Здравствуйте! Меня зовут Парамонов Евгений, и сегодня я представляю свой проект — IT-Cube Forum. Это форум для образовательных центров IT-Cube, который интегрирован с Telegram. Всё сделано для удобства учеников и преподавателей.

1. Описание проекта

Этот форум тесно связан с Telegram. Через ботов можно быстро входить в систему и создавать темы для обсуждения. Преподаватели могут управлять форумом прямо из чата. Также реализована защита данных: безопасный вход, личная информация и учебные материалы надёжно защищены.

2. Структура проекта

Проект состоит из нескольких частей:

Скрипты для запуска и просмотра логов

Основные настройки

Папки для файлов и медиа

Интерфейс сайта

Два приложения

3. Telegram-боты

Бот привязки аккаунтов:

Команды: /bind, /unbind, /login

Привязывает Telegram к аккаунту, выдаёт одноразовые коды для входа

Бот для преподавателей:

Команды: /topic, /done, /cancel

Помогает создавать темы, загружать материалы, проверяет соответствие правилам

4. Работа с базой данных

В базе данных хранится:

Информация о пользователях и их Telegram-ID

Темы и сообщения форума

Загруженные файлы

Временные токены для входа

5. Конфигурация

Всё настраивается в файле config.py: API-ключи, пути к папкам и файлы с ролями (roles.json) и направлениями (directions.json), которые отвечают за доступ.

6. Логирование

Система записывает:

Кто заходил и что делал

Ошибки и сбои

Работа с сетью и API, базой данных

Всё это можно посмотреть через view\_logs.py.

7. Зависимости

Проект работает на:

Основных библиотеках: aiogram, flask, python-telegram-bot, aiohttp

Дополнительные: requests, werkzeug, python-dotenv

Все они указаны в requirements.txt.

8. Безопасность и защита

Проект защищён от хакерских атак:

Проверяется браузер, поддержка JS и cookie

Есть защита от брутфорса, SQL-инъекций и XSS

Используются CSRF-токены

Шифрование паролей (bcrypt)

Двухфакторная авторизация через Telegram

Ограничение количества запросов

Мониторинг активности

9. Спасибо за внимание

Спасибо за внимание! Буду рад ответить на ваши вопросы.  
  
 **Брутфорс-атака** — подбор пароля или ключа перебором всех возможных вариантов.

 **CSRF-атака** — заставляет авторизованного пользователя выполнить нежелательный запрос.

 **SQL-инъекция** — внедрение вредоносного SQL-кода в запрос для взлома базы данных.

 **XSS-защита** — меры против атак через внедрение вредоносного скрипта на сайт.

 **CSRF-токены** — уникальные значения для защиты от CSRF-атак.

 **BCrypt** — безопасное хеширование паролей на основе шифра Blowfish.