Основы информационной безопасности

Индивидуальный проект. Этап № 2. Установка DVWA

Подлесный Иван Сергеевич

Содержание

# 1 Цель работы

Целью данной работы является установка DVWA на Kali Linux.

# 2 Теоретические сведения

Damn Vulnerable Web Application (DVWA) — это намеренно уязвимое веб-приложение на PHP/MySQL. Цель проекта — помочь этичным хакерам и специалистам ИБ отточить свои навыки и протестировать инструменты.

DVWA также может помочь веб-разработчикам и изучающим ИБ, лучше понять процесс безопасности веб-приложений.

# 3 Ход работы

Скопируем в каталог /var/www/html файлы веб-приложения DVWA с гита(рис. fig. 1)

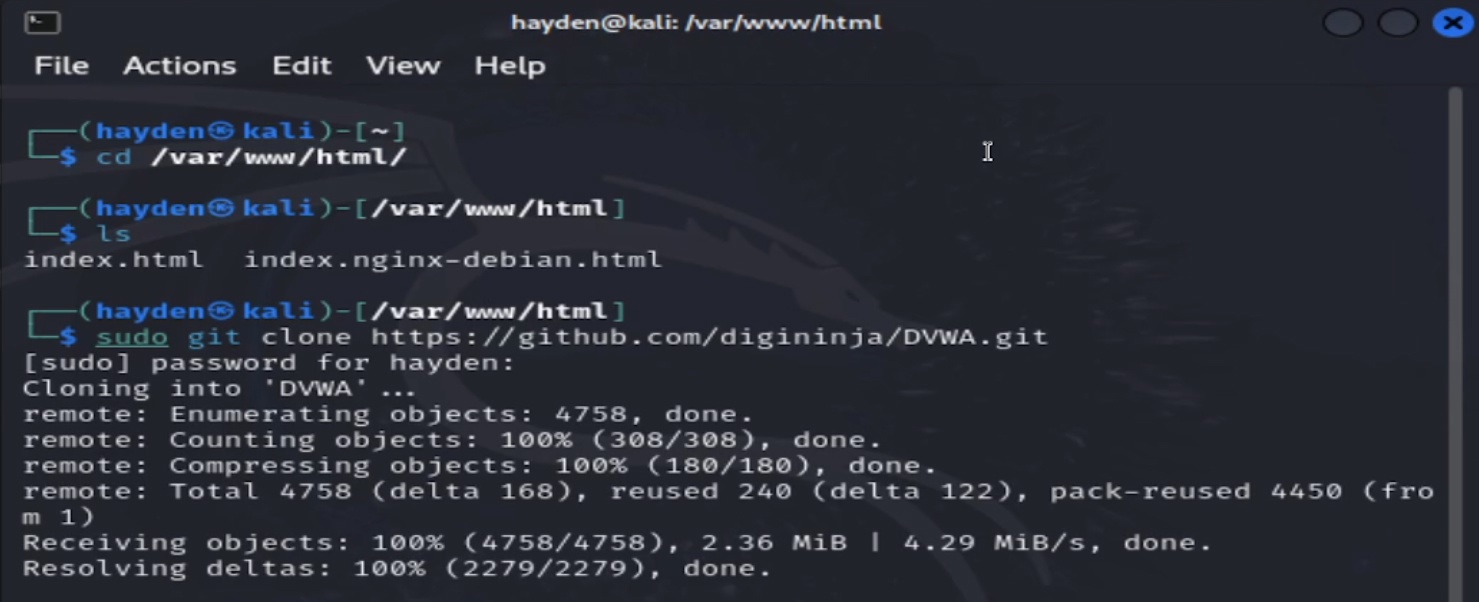


Рис. 1: Клонирование репозитория с DVWA

Затем запускаем веб сервер(рис. fig. **¿fig:002?**, fig. 2).

