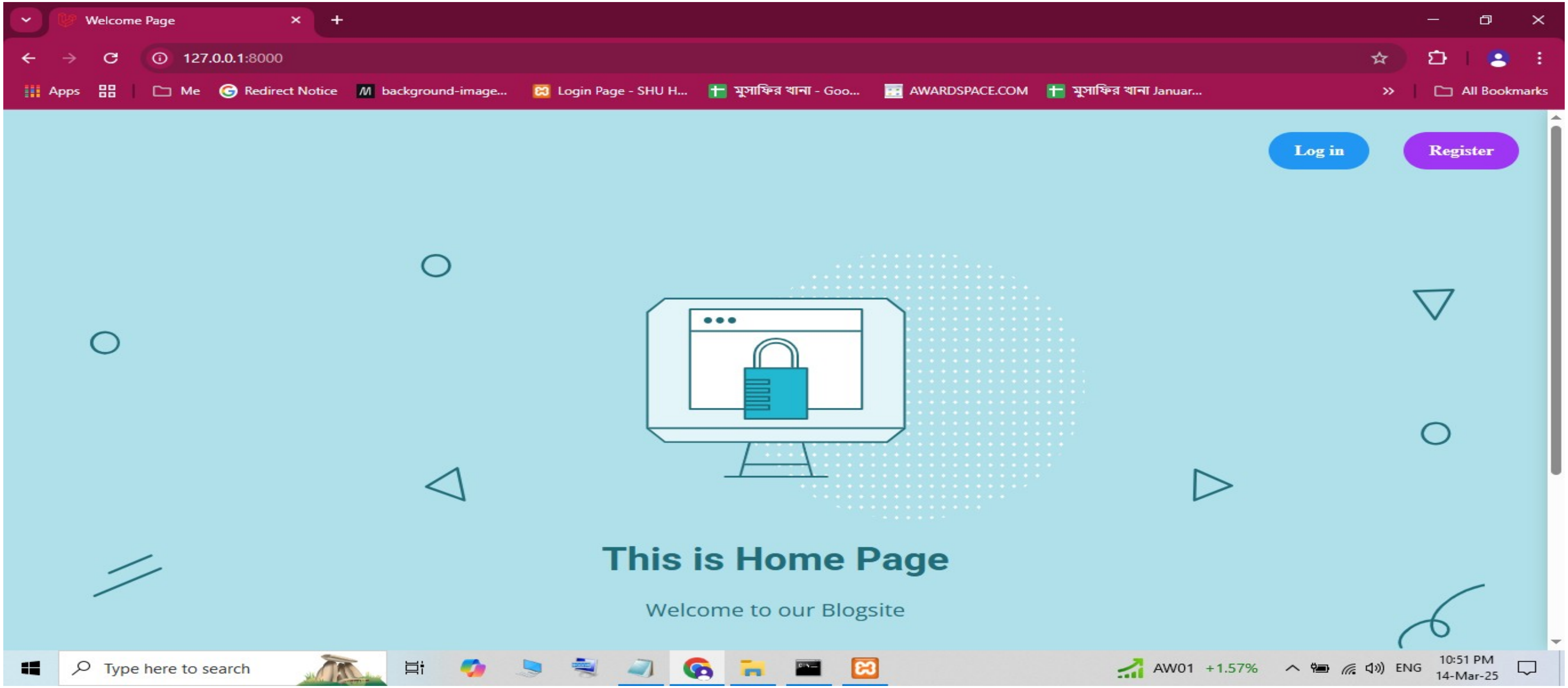
Assignment: 17

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())

