Индивидуальный проект

Этап 2. Установка DVWA

Артамонов Тимофей Евгеньевич

Содержание

# 1 Цель работы

Установить DVWA и сделать приготовления для последующей работы.

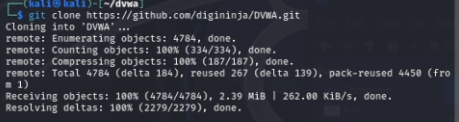
# 2 Теоретеческое введение

DVWA (Damn Vulnerable Web Application) - это веб-приложение на PHP/MySQL, которое “чертовски” уязвимо. Его основная цель — помочь специалистам по безопасности протестировать свои навыки и инструменты в легальной среде, помочь веб-разработчикам лучше понять процессы обеспечения безопасности веб-приложений, а также помочь студентам и преподавателям изучить вопросы безопасности веб-приложений в контролируемой учебной среде. Цель DVWA — отработать некоторые из наиболее распространенных веб-уязвимостей с различными уровнями сложности, используя простой и понятный интерфейс. Пожалуйста, обратите внимание, что в этом программном обеспечении есть как задокументированные, так и незадокументированные уязвимости. Это сделано намеренно. Вам предлагается попытаться обнаружить как можно больше проблем. [1]

Некоторые из уязвимостей веб приложений, который содержит DVWA: Брутфорс: Брутфорс HTTP формы страницы входа - используется для тестирования инструментов по атаке на пароль методом грубой силы и показывает небезопасность слабых паролей. Исполнение (внедрение) команд: Выполнение команд уровня операционной системы. Межсайтовая подделка запроса (CSRF): Позволяет «атакующему» изменить пароль администратора приложений. Внедрение (инклуд) файлов: Позволяет «атакующему» присоединить удалённые/локальные файлы в веб приложение. SQL внедрение: Позволяет «атакующему» внедрить SQL выражения в HTTP из поля ввода, DVWA включает слепое и основанное на ошибке SQL внедрение. Небезопасная выгрузка файлов: Позволяет «атакующему» выгрузить вредоносные файлы на веб сервер. Межсайтовый скриптинг (XSS): «Атакующий» может внедрить свои скрипты в веб приложение/базу данных. DVWA включает отражённую и хранимую XSS. Пасхальные яйца: раскрытие полных путей, обход аутентификации и некоторые другие. DVWA имеет три уровня безопасности, они меняют уровень безопасности каждого веб приложения в DVWA: Невозможный — этот уровень должен быть безопасным от всех уязвимостей. Он используется для сравнения уязвимого исходного кода с безопасным исходным кодом. Высокий — это расширение среднего уровня сложности, со смесью более сложных или альтернативных плохих практик в попытке обезопасить код. Уязвимости не позволяют такой простор эксплуатации как на других уровнях. Средний — этот уровень безопасности предназначен главным образом для того, чтобы дать пользователю пример плохих практик безопасности, где разработчик попытался сделать приложение безопасным, но потерпел неудачу. Низкий — этот уровень безопасности совершенно уязвим и совсем не имеет защиты. Его предназначение быть примером среди уязвимых веб приложений, примером плохих практик программирования и служить платформой обучения базовым техникам эксплуатации. [2]

# 3 Выполнение лабораторной работы

Загружаем репозиторий по ссылке. (рис. [??])



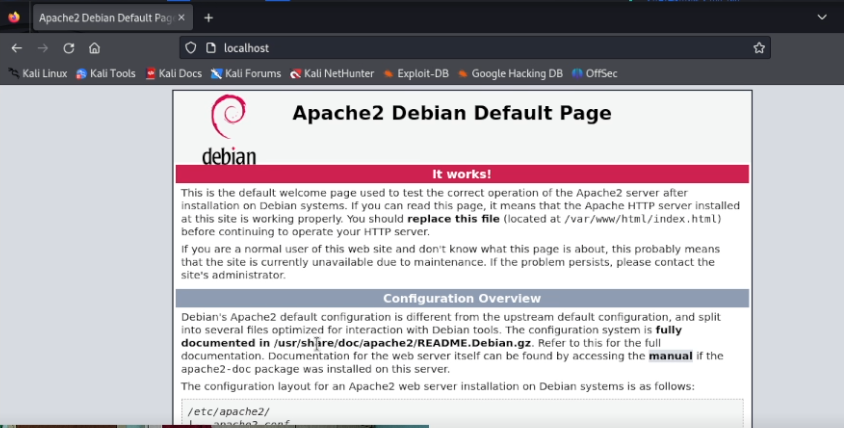
git clone

Запускаем Apache. (рис. [??])

