Основы информационной безопасности

Индивидуальный проект. Этап №2. Установка DVWA

Нзита Диатезилуа Катенди

Содержание

# Постановка задачи

Целью данной работы является установка DVWA на Kali Linux в виртуальную машину.

# Теоретические сведения

Damn Vulnerable Web Application (DVWA) – это веб-приложение PHP/MySQL, которое чертовски уязвимо[~@dvwa]. Его основная цель – помочь специалистам по безопасности проверить свои навыки и инструменты в правовой среде, помочь веб-разработчикам лучше понять процессы обеспечения безопасности веб-приложений, а также помочь студентам и преподавателям узнать о безопасности веб-приложений в контролируемом классе. обстановка помещения.

DVWA (Damn Vulnerable Web Application) — это приложение, предназначенное для практики работы с распространёнными веб-уязвимостями, предлагая пользователю интуитивно понятный интерфейс. Оно содержит как документированные, так и недокументированные уязвимости, позволяя исследовать безопасность веб-приложений на разных уровнях сложности.

Некоторые из уязвимостей, представленных в DVWA, включают:

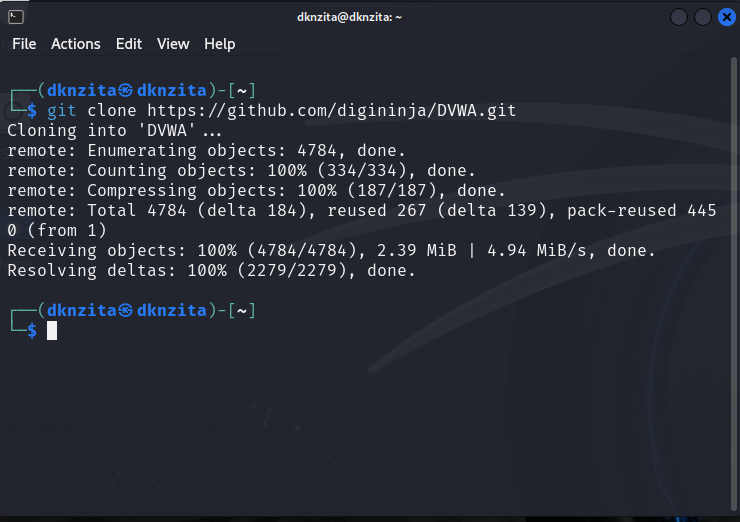
* **Брутфорс**: Атака на формы входа, используемая для тестирования инструментов, позволяющих подбирать пароли, и демонстрации уязвимости слабых паролей.
* **Выполнение команд**: Позволяет злоумышленнику исполнять команды на уровне операционной системы.
* **Межсайтовая подделка запроса (CSRF)**: Позволяет злоумышленнику изменять пароль администратора.
* **Внедрение файлов**: Злоумышленник может подключать удалённые или локальные файлы к веб-приложению.
* **SQL-внедрение**: Позволяет вставлять SQL-код в запросы через поля ввода, включая слепое и основанное на ошибках внедрение.
* **Небезопасная выгрузка файлов**: Позволяет загружать вредоносные файлы на сервер.
* **Межсайтовый скриптинг (XSS)**: Злоумышленник может внедрять свои скрипты в веб-приложение или базу данных, включая отражённые и сохранённые XSS.
* **Пасхальные яйца**: Раскрытие путей к файлам, обход аутентификации и другие уязвимости.

DVWA предлагает четыре уровня безопасности, которые меняют уязвимость веб-приложений:

* **Невозможный**: Уровень безопасности, при котором приложение защищено от всех уязвимостей. Используется для сравнения уязвимого кода с безопасным.
* **Высокий**: Уровень сложности с элементами более сложных и альтернативных плохих практик, который снижает возможности эксплуатации.
* **Средний**: Уровень, показывающий примеры плохих практик безопасности, где разработчик пытался обеспечить безопасность, но не смог.
* **Низкий**: Полностью уязвимый уровень, предназначенный для демонстрации плохих практик программирования и обучения базовым методам эксплуатации.