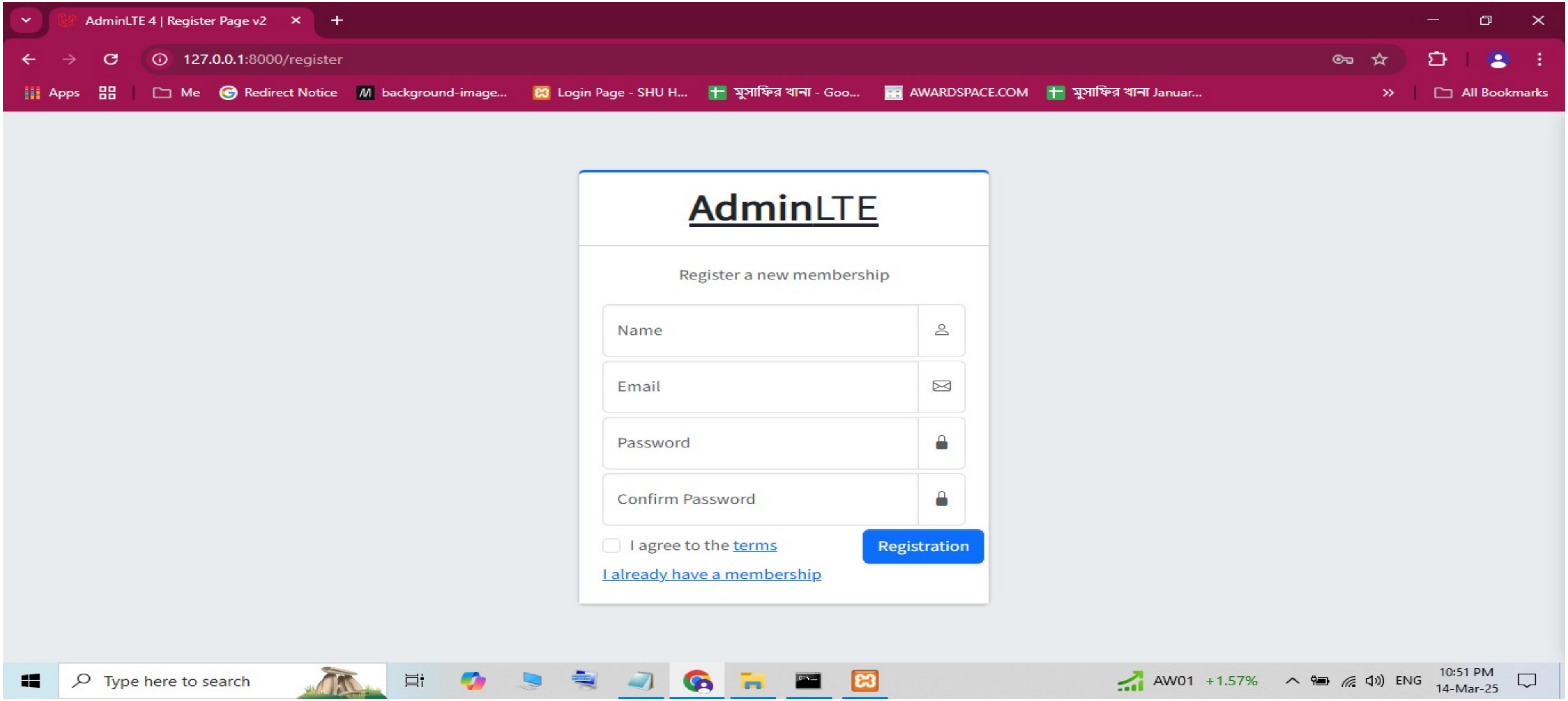
Blog site Home page



This is Home Page

Welcome to our Blogsite

Registration page



AdminLTE

Register a new membership

Name

Email

Password

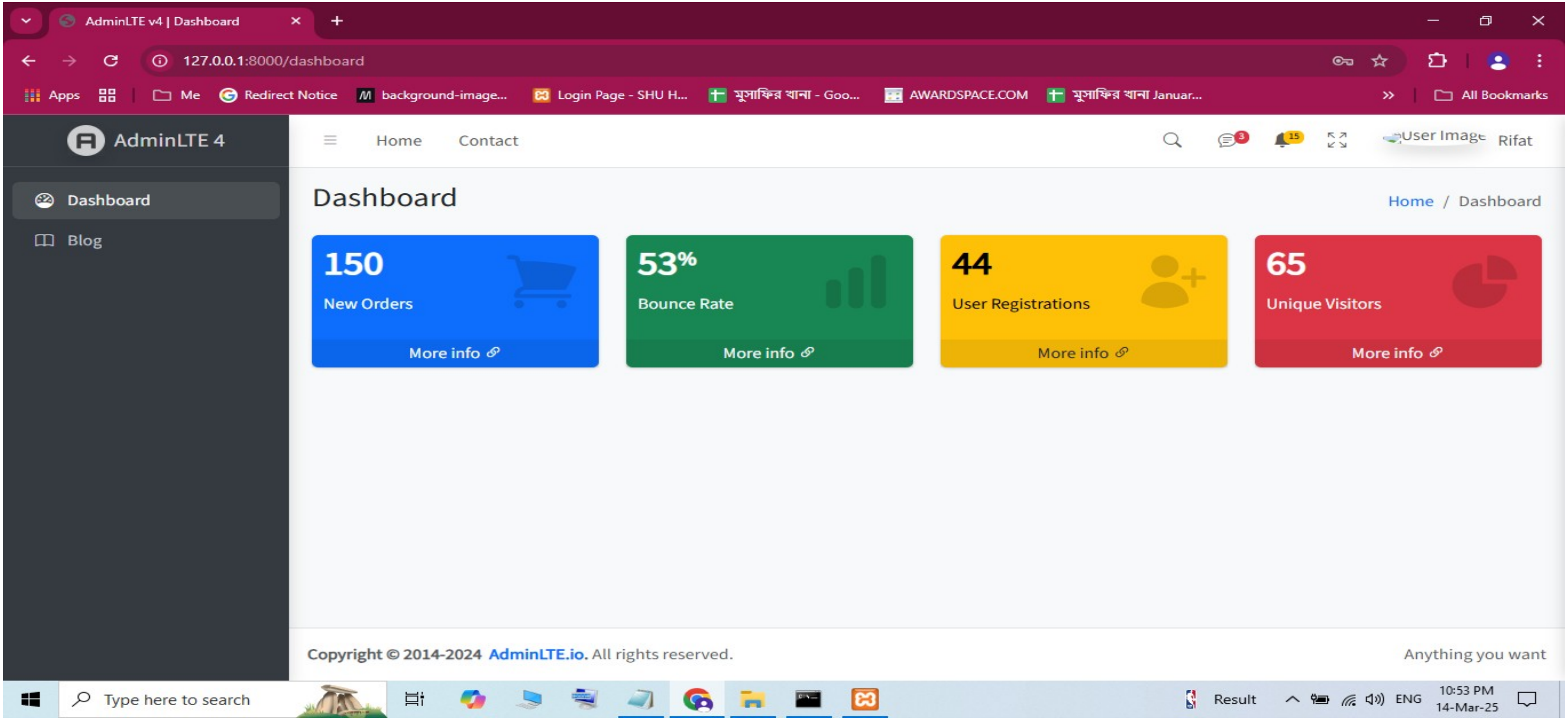
Confirm Password

☐ I agree to the terms

Registration

I already have a membership

After login



Dashboard

150 New Orders More info

53% Bounce Rate More info

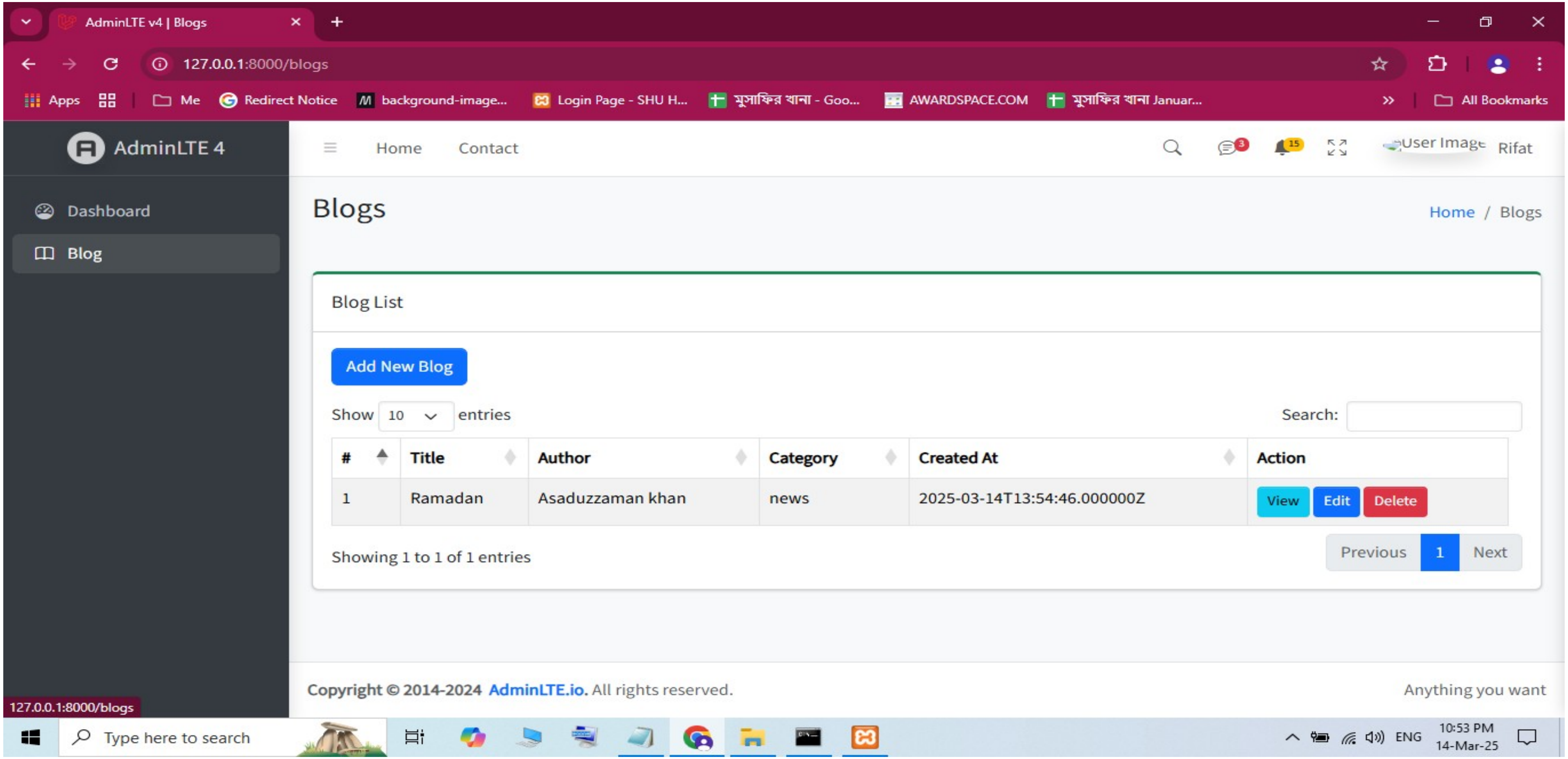
44 User Registrations More info

