WAPH - Web Application Programming and Hacking

WAPH-Web Application Programming and Hacking
Instructor: Dr. Phu Phung

Student

Name: Ryan Cheng
Email: chengr4@udayton.edu

Short-bio: Ryan Cheng has an interest in computer security and playing the violin.

Figure 1: Ryan Cheng

Repository's URL: Github Repo

Team Repository: Team Repo

miniFacebook - Sprint 1

Team Project - Web Application Programming and Hacking

Project Description

This is Sprint 1 of the miniFacebook project, a simplified yet secure social networking web application built with PHP/MySQL technologies and implementing secure programming principles.

Sprint 1 Features Implemented

Database Design: Users table with phone field, Posts table with foreign key relationships **User Registration**: Complete registration system with input validation **User Login**: Secure authentication system accepting username or email **Profile Management**: Users can edit their profile including name, email, and phone **Password Management**: Secure password change functionality **Posts Viewing**: Users can view all posts from the database **Session Management**: Secure session handling with hijacking protection **CSRF Protection**: All forms protected against CSRF attacks **Input Validation**: Multi-layer validation (HTML5, PHP, SQL)

Setup Instructions

1. **Database Setup**:

   ```
   mysql -u root -p < database_account.sql
   mysql -u team12 -p  waph_team < database_data.sql
   ```

2. **Default Login**: Username: `admin` Password: `team12`

Security Features That Have Been Implemented

Passwords hashed in database using PHP's password_hash() All SQL queries use prepared statements Input validation at HTML, PHP, and SQL layers HTML outputs sanitized to prevent XSS Session hijacking protection (browser/IP validation) CSRF protection with random tokens Secure session cookie parameters

Database Schema

Users Table: username (VARCHAR, PRIMARY KEY) password (VARCHAR, hashed) email (VARCHAR) full_name (VARCHAR) phone (VARCHAR)

Posts Table: id (INT, AUTO_INCREMENT, PRIMARY KEY) title (VARCHAR) content (TEXT) owner (VARCHAR, FOREIGN KEY) created_at (TIMESTAMP)

Sprint 1 Requirements Status

In this Sprint, I implemented the followings: Database Design and Implementation User registration and login Change password functionality Edit profile (name, email, phone) View posts from database All security requirements met

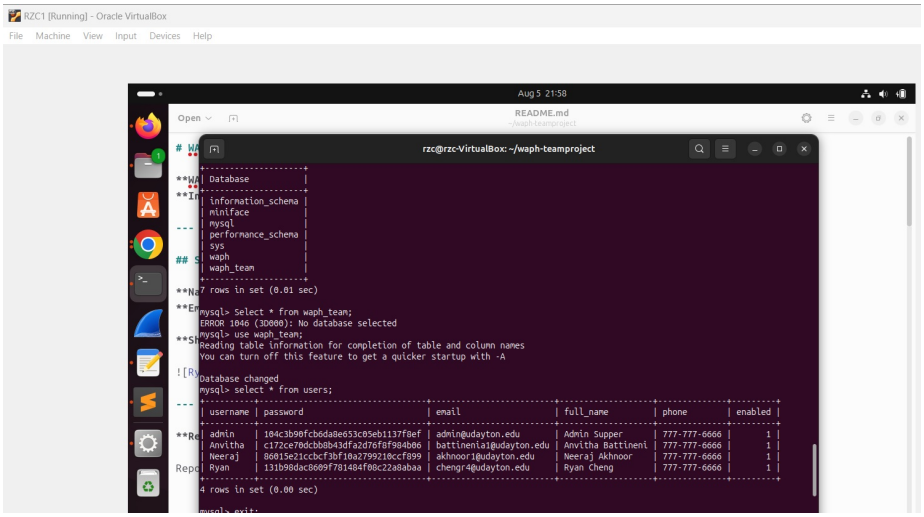

Figure 0.3. – Database - User Table

```
mysql> describe users;
+-----------+--------------+------+-----+---------+-------+
| Field     | Type         | Null | Key | Default | Extra |
+-----------+--------------+------+-----+---------+-------+
| username  | varchar(50)  | NO   | PRI | NULL    |       |
| password  | varchar(100) | NO   |     | NULL    |       |
| email     | varchar(255) | YES  |     | NULL    |       |
| full_name | varchar(255) | YES  |     | NULL    |       |
+-----------+--------------+------+-----+---------+-------+
4 rows in set (0.00 sec)
```

