**ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ**

**«НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ УНИВЕРСИТЕТ ИТМО»**

**Факультет безопасности информационных технологий**

**Дисциплина:**

**«*Разработка систем аутентификации и криптографии*»**

**Отчет по лабораторной работе №2на тему «Методы аутентификации»**

***Вариант 7***

**Выполнила:**

Магистрант гр. N42514c

Гафарова Язгуль Камилевна



**Проверил:**

Федоров Иван Романович

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Санкт-Петербург

2020 г.

**Содержание**

[1. Цель работы: 3](#_Toc56956732)

[2. Описание выбранных средств реализации и обоснования выбора 3](#_Toc56956733)

[3. Исходный код и демонстрация работы программы 4](#_Toc56956734)

[3.1. Демонстрация работы программы 4](#_Toc56956735)

[4. Выводы 7](#_Toc56956736)

**Лабораторная работа №2**

1. Цель работы:

— реализовать механизм аутентификации в клиент-серверном веб-приложении**.**

**Требования к реализации:**

* необходимо реализовать метод аутентификации в клиент-серверном приложении согласно варианту 7;
* клиент должен представлять собой веб-страницу с формой авторизации пользователя;
* сервер должен включать в себя две части:

1) таблица идентификаторов (данные о пользователях для аутентификации: логин/пароль/токен/итд в зависимости от метода аутентификации);

2) процесс с реализованной логикой метода аутентификации.

* программа не должна разрешать переход на страницу-заглушку без успешной аутентификации (напрямую по URL).

**Вариант 7:**

Реализовать аутентификацию по одноразовому паролю с хешированием MD5 (можно использовать функцию из библиотеки). В таблице идентификаторов должны храниться: логин, email, хеш пароля (md5), срок действия пароля. Таблица идентификаторов должна представлять собой таблицу в реляционной БД, данные должны передаваться через SQL-запросы. При истечении срока действия пароля аутентификация не должна проходить. При аутентификации на сервере генерируется пароль для отправки на почту и в таблицу идентификаторов сохраняется его хэш. Сравниваются не пароли, а результаты MD5.

1. Описание выбранных средств реализации и обоснования выбора

Для реализации алгоритма был выбран язык Python 3.8.2, так как это понятный и простой язык программирования.

В качестве среды разработки использовался **Visual Studio Code (VS Code)** – хоть это и не полноценная среда разработки, а редактор кода в первую очередь. Очень легкий и быстрый. Огромное количество плагинов, можно гибко настроить редактор под себя.

Использовался фреймворк **Flask**, который позволяет создавать сайты самых разных типов с использованием языка Python. Flask относится к разряду микрофреймворков, то есть, он предоставляет лишь базовый инструментарий для построения сайтов, все по минимуму – ничего лишнего. Однако, этого вполне достаточно, чтобы создавать большинство типовых сайтов с поддержкой шаблонов страниц, баз данных и прочими стандартными возможностями. И, кроме того, простота и достаточность функционала для типовых решений позволяют достаточно быстро разобраться в этом пакете и начать сразу его применять.

Также использовался **Bootstrap** — бесплатный HTML/CSS/JavaScript фреймворк для быстрого создания адаптивного дизайна сайта. Bootstrap позволяет с минимальными знаниями создавать интерфейсы, которые работают во всех популярных браузерах и не ломаются при изменении разрешения экрана.

1. Исходный код и демонстрация работы программы

Исходный код представлен по ссылке:

