Отчёт по 2-ому этапу индивидуального проекта

Основы информационной безопасности

Бережной Иван Александрович

Содержание

Список иллюстраций

# 1 Цель работы

Попрактиковать навыки установки ПО на дистрибутив Linux - Kali.

# 2 Задание

Установить DVWA на ОС.

# 3 Теоретическое введение

**DVWA (Damn Vulnerable Web Application)** — это веб-приложение, специально созданное для тестирования на уязвимости и обучения основам веб-безопасности. Оно содержит множество уязвимостей, таких как SQL-инъекции, XSS, CSRF, файловые включения и другие, что позволяет безопасно практиковаться в их эксплуатации и устранении.

## 3.1 Основные особенности:

* **Цель**: Обучение и тестирование навыков пентеста.
* **Уязвимости**: Включает широкий спектр уязвимостей для изучения.
* **Уровни сложности**: Низкий, средний, высокий и невозможный (для разных уровней подготовки).
* **Простота установки**: Работает на локальном сервере (например, XAMPP, Docker).

## 3.2 Как использовать:

1. Установите DVWA на локальный сервер или используйте готовый образ Docker.
2. Войдите в систему (по умолчанию логин: admin, пароль: password).
3. Выберите уровень сложности и начинайте тестирование.

## 3.3 Примеры уязвимостей:

* **SQL Injection**: Внедрение SQL-кода для получения доступа к базе данных.
* **XSS (Cross-Site Scripting)**: Внедрение вредоносных скриптов в веб-страницы.
* **CSRF (Cross-Site Request Forgery)**: Подделка запросов от имени пользователя.

# 4 Выполнение лабораторной работы

Перейдём в каталог html и клонируем репозиторий git (рис. 1).

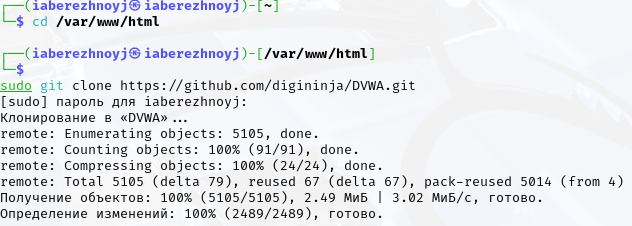


Рис. 1: Клонирование репозитория

Изменим права доступа к папке установки и перейдём к файлу конфигурации (рис. 2).

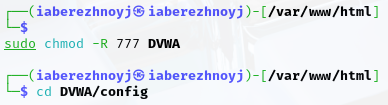


Рис. 2: Изменения прав доступа

Скопируем файл конфига и переименуем его (рис. 3). Откроем файл конфигурации и изменим имя пользователя и пароль (рис. 4).

