

# ДОКУМЕНТАЦИЈА ЗА ЛАБОРАТОРИСКА ВЕЖБА 2 ПО ПРЕДМЕТОТ ИНФОРМАЦИСКА БЕЗБЕДНОСТ

## 1. Вовед

### 1.1 Цел на лабораториската вежба

Цел на оваа лабораториска вежба е имплементација на систем за дво-факторна корисничка автентификација. Системот обезбедува двофазна регистрација, при што корисниците по регистрација добиваат верификациски код за потврда на емаил адресата. По успешно верификација, корисникот може да се најави на системот, каде повторно користи 2FA код за потврда на идентитетот. Системот дополнително овозможува и безбедно менаџирање на корисничките информации и сесии.

Оваа лабораториска вежба е изработена од Мартина Петковска со индекс број 223313.

Целиот документ може да се најде на GitHub: [https://github.com/mpetkovska27/IB\\_2025\\_lab2](https://github.com/mpetkovska27/IB_2025_lab2)

### 1.2 Користени технологии

- Backend: PHP
- Frontend: HTML5, CSS
- База на податоци: SQLite

#### СТРУКТУРА НА ПРОЕКТОТ:

ib\_lab2\_223313/

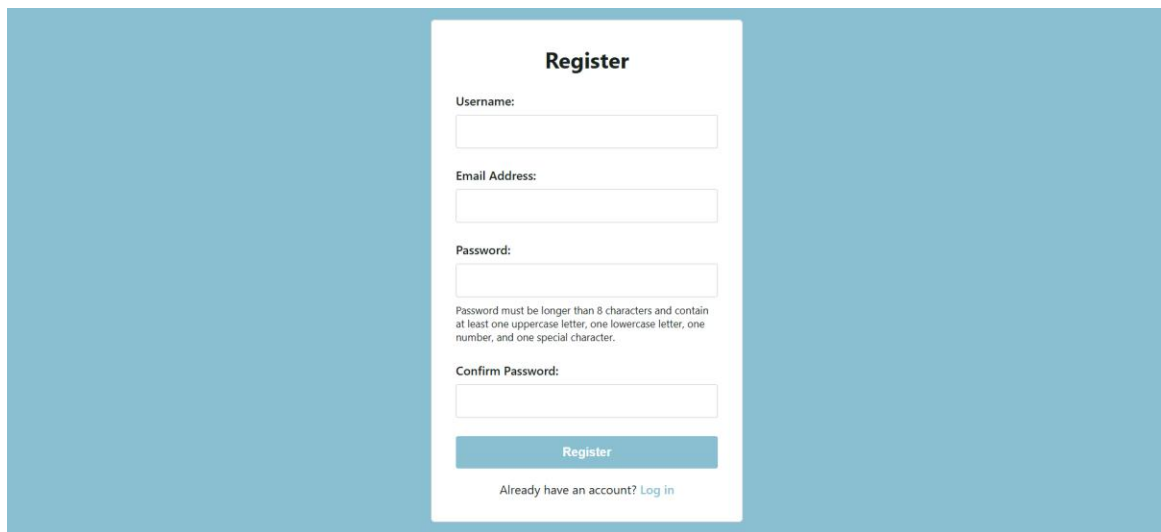
- assets/
- css/
  - o style.css # Стили за апликацијата
- config/
  - o db\_connection.php # Конекција со SQLite база
  - o session.php # Управување со сесии и cookies
  - o two\_factor\_verification.php # Функции за верификациски кодови
- includes/
  - o auth.php # Функции за автентификација
- database/
  - o db.sqlite # SQLite база на податоци
- index.php # Главна страна (за најавени корисници)
- register.php # Регистрација
- login.php # Најава
- logout.php # Одјава
- edit\_profile.php # Менаџирање со корисничките податоци

## 2. Функционалности

### 2.1 Корисничка регистрација (register.php)

#### ЧЕКОР 1: Внес на кориснички податоци

- Внес на кориснички податоци (Username, Email Address и Password)
- Валидација
  - Username: 3-50 карактери
  - Email: валиден формат
  - Password: повеќе од 8 карактери, барем една голема буква, една мала, бројка и специјален знак.