https://github.com/vukira/cryptography/tree/master/Lab2/AUTH\_7/auth\_var7

* 1. Демонстрация работы программы

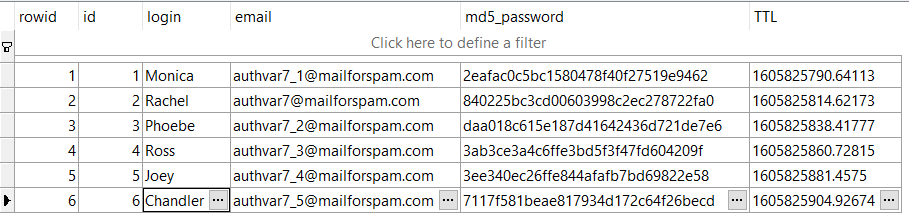


Рисунок 1 – Таблица идентификаторов

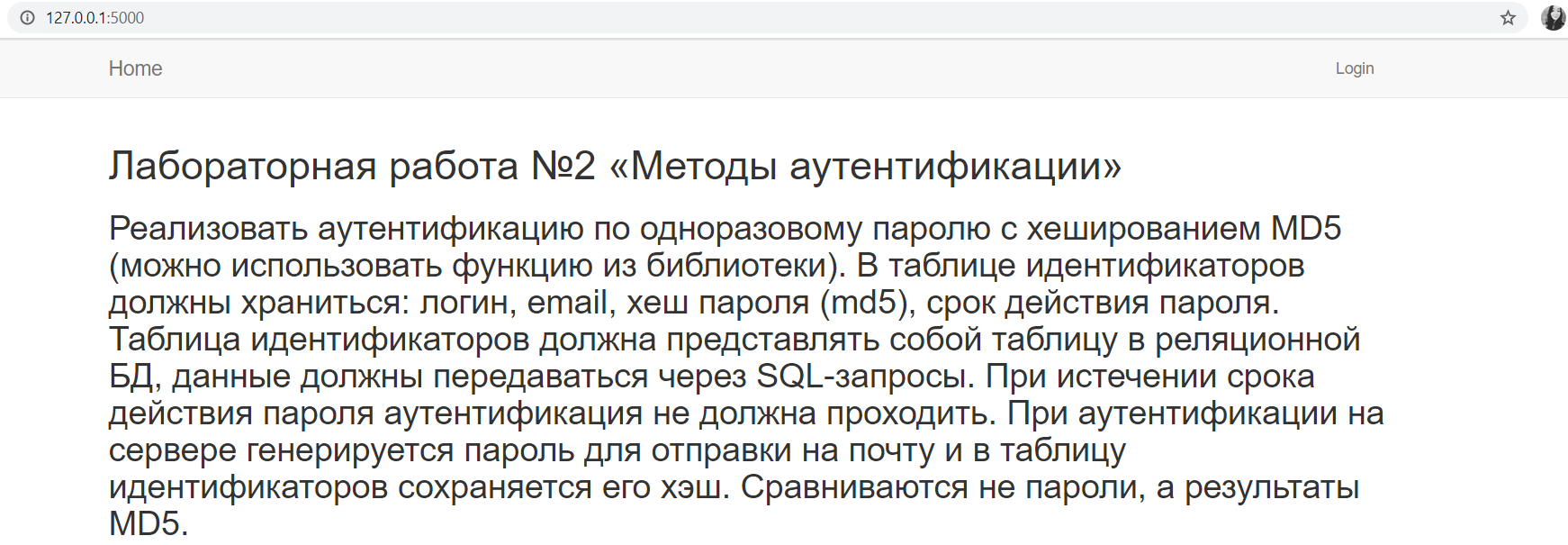


Рисунок 2 – Стартовая страница

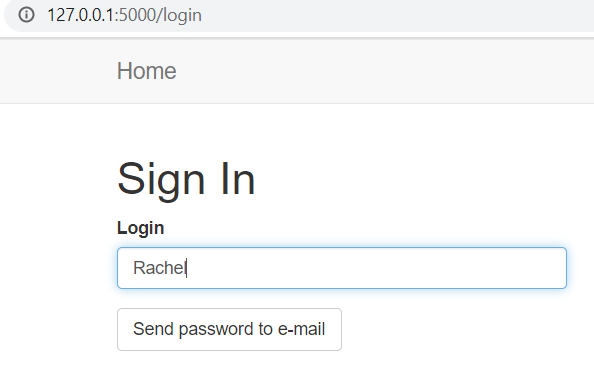


Рисунок 3 – Страница Входа с вводом логина

После нажатия кнопки «Send password to e-mail» мы получаем письмо с паролем (Рисунок 4) на указанную соответствующе логину почту (Рисунок 1) и вводим этот пароль в появившееся для этого поле (Рисунок 5).

