### Отчет по пентесту 14.4.5 (Задание 14.4.5)

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

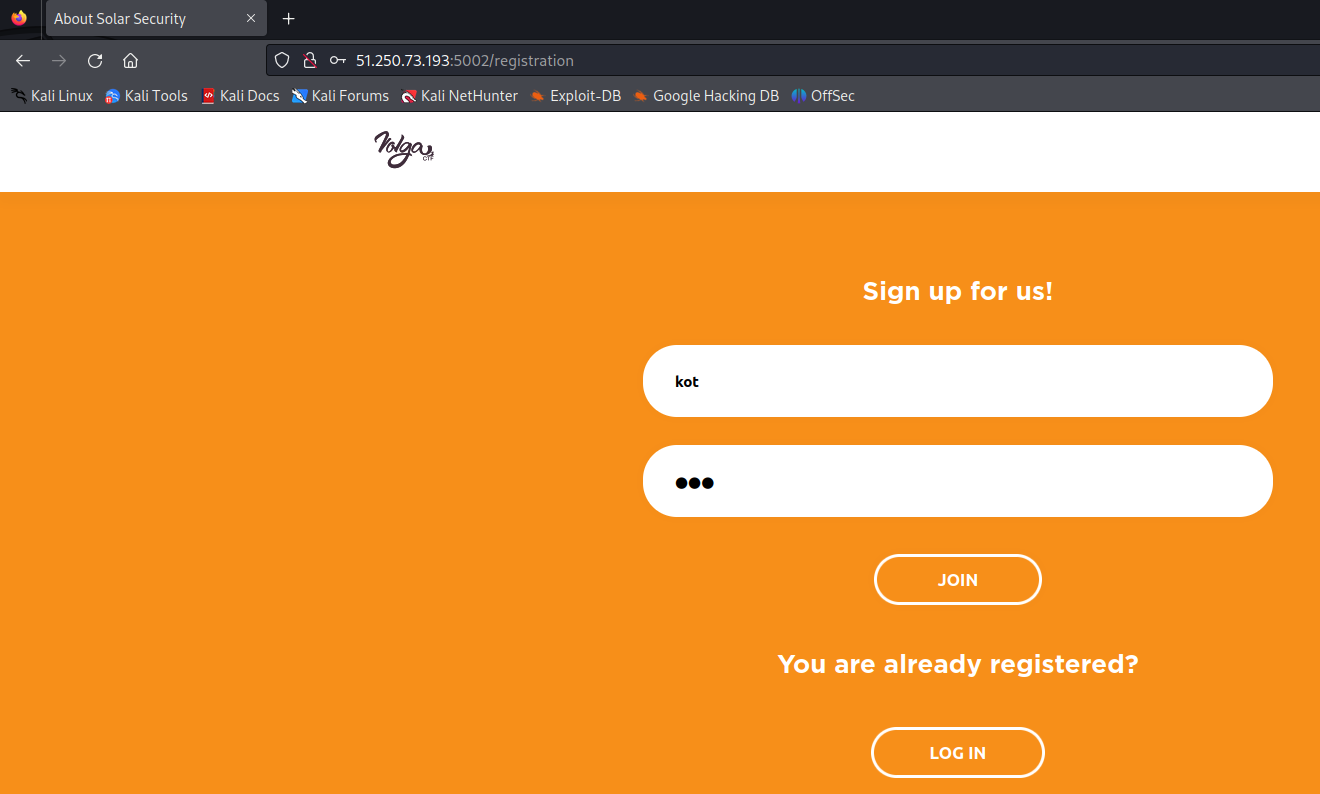
**Лабораторная работа** Задание 14.4.5**“ HTML инъекции” :**

* Общая информация:
* Период тестирования: 15.01.2024
* Объект тестирования: <http://51.250.73.193:5002>
* Описание действий:

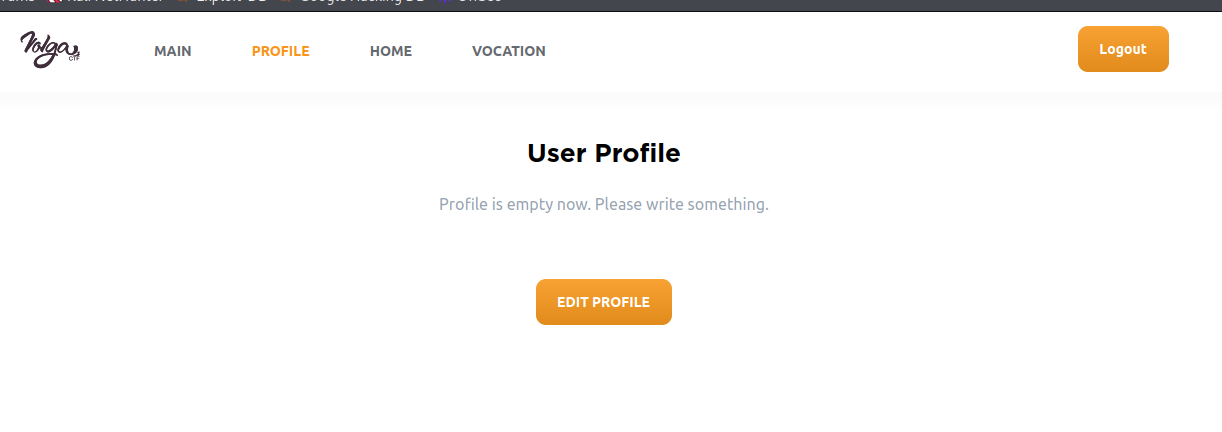
**Используемые инструменты:**

* HTML форма
* Chrome

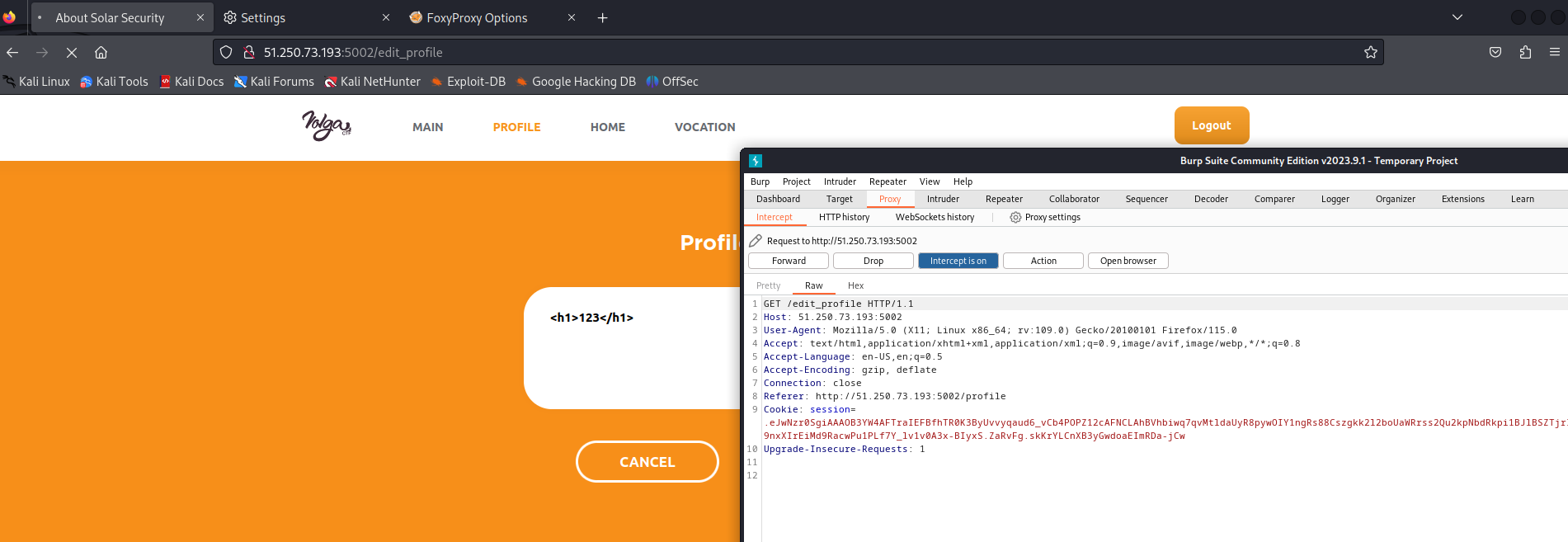
**1 этап:  
Зайти и зарегистрироваться на сайте под любым логином/паролем**



