Научная статья
Original article
УДК 004

СОВРЕМЕННЫЕ ПРОБЛЕМЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ, СВЯЗАННЫЕ С ЗАЩИТОЙ ПЕРСОНАЛЬНЫХ ДАННЫХ ПОЛЬЗОВАТЕЛЯ

MODERN INFORMATION SECURITY ISSUES ASSOCIATED WITH THE PROTECTION OF THE USER'S PERSONAL DATA

Маврин Андрей Валериевич, бакалавр, Волгоградский Государственный Университет, г. Волгоград

Mavrin Andrey Valerievich, Master Student, Volgograd State University, Volgograd, email: whbrat@gmail.com

Аннотация

В данной статье рассматриваются современные проблемы информационной безопасности, связанные с защитой персональных данных пользователя. Особое внимание уделяется проблеме использования повторяющихся паролей от различных облачных сервисов и проблемы к котором приводит такой подход защиты персональных данных. Рассматриваются современные подходы позволяющие организовать хранение паролей пользователя. Научная новизна исследования заключается в разработке нового программного обеспечения с открытым исходных кодом с возможностью авторизированного развёртывания информационной системы в изолированной

сети на стороне пользователя, что увеличивает безопасность использования инструмента для хранения паролей.

Annotation

This article discusses modern problems of information security related to the protection of user's personal data. Particular attention is paid to the problem of using repeated passwords from various cloud services and the problems that this approach to protecting personal data leads to. Modern approaches are considered that allow organizing the storage of user passwords. The scientific novelty of the research lies in the development of new open-source software with the possibility of authorized deployment of an information system in an isolated network on the user side, which increases the security of using a tool for storing passwords.

Ключевые слова: менеджер паролей, учетная запись, нулевое разглашение, конфиденциальность информации, информация, пользовательский аккаунт.

Keywords: password-manager, account, zero-knowledge, information privacy, information, user account.

Введение

Одним из главных ресурсов в современном мире является информация, с каждым днем количество данных, хранящихся на жестких дисках компьютера, постоянно растёт. В наше время особой популярностью пользуются облачные сервисы, количество таких сервисов постоянно растёт, а вместе с этим увеличивается и количество персональной информации, которое требует защищенного хранения.

С тех пор как интернет был представлен публике, пользователи во всем мире столкнулись с «проблемой пароля». С ростом числа онлайн-аккаунтов, которыми можно пользоваться на любом устройстве подключенному к интернету, пользователи предпочитают использовать один запоминающийся пароль для всех своих учетных записей, пренебрегая использованию надёжных, уникальных паролей для каждого сервиса.

В данной статье приводится информация о построение облачного менеджера паролей с нулевым разглашением, а также с возможность автоматизированного развёртывания системы.

Структура разрабатываемой системы

Одной из наиболее важный частей в реализации разрабатываемого приложения, является проектирование схемы базы данных (рисунок 1). Для функционирования разрабатываемого приложения было создано три таблицы: users, user-roles и notes.

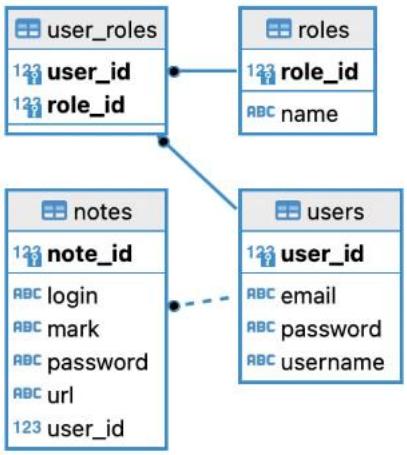

Рисунок 1. Схема базы данных

Разрабатываемого приложение состоит из нескольких компонентов, который взаимодействуют между собой и представляют функционирующую систему. Благодаря такому подходу, разрабатываемую систему можно горизонтально масштабировать в зависимости от нагрузок на отдельные части системы.

В качестве инструмента, который позволяет автоматизировать процесс развёртывания и управления приложений с поддержкой контейнеризации используется Docker. Для автоматизированного развёртывания разрабатываемой системы необходимо поместить все компоненты в контейнеры, которыми будет оперировать Docker, затем необходимо написать docker-compose файла (рисунок 2).

```yaml
version: '3.1'

services:
  postgres:
    image: postgres
    restart: always
    ports:
      - "15432:5432"
    volumes:
      - ./docker-postgresql-multiple-databases:/docker-entrypoint-initdb.d
    environment:
      - POSTGRES_MULTIPLE_DATABASES=manager
      - POSTGRES_USER=postgres
      - POSTGRES_PASSWORD=postgres

  password-manager:
    image: docker.io/library/application:latest
    ports:
      - "8888:8888"
    depends_on:
      - postgres
    environment:
      SPRING_DATASOURCE_URL: "jdbc:postgresql://postgres:5432/manager"
      SPRING_DATASOURCE_USERNAME: "postgres"
      SPRING_DATASOURCE_PASSWORD: "postgres"
```

Рисунок 2. Docker-compose файл

Взаимодействие клиент-сервера происходит при помощи HTTP запросов, для аутентификации пользователя на сервере используется Baerer токен. Клиентское приложение подписывает каждое обращение к серверу, для предоставления данных за исключением запросов регистрации и авторизации (рисунок 3).

