Отчёт о выполнении индивидуальный проект Этап 2

Установка DVWA

Акондзо Жордани Лади Гаэл

Содержание

# Цель работы

Научиться основным способам тестирования веб приложений

# Задание

* Найти максимальное количество уязвимостей различных типов.
* Реализовать успешную эксплуатацию каждой уязвимости.

# Выполнение лабораторной работы

## Установка необходимых зависимостей

* DVWA требует наличия некоторых зависимостей для работы, таких как Apache, MariaDB (или MySQL), PHP и несколько модулей PHP (рис. 1).



Рис. 1: Установка необходимых зависимостей

## Запуск служб Apache и MariaDB

* Убедился, что службы Apache и MariaDB запущены (рис. 2).

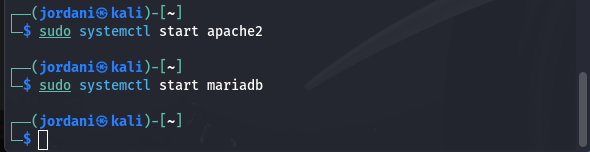


Рис. 2: Запуск служб Apache и MariaDB

* Чтобы эти службы запускались автоматически при старте системы, выполнил следующие команды (рис. 3).

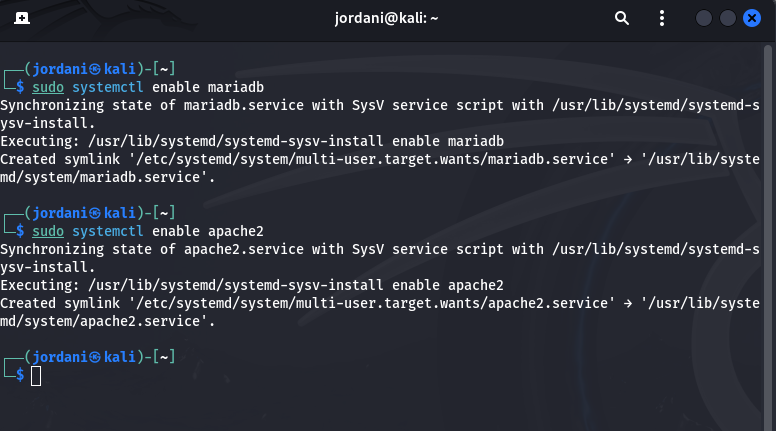


Рис. 3: Запуск служб Apache и MariaDB

## Настройка MariaDB

* Подключусь к MariaDB для создания базы данных и пользователя для DVWA. Потом в командной строке MariaDB выполнил следующие команды (рис. 4).

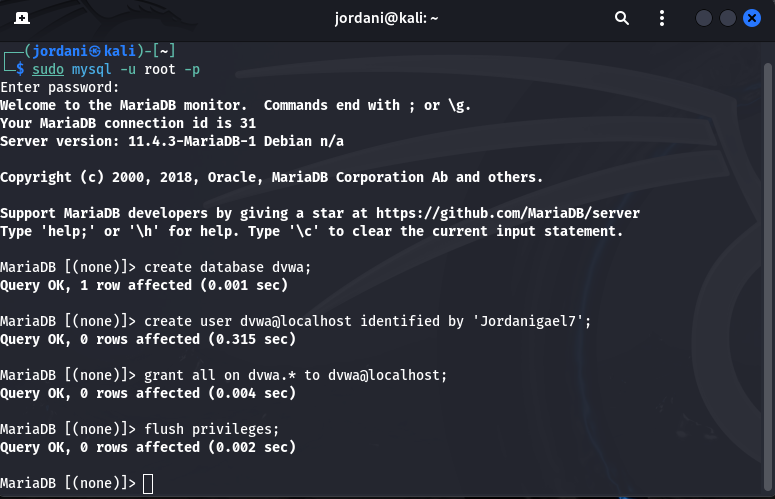


Рис. 4: Настройка MariaDB

## Загрузка и настройка DVWA

* Скачайл последнюю версию DVWA из репозитория GitHub (рис. 5).



Рис. 5: Загрузка и настройка DVWA

* Потом создал файл конфигурации для DVWA (рис. 6).



Рис. 6: Загрузка и настройка DVWA

* Открыл этот файл для редактирования и внёс изменения в информацию о базе данных (рис. 8) и (рис. 7).