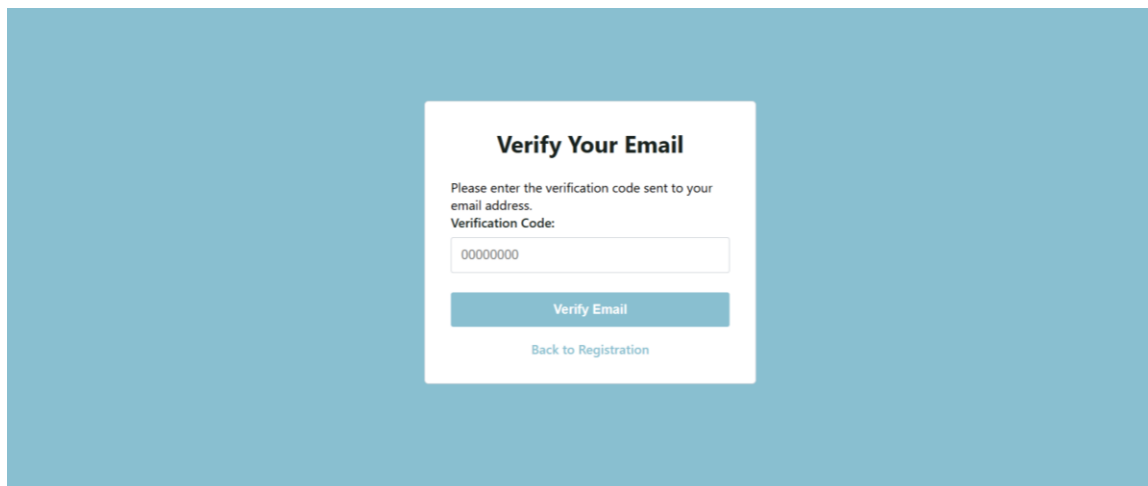
A screenshot of a web form titled "Register" on a light blue background. The form is white and contains four input fields: "Username:", "Email Address:", "Password:", and "Confirm Password:". Below the "Password:" field, there is a small text note: "Password must be longer than 8 characters and contain at least one uppercase letter, one lowercase letter, one number, and one special character." At the bottom of the form is a blue button labeled "Register" and a link that says "Already have an account? Log in".

#### ЧЕКОР 2: Верификација на електронска пошта

По успешна регистрација, системот:

- Генерира 8-цифрен верификациски код со времетраење од 15 минути
- Корисникот го внесува кодот за да ја потврди својата емаил поштата

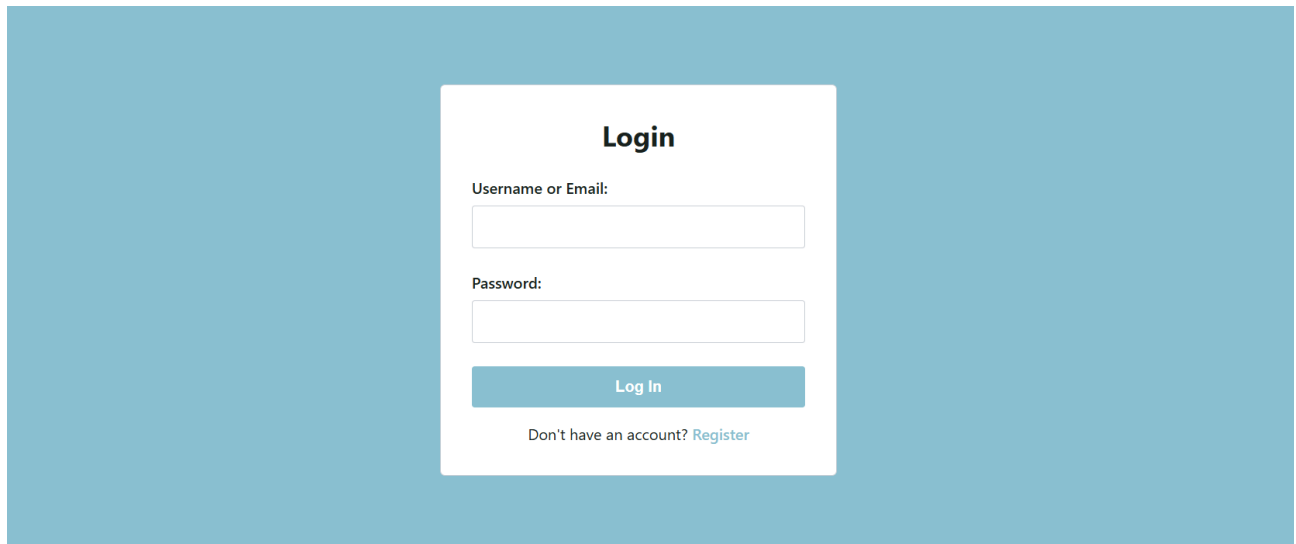
**Важно:** Корисникот не може да се најави додека не ја верифицира емаил адресата.