Рис. 3: Копировани конфига

Рис. 3: Копировани конфига

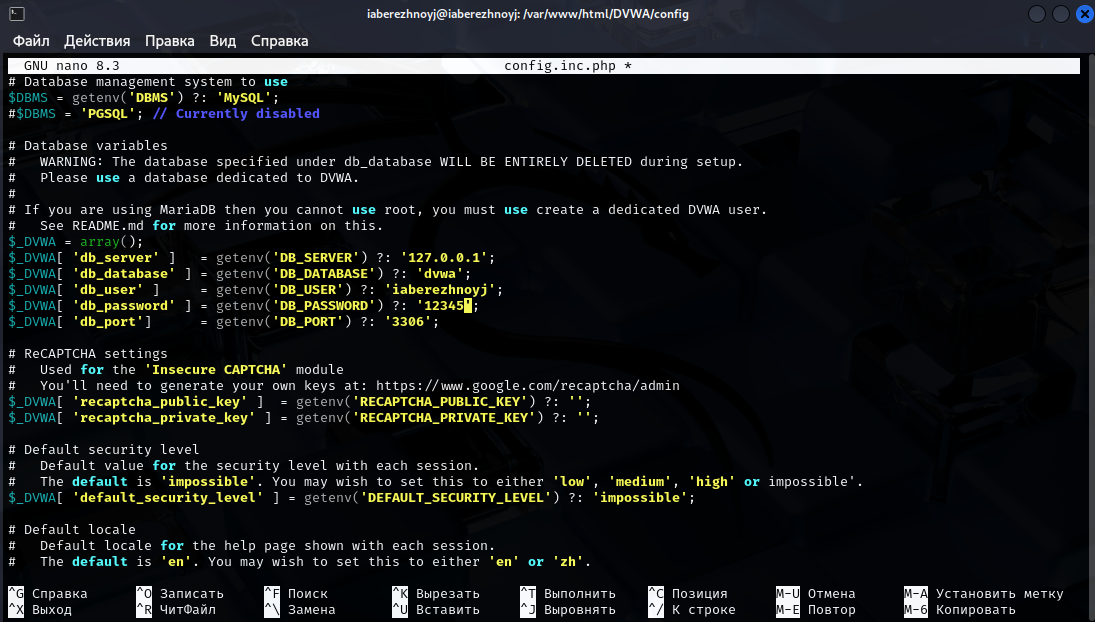


Рис. 4: Редактирование конфига

Поскольку mysql уже установлен, запустим его (рис. 5) и войдём в базу данных (рис. 6).

Рис. 5: Запуск mysql

Рис. 5: Запуск mysql

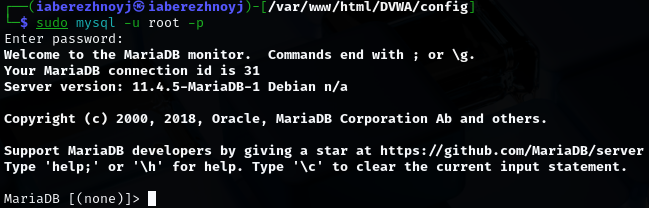


Рис. 6: Вход в бд

Создадим пользователя базы данных, указав имя и пароль такие же, как в файле конфигурации (рис. 7), а также предоставим этому пользователю все привилегии (рис. 8).

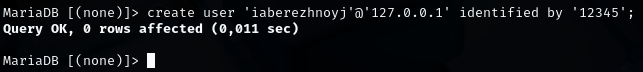


Рис. 7: Создание пользователя бд

Рис. 8: Привилегии пользователя

Рис. 8: Привилегии пользователя

Перейдём в каталог apache (рис. 9) и откроем файл php.ini, чтобы включить параметр allow\_url\_include (рис. 10).

Рис. 9: Переход к apache

Рис. 9: Переход к apache

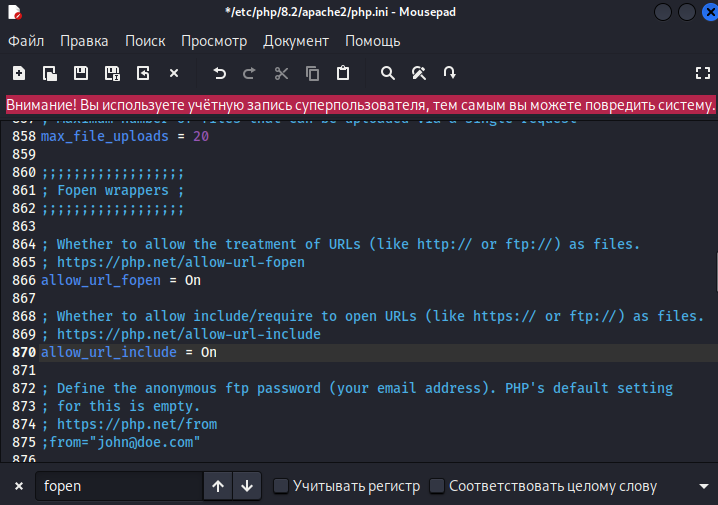


Рис. 10: Изменение php.ini

Запустим apache (рис. 11).