Figure 0.3. – Describe Users

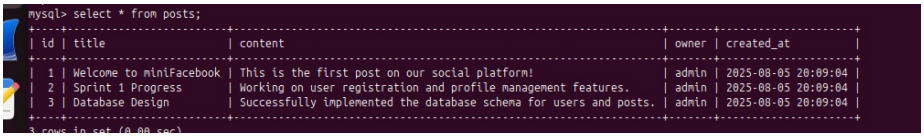

Figure 0.3. – Posts Description

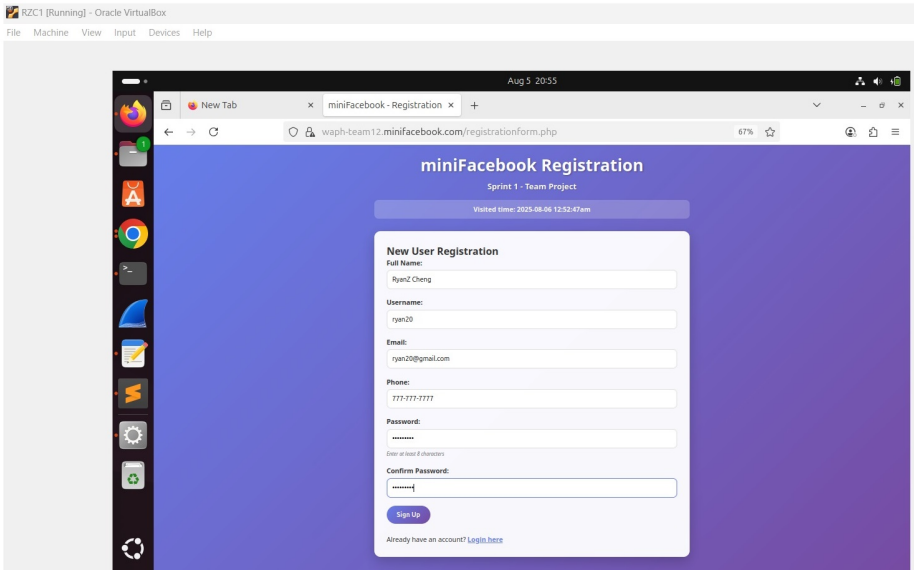

Figure 1. – new user registration form

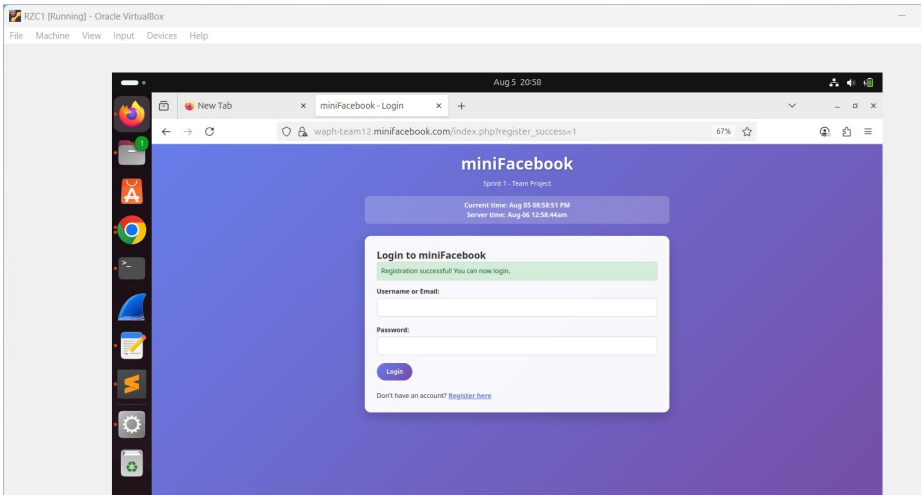

Figure 2. – Successful Registration

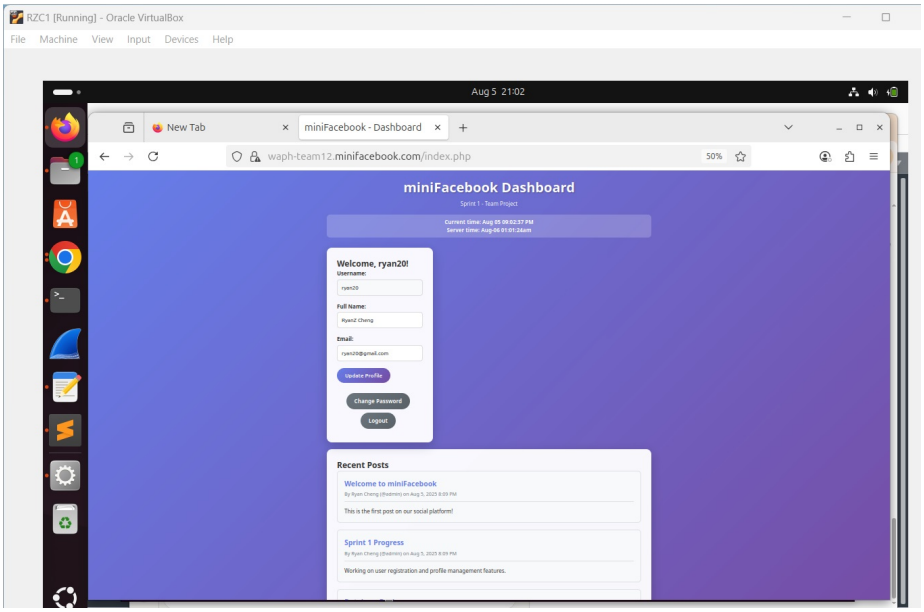

Figure 3. – Successful Login Showing Recent Posts