Отчёт по 2 этапу индивидуального проекта

Дисциплина: Информационная безопасность

Андрианова Марина Георгиевна

Содержание

[Цель работы 1](#_Toc177828824)

[Выполнение 2-го этапа индивидуального проекта 1](#_Toc177828825)

[Выводы 6](#_Toc177828826)

# Цель работы

Установить DVWA на дистрибутив Kali Linux.

# Выполнение 2-го этапа индивидуального проекта

Переходим в каталог html, введя команду “cd /var/www/html”. Клонируем репозиторий git командой “sudo git clone https://github.com/digininja/DVWA” (рис.1).

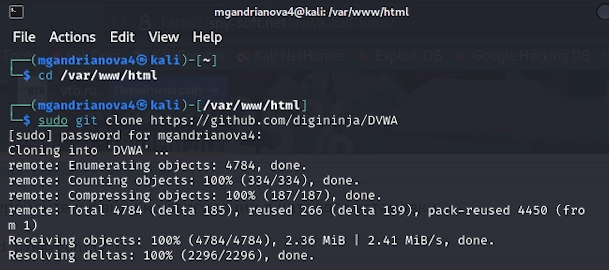


Рис.1:Переход в каталог и клонирование репозитория

Проверяем, что файлы склонировались правильно и изменяем права доступа к папке установки(рис.2).

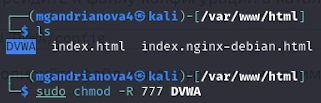


Рис.2:Изменение прав доступа

Переходим к файлу конфигурации в каталоге установки: /dvwa/config. Проверяем содержимое каталога (рис.3).

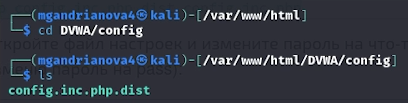


Рис.3:Переход к файлу конфигурации

Копируем файл конфигурации (config.inc.php.dist) и переименовываем его на config.inc.php (рис.4).



Рис.4:Копирование и переименование файла

Открываем файл настроек (рис.5) и изменяем пароль на что-то более простое для ввода (я изменю пароль на toor20) (рис.6).

Рис.5:Открытие файла настроек

Рис.5:Открытие файла настроек

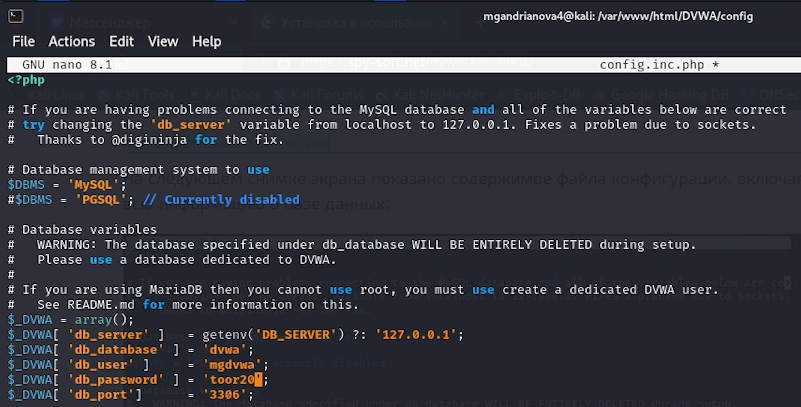


Рис.6:Редактирование файла

Запускаем базу данных mysql и проверяем, запущен ли процесс (рис.7).



Рис.7:Запуск mysql

Входим в базу данных от имени пользователя root; (пароля нет, поэтому просто нажимаем Enter при появлении запроса ввода пароля). Появляется командная строка с приглашением “MariaDB”(рис.8).