65 Unique Visitors More info

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

Anything you want

Blogs



Blogs

Home / Blogs

Blog List

Show 10 entries

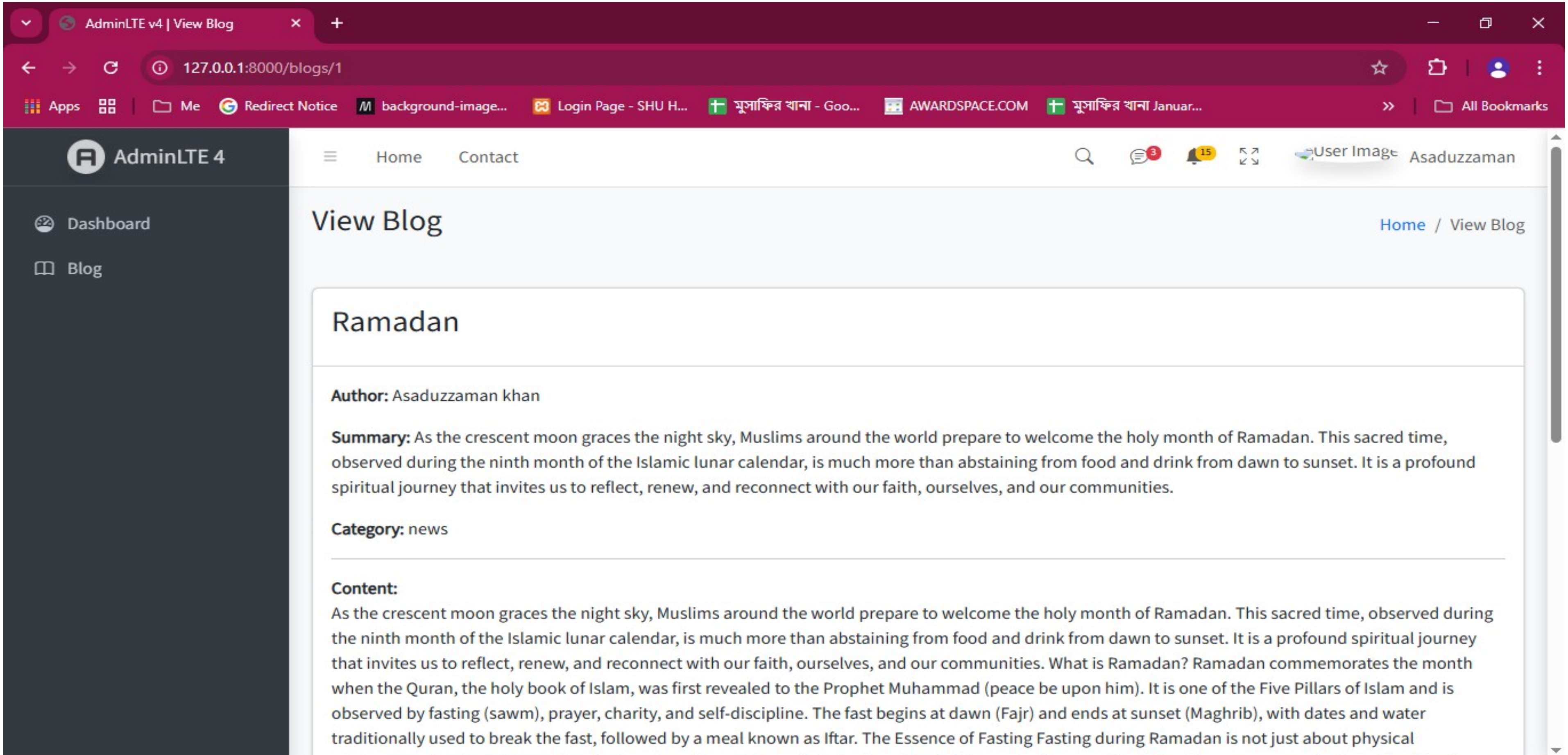
#	Title	Author	Category	Created At	Action
1	Ramadan	Asaduzzaman khan	news	2025-03-14T13:54:46.000000Z	View Edit Delete

Showing 1 to 1 of 1 entries

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

Anything you want

Problem(the id was visible on url)



