### Отчет по пентесту 15.7.2 (Задание 15.7.2)

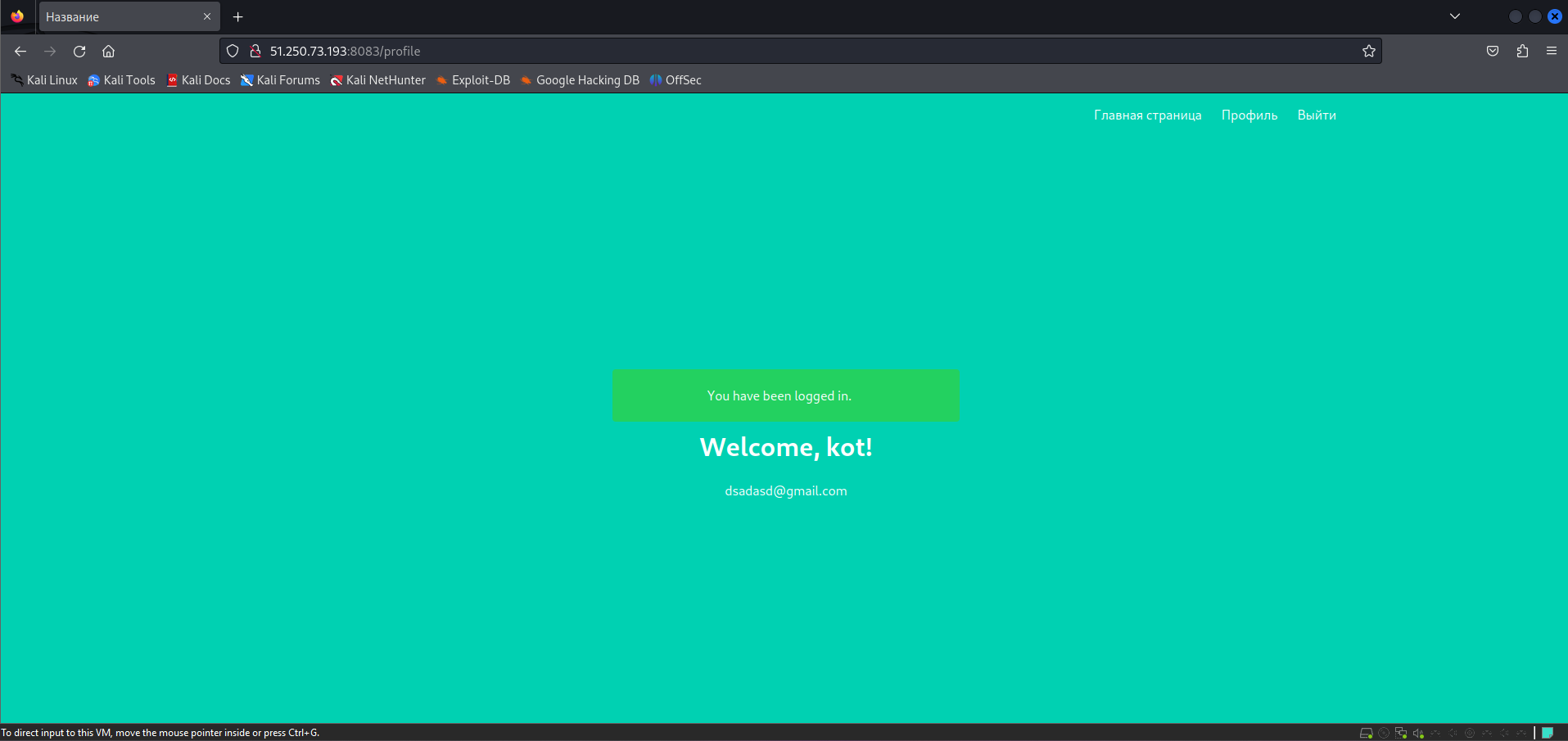
**Персонализация:** Михайлов Юрий Никитич (uramihajlov481@gmail.com)

**Лабораторная работа** Задание 15.7.2 **“ Security Misconfiguration” :**

* Общая информация:
* Период тестирования: 27.01.2024
* Объект тестирования: [http://51.250.73.193:8083](http://51.250.73.193:8083/)
* Описание действий:

**1 Этап:**

Зайдя на сайт зарегистрировался и проследовал в свой профиль

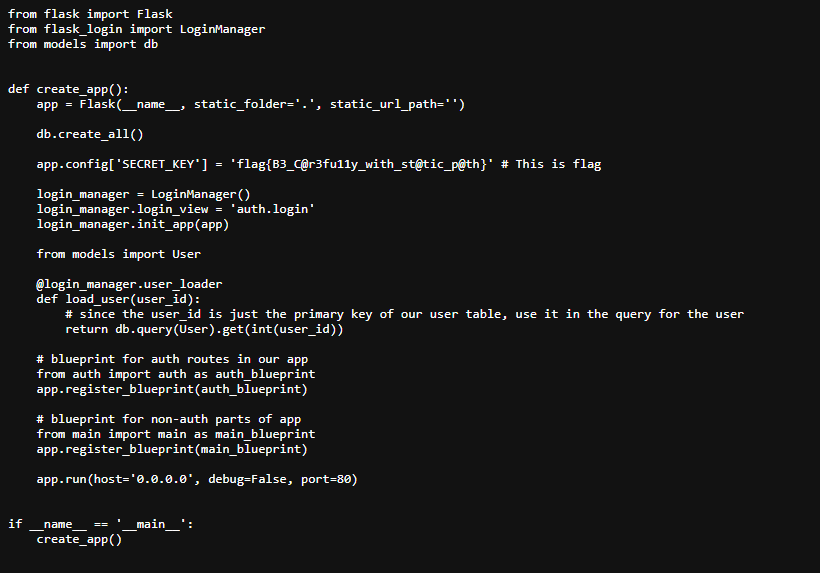


**2 Этап:**

**Решил поискать скрытые файлы внедряя в URL свои запросы (Зная что корневая папка имеет название . )**

**3 Этап:**

**Чуть поискав нашёл подходящий для меня URL /./../app.py**

**4 Этап:  
**

**Используемые инструменты:**

* LFI
* Opera

**Обнаруженные уязвимости:**

* LFI
* Найден файл app.py
* **Security Misconfiguration (найдены данные hots, port,** **login\_manager и т.д.)**

**Дайте совет по улучшению защиты:**

1. **Использование контроля доступа:**
   * Реализуйте строгий контроль доступа, чтобы предотвратить несанкционированный доступ к файлам. Убедитесь, что только аутентифицированным пользователям предоставляется доступ к необходимым файлам.
2. **Проверка на сервере:**
   * На уровне сервера обеспечьте проверку и авторизацию для запросов на доступ к файлам. Убедитесь, что сервер отклоняет запросы на файлы, которые не должны быть доступны.
3. **Использование .htaccess (если используется Apache):**
   * Если ваш веб-сервер использует Apache, используйте файл .htaccess для дополнительной защиты и контроля доступа. Например, вы можете использовать директиву Deny from all, чтобы запретить доступ к определенным директориям.
4. **Ограничение списка разрешенных файлов:**
   * Ограничьте список файлов, которые могут быть запрошены напрямую через URL. Не доверяйте пользовательскому вводу и убедитесь, что вы обрабатываете запросы только для разрешенных файлов.