A screenshot of a web form titled "Verify Your Email" on a light blue background. The form is white and contains a text prompt: "Please enter the verification code sent to your email address." Below this is a label "Verification Code:" followed by an input field containing the placeholder text "00000000". At the bottom of the form is a blue button labeled "Verify Email" and a link that says "Back to Registration".

## 2.2 Корисничка најава (login.php)

### ЧЕКОР 1: Внес на кориснички податоци

- Најава со username или email
  - Верификација на лозинка со password\_verify() - повеќе од 8 карактери, барем една голема буква, една мала, бројка и специјален знак.

A screenshot of a login form titled "Login" centered on a light blue background. The form is white and contains two input fields: "Username or Email:" and "Password:". Below the password field is a blue "Log In" button. At the bottom of the form, there is a link that says "Don't have an account? Register".

**Login**

Username or Email:

Password:

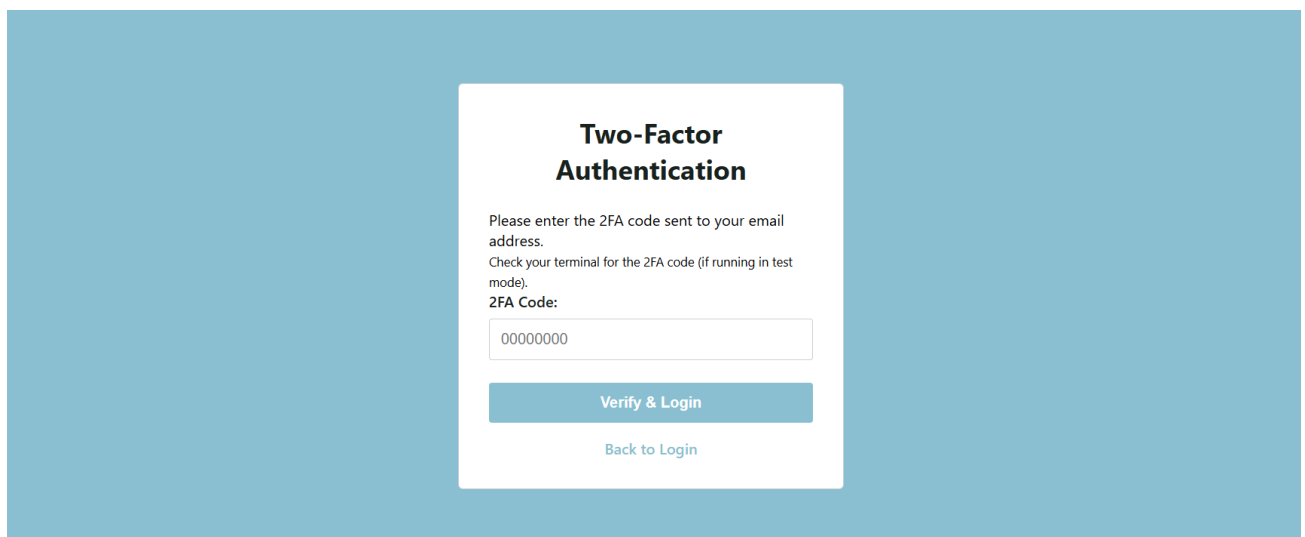
Log In

Don't have an account? [Register](#)