127.0.0.1:8000/blogs/1

View Blog

Ramadan

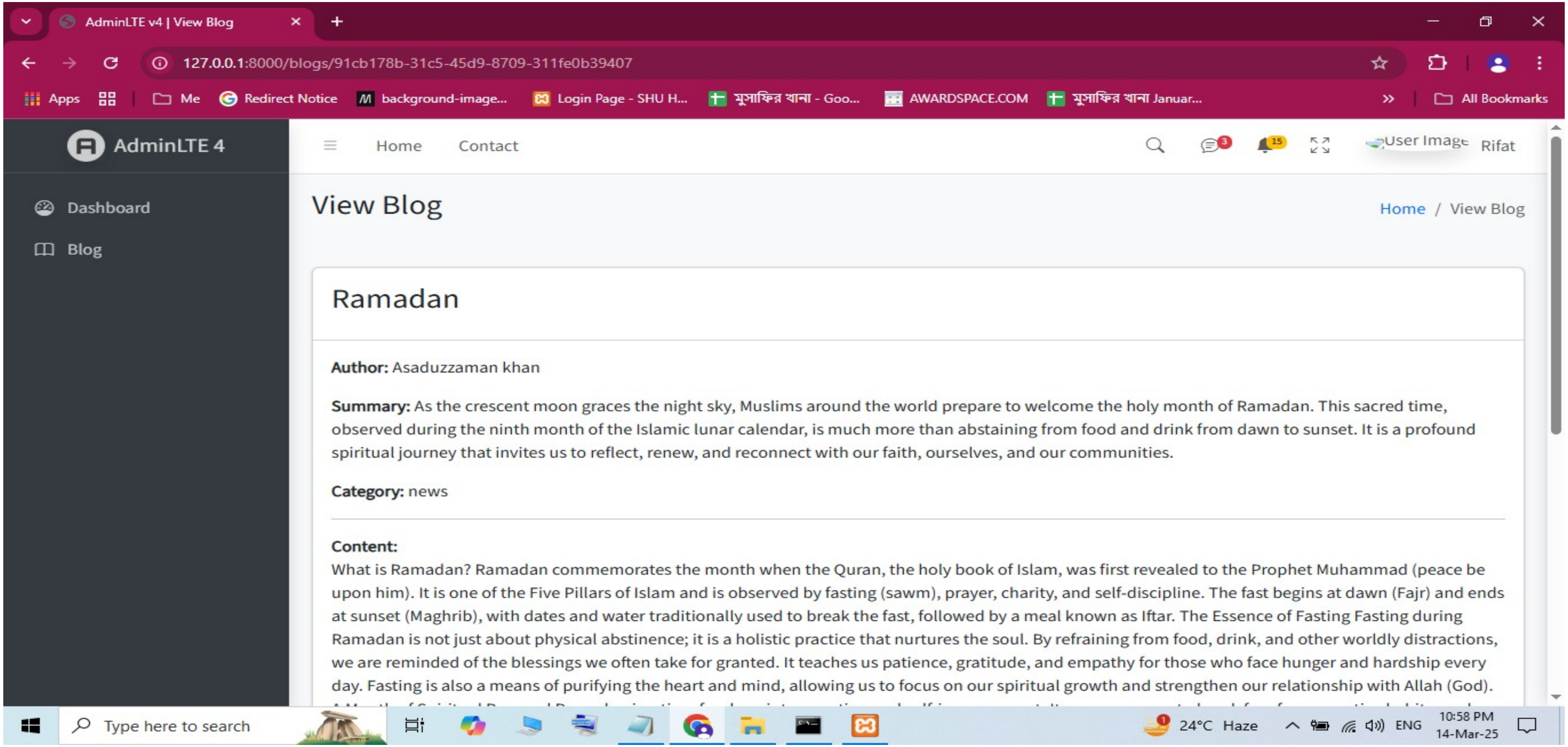
Author: Asaduzzaman khan

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:
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