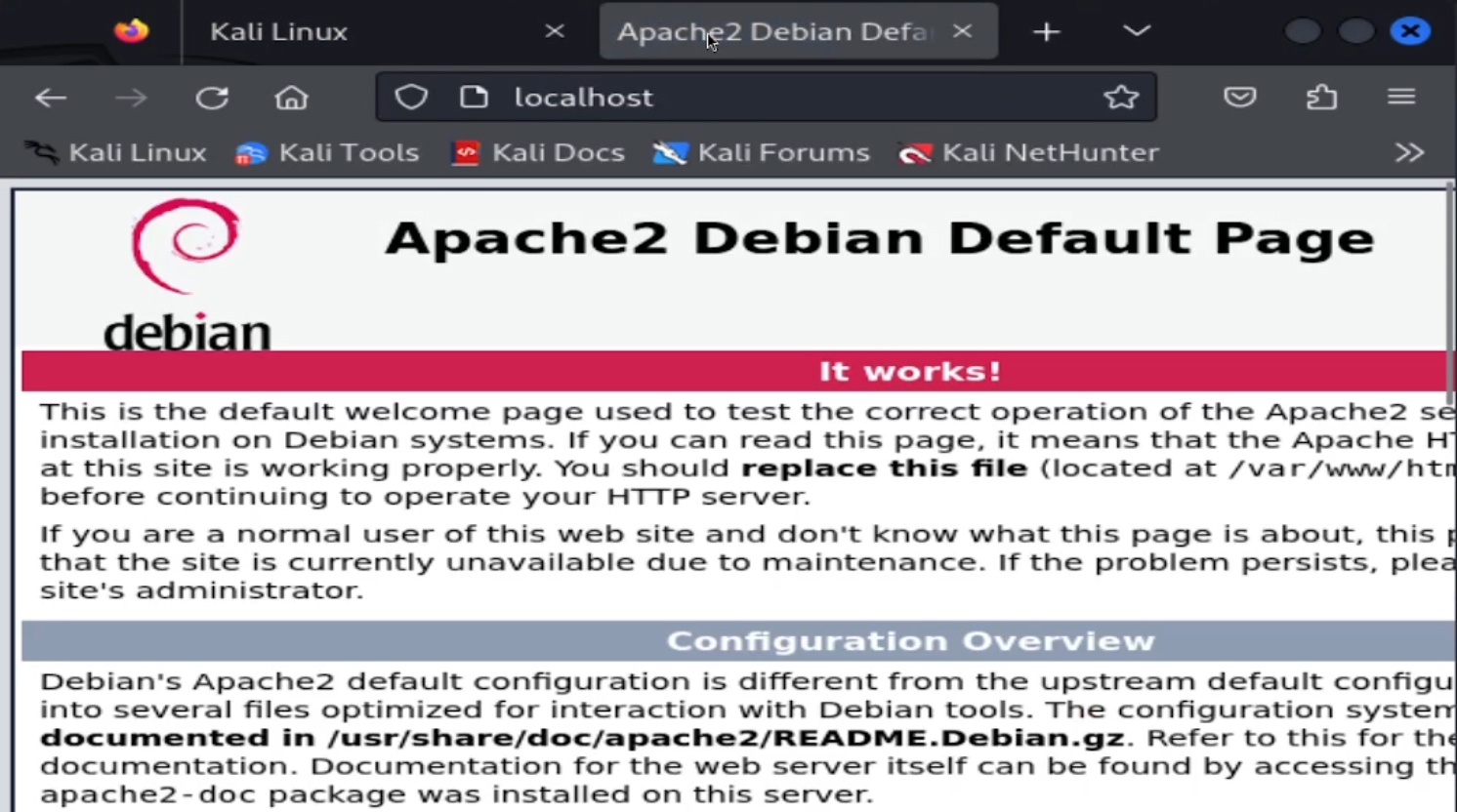


Рис. 2: Запуск apache2 и проверка работы веб-сервера

Копируем файл конфигураций DVWA, чтобы затем можно было его безопасно изменять. Мы воспользуемся именем пользователя и паролем по умолчанию(рис. fig. 3, fig. 4).