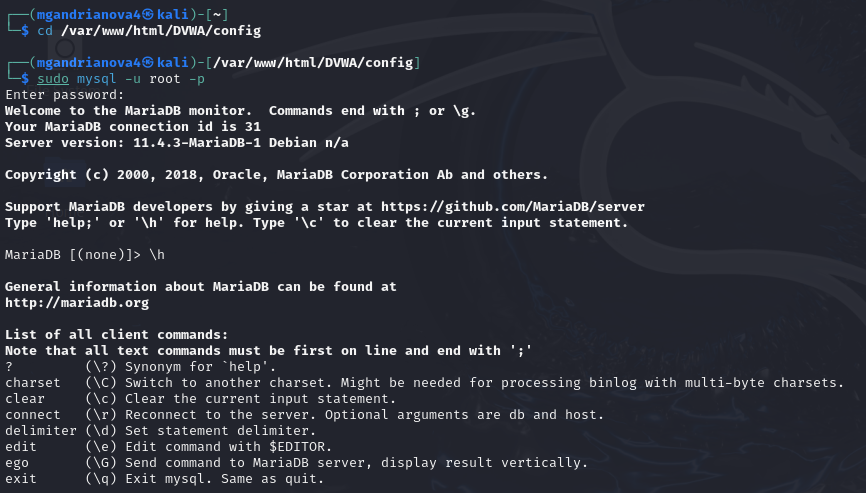


Рис.8:Вход в базу данных

Далее создаём в ней нового пользователя, используя учётные данные из файла config.inc.php. Также предоставляем пользователю привилегии для работы с этой базой данных (рис.9).

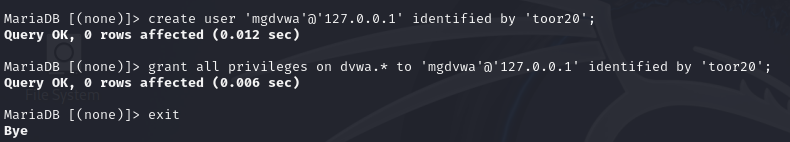


Рис.9:MariaDB

Для настройки сервера apache2 переходим в соответствующую директорию (рис.10).

Рис.10:Переход в каталог apache2

Рис.10:Переход в каталог apache2

Открываем для редактирования файл php.ini (с помощью команды “sudo nano php.ini”) (рис.11), чтобы включить следующие параметры: allow\_url\_fopen и allow\_url\_include.

Рис.11:Редактирование файла

Рис.11:Редактирование файла

Файл большой, поэтому нам потребовалось прокрутить до середины файла, чтобы добраться до fopen и изменить значения “off” на ‘on’(рис.12).

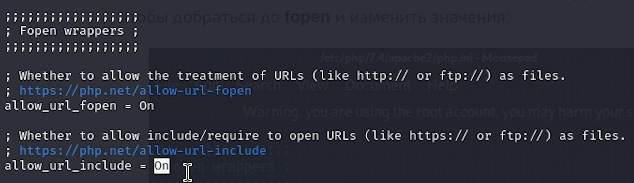


Рис.12:Fopen wrappers

Запускаем сервер Apache и проверяем, запущена ли служба(рис.13).

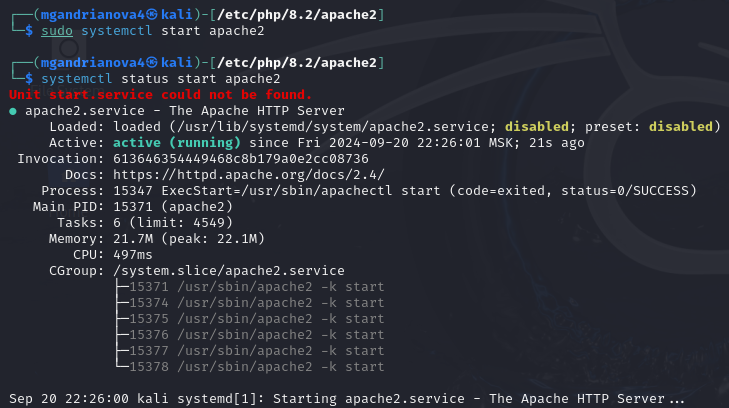


Рис.13:Запуск сервера Apache

Пробуем открыть DVWA в браузере, введя в адресной строке следующее: “127.0.0.1/DVWA/”. Перед нами открылась страница настройки, это означает, что мы успешно установили DVWA на Kali Linux(рис.14).

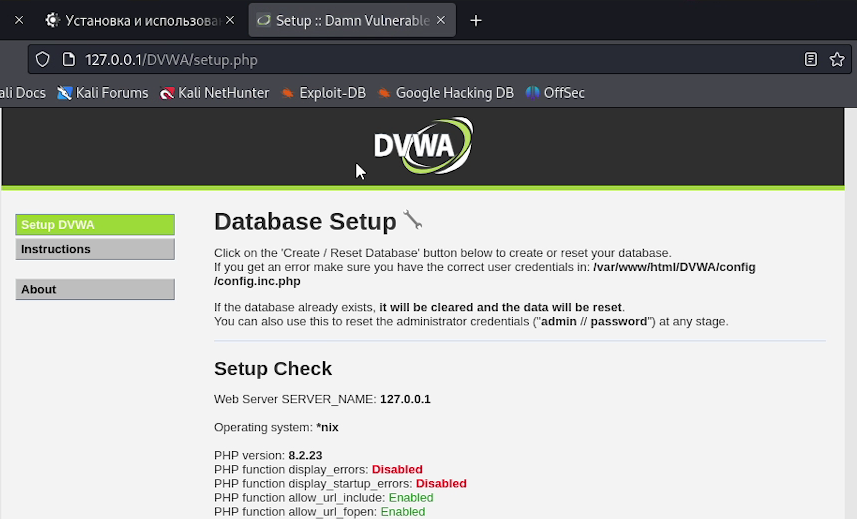


Рис.14:Запуск DVWA в браузере

Прокручиваем вниз и нажимаем “Create / Reset Database” (Создать / сбросить базу данных) (рис.15).