View Blog

Ramadan

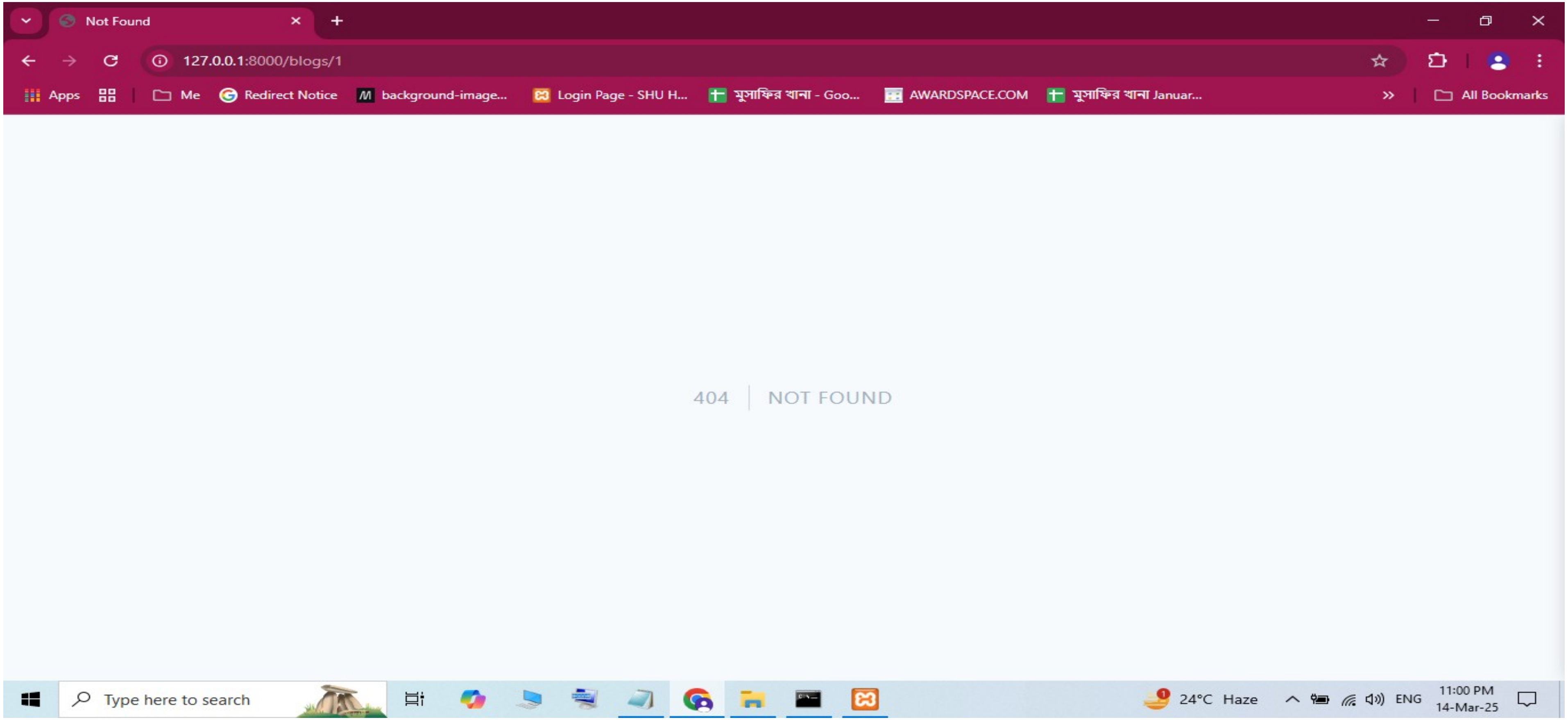
Author: Asaduzzaman khan

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

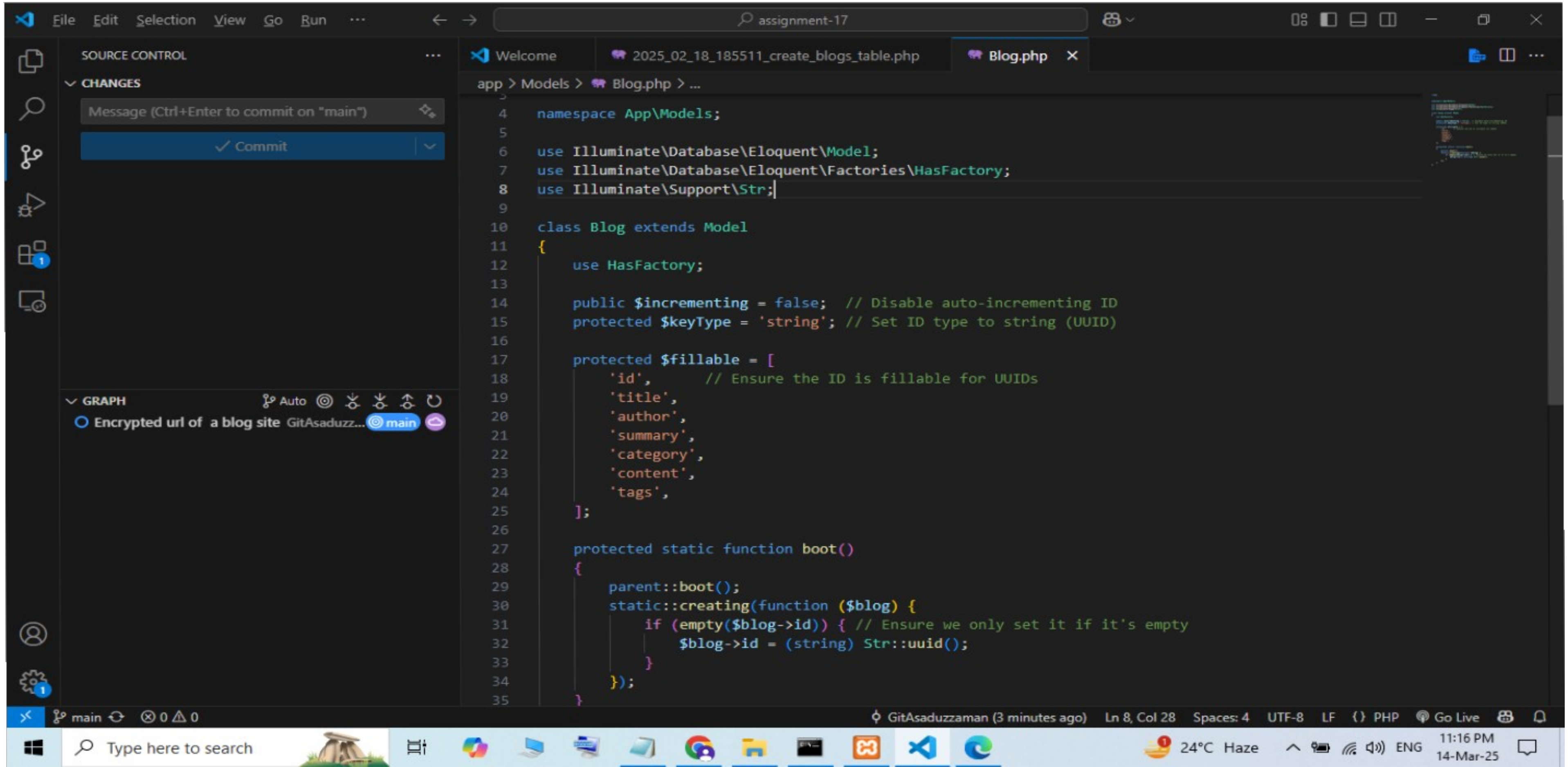
Content:
What is Ramadan? Ramadan commemorates the month when the Quran, the holy book of Islam, was first revealed to the Prophet Muhammad (peace be upon him). It is one of the Five Pillars of Islam and is observed by fasting (sawm), prayer, charity, and self-discipline. The fast begins at dawn (Fajr) 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).