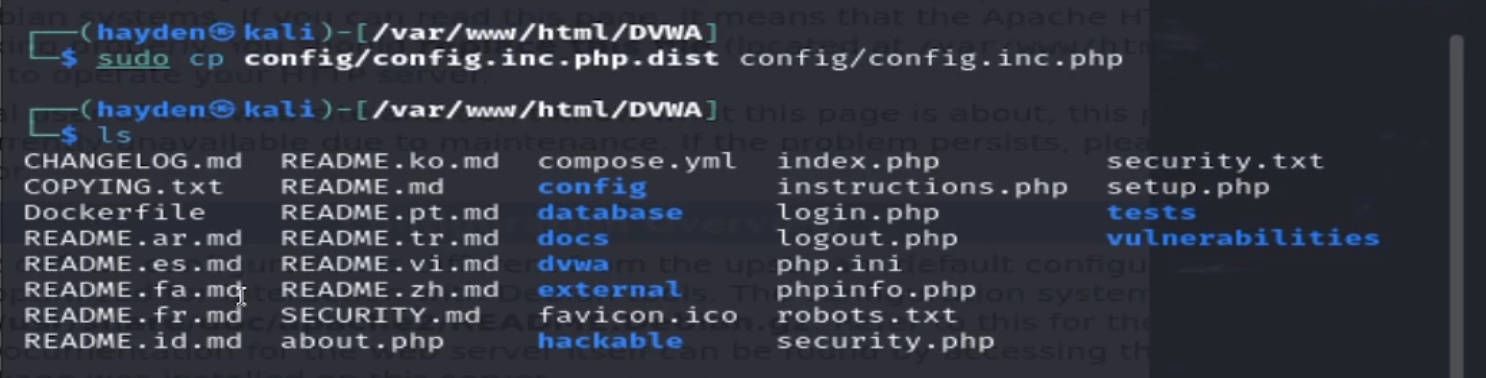


Рис. 3: Просмтр файла конфигураций

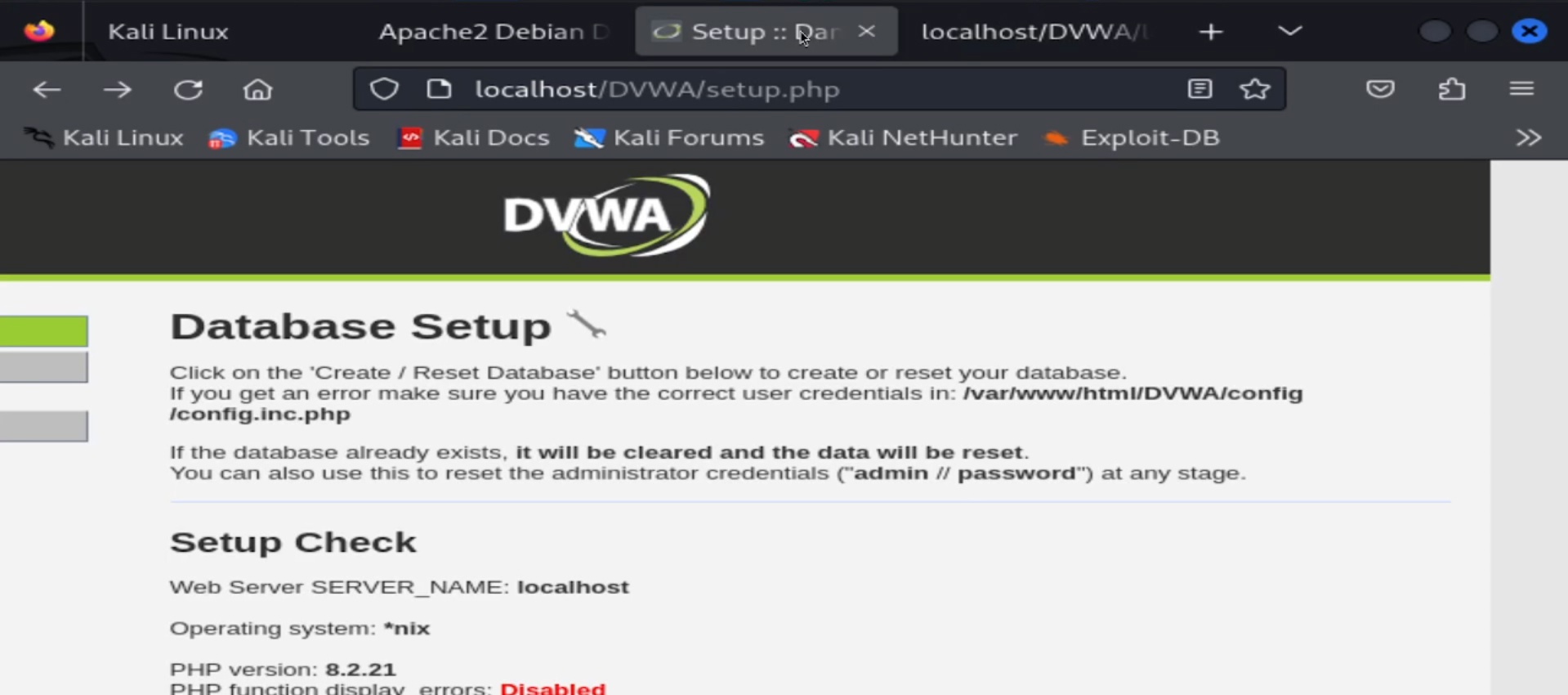


Рис. 4: Просмотр стартового окна DVWA

Запустим сервер mariadb и создадим на нем пользователя(имя и пароль совпадают с данными в файле конфигураций dvwa)(рис. fig. 5, fig. 6).