### ЧЕКОР 2: Двофакторна верификација (2FA)

По успешна верификација на податоците од корисникот, системот:

- Генерира 8-цифрен 2FA код
- Корисникот го внесува кодот за да ја заврши најавата
- По успешна верификација, се креира session token и сесија

A screenshot of a two-factor authentication form titled "Two-Factor Authentication" centered on a light blue background. The form is white and contains a text block with instructions: "Please enter the 2FA code sent to your email address. Check your terminal for the 2FA code (if running in test mode)." Below this is a label "2FA Code:" followed by an input field containing "00000000". At the bottom of the form, there is a blue "Verify & Login" button and a link that says "Back to Login".

**Two-Factor Authentication**

Please enter the 2FA code sent to your email address.  
Check your terminal for the 2FA code (if running in test mode).

2FA Code:

Verify & Login

[Back to Login](#)

## 2.3 Главна страна (index.php)

- Приказ на информации за најавениот корисник
- Листа на сите регистрирани корисници
- Навигација до Edit Profile и Logout
- Само за најавени корисници

[Auth System](#)

Welcome, mpet![Edit Profile](#)[Logout](#)

## User Two-Factor Authentication System

Lab exercise, made by Martina Petkovska - 223313, that implements a complete two-factor authentication solution for secure user management

### About This Lab Exercise

This application demonstrates a complete user authentication system implemented as part of a laboratory exercise. The system provides:

- secure user registration with email verification,
- two-factor authentication (2FA) for login,
- secure session management with HTTP-only cookies,
- and user data management.

### Your Account Information

Username: mpet

Email: mpet@test.com

Registered on: November 11, 2025 at 4:48 PM

### Registered Users

ID	Username	Email	Registered
9	vbla	vbla@test.com	Nov 11, 2025
8	asto	asto@test.com	Nov 11, 2025
7	ilat	ilat@test.com	Nov 11, 2025
6	mpet	mpet@test.com	Nov 11, 2025
3	mso	mso@test.com	Nov 11, 2025

Total users: 5

© 2025 User Authentication System - Laboratory Exercise 1

## 2.4 Менаџирање со кориснички податоци (edit\_profile.php)

- Ажурирање на веќе постоечки информации (име, презиме, username и email)
- Промени лозинка (со верификација на тековната лозинка)
- Избрише профил (со потврда на лозинка)

[Auth System](#)

Welcome, mpet![Home](#)[Logout](#)

### Edit Profile

#### Personal Information

First Name:

Last Name:

Username:

Email Address:

Update Personal Information

#### Change Password

Current Password:

New Password:

Password must be longer than 8 characters and contain at least one uppercase letter, one lowercase letter, one number, and one special character.

Confirm New Password:

Change Password

#### Delete Account

**Warning:** This action cannot be undone. All your data will be permanently deleted.

Enter your password to confirm deletion:

Delete My Account

Back to Home

© 2025 User Authentication System - Laboratory Exercise 1

## 2.5 Одјава (logout.com)

- Бришење на сесија
- Пренасочување на login.php

## Управување со сесии

Системот користи два механизми за управување со сесии:

- PHP сесии: Зачувува user\_id, username, email и session\_token
- HTTP-only колачиња: Зачувува session\_token

При секоја страница се проверува:

- Дали постои валидна сесија
- Дали токенот во сесијата се совпаѓа со токенот во колачето
- Дали корисникот е најавен

## База на податоци

```
CREATE TABLE IF NOT EXISTS users (  
  id INTEGER PRIMARY KEY AUTOINCREMENT,  
  username TEXT NOT NULL UNIQUE,  
  email TEXT UNIQUE NOT NULL,  
  password_hash TEXT NOT NULL,  
  first_name TEXT,  
  last_name TEXT,  
  email_verified INTEGER DEFAULT 0,  
  email_verification_code TEXT,  
  email_verification_expires DATETIME,  
  two_factor_code TEXT,  
  two_factor_code_expires DATETIME,  
  created_at DATETIME DEFAULT CURRENT_TIMESTAMP,  
  updated_at DATETIME DEFAULT CURRENT_TIMESTAMP  
);
```

Се користи фајлот db\_connection.php за конекција со SQLite база на податоци.

