

Министерство науки и высшего образования Российской Федерации
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 №2
Разработка системы парольной аутентификации в клиент-серверном
приложении
«Вариант 2 - Реализация аутентификации по паролю с
подтверждением по email»

Выполнили:
Магистрант гр. N42514с Э.Р. Кочкаров



Санкт-Петербург
2020 г.

- **Цель работы (задача)** – реализация механизма аутентификации в клиент-серверном веб-приложении
- Требования к реализации программы:
 - необходимо реализовать метод аутентификации в клиент-серверном приложении согласно варианту
 - 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/и т. д. в зависимости от метода аутентификации);
 - 2) процесс с реализованной логикой метода аутентификации.

1. Описание выбранных средств реализации и обоснования выбора

Для реализации алгоритма был выбран язык Python, так как к скорости выполнения программы не предъявлялось каких-либо особых требований.

Python – высокоуровневый язык программирования общего назначения, ориентированный на повышение производительности разработчика и читаемости кода. Синтаксис ядра Python минималистичен. В то же время стандартная библиотека включает большой объём полезных функций. Этот язык имеет довольно простой синтаксис, лёгок в изучении и имеет низкий порог вхождения. В то же время язык является очень мощным средством разработки. Такой выбор также обусловлен тем, что это достаточно распространённый язык в настоящее время.

Для реализации клиент-серверной архитектуры был выбран фреймворк Flask.

Flask — это упрощенная платформа Python для веб-приложений, которая обеспечивает основные возможности маршрутизации URL-адресов и визуализации страниц.

2.Описание алгоритма.

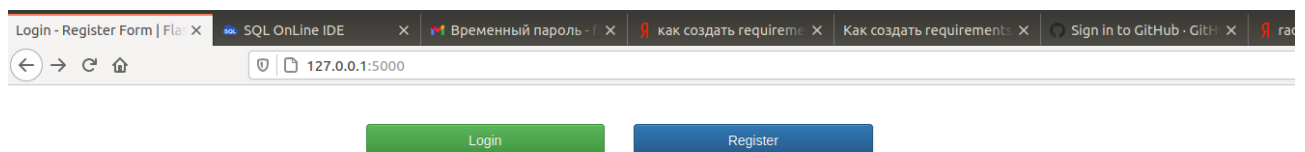
Реализовать аутентификацию по паролю с подтверждением по email. В таблице идентификаторов должны храниться: логин, email, пароль, временный код подтверждения. Таблица идентификаторов должна представлять собой таблицу в реляционной БД, данные должны передаваться через SQL-запросы. При аутентификации на сервере сравниваются пароли и на email пользователя отправляется сгенерированный на сервере временный код подтверждения. На клиенте после отправки данных с паролем должен произойти редирект на форму для ввода временного кода подтверждения. После отправки кода на сервере сравниваются пришедший код и код из БД. При совпадении кодов аутентификация считается успешной и происходит редирект на страницу-заглушку.

3.Ссылка на исходный код.

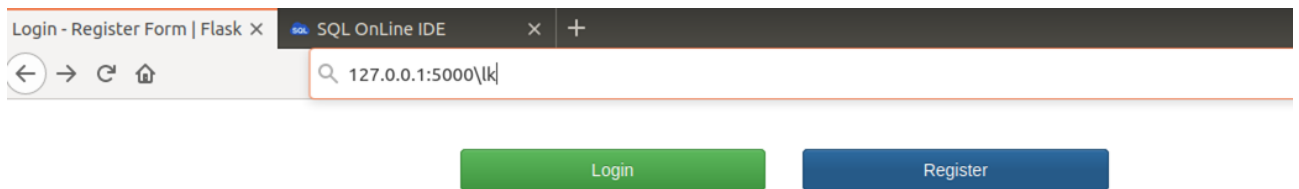
<https://github.com/elmurza/crypto/blob/main/task2/app.py>

4.Демонстрация работы

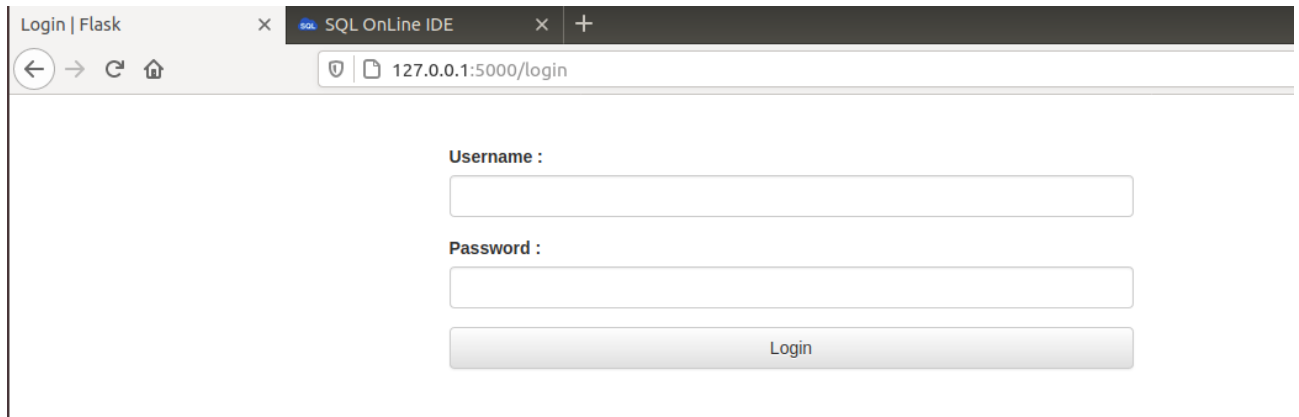
1. Вход на главную страницу.