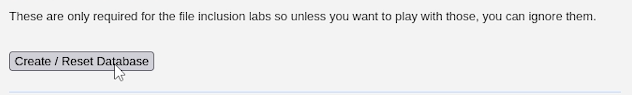


Рис.15:Создание базы данных

И через несколько секунд нас перенаправили на страницу входа в DVWA. Авторизуемся с помощью предложенных по умолчанию данных (рис.16).

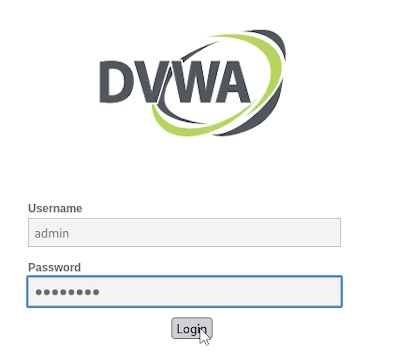


Рис.16:Авторизация

Оказываемся на домашней странице веб-приложения. Можем заметить, что существует множество интересных уязвимостей, которые мы можем протестировать, например, брутфорс, SQL-инъекция и другие (рис.17). На этом установка окончена.

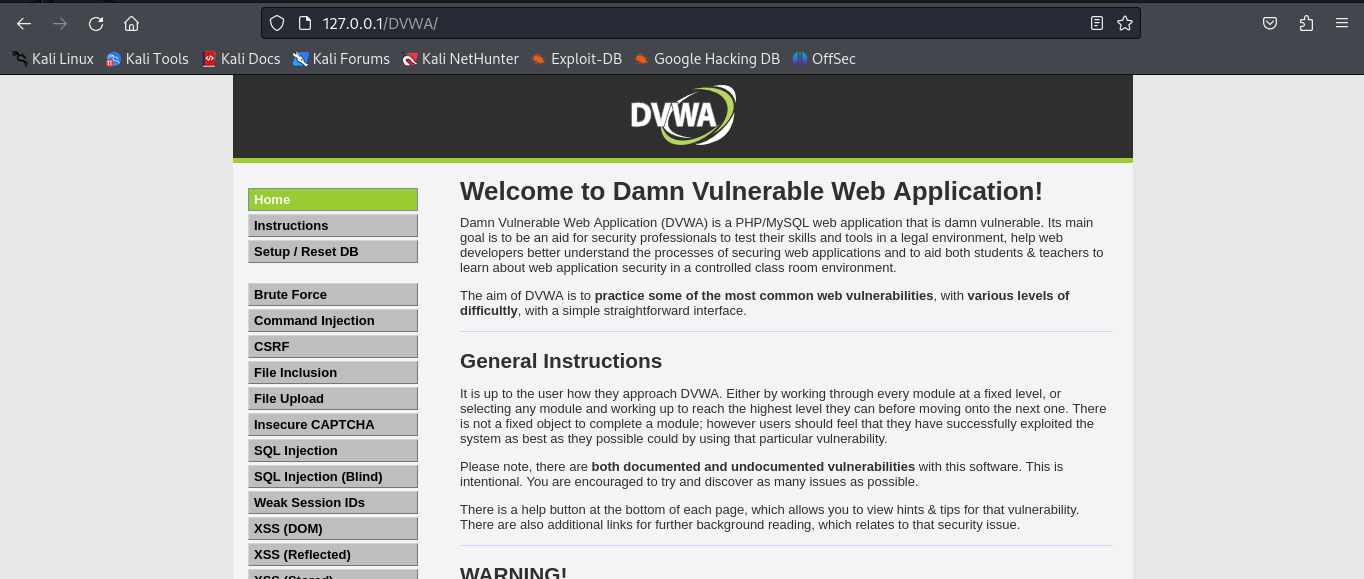


Рис.17:Домашняя страница DVWA

# Выводы

Установила веб-приложение DVWA на дистрибутив Kali Linux.