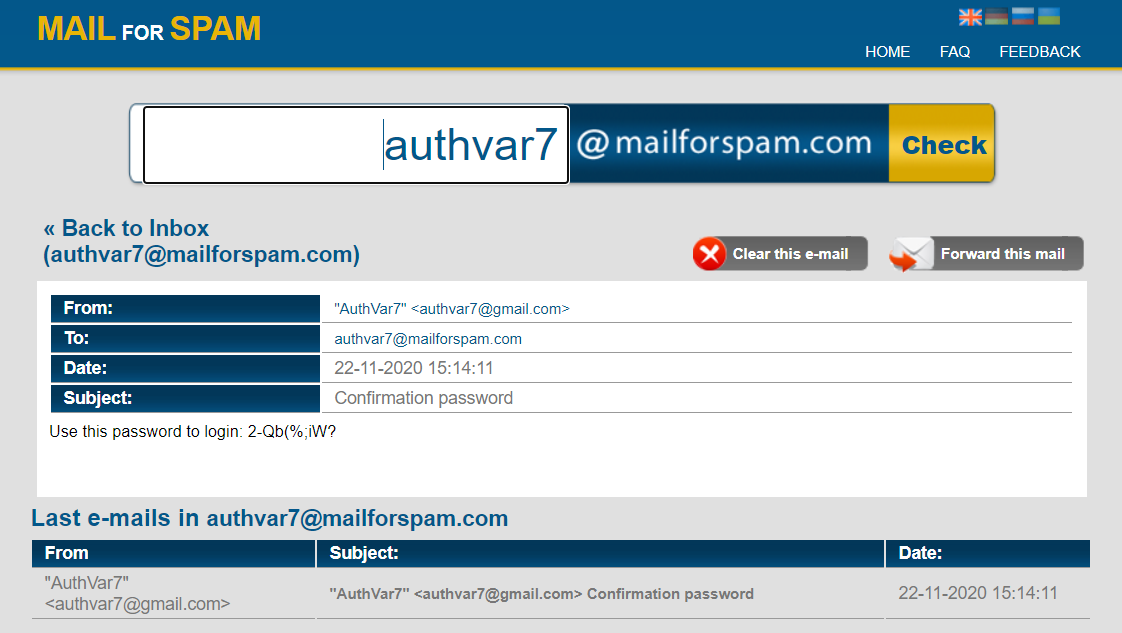


Рисунок 4 – Письмо с временным паролем

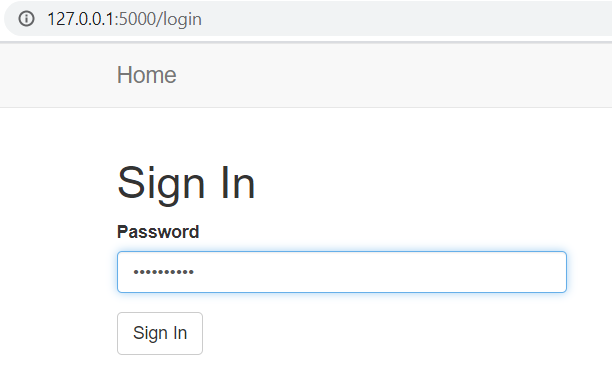


Рисунок 5 – Страница Входа с вводом пароля

Если пароль верен и валиден, то открывается страница профиля (Рисунок 6).

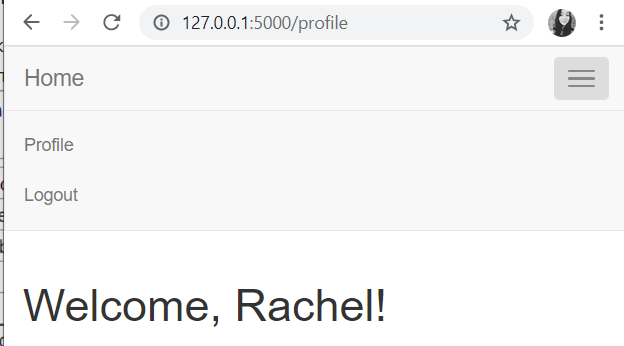


Рисунок 6 – Страница Профиля при успешной аутентификации

Если пароль неверен, то мы получаем сообщение об этом (Рисунок 7).

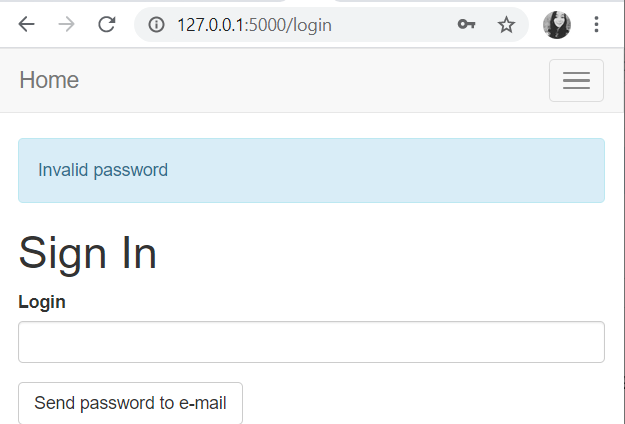


Рисунок 7 – Ввод неверного пароля

В случае, когда пытаются ввести пароль спустя 5 минут после ввода логина и отправки сообщения с паролем на почту, получаем сообщение о том, что срок действия пароля истек (Рисунок 8).