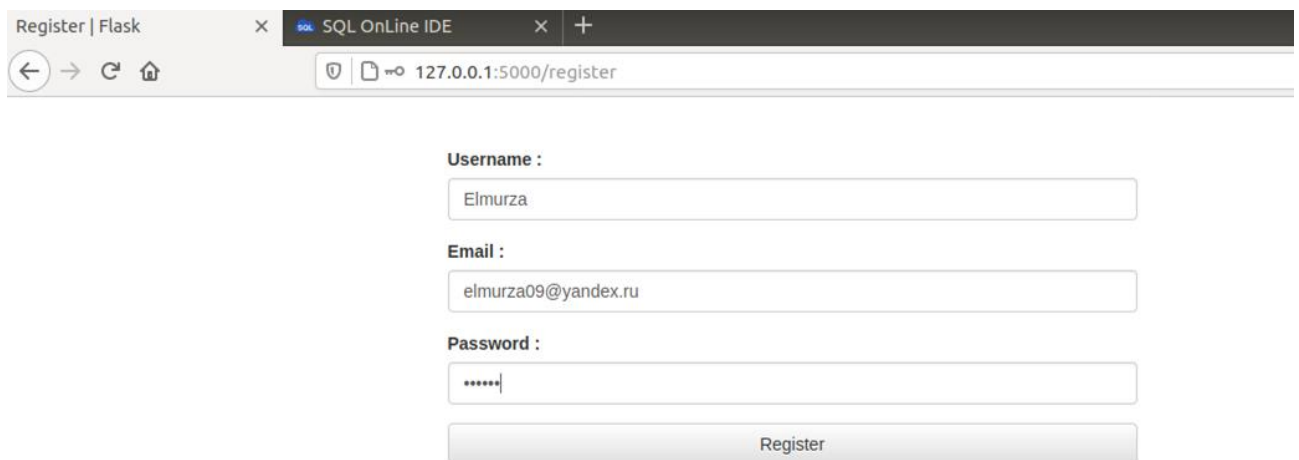
2. Попытка входа в личный кабинет без авторизации.



3. При попытке входа перенаправляет на страницу ввода логина и пароля.