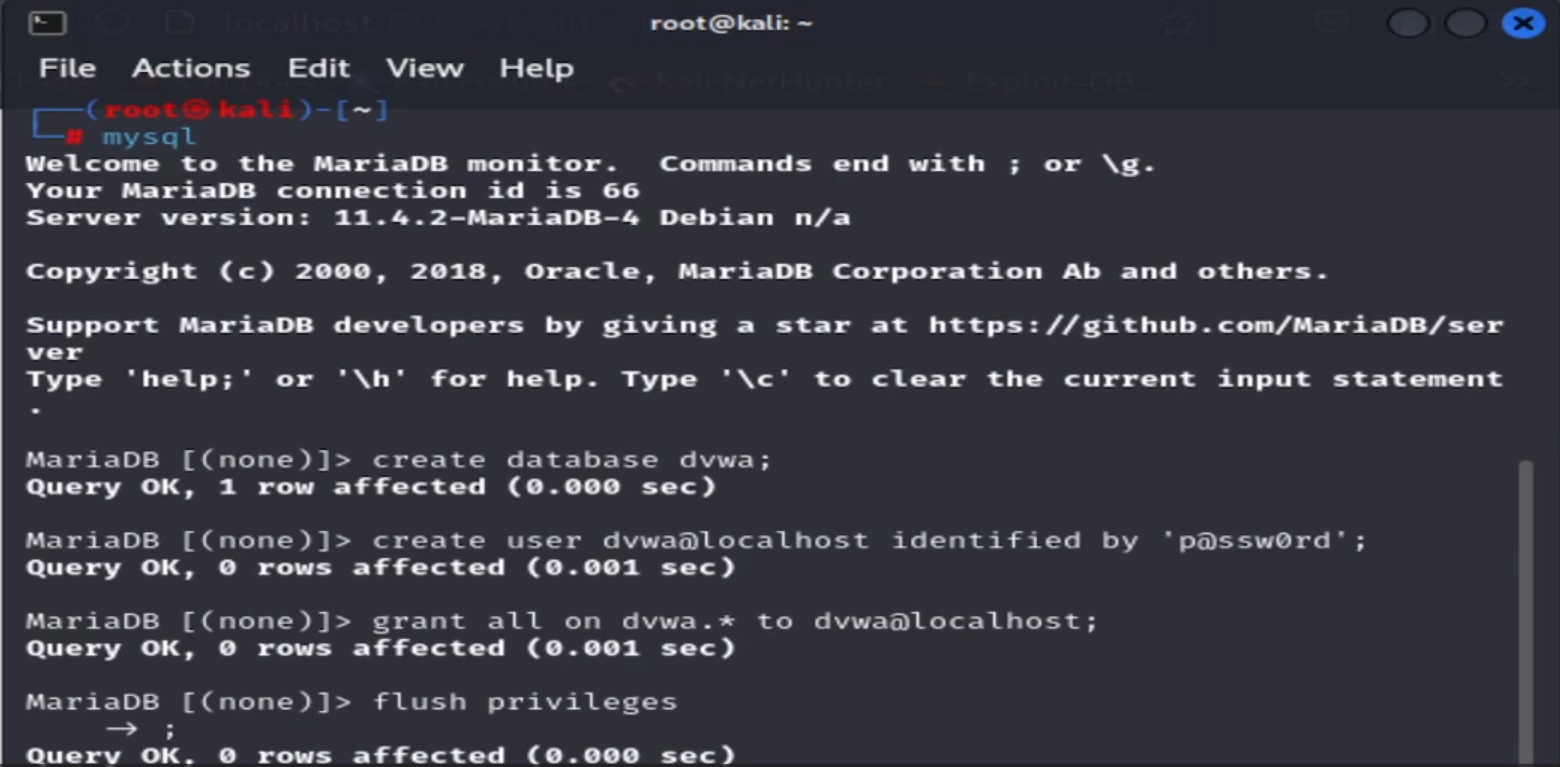


Рис. 5: Создание пользователя mariadb и базы данных

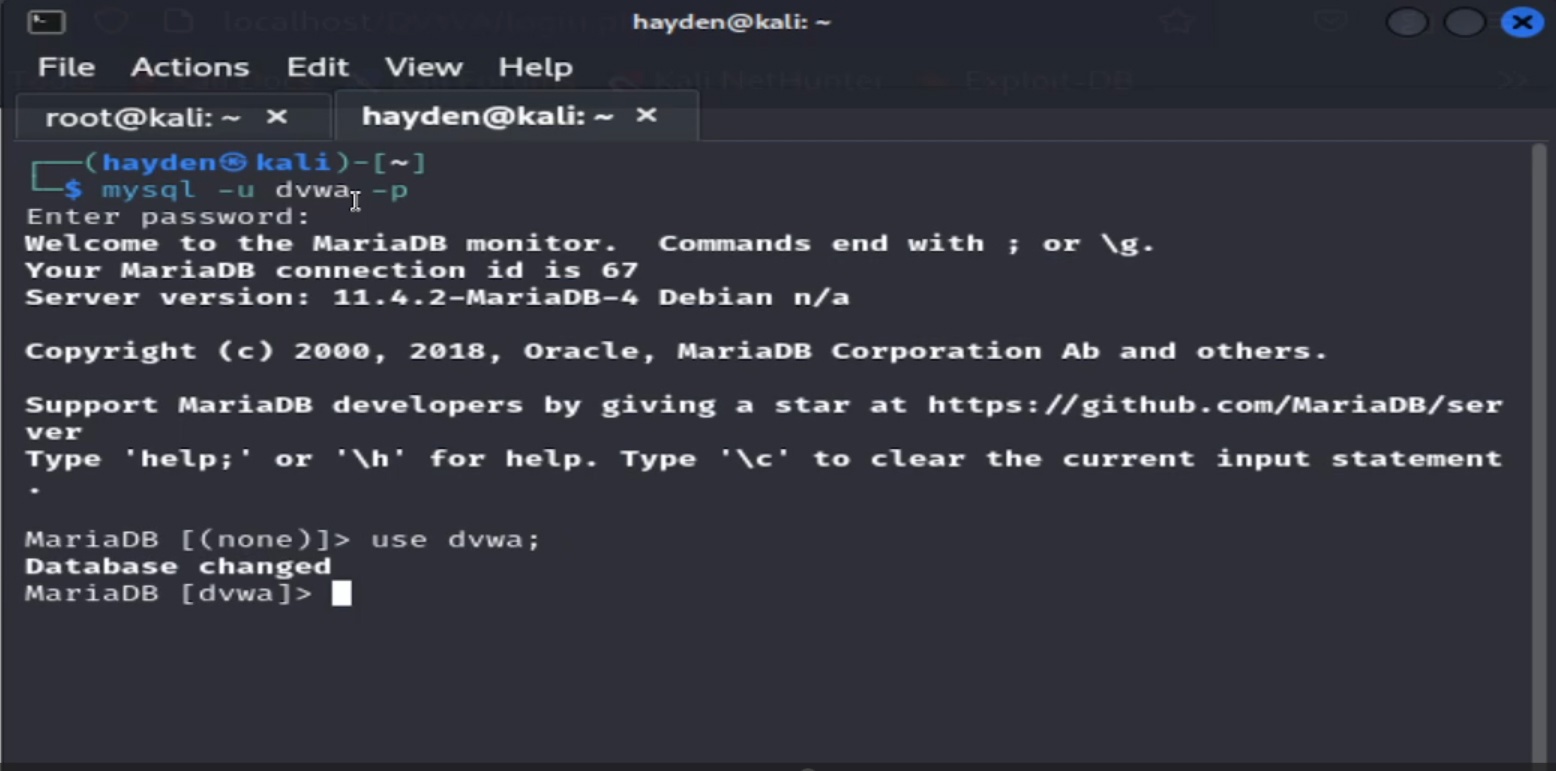


Рис. 6: Проверка пользователя mariadb

Затем на стартовом окне DVWA нажмем кнопку Create/Reset Database, и нас перекинет на страницу ввода данных учетной записи. После ввода увидим рабочую область DVWA(рис. fig. 7, fig. 8).