# Выполнение лабораторной работы

Скопируем в каталог /etc/www/html файла веб приложения DVWA с Гита (рис. @fig:001)

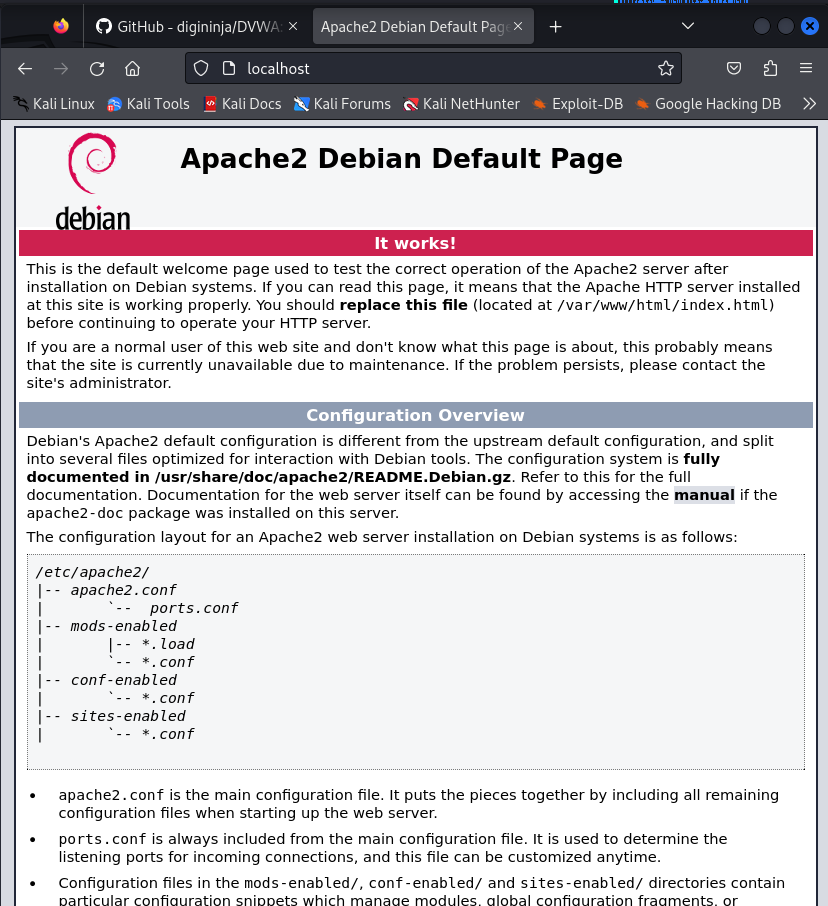


Клонирование репозитория с DVWA

Затем запускаем веб сервер(рис. @fig:002, @fig:003).