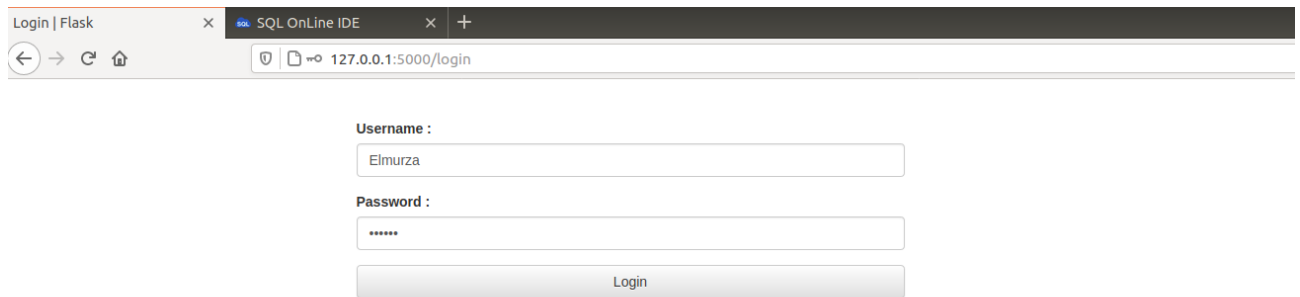
4. Форма регистрации



5. Форма ввода логина и пароля



6. Регистрируем аккаунт и заполняем форму

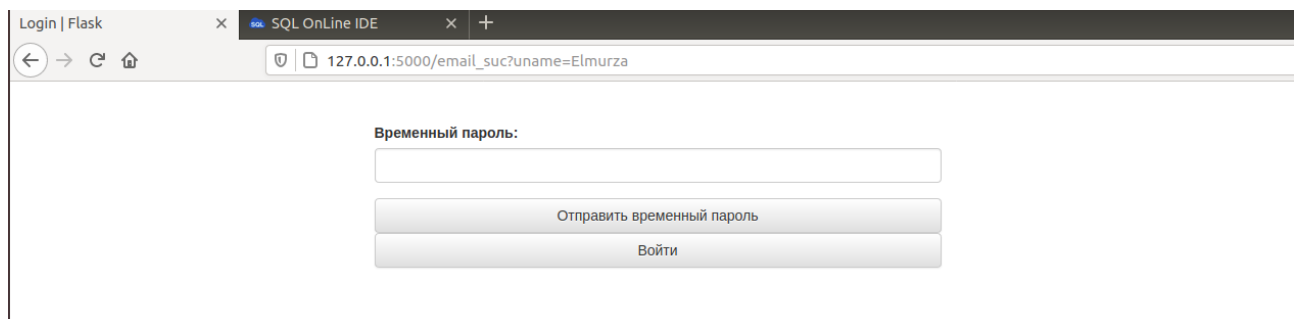


Username :
Elmurza

Password :

Login

7. Идёт перенаправление на форму ввода временного пароля, нажимаем отправить



Временный пароль:

Отправить временный пароль

Войти

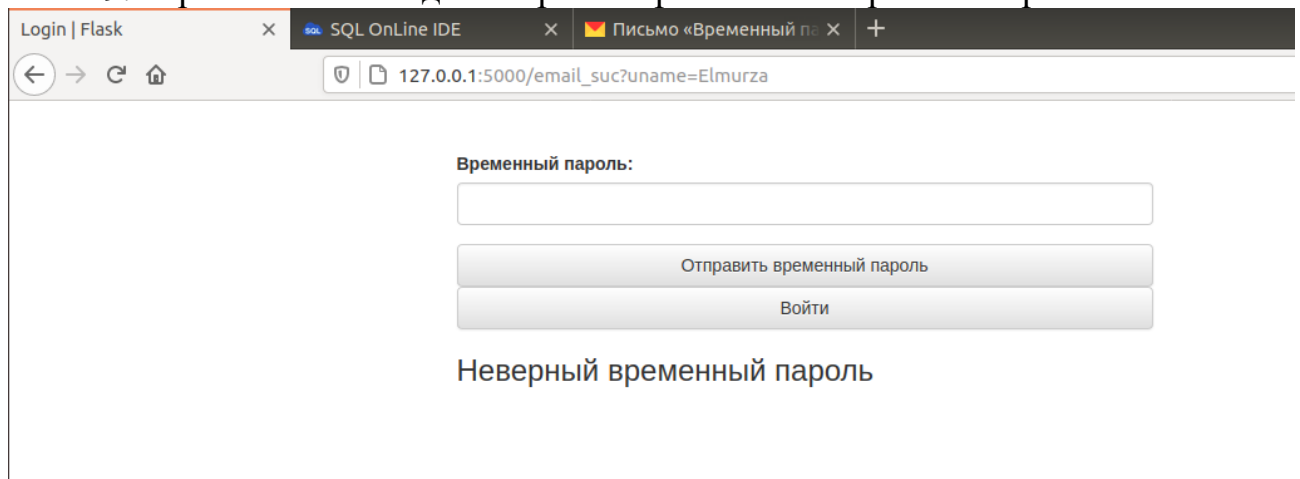
8. На почту приходит временный пароль

Временный пароль



Ваш пароль 91505 действует в течении 300 секунд

9. При попытке ввода неверного временного пароля отображается Alert



Временный пароль:

Отправить временный пароль

Войти

Неверный временный пароль

10. После ввода верного пароля нажимаем на кнопку Войти

Временный пароль:

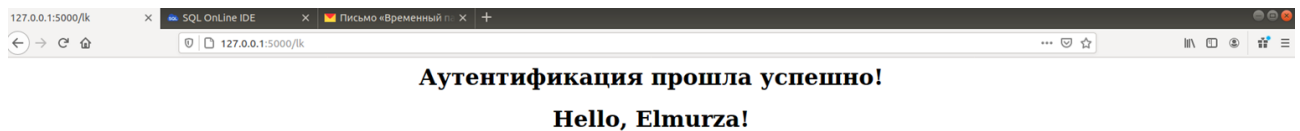
91505

Отправить временный пароль

Войти

Неверный временный пароль

11. Страница личного кабинета



12. База данных sql

	userid	username	password	email	temp
1	1	1	1@1.ru	1	
2	2	2	4@d	2	
3	1	1	1@1.ru		
4	2	2	1@1.ru	25104	
5	0	0	elmurza09@yand...	29471	
6	09	09	elmurza09@yand...	41721	
7		Elmurza	123456	elmurza09@yand...	91505

5. Выводы

В ходе лабораторной работы разработана система парольной аутентификации с подтверждением по email в клиент-серверном приложении.