Рис. 7: Загрузка и настройка DVWA

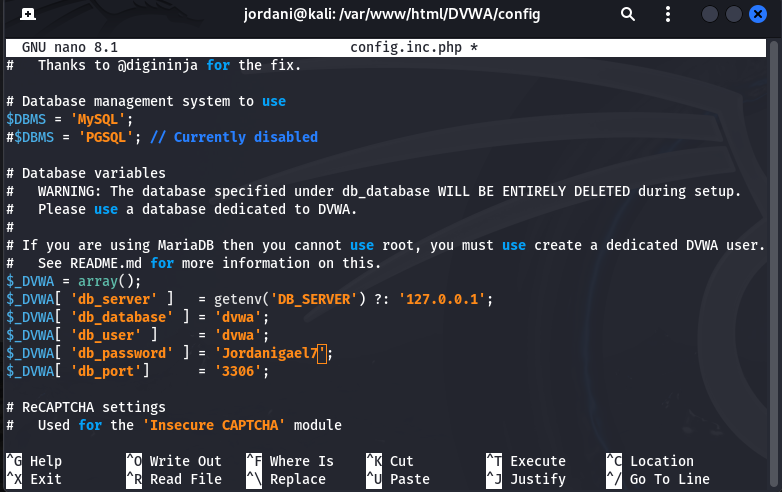


Рис. 8: Загрузка и настройка DVWA

## Завершение установки DVWA

* Потос открыл браузер и перешёл по адресу: http://localhost/DVWA/setup.php. Следовал инструкциям на странице для завершения установки. По окончании установки, вошёл в DVWA, используя следующие данные для входа (рис. 9):

Логин: admin  
 Пароль: password

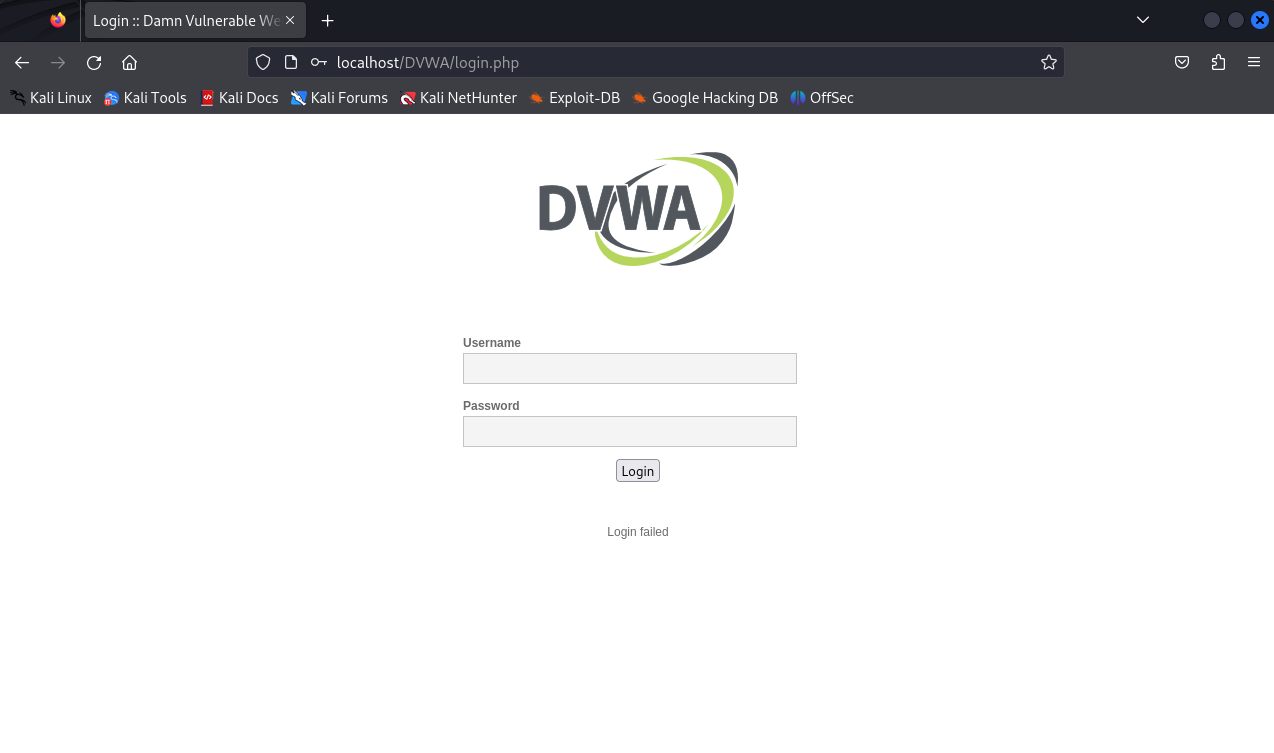


Рис. 9: Завершение установки DVWA

## Окончательная настройка

* **Проверка настроек базы данных (Setup Check)** (рис. 10).