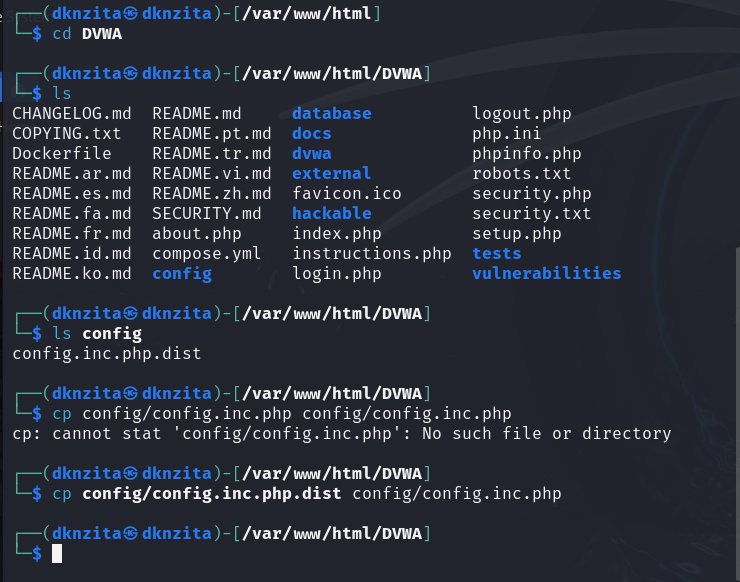


Запуск apache2

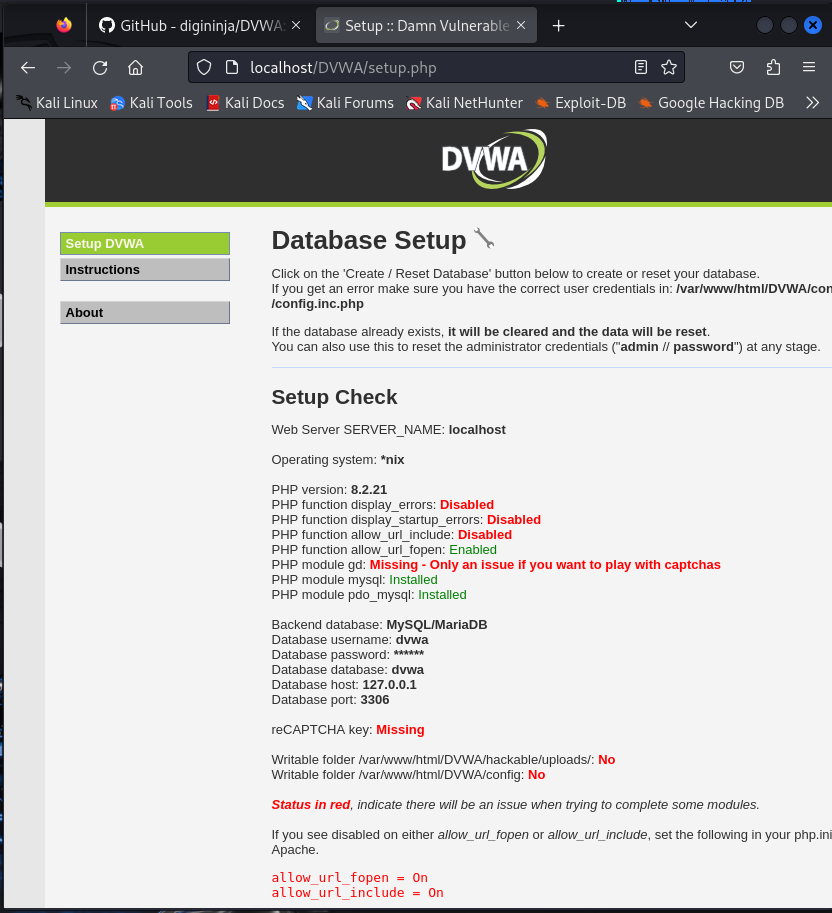


Проверка работы веб-сервера

Затем скопируем файл конфигураций DVWA, чтобы затем можно было его безопасно изменять. Мы воспользуемся именем пользователя и паролем по умолчанию(рис. @fig:004, @fig:005).

