Основы информационной безопасности

Индивидуальный проект. Этап № 2. Установка DVWA

Демидова Екатерина Алексеевна

Содержание

# 1 Постановка задачи

Целью данной работы является установка DVWA на Kali Linux.

# 2 Теоретические сведения

Damn Vulnerable Web Application (DVWA) – это веб-приложение PHP/MySQL, которое чертовски уязвимо[~ 1]. 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.

Цель DVWA – отработать некоторые из наиболее распространенных веб-уязвимостей различного уровня сложности с помощью простого и понятного интерфейса. В этом программном обеспечении существуют как задокументированные, так и недокументированные уязвимости.

Некоторые из уязвимостей веб приложений, который содержит DVWA:

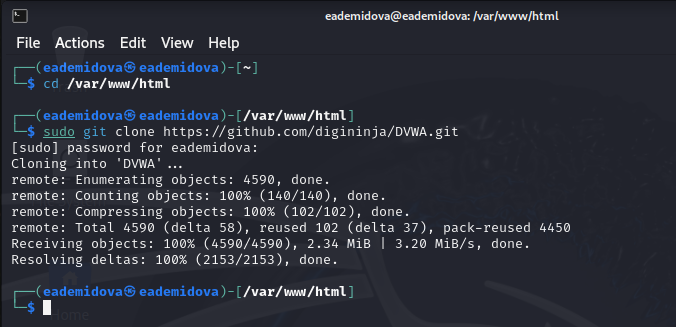
* Брутфорс: Брутфорс HTTP формы страницы входа - используется для тестирования инструментов по атаке на пароль методом грубой силы и показывает небезопасность слабых паролей.
* Исполнение (внедрение) команд: Выполнение команд уровня операционной системы.
* Межсайтовая подделка запроса (CSRF): Позволяет «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.

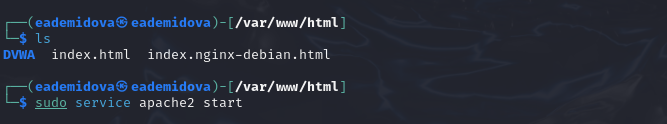
# 3 Выполнение лабораторной работы

Скопируем в каталог /etc/www/html файлы веб-приложения DVWA с гита(рис. ??)

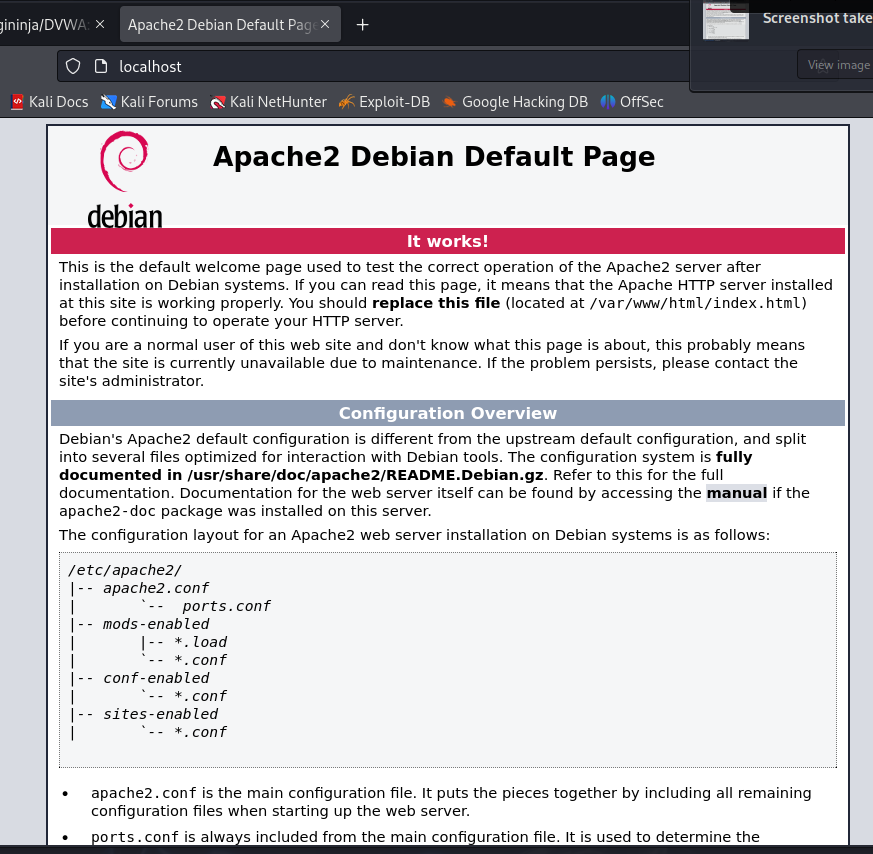


Клонирование репозитория с DVWA

Затем запускаем веб сервер(рис. ??, ??).