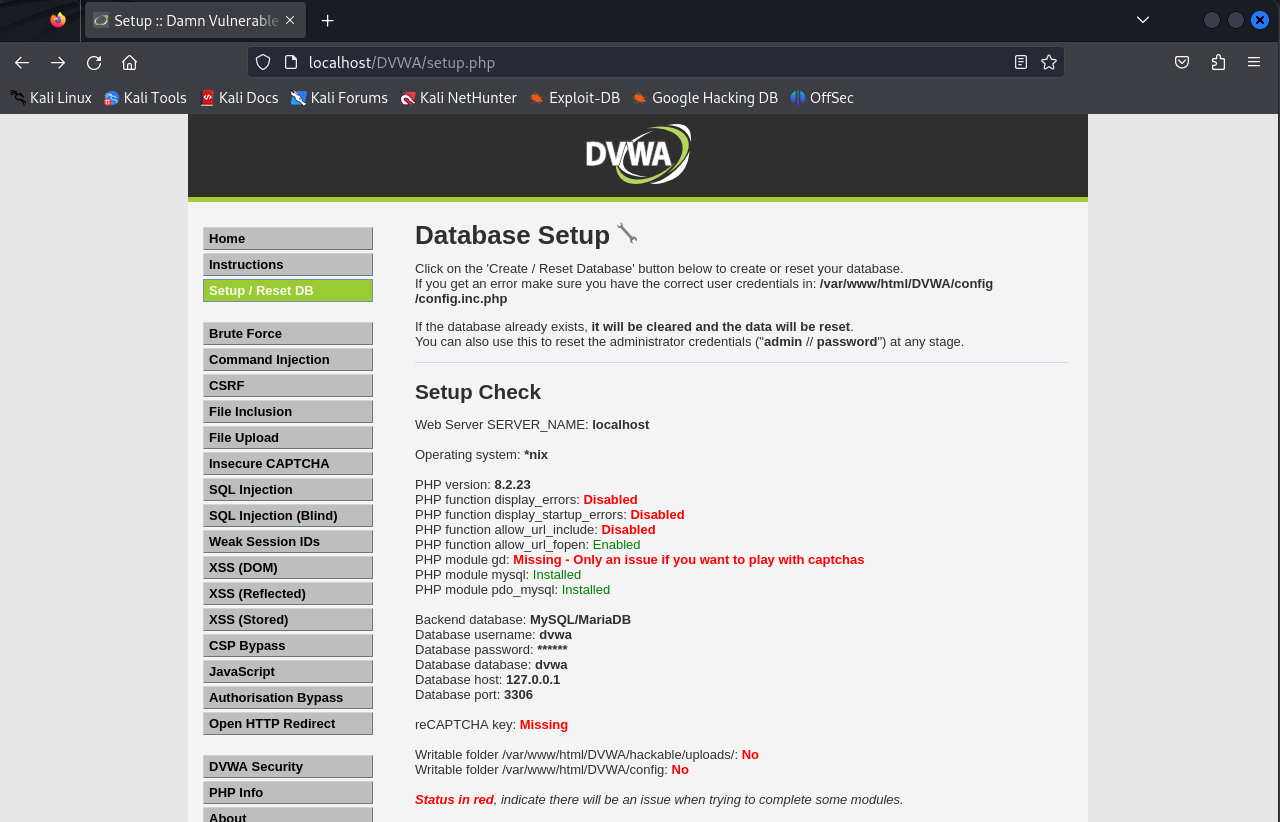


Рис. 10: Проверка настроек базы данных (Setup Check)

* **Уровень безопасности DVWA:** Протестировал несколько уровней безопасности, начиная с Impossible, где все уязвимости заблокированы, и продолжив с Low, который позволяет изучать наиболее распространенные уязвимости без каких-либо мер безопасности (рис. 11) и (рис. 12).