**2 Этап:  
Заходим в профиль аккаунта и видим форму статуса о себе**

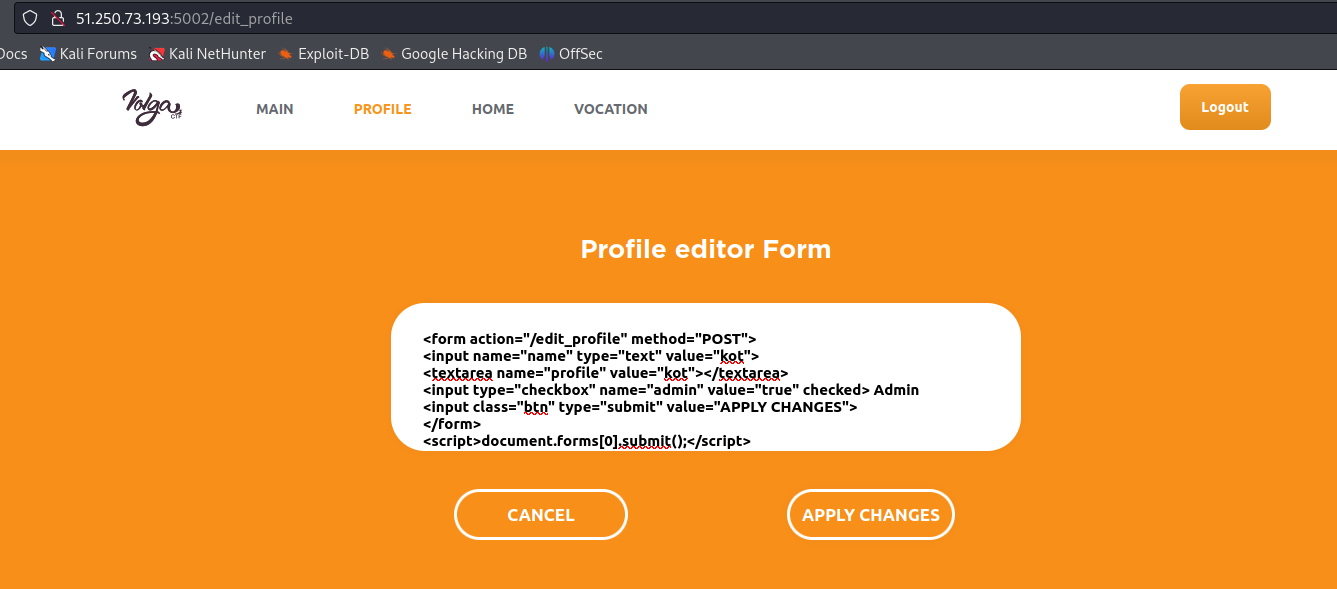


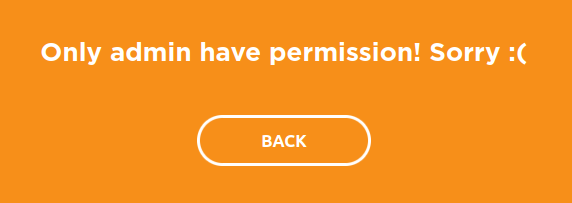
**3 Этап:**

**Перехватываем трафик через Burp Suite и видим POST и остальную информацию далее слегка покопавшись в консоли разработчика находим checkbox строчку с данными «Admin»**

**4 Этап:**

1. **Используем код для CSRF  
   <form action="/edit\_profile" method="POST"> <input name="name" type="text" value="kot"> <textarea name="profile" value="kot"></textarea> <input type="checkbox" name="admin" value="true" checked> Admin <input class="btn" type="submit" value="APPLY CHANGES"> </form> <script>document.forms[0].submit();</script>**



**5 Этап:  
Сохранив код и обновив сайт получим сообщение ниже** **после перейдя на страницу Home получим наш flag**

**Обнаруженные уязвимости:**

* HTML injection
* CSRF

**Дайте совет по улучшению защиты:**

* Экранируйте данные
* Фильтруйте ввод
* Использование токена CSRF
* Проверка Referer