

ЗВІТ ПРО ТЕСТУВАННЯ

Проект: The Internet – Login Form

Посилання: <https://the-internet.herokuapp.com/login>

Тип тестування: Ручне (Manual QA)

Дата: 19.02.2026

Тестувальник: Богдан Когут

Короткий опис тестування

Проведено ручне функціональне тестування форми входу.

Перевірено позитивні та негативні сценарії авторизації, обробку помилок та граничні випадки (edge cases).

БАГ-РЕПОРТИ

БАГ №1

Назва: Некоректне повідомлення про помилку при порожньому Username

Кроки відтворення:

1. Відкрити сторінку логіну
2. Залишити поле Username порожнім
3. Ввести пароль
4. Натиснути Login

Очікуваний результат:

Система повинна показати повідомлення про обов'язковість заповнення поля Username.

Фактичний результат:

Відображається повідомлення:

“Your username is invalid!”

Пріоритет: Низький

БАГ №2

Назва: Вхід з неправильним паролем відображає неточне повідомлення про помилку

Кроки відтворення:

1. Відкрити сторінку логіну
2. Ввести правильний username: tomsmith
3. Ввести неправильний пароль
4. Натиснути кнопку "Login"

Очікуваний результат:

Система повинна повідомити, що пароль введено неправильно.

Фактичний результат:

Відображається повідомлення:
"Your username is invalid!"

Коментар:

Повідомлення не уточнює, що саме є неправильним (логін чи пароль), що може вводити користувача в оману.

Пріоритет: Низький

БАГ №3

Назва: Система не обробляє пробіли перед та після введення Username

Кроки відтворення:

1. Відкрити сторінку логіну
2. Ввести username: tomsmith (з пробілами на початку та в кінці)
3. Ввести правильний пароль: SuperSecretPassword!
4. Натиснути кнопку "Login"

Очікуваний результат:

Система повинна автоматично ігнорувати зайві пробіли перед та після username та дозволити успішний вхід.

Фактичний результат:

Система не здійснює вхід та відображає повідомлення про помилку.

Коментар:

Відсутність обробки зайвих пробілів може спричиняти помилки авторизації та негативно впливати на користувацький досвід.

Пріоритет: Середній

БАГ №4

Назва: Відсутнє обмеження кількості спроб входу (можливість brute-force атак)

Кроки відтворення:

1. Відкрити сторінку логіну
2. Ввести будь-який username
3. Ввести неправильний пароль
4. Натиснути кнопку "Login"
5. Повторити спробу входу 10+ разів

Очікуваний результат:

Після декількох невдалих спроб система повинна:

- тимчасово заблокувати обліковий запис, або
- обмежити кількість спроб входу, або
- запропонувати CAPTCHA.

Фактичний результат:

Система дозволяє необмежену кількість спроб входу без додаткових перевірок або обмежень.

Коментар:

Відсутність обмеження спроб входу створює ризик brute-force атак та знижує рівень безпеки системи.

Пріоритет: Високий

БАГ №5

Назва: Повідомлення про помилку не прив'язане до конкретного поля (незрозуміло, що саме неправильно)

Кроки відтворення:

1. Відкрити сторінку логіну
2. Ввести неправильний username **або** залишити поле Username порожнім
3. Ввести будь-який пароль
4. Натиснути кнопку "Login"

Очікуваний результат:

Система повинна показувати помилку біля конкретного поля (Username або Password) та/або явно вказати, яке саме поле заповнено неправильно (наприклад: "Username is required" або "Incorrect password").

Фактичний результат:

Система показує загальне повідомлення про помилку без чіткої прив'язки до поля, через що користувачу складніше зрозуміти, що саме потрібно виправити.

Коментар:

UX можна покращити, якщо показувати помилки під відповідними полями та робити повідомлення більш конкретним.

Пріоритет: Середній



Назва: Поле Username не отримує автоматичний фокус після помилки авторизації

Кроки відтворення:

1. Відкрити сторінку логіну
2. Ввести неправильний username або пароль
3. Натиснути кнопку "Login"
4. Дочекатися відображення повідомлення про помилку

Очікуваний результат:

Після відображення помилки курсор повинен автоматично переміститися в поле Username або Password для зручного повторного введення даних.

Фактичний результат:

Курсор не встановлюється автоматично в поле введення, користувачу потрібно вручну клікати в поле для повторної спроби.

Коментар:

Відсутність автоматичного фокусу знижує зручність використання форми та сповільнює повторну спробу входу.

Пріоритет: Низький