МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ УКРАЇНИ
«КИЇВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ імені ІГОРЯ СІКОРСЬКОГО»

Навчально-науковий інститут атомної та теплової енергетики
Кафедра інженерії програмного забезпечення в енергетиці

Методика забезпечення функціональної стійкості кіберзахисту систем керування базами данних

Виконала:

Студентка групи ТВ-42мп

Плачинда Маргарита Володимирівна

Керівник:

доцент

Шуклін Герман Вікторович

м. Київ - 2025

Постановка задач

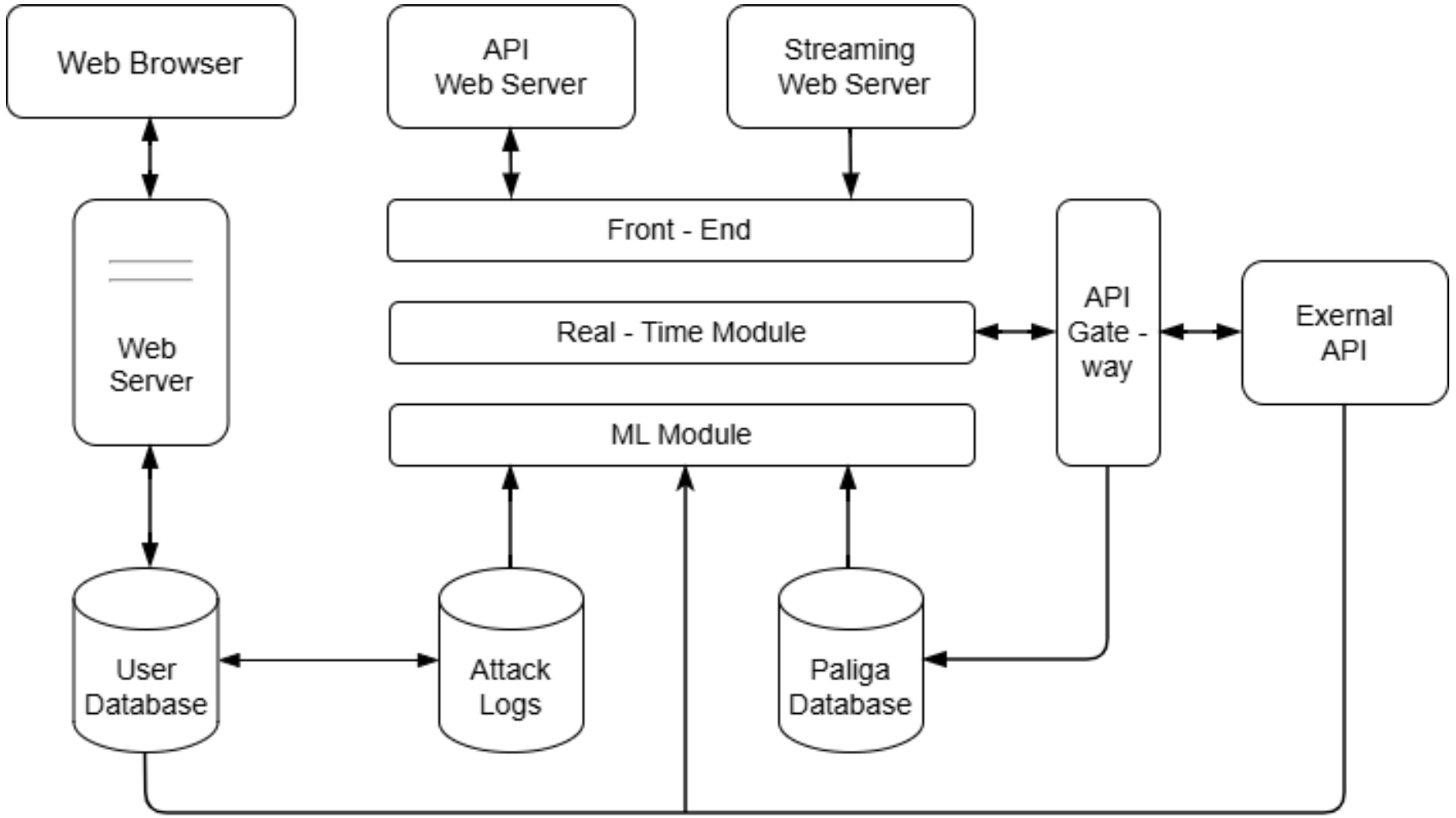
Мета роботи - розробка веб-застосунку для забезпечення функціональної стійкоскі кіберзахисту системи керування базами даних.