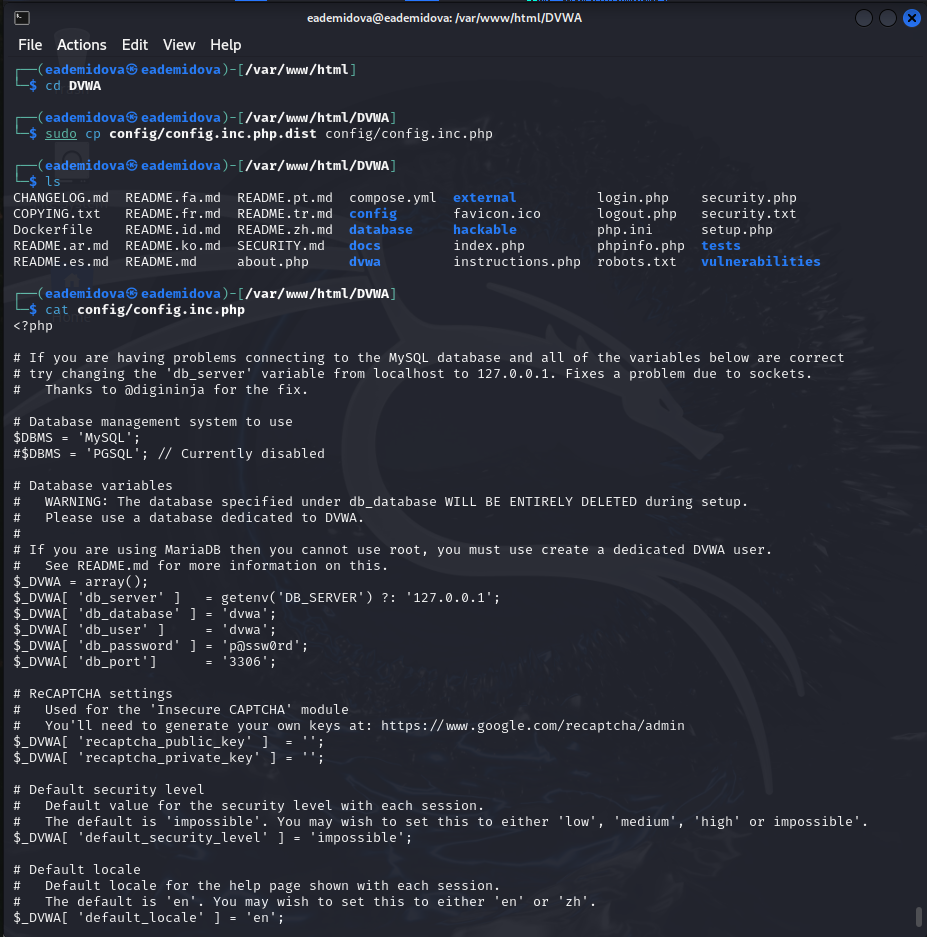


Запуск apache2

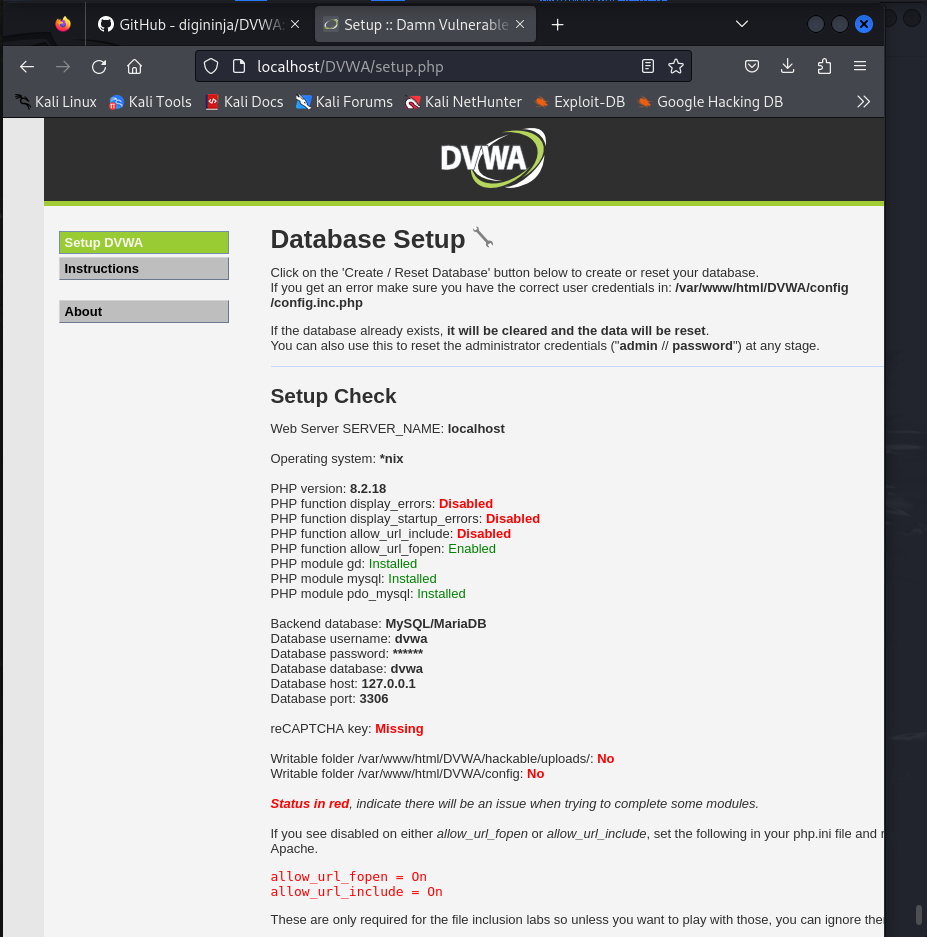


Проверка работы веб-сервера

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