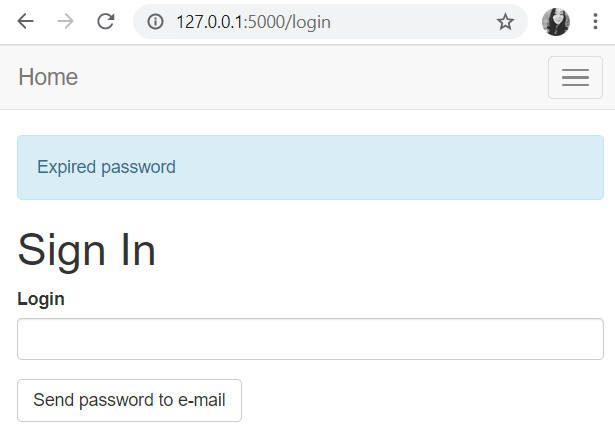


Рисунок 8 – Ввод пароля с истекшим сроком действия

При попытке перехода напрямую по URL(http://127.0.0.1:5000/profile)без успешной аутентификации получаем сообщение с просьбой выполнить вход (Рисунок 6).

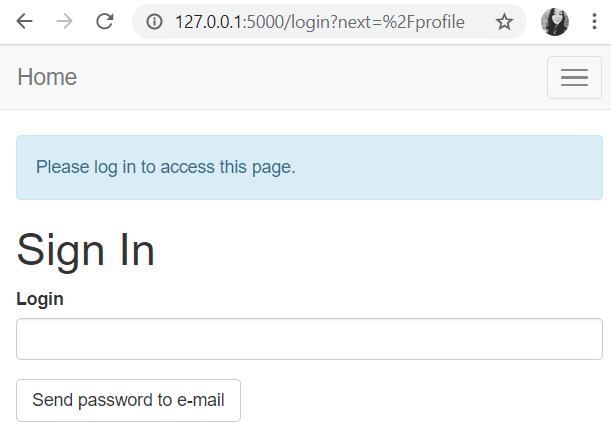


Рисунок 9 – Попытка перехода по URL

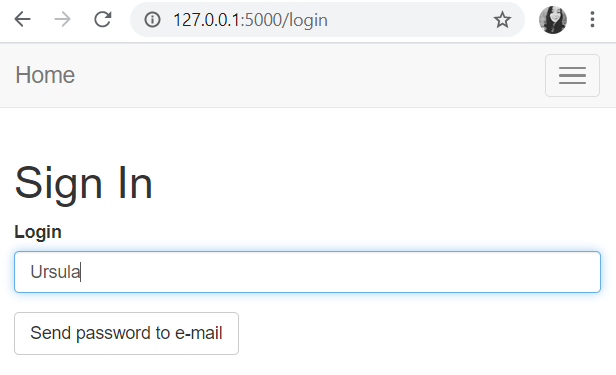


Рисунок 10 – Попытка входа с отсутствующим в БД идентификатором

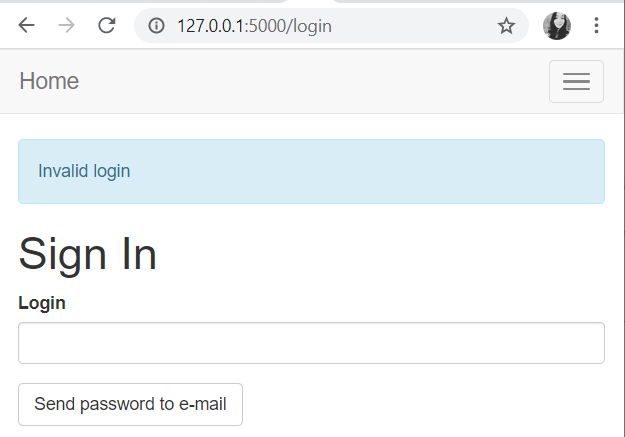


Рисунок 11 – Недействительный логин

1. Выводы

В ходе лабораторной работы был реализован метод аутентификации в клиент-серверном приложении согласно варианту 7. Была изучена работа с фреймворками для построения сайтов: Flask и Bootstrap.