1) Проаналізувати існуючі методи кіберзахисту системи керування БД.
2) Розробити архітектури веб-застосунку.
3) Реалізувати модуль перевірки SQL-запитів на основі правил і ML-моделі.
4) Створити модуль симуляції атак та моніторингу в реальному часі.
5) Провести дослідження ефективності розробленої системи.

Опис предметної області

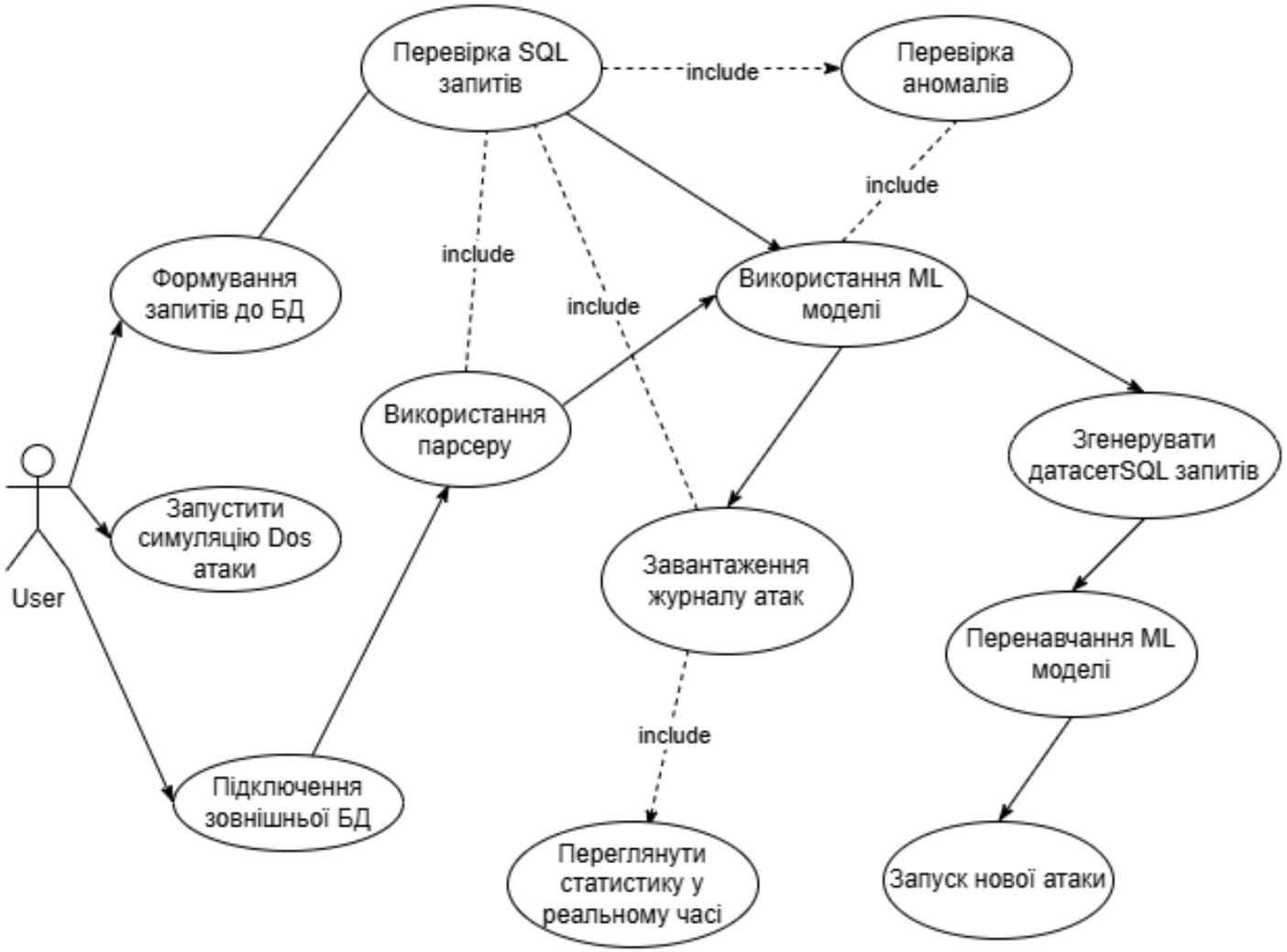
Предметна область охоплює процеси взаємодії користувача з системами керування базами даних у контексті аналізу й оцінювання SQL-запитів та поведінки бази даних під час навантаження. Центральним елементом є можливість підключення до зовнішніх реальних баз, отримання їхньої структури та автоматичне формування на основі цих даних різноманітних SQL-запитів, що створюють репрезентативні датасети. У межах цієї області розглядається комбінований механізм перевірки запитів, який включає синтаксичний аналіз за правилами й машинне навчання для класифікації нормальних та підозрілих операцій. Також важливим аспектом є реєстрація всіх виконаних запитів, їх подальший аналіз, а також відображення ключових показників роботи системи в режимі реального часу. Окремим процесом предметної області є адаптивне оновлення моделі класифікації на основі нових логів і згенерованих датасетів, що забезпечує здатність системи самонавчатися й підтримувати свою ефективність у змінних умовах.

