УДК 004.49

АНАЛИЗ УЯЗВИМОСТЕЙ, МЕТОДОВ ЗАЩИТЫ ДАННЫХ И УПРАВЛЕНИЯ ДОСТУПОМ В ТРЕНАЖЁРЕ УПРАВЛЕНИЯ УЧЕБНЫМИ ПРОЕКТАМИ

Терещенко Н. Ю.[1], Румянцев А. М.[1]
Научный руководитель – канд. техн. наук, доцент Горлушкина Н. Н.[1]
[1]Университет ИТМО
nutereshchenko@itmo.ru

Введение

Большинство современных веб-приложений взаимодействуют с персональными данными пользователей, делая их потенциальной целью для атаки злоумышленника. Тренажёр управления учебными проектами разрабатывается как замена использовавшейся ранее системы на платформе Odoo и ориентирован на специфику учебного процесса факультета. Тренажёр обрабатывает персональные данные студентов и научных руководителей, предлагает веб-доступ по сети, а также включает в себя большое количество сценариев взаимодействия, что делает вопрос безопасности данных крайне актуальным.

Основная часть

Разрабатываемый тренажёр является монолитной клиент-серверной архитектурой, которая включает в себя серверную часть на основе FastAPI, SQLAlchemy, PostgreSQL и Redis, а также клиентский интерфейс, реализованный на React, взаимодействие осуществляется с использованием REST API.

Прикладной анализ безопасности системы с опорой на OWASP Top 10 (2025) и формализованной оценкой угроз по базовым метрикам CVSS v4.0 позволил выделить и приоритизировать наиболее критичные риски [1,2,3]. Наивысший приоритет получили уязвимости цепочки поставки и зависимостей, нарушения целостности ПО и данных, а также инъекционные уязвимости. К рискам высокого приоритета отнесены ошибки контроля доступа, аутентификации, криптографические и конфигурационные ошибки, а также некорректная обработка исключений.

В текущей версии разрабатываемого тренажёра реализованы хэширование паролей, иерархическая модель разграничения прав доступа, логирование действий пользователей, использование ORM и параметризованных запросов, серверная валидация входных данных, code review и контроль зависимостей [4]. Перспективные меры включают формирование SBOM для контроля зависимостей, интеграцию SAST и DAST-инструментов, централизованный сбор логов, настройку уведомлений об аномалиях и поведенческий анализ, а также возможную интеграцию RASP‑подходов [5].

Выводы

Проведённый анализ продемонстрировал возможность комбинированного применения OWASP Top 10 и CVSS v4.0 к конкретной архитектуре учебного веб‑приложения, что позволило определить и обосновать приоритеты развития его подсистем безопасности. Результатом работы также является сопоставление выявленных потенциальных угроз с уже реализованными мерами защиты и формирование направления для дальнейшего развития защиты данных и управления доступом в тренажёре управления учебными проектами.

Литература

1. Williams J., Wichers D., et al. OWASP Top 10:2025 – The Ten Most Critical Web Application Security Risks // OWASP Foundation. 2025. – Режим доступа: https://owasp.org/Top10/2025 (дата обращения: 20.01.2026).
2. Mell P., Scarfone K., Romanosky S. et al. Common Vulnerability Scoring System Version 4.0: Specification Document // FIRST. 2024. – Режим доступа: https://www.first.org/cvss/specification-document (дата обращения: 21.01.2026).
3. Penelova M. Access control models //Cybernetics and Information Technologies. – 2021. – Т. 21. – №. 4. – С. 77-104.
4. Gowda P., Gowda A. N. Best Practices in REST API Design for Enhanced Scalability and Security //Journal of Artificial Intelligence, Machine Learning and Data Science. – 2024. – Т. 2. – №. 1. – С. 827-830.
5. Dencheva L. Comparative analysis of Static application security testing (SAST) and Dynamic application security testing (DAST) by using open-source web application penetration testing tools : дис. – Dublin, National College of Ireland, 2022.