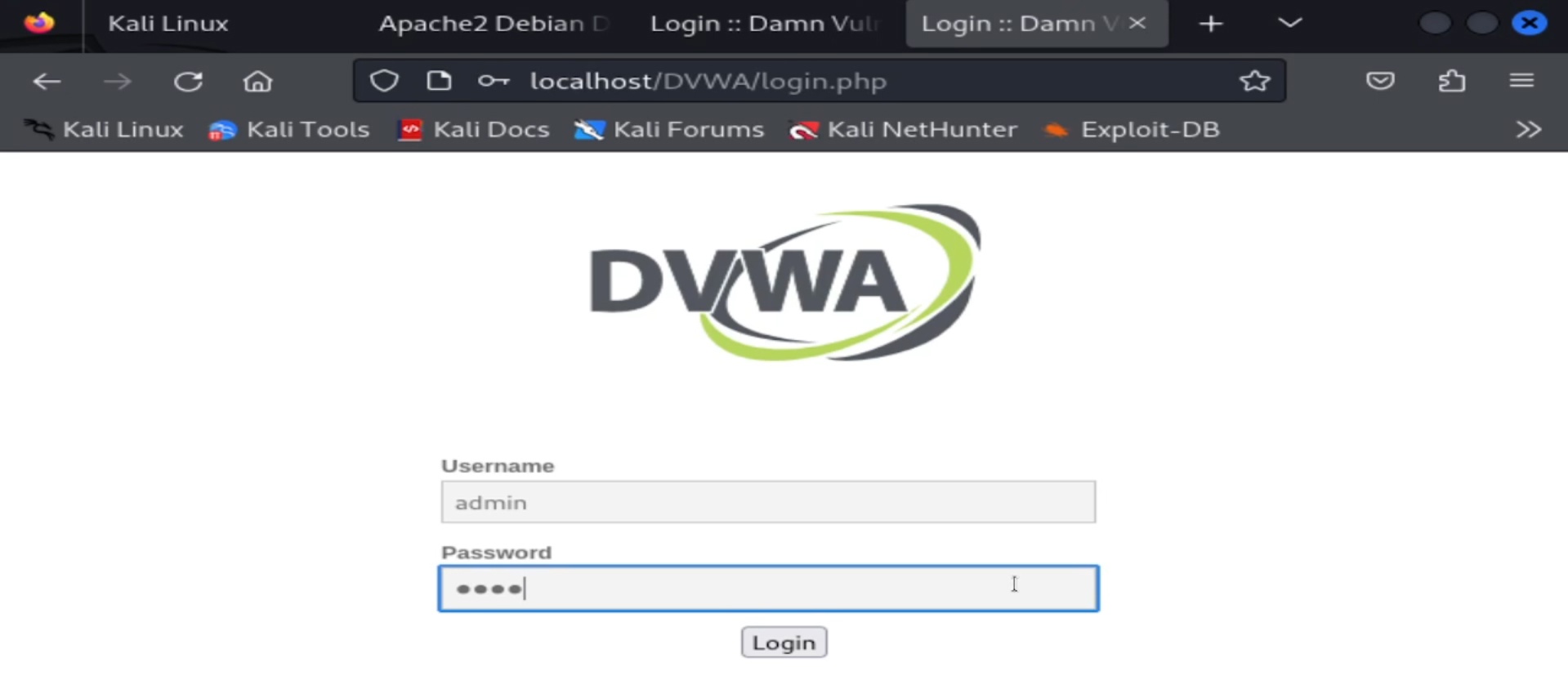


Рис. 7: Аутентификация

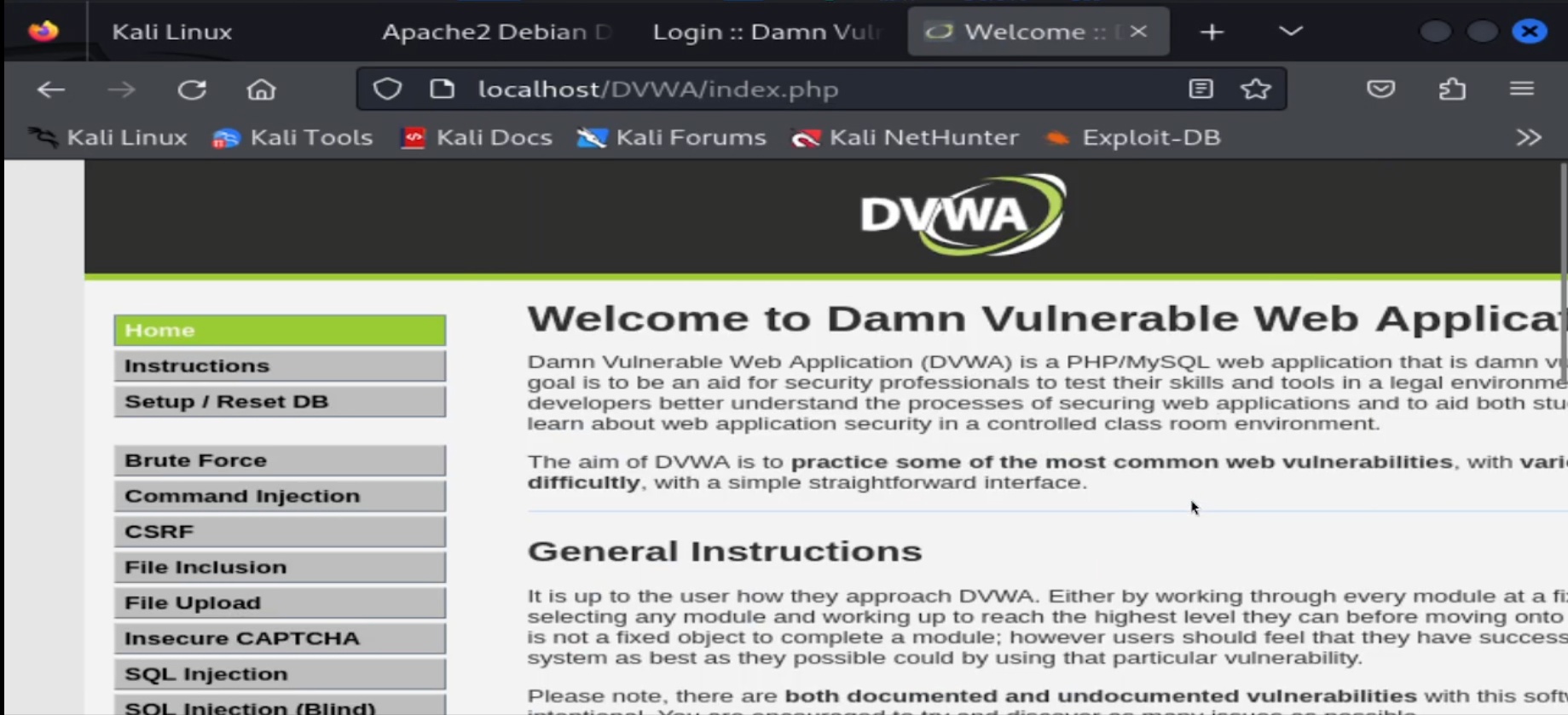


Рис. 8: Запуск DVWA

# 4 Выводы

В результате выполнения DVWA было установлено на Kali Linux.