Архітектура системи

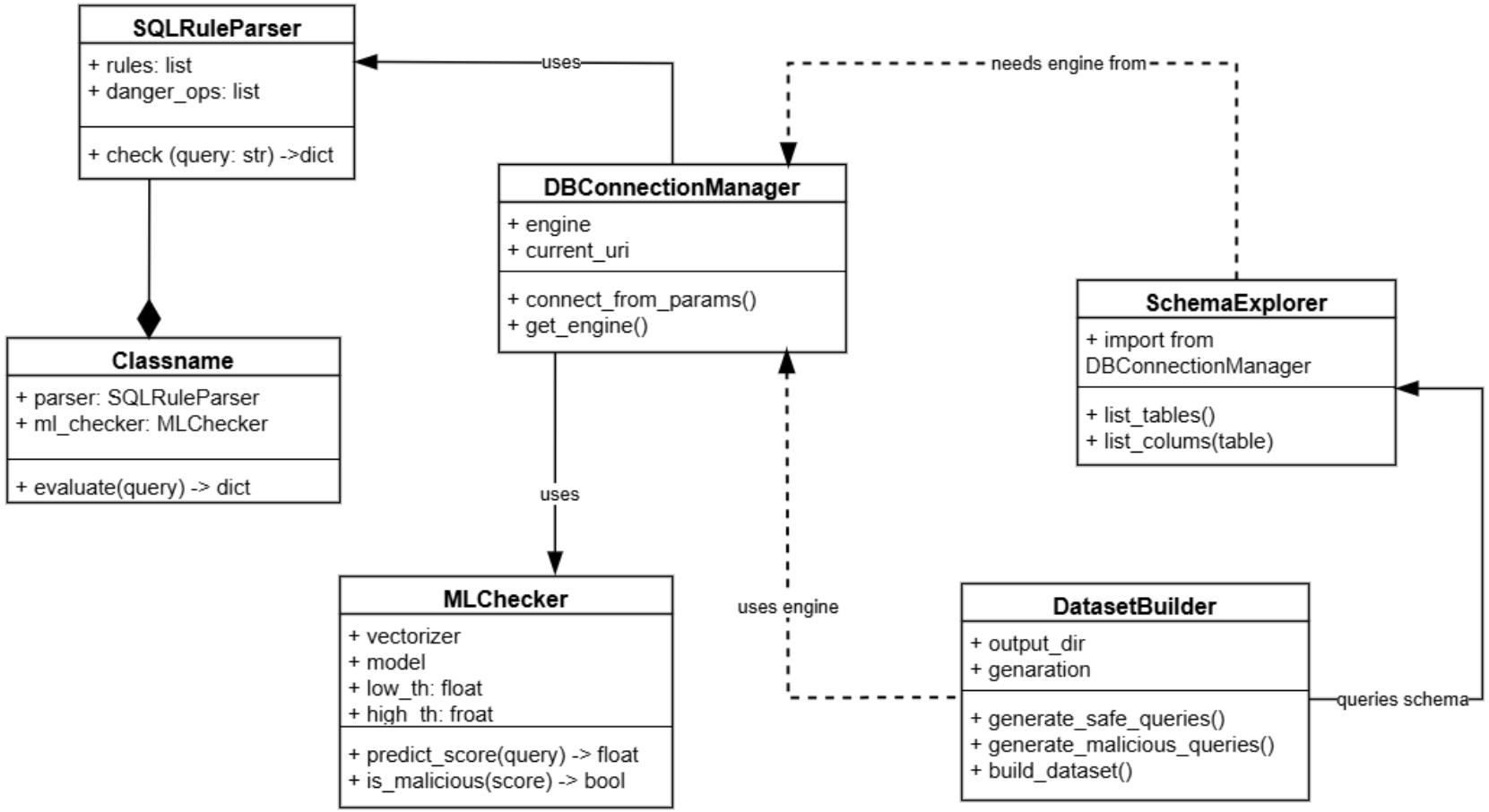


Концептуальна модель ситеми

Діаграма прецедентів



Uml діаграма



Засоби розробки