sql injection will not work



404 | NOT FOUND

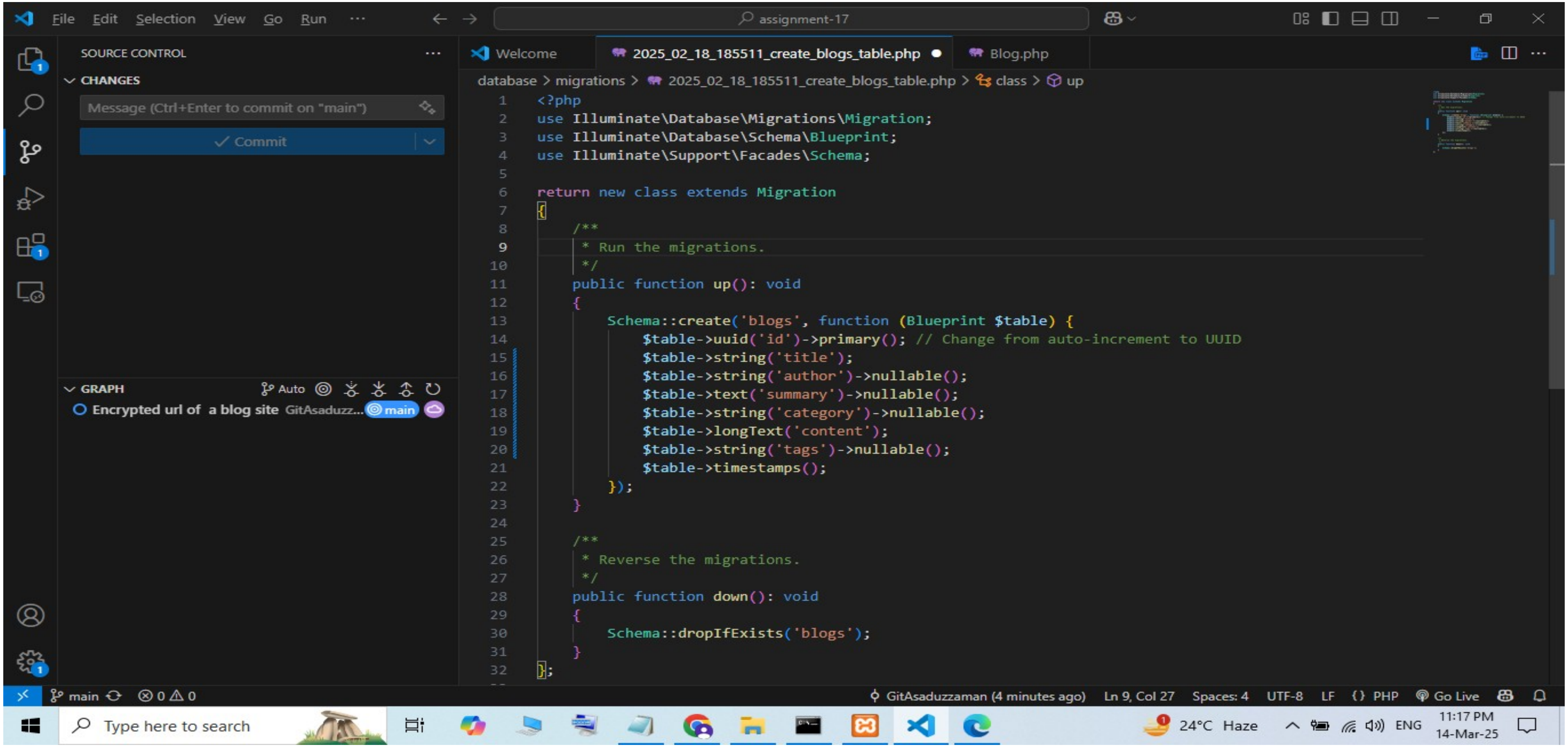
uuid implementation



File Edit Selection View Go Run ···
assignment-17
SOURCE CONTROL
CHANGES
Message (Ctrl+Enter to commit on "main")
✓ Commit
GRAPH
Auto
Encrypted url of a blog site GitAsaduzz... main
Welcome
2025_02_18_185511_create_blogs_table.php
Blog.php
app > Models > Blog.php > ...
main 0 0
GitAsaduzzaman (3 minutes ago) Ln 8, Col 28 Spaces: 4 UTF-8 LF {} PHP Go Live
Type here to search
24°C Haze
ENG
11:16 PM
14-Mar-25

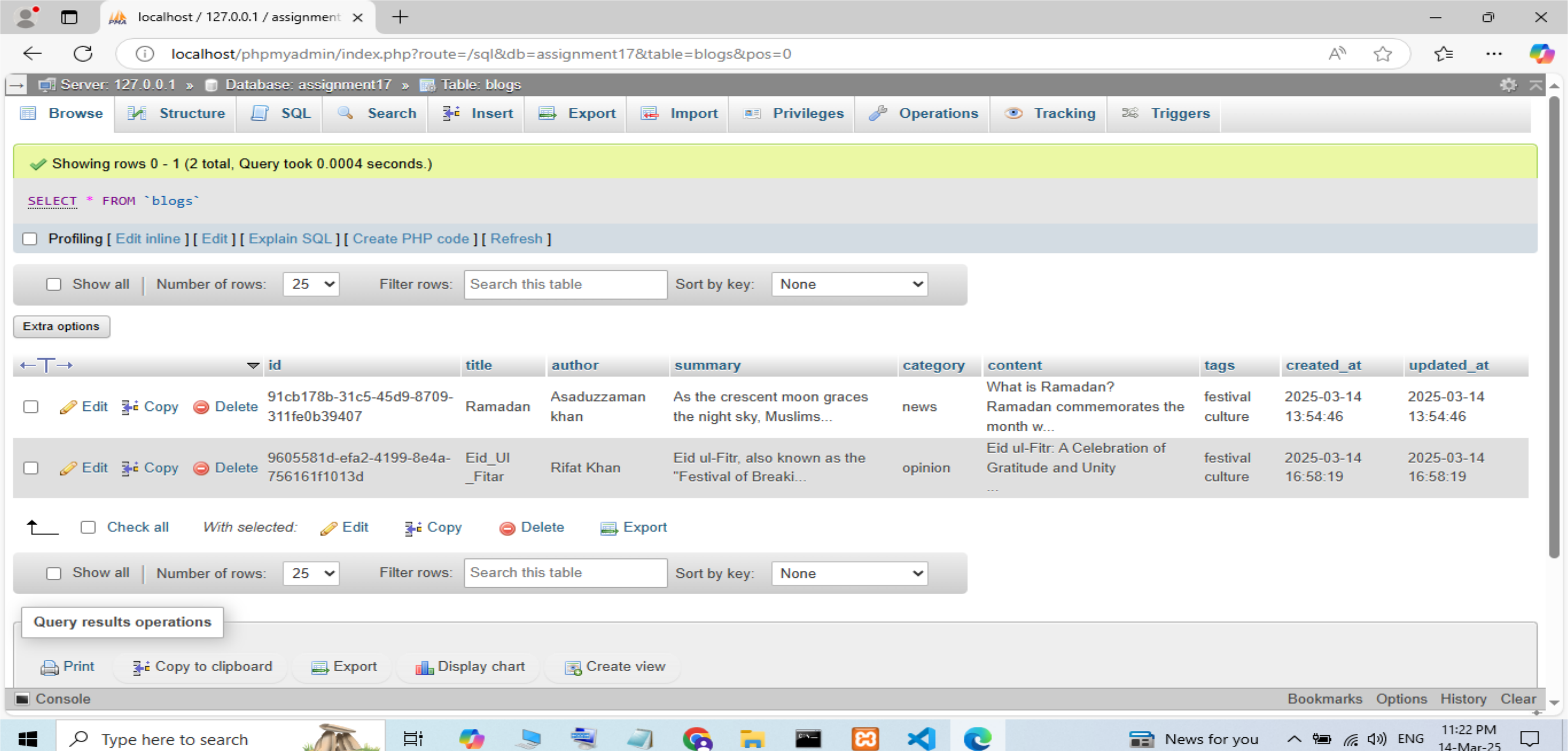
```php
namespace App\Models;

use Illuminate\Database\Eloquent\Model;
use Illuminate\Database\Eloquent\Factories\HasFactory;
use Illuminate\Support\Str;

class Blog extends Model
{
    use HasFactory;

    public $incrementing = false;  // Disable auto-incrementing ID
    protected $keyType = 'string'; // Set ID type to string (UUID)

    protected $fillable = [
        'id',       // Ensure the ID is fillable for UUIDs
        'title',
        'author',
        'summary',
        'category',
        'content',
        'tags',
    ];

    protected static function boot()
    {
        parent::boot();
        static::creating(function ($blog) {
            if (empty($blog->id)) { // Ensure we only set it if it's empty
                $blog->id = (string) Str::uuid();
            }
        });
    }
```