## Auth функции (includes/auth.php)

### validatePassword(\$password)

- Проверува: должина >8, голема буква, мала буква, бројка, специјален знак.
- Враќа: ['valid' => false, 'message' => 'Password must be longer than 8 characters.']

### registerUser(\$username, \$email, \$password)

- Регистрира нов корисник, проверува уникатност на username и email, валидира и зачувува во база
- Хешира лозинка со password\_hash()
- Генерира email verification code (8 цифри, валиден 15 минути)
- Испраќа email со кодот
- Враќа: ['success' => bool, 'message' => string]

### **verifyEmailWithCode(\$userId, \$code)**

- Проверува дали внесениот код се совпаѓа и дали е валиден (не е истечен) и ако е точен, ажурира `is_verified = 1`
- Враќа: `['success' => bool, 'message' => string]`

### **loginUser(\$usernameOrEmail, \$password)**

- Најава на корисник, прима влезни податоци за корисникот, прави валидација на лозинката
- Проверува дали `is_verified = 1`
- Верифицира лозинка со `password_verify()`
- Ако е успешна, генерира и зачувува 8-цифрен 2FA код (валиден 10 минути)
- Враќа: `['success' => bool, 'message' => string, 'user_id' => int|null]`

### **verifyTwoFactorCode(\$userId, \$code)**

- Проверува дали внесениот 2FA код се совпаѓа и дали е валиден
- Ако е точен, генерира session token и креира сесија за корисникот
- Враќа: `['success' => bool, 'message' => string]`

Останати функции:

- `getCurrentUser()`
- `getAllUsers()`
- `updateUserInfo($userId, $username, $email, $firstName = "", $lastName = "")`
- `updatePassword($userId, $currentPassword, $newPassword, $confirmPassword)`
- `deleteUser($userId, $password)`

## **Session функции (config/session.php)**

### **generateSessionToken()**

- Генерира 64-карактерен hex токен со `random_bytes()` и `bin2hex()`
- Враќа string (session token)

### **setSessionTokenCookie(\$token)**

- Поставува cookie со името `session_token`
- `HttpOnly` и `Secure` (ако е HTTPS)
- Истекува после 7 дена
- Се повикува само по успешна 2FA верификација

### **clearSessionTokenCookie()**

- Брише session token cookie
- Поставува `expire` на минус време

Останати функции:

- `isLoggedIn()`
- `requireLogin()`
- `requireGuest()`
- `logout()`

## Двофакторна верификација (two\_factor\_verification.php)

**Цел:** Проверка на 2FA код по успешна најава.

### verifyTwoFactorCode(\$userId, \$code)

- Ако е точен и валиден:
  - Се генерира session token (generateSessionToken())
  - Се поставува cookie (setSessionTokenCookie(\$token))
  - Се креира PHP сесија за најавениот корисник
- Ако не е точен: се прикажува порака за грешка

По успешна верификација, корисникот се пренасочува на index.php

## Тестирање

1. Регистрација: Отворете register.php и регистрирајте нов корисник
2. Верификација: Внесете го кодот што се прикажува во терминалот
3. Најава: Отворете login.php и најавете се со корисничко име и лозинка
4. 2FA: Внесете го 2FA кодот што се прикажува во терминалот
5. Профил: Ажурирајте ги информациите или променете лозинка

**Забелешка:** Во тест режим, верификациските кодови се прикажуваат во терминалот. Во продукција, тие би се праќале по е-пошта.

## 3. Забелешки

- Базата се креира автоматски при прво повикување
- Session cookie се креира само по успешна 2FA верификација и истекува после 7 дена.
- First Name и Last Name се опционални
- При регистрација се генерира верификациски код за емаил адреса, кој е валиден 15 минути и без кој не е дозволена најава.
- 2FA кодот се генерира по успешна проверка на податоците при најава и е валиден 10 минути.
- Се користат пастелни бои и едноставен, минималистички дизајн.
- Проектот имплементира основни безбедносни практики за веб-апликација за автентикација.