Рис. 11: Запуск apache

Рис. 11: Запуск apache

Теперь можем перейти в браузер и открыть DVWA по адресу 127.0.0.1/DVWA/setup.php (рис. 12)

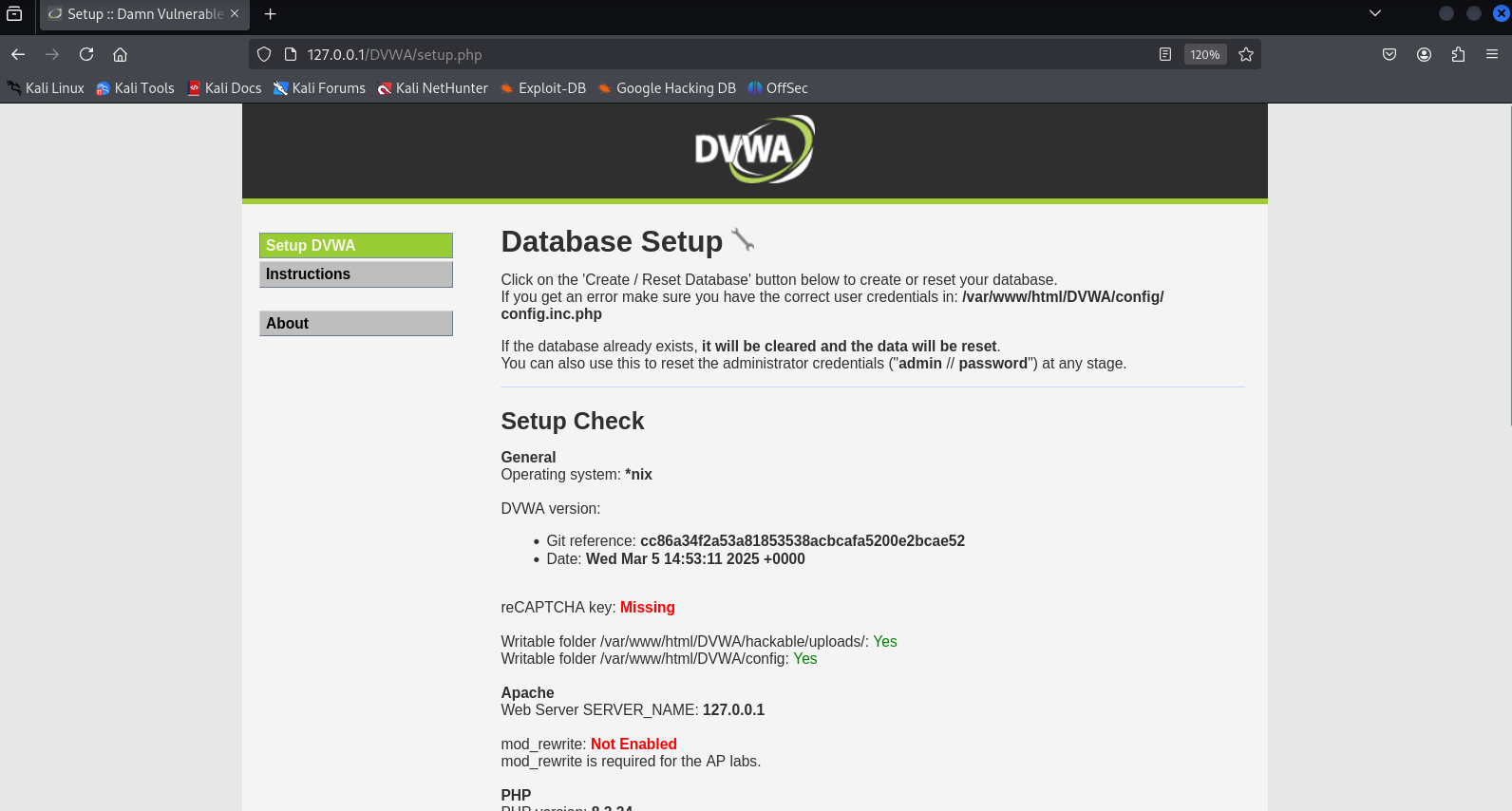


Рис. 12: Открытие DVWA

Внизу нажмём Create Database, введём “admin” и “password” в соответствующих строках. Увидим следующую страницу (рис. 13)