Changing on database


File Edit Selection View Go Run ···
assignment-17
SOURCE CONTROL
CHANGES
Message (Ctrl+Enter to commit on "main")
✓ Commit
GRAPH
Auto
Encrypted url of a blog site GitAsaduzz... main
Welcome
2025_02_18_185511_create_blogs_table.php
Blog.php
database > migrations > 2025_02_18_185511_create_blogs_table.php > class > up
main ⊗ 0 ⚠ 0
GitAsaduzzaman (4 minutes ago) Ln 9, Col 27 Spaces: 4 UTF-8 LF {} PHP Go Live
Type here to search
24°C Haze
ENG
11:17 PM
14-Mar-25

```php
<?php
use Illuminate\Database\Migrations\Migration;
use Illuminate\Database\Schema\Blueprint;
use Illuminate\Support\Facades\Schema;

return new class extends Migration
{
    /**
     * Run the migrations.
     */
    public function up(): void
    {
        Schema::create('blogs', function (Blueprint $table) {
            $table->uuid('id')->primary(); // Change from auto-increment to UUID
            $table->string('title');
            $table->string('author')->nullable();
            $table->text('summary')->nullable();
            $table->string('category')->nullable();
            $table->longText('content');
            $table->string('tags')->nullable();
            $table->timestamps();
        });
    }

    /**
     * Reverse the migrations.
     */
    public function down(): void
    {
        Schema::dropIfExists('blogs');
    }
};
```

uuid at database


localhost / 127.0.0.1 / assignment
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.)

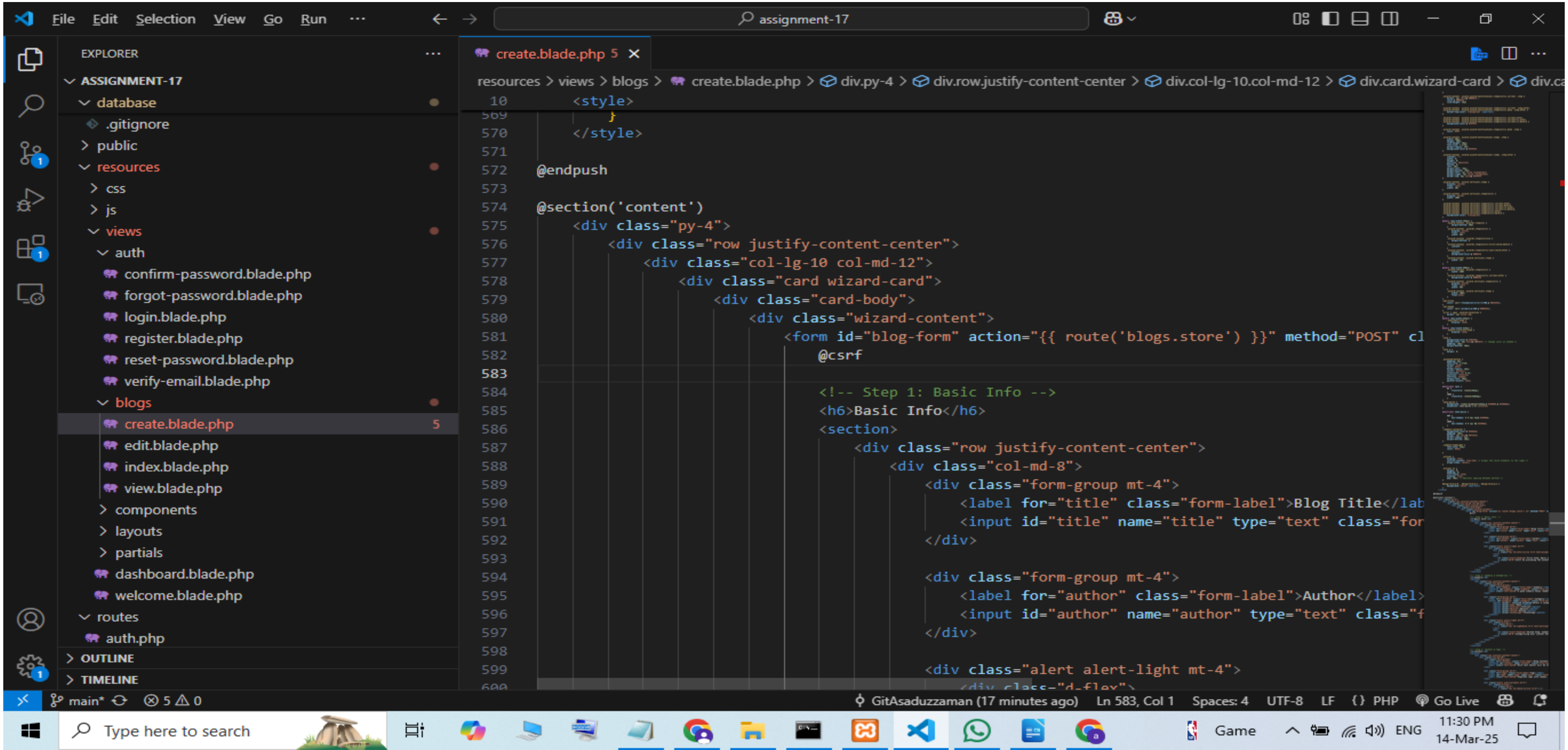
```
SELECT * FROM `blogs`
```

□ 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
□ 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
□ 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