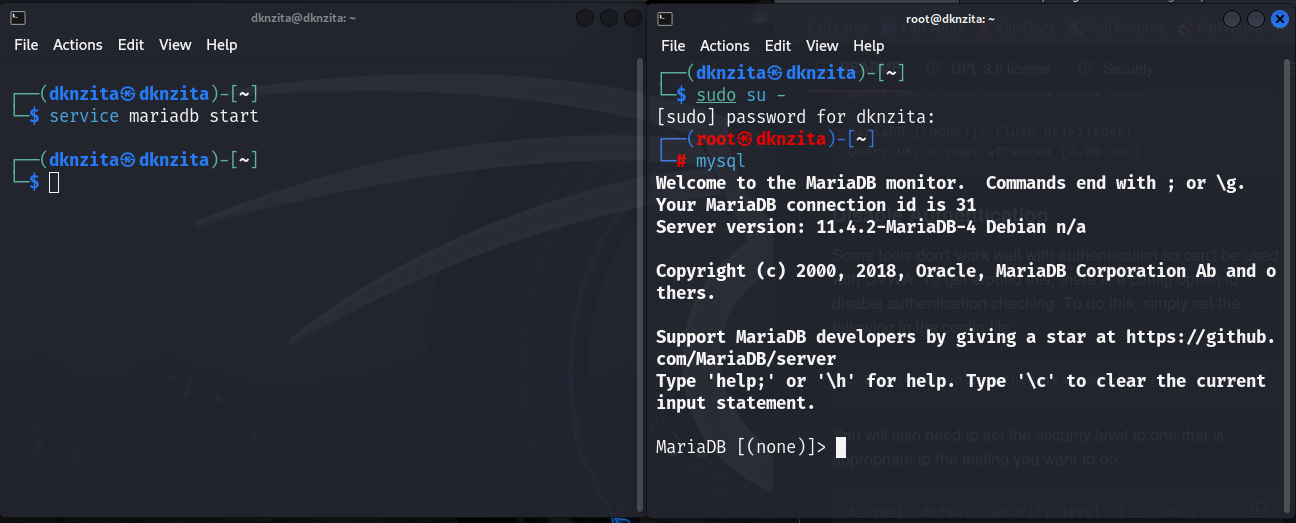


Просмтр файла конфигураций

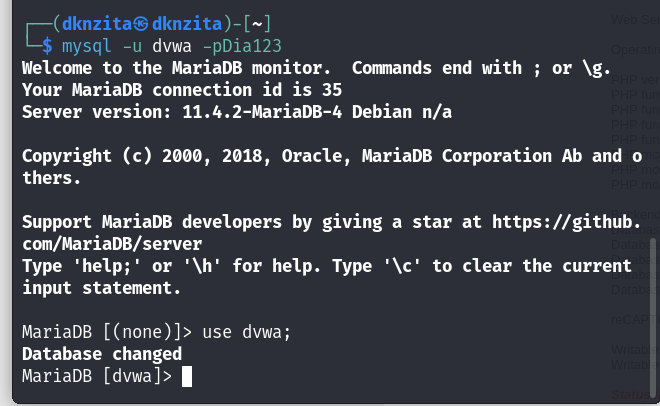


Просмотр стартового окна DVWA

Запустим сервер mariadb и создадтм на нем пользоватедя и пароль совпадают с данными в файле конфигураций dvwa)(рис. @fig:006, @fig:007).