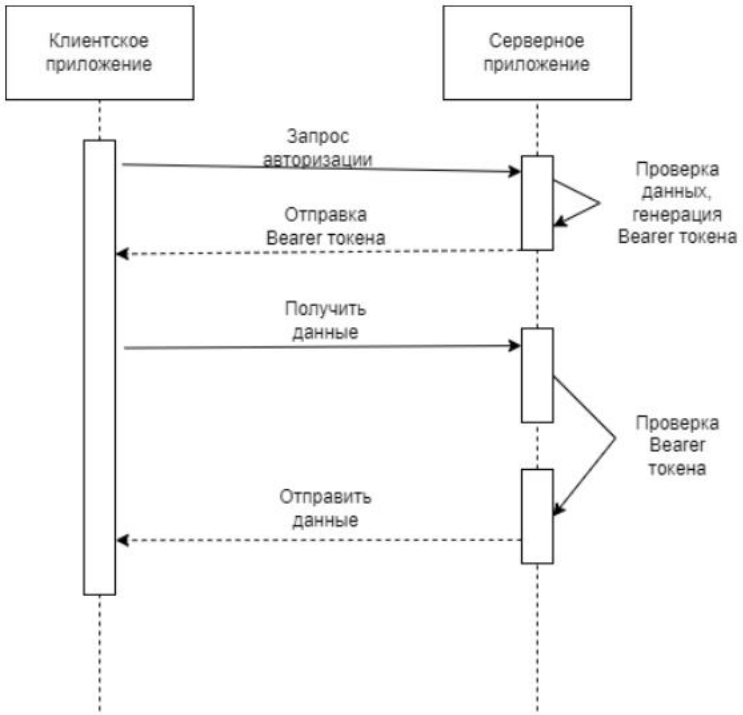

Рисунок 3. Взаимодействия клиент-сервера

Пользователь взаимодействует с облачным сервисом при помощи веб-приложения, в котором пользователь может: создавать, редактировать, удалять новые записи и генерировать уникальные надежные пароли (рисунок 4).

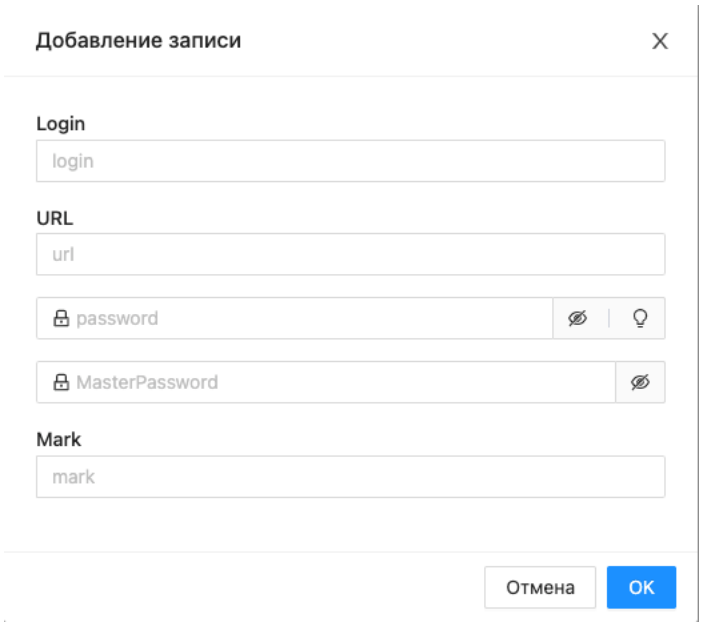

Рисунок 4. Интерфейс веб-приложения

Литература

1. Борисович С. М. Информационное общество и информационная безопасность // Официальный сайт. [электронный ресурс] – Режим доступа. – URL: https://cyberleninka.ru/article/n/informatsionnoe-obschestvo-i-informatsionnaya-bezopasnost
2. How to stop reusing passwords for good // Официальный сайт. [электронный ресурс] – Режим доступа. – URL: https://blog.dashlane.com/how-to-stop-reusing-passwords/
3. Always change your password after a Breach // Официальный сайт. [электронный ресурс] – Режим доступа. – URL: https://blog.dashlane.com/should-i-always-change-my-password-after-a-breach/
4. How to Improve your passwords // Официальный сайт. [электронный ресурс] – Режим доступа. – URL: https://blog.dashlane.com/how-to-stop-reusing-passwords/
5. Americans and Cybersecurity // Официальный сайт. [электронный ресурс] – Режим доступа. – URL: https://assets.pewresearch.org/wp-content/uploads/sites/14/2017/01/26102016/Americans-and-Cyber-Security-final.pdf

Literature

1. Borisovich S. M. Information society and information security // Official site. [electronic resource] - Access mode. – URL: https://cyberleninka.ru/article/n/informatsionnoe-obschestvo-i-informatsionnaya-bezopasnost
2. How to stop reusing passwords for good // Official site. [electronic resource] - Access mode. – URL: https://blog.dashlane.com/how-to-stop-reusing-passwords/
3. Always change your password after a Breach // Official site. [electronic resource] - Access mode. – URL: https://blog.dashlane.com/should-i-always-change-my-password-after-a-breach/
4. How to Improve your passwords // Official site. [electronic resource] - Access mode. – URL: https://blog.dashlane.com/how-to-stop-reusing-passwords/

5. Americans and Cybersecurity // Official site. [electronic resource] - Access mode. – URL: https://assets.pewresearch.org/wp-content/uploads/sites/14/2017/01/26102016/Americans-and-Cyber-Security-final.pdf

© Маврин А.В., 2022 Научно-образовательный журнал для студентов и преподавателей «StudNet» №6/2022

Для цитирования: Маврин А.В. Современные проблемы информационной безопасности, связанные с защитой персональных данных пользователя // Научно-образовательный журнал для студентов и преподавателей «StudNet» №6/2022