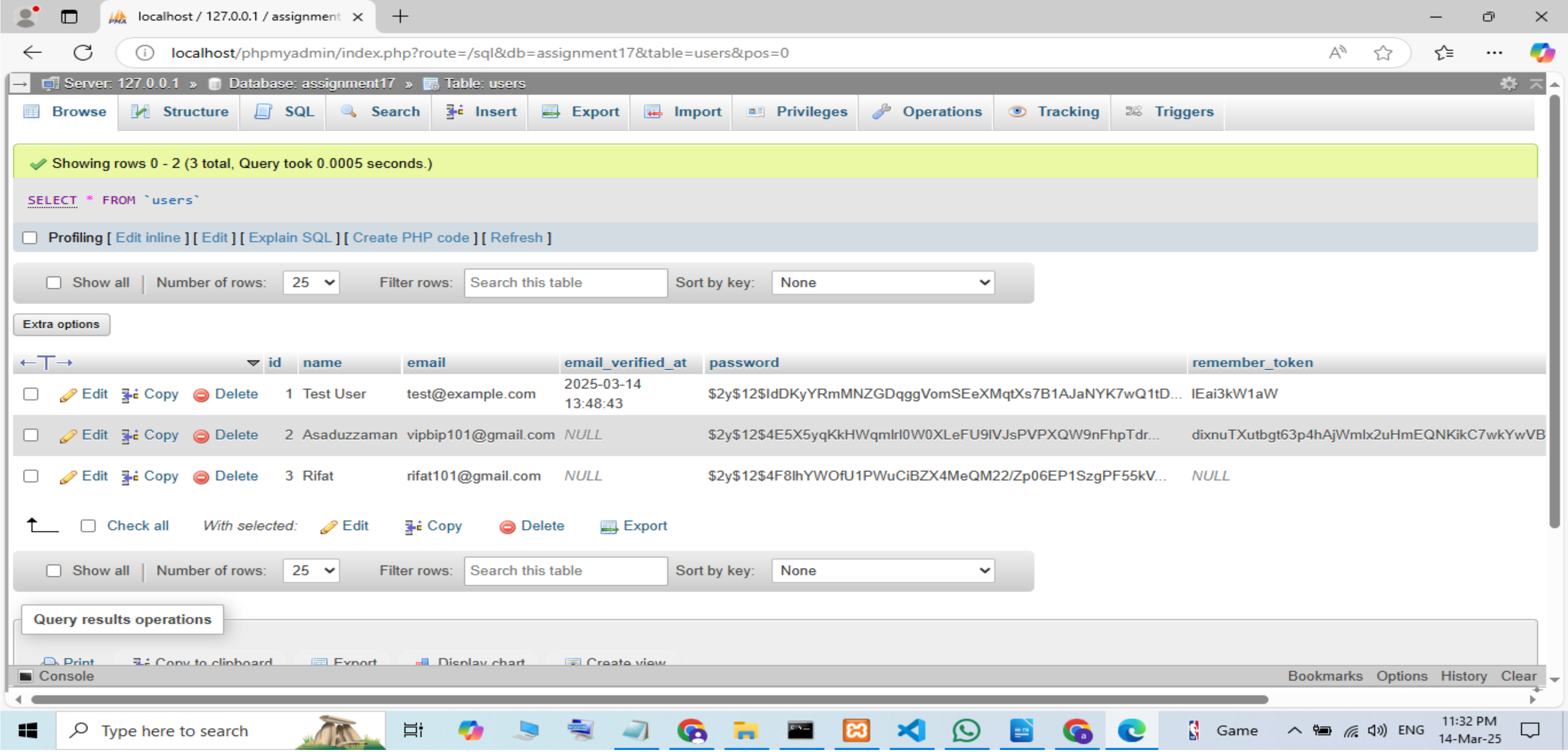
□ Check all With selected: Edit Copy Delete Export
□ Show all | Number of rows: 25 | Filter rows: Search this table | Sort by key: None
Query results operations
Print
Copy to clipboard
Export
Display chart
Create view
Console
Bookmarks Options History Clear
Type here to search
News for you
ENG
11:22 PM
14-Mar-25

CSRF



```
    <style>
        }
    </style>

@endpush

@section('content')
    <div class="py-4">
        <div class="row justify-content-center">
            <div class="col-lg-10 col-md-12">
                <div class="card wizard-card">
                    <div class="card-body">
                        <div class="wizard-content">
                            <form id="blog-form" action="{{ route('blogs.store') }}" method="POST" cl
                                @csrf

                                <!-- Step 1: Basic Info -->
                                <h6>Basic Info</h6>
                                <section>
                                    <div class="row justify-content-center">
                                        <div class="col-md-8">
                                            <div class="form-group mt-4">
                                                <label for="title" class="form-label">Blog Title</lab
                                                <input id="title" name="title" type="text" class="for
                                            </div>

                                            <div class="form-group mt-4">
                                                <label for="author" class="form-label">Author</label>
                                                <input id="author" name="author" type="text" class="f
                                            </div>

                                            <div class="alert alert-light mt-4">
                                                <div class="d-flex">
```

Password Hashing



localhost / 127.0.0.1 / assignment
localhost/phpmyadmin/index.php?route=/sql&db=assignment17&table=users&pos=0
Server: 127.0.0.1 » Database: assignment17 » Table: users
Browse
Structure
SQL
Search
Insert
Export
Import
Privileges
Operations
Tracking
Triggers

✓ 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

				id	name	email	email_verified_at	password	remember_token
□	Edit	Copy	Delete	1	Test User	test@example.com	2025-03-14 13:48:43	$2y$12$IdDKyYRmMNZGDqggVomSEeXMqtXs7B1AJaNYK7wQ1tD...	lEai3kW1aW
□	Edit	Copy	Delete	2	Asaduzzaman	vipbip101@gmail.com	NULL	$2y$12$4E5X5yqKkHWqmlrl0W0XLeFU9lVJsPVPXQW9nFhpTdr...	dixnuTXutbgt63p4hAjWmlx2uHmEQNKikC7wkYwVB
□	Edit	Copy	Delete	3	Rifat	rifat101@gmail.com	NULL	$2y$12$4F8lhYWOfU1PWuCiBZX4MeQM22/Zp06EP1SzgPF55kV...	NULL

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

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