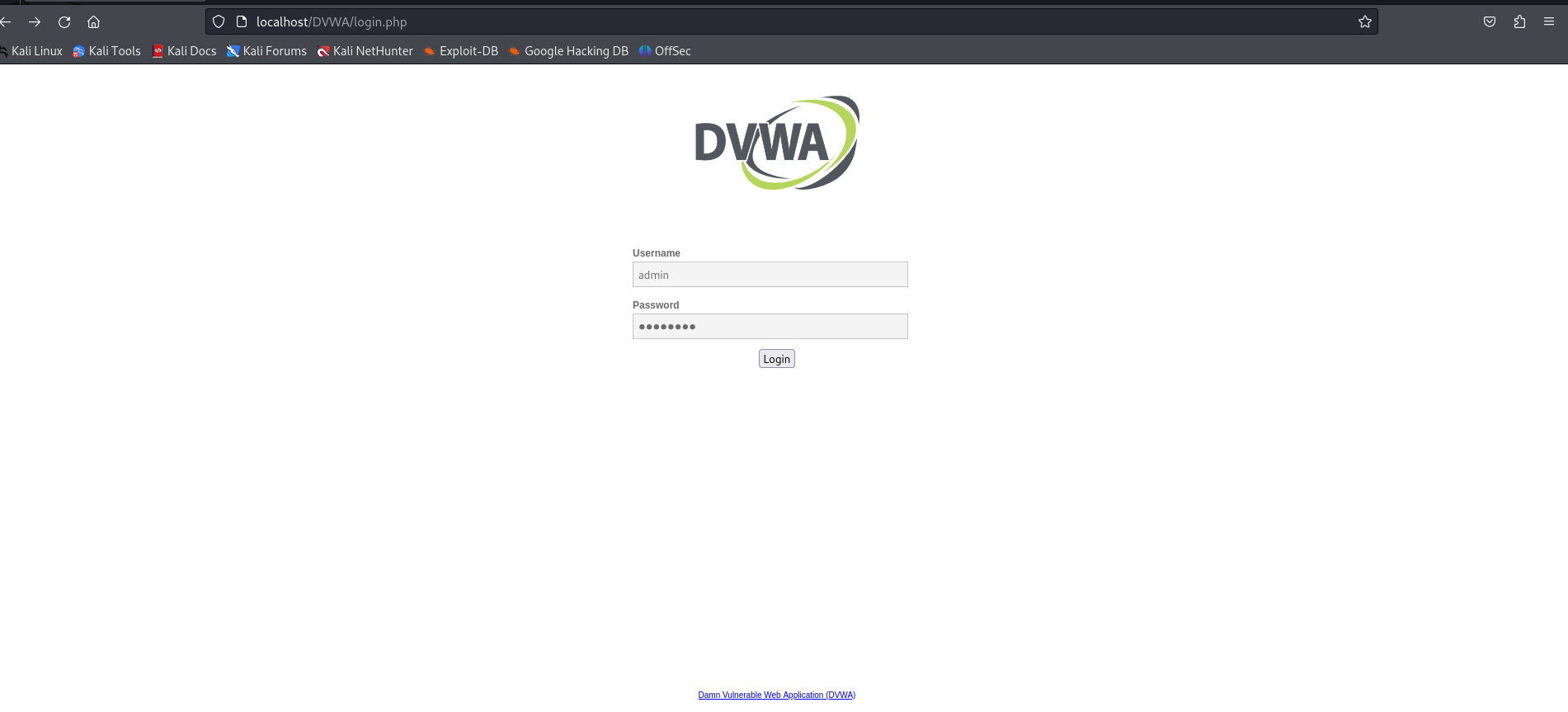


Создание пользователя mariadb и базы данных

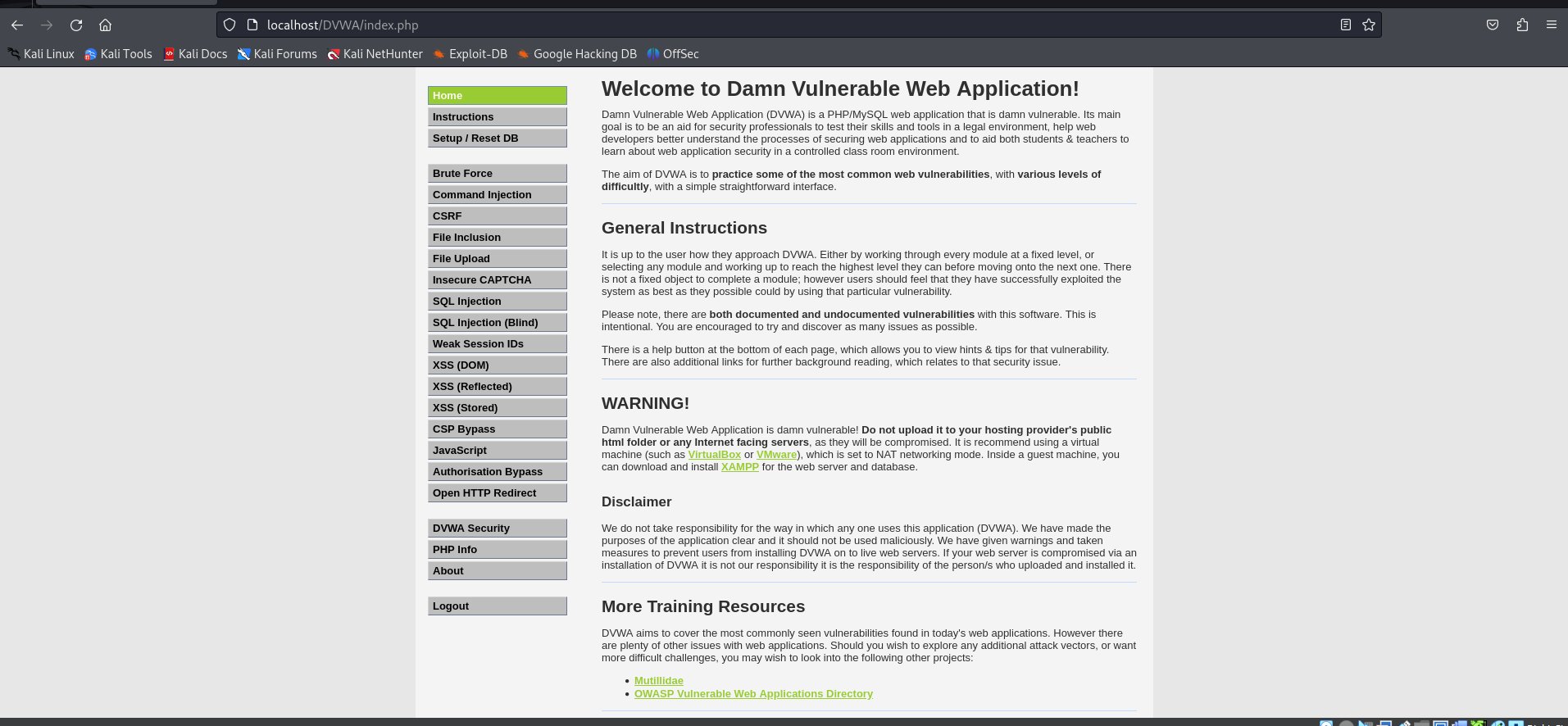


Проверка пользователя mariadb

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:008, @fig:009).



Аутентификация



Запуск DVWA

# Выводы

В резултате выпольнения работы был установлен DVWA на Kali Linux.

# Список литературы

:::::: :::