Запуск apache2

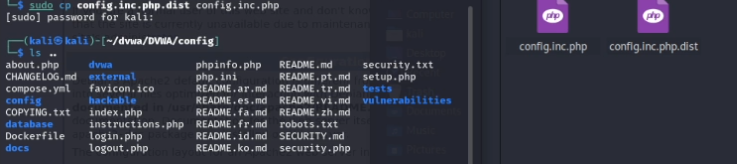
Запуск apache2

Открываем веб-страницу Apache. (рис. [??])



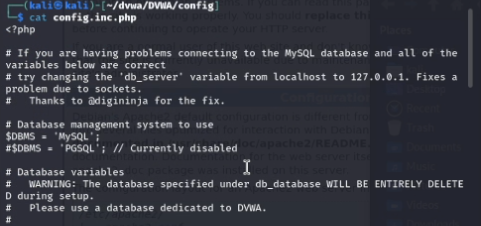
Веб-страница Apache2 Debian Default Page

Копируем файл config.inc.php.dist в config.inc.php. (рис. [??])



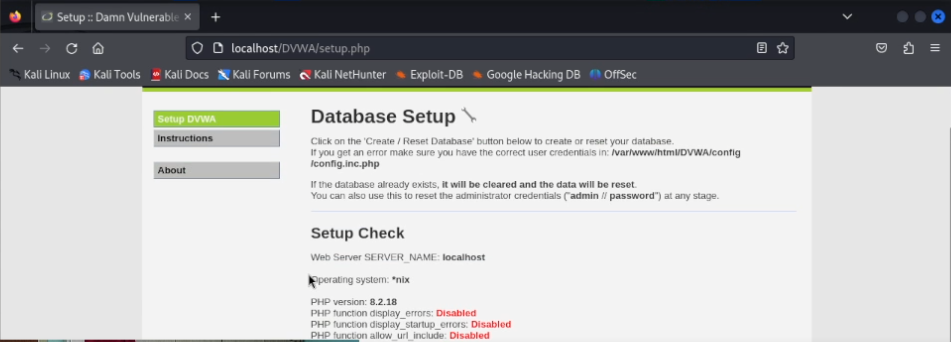
Новый файл config.inc.php с содержимым config.inc.php.dist

Посмотрим содержимое файла. (рис. [??])



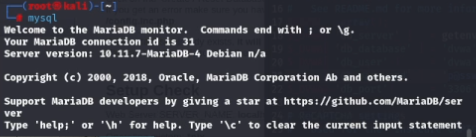
Содержимое файла config.inc.php.dist

Откроем стартовую страницу DVWA. (рис. [??])



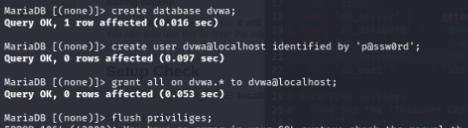
Стартовую страница DVWA

Запустим mysql. (рис. [??])



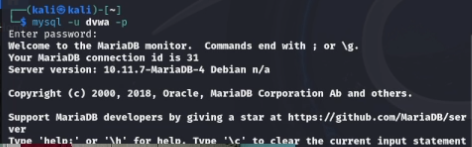
MariaDB monitor

Создадим базу данных и пользователя, указав данные из файла. (рис. [??])