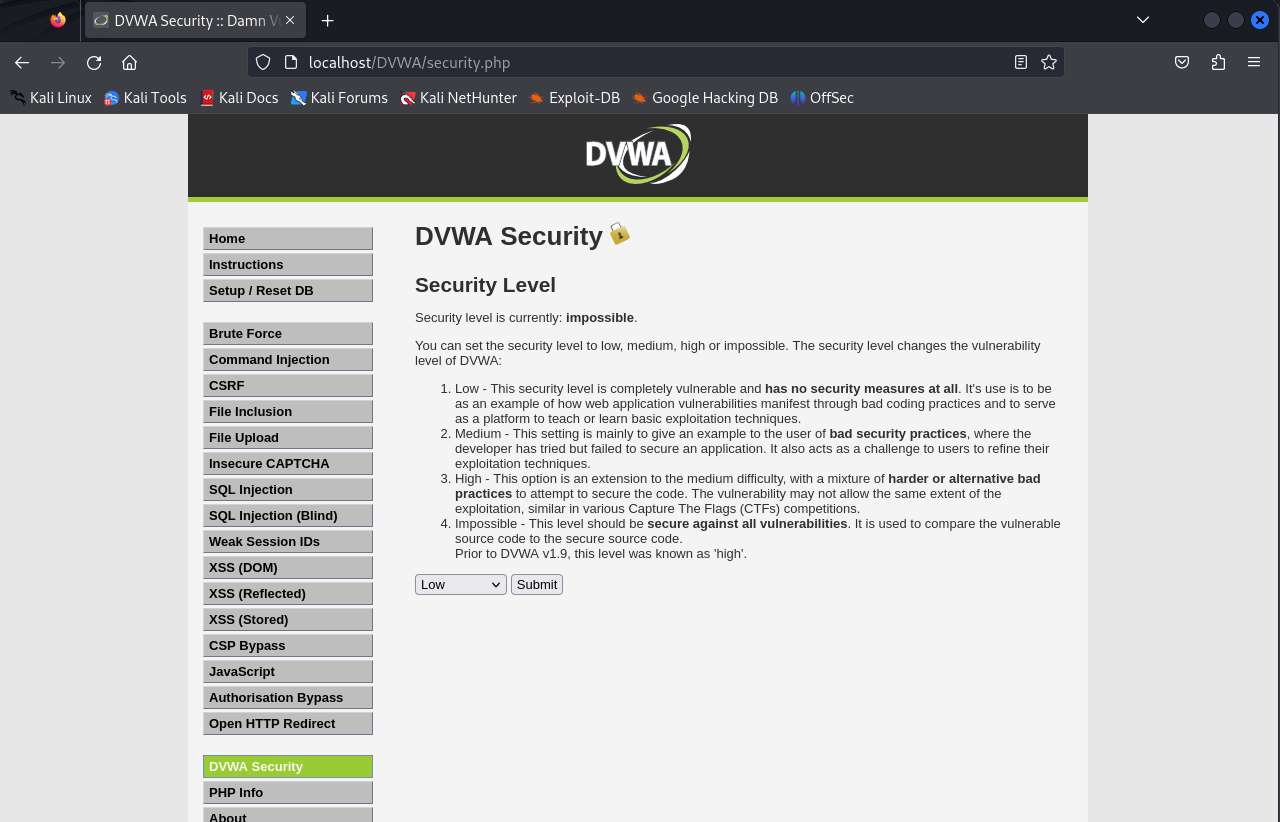


Рис. 11: Уровень безопасности DVWA

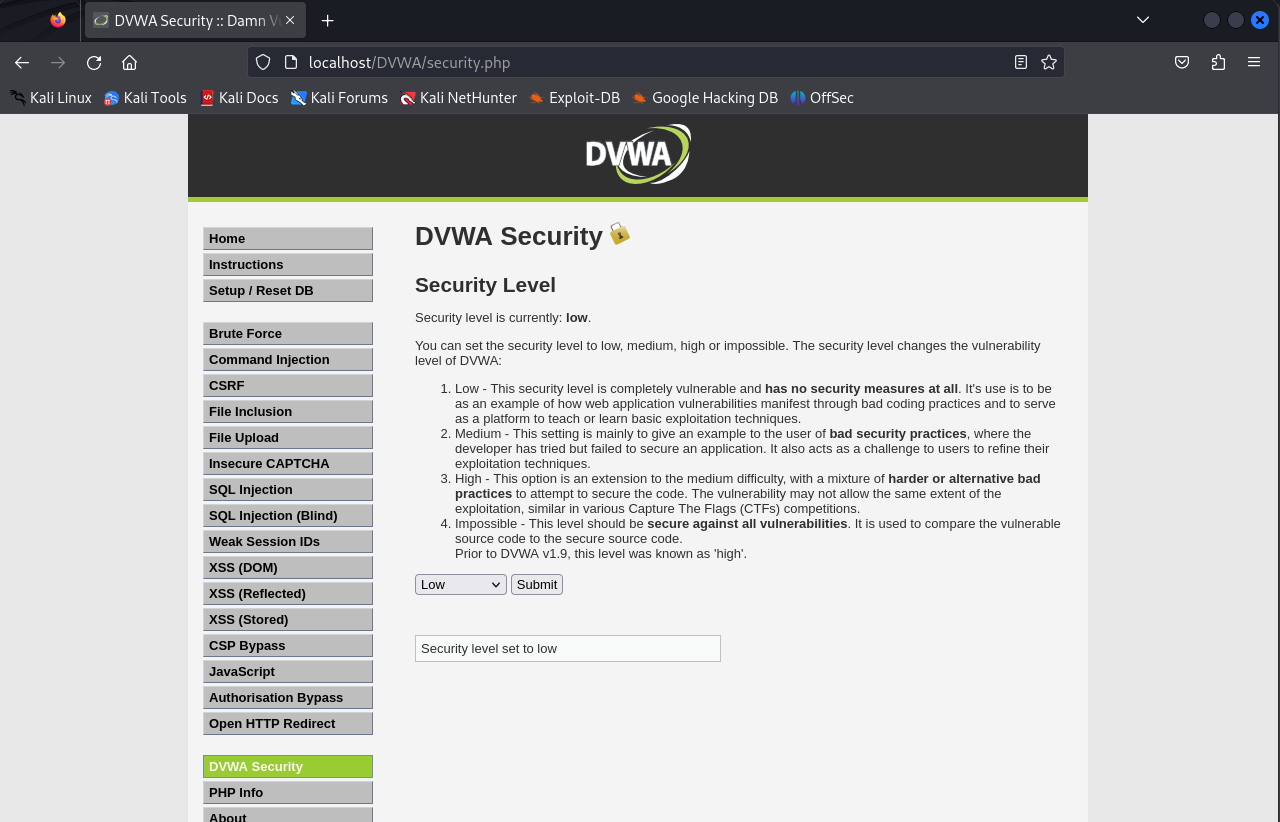


Рис. 12: Уровень безопасности DVWA

* **Изменения в файле php.ini:** Параметры *allow\_url\_fopen = On и allow\_url\_include = On* были включены, что важно для тестирования уязвимостей, связанных с включением локальных или удалённых файлов **(LFI/RFI)** (рис. 13), (рис. 14) и (рис. 15).