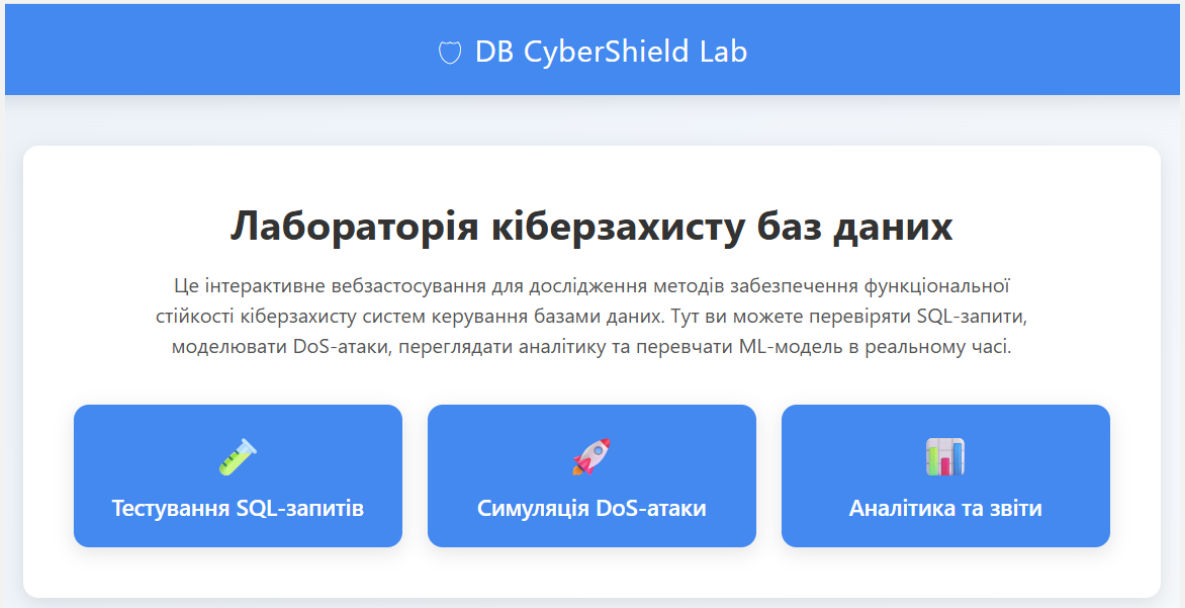
PyCharm

Flask

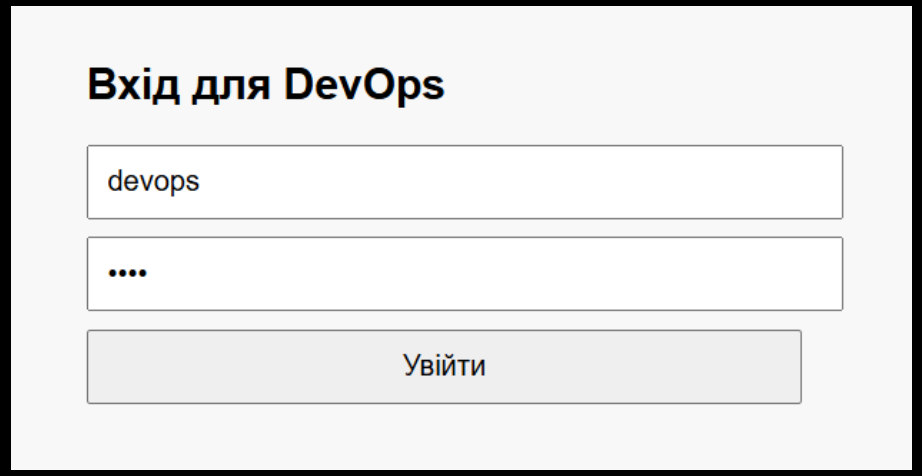
PostgreSQL

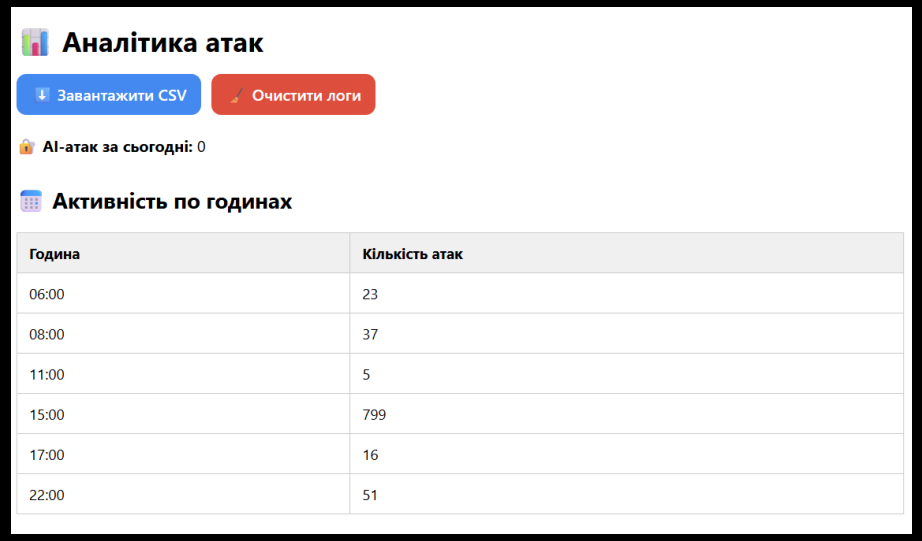
python™

Інтерфейс застосунку



- Основні модулі:
  - Тестування SQL-запитів
  - Симуляція DoS-атак у реальному часі
  - Аналітика аномалій

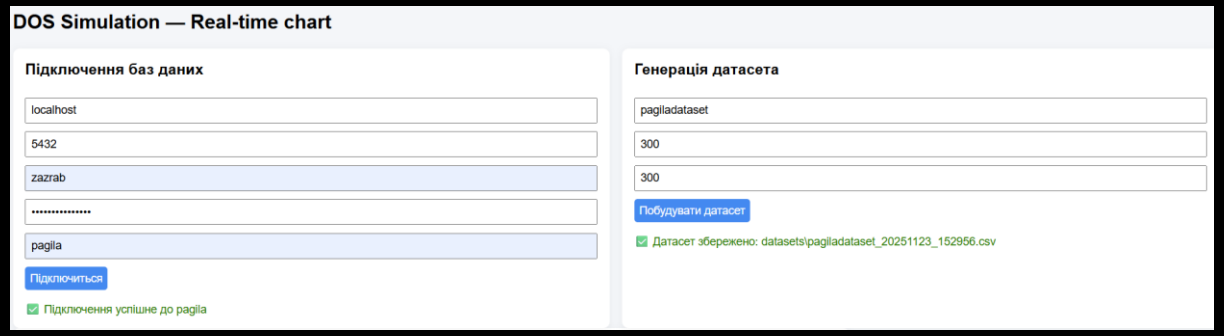


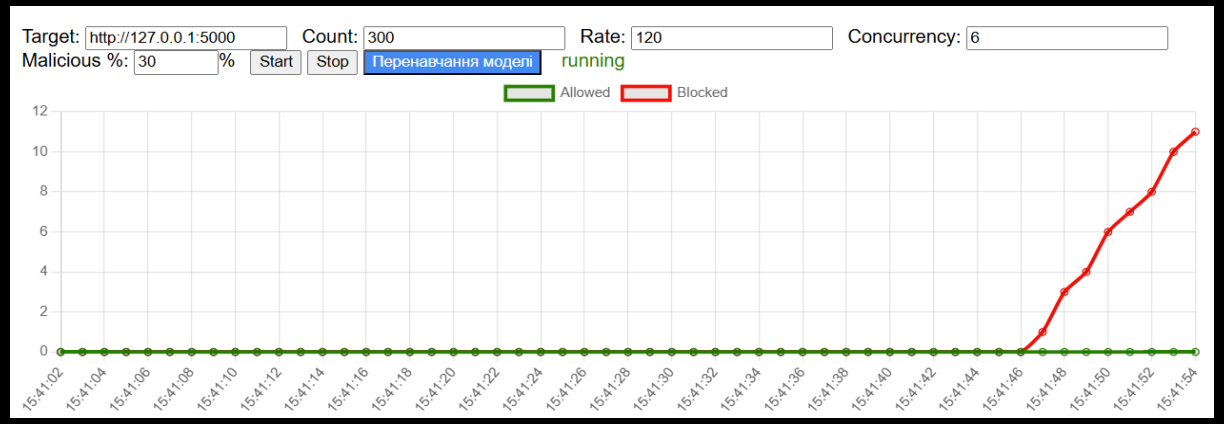


Інтерфейс застосунку

- Система вимагає перевірку доступу перед роботою з даними
- Система відображає журнал запитів та виявлених аномалій

Інтерфейс застосунку





- Підключення БД
- Генерація датасету на основі реальних SQL-запитів
- Відображення графіка обробки атак
- Можливість перенавчання ML-моделі

```
ROC AUC: 0.9855

              precision    recall  f1-score   support

           0     0.0000    0.0000    0.0000         1
           1     0.9942    0.9942    0.9942       172

    accuracy                         0.9884       173
   macro avg     0.4971    0.4971    0.4971       173
weighted avg     0.9884    0.9884    0.9884       173
```

Висновки

1. Проаналізовано сучасні методи кіберзахисту систем керування базами даних.
Визначено підходи до виявлення SQL-ін’єкцій, способи моніторингу активності та інструменти машинного навчання для підвищення стійкості систем.

2. Спроєктовано архітектуру веб-застосунку.
Сформовано модульну структуру системи з окремими компонентами: перевірка SQL-запитів, симуляція атак, аналітика, робота з ML-моделлю та зовнішніми БД.

3. Реалізовано модуль перевірки SQL-запитів.
Розроблено механізм подвійної перевірки — на основі правил SQL-парсера та ML-моделі, що забезпечує виявлення небезпечних запитів.

4. Створено модуль симуляції атак і моніторингу в реальному часі.
Забезпечено відтворення потоків запитів, збір статистики та побудову графіків Allowed/Blocked у реальному часі.

5. Проведено оцінку ефективності системи.
Отримано високі показники якості моделі (ROC AUC, precision, recall), перевірено стабільність роботи та підтверджено функціональну стійкість розробленого застосунку.