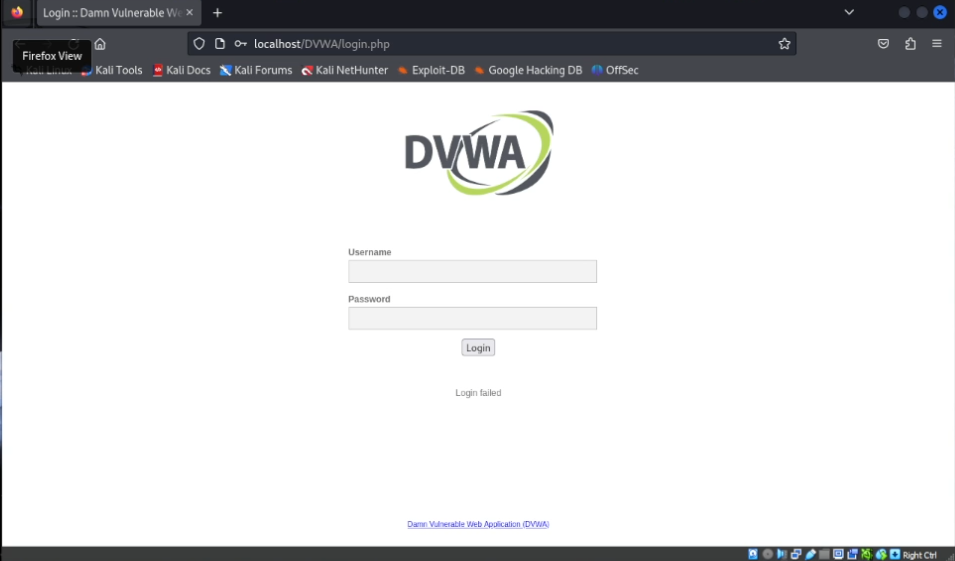
Создание базы данных и пользователя

Запустим MariaDB monitor с созданным пользователем и выберем нашу базу данных. (рис. [??])



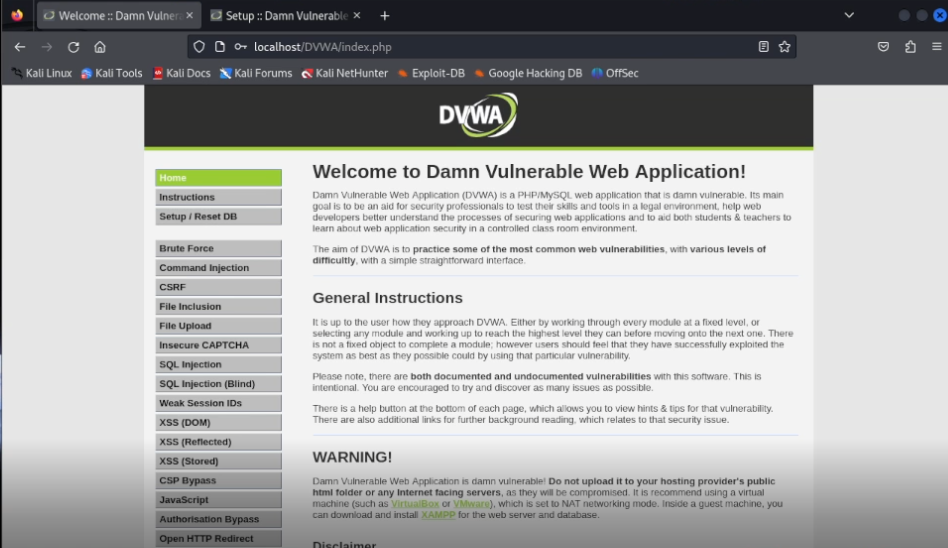
Запуск MariaDB monitor

Нажмем на странице DVWA create/reset database и попадем на страницу с логином. (рис. [??])



Страница входа DVWA

После входа увидим рабочую область DVWA. (рис. [??])



Рабочая область DVWA

# 4 Выводы

Установили DVWA и сделали приготовления для последубщей работы.

# Список литературы

1. DVWA [Электронный ресурс]. 2024 GitHub, Inc., 2024. URL: <https://github.com/digininja/DVWA>.

2. Этап 2. DVWA [Электронный ресурс]. RUDN, 2024. URL: <https://esystem.rudn.ru/mod/page/view.php?id=1140704>.