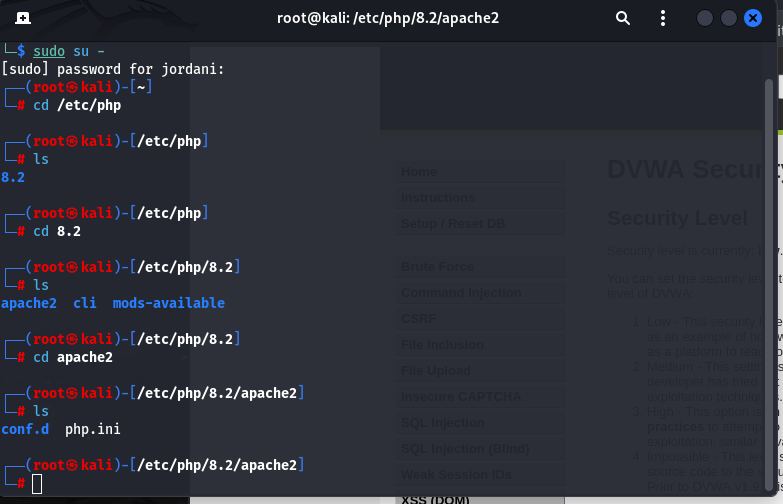


Рис. 13: Изменения в файле php.ini

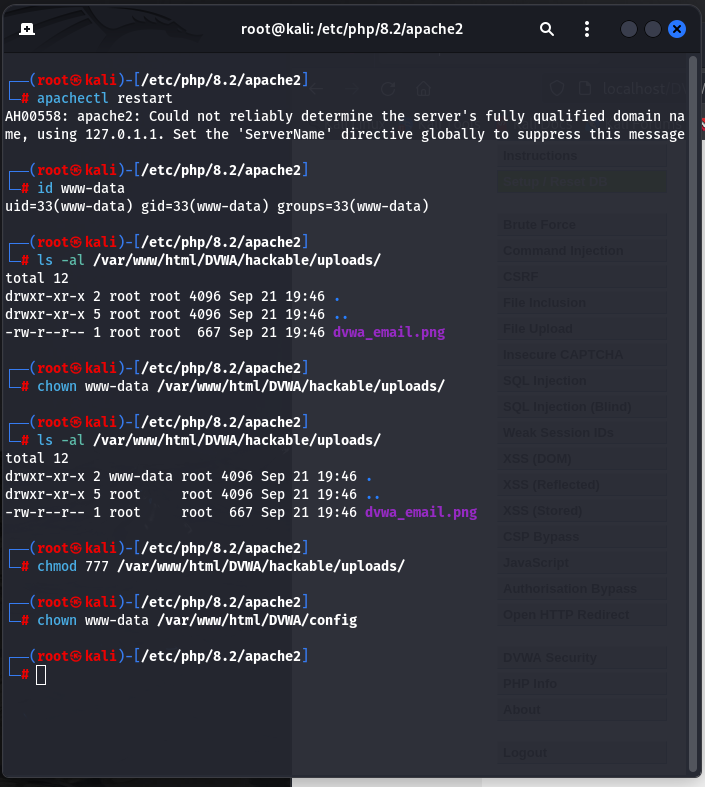


Рис. 14: Изменения в файле php.ini

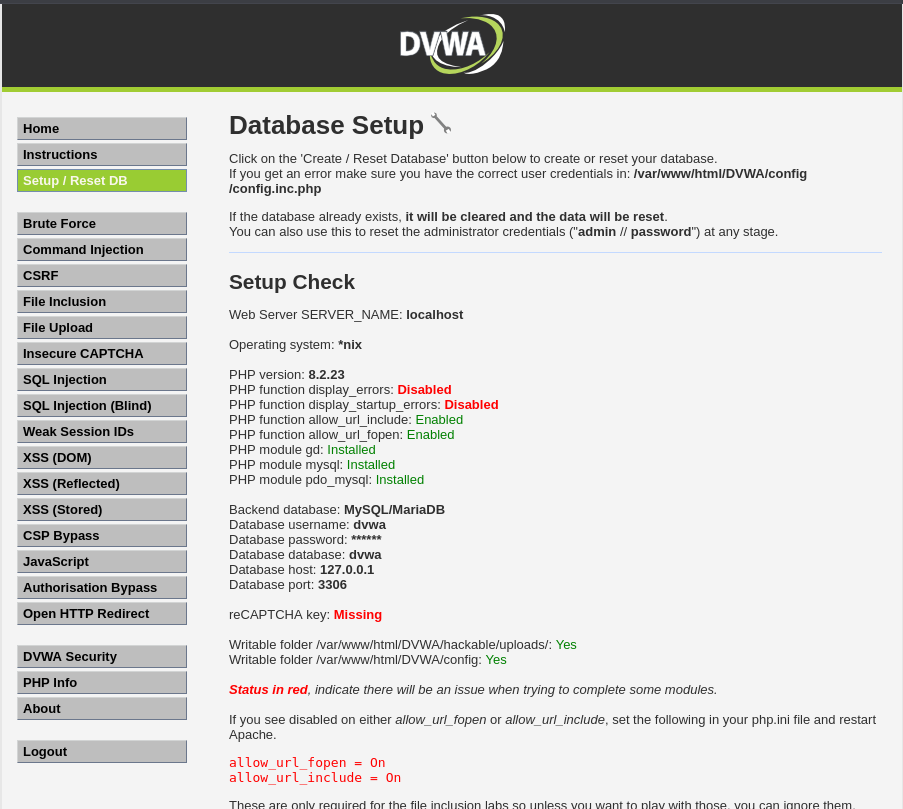


Рис. 15: Изменения в файле php.ini

# Выводы

На этом этапе я научился устанавливать и настраивать DVWA на Kali Linux. Я освоил конфигурацию баз данных, работу с Apache и MariaDB, а также внес необходимые изменения в настройки PHP для тестирования уязвимостей. Изучение разных уровней безопасности в DVWA позволило понять, как плохие практики разработки делают приложения уязвимыми для атак.