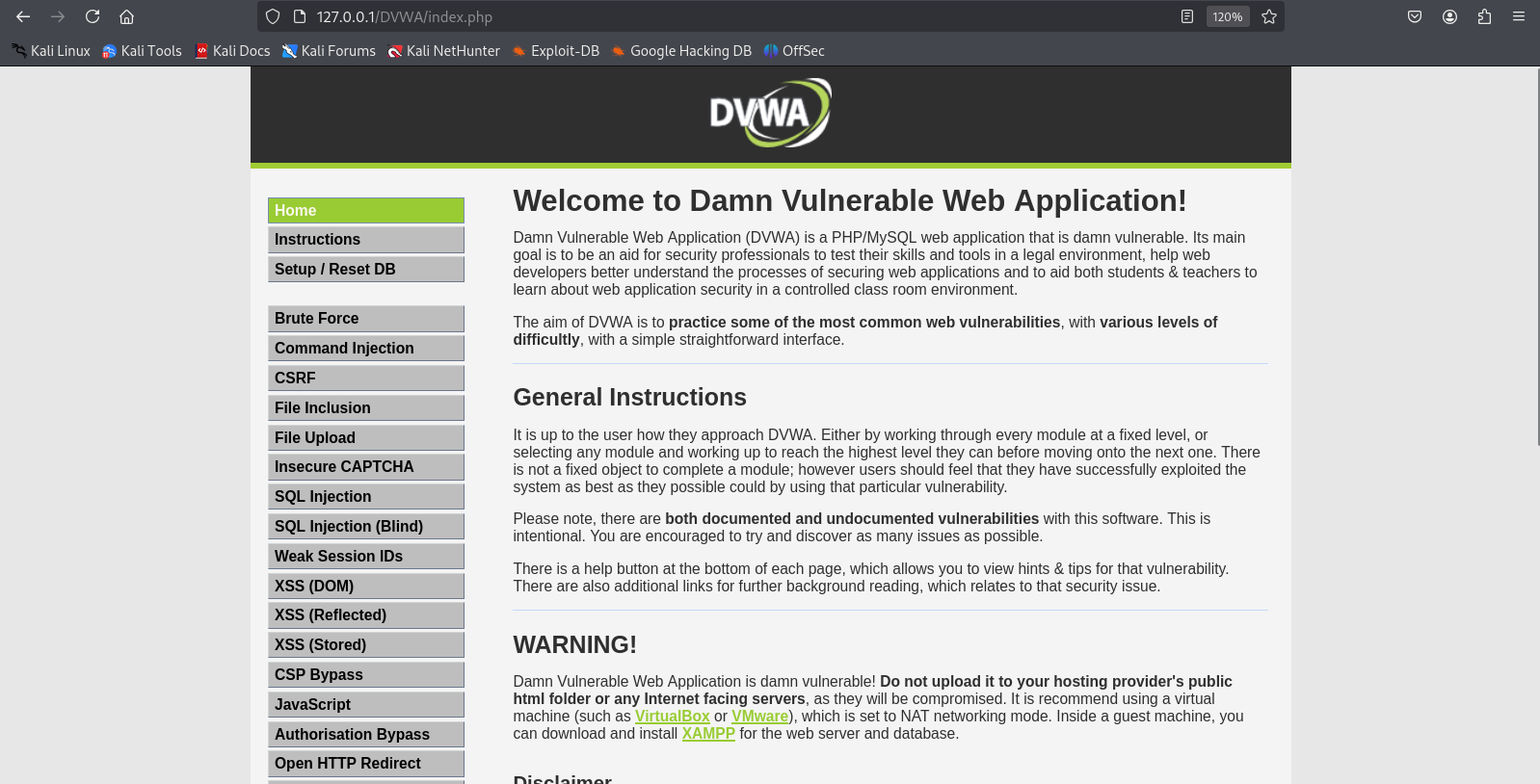


Рис. 13: Вход

# 5 Выводы

В ходе выполнения этапа проекта мы потренировались устанавливать ПО на виртуальную машину, а конкретно на дистрибутив Linux - Kali.