PROGRAM (backend)

<?php

// Check if the session is already started

if (session\_status() == PHP\_SESSION\_NONE) {

session\_start();

}

// Initializing variables

$username = "";

$email = "";

$errors = array();

// Connect to the database

$db = mysqli\_connect('localhost', 'root', '', 'registration');

// Check connection

if (!$db) {

die("Connection failed: " . mysqli\_connect\_error());

}

// Clean up the database before any operations

// Check for existing rows with primary key 0

$result = mysqli\_query($db, "SELECT \* FROM users WHERE id = 0");

if (mysqli\_num\_rows($result) > 0) {

// Delete rows with primary key 0

mysqli\_query($db, "DELETE FROM users WHERE id = 0");

}

// Reset AUTO\_INCREMENT

mysqli\_query($db, "ALTER TABLE users AUTO\_INCREMENT = 1");

// REGISTER USER

if (isset($\_POST['reg\_user'])) {

// Receive all input values from the form

$username = mysqli\_real\_escape\_string($db, $\_POST['username']);

$email = mysqli\_real\_escape\_string($db, $\_POST['email']);

$password\_1 = mysqli\_real\_escape\_string($db, $\_POST['password\_1']);

$password\_2 = mysqli\_real\_escape\_string($db, $\_POST['password\_2']);

// Form validation

if (empty($username)) {

array\_push($errors, "Username is required");

}

if (empty($email)) {

array\_push($errors, "Email is required");

}

if (empty($password\_1)) {

array\_push($errors, "Password is required");

}

if ($password\_1 != $password\_2) {

array\_push($errors, "The two passwords do not match");

}

// Check if user already exists

$user\_check\_query = "SELECT \* FROM users WHERE username=? OR email=?";

$stmt = mysqli\_prepare($db, $user\_check\_query);

mysqli\_stmt\_bind\_param($stmt, "ss", $username, $email);

mysqli\_stmt\_execute($stmt);

$result = mysqli\_stmt\_get\_result($stmt);

$user = mysqli\_fetch\_assoc($result);

if ($user) { // if user exists

if ($user['username'] === $username) {

array\_push($errors, "Username already exists");

}

if ($user['email'] === $email) {

array\_push($errors, "Email already exists");

}

}

// Register user if there are no errors

if (count($errors) == 0) {

$password = md5($password\_1); // Encrypt the password

$query = "INSERT INTO users (username, email, password) VALUES (?,?,?)";

$stmt = mysqli\_prepare($db, $query);

if ($stmt) {

mysqli\_stmt\_bind\_param($stmt, "sss", $username, $email, $password);

mysqli\_stmt\_execute($stmt);

$\_SESSION['username'] = $username;

$\_SESSION['success'] = "You are now logged in";

header('location: index.php');

exit(); // Always exit after header redirect

} else {

array\_push($errors, "Error preparing statement: " . mysqli\_error($db));

}

}

}

// LOGIN USER

if (isset($\_POST['login\_user'])) {

$username = mysqli\_real\_escape\_string($db, $\_POST['username']);

$password = mysqli\_real\_escape\_string($db, $\_POST['password']);

if (empty($username)) {

array\_push($errors, "Username is required");

}

if (empty($password)) {

array\_push($errors, "Password is required");

}

if (count($errors) == 0) {

$password = md5($password); // Encrypt the password

$query = "SELECT \* FROM users WHERE username=? AND password=?";

$stmt = mysqli\_prepare($db, $query);

mysqli\_stmt\_bind\_param($stmt, "ss", $username, $password);

mysqli\_stmt\_execute($stmt);

$results = mysqli\_stmt\_get\_result($stmt);

if (mysqli\_num\_rows($results) == 1) {

$\_SESSION['username'] = $username;

$\_SESSION['success'] = "You are now logged in";

header('location: index.php');

exit(); // Always exit after header redirect

} else {

array\_push($errors, "Wrong username/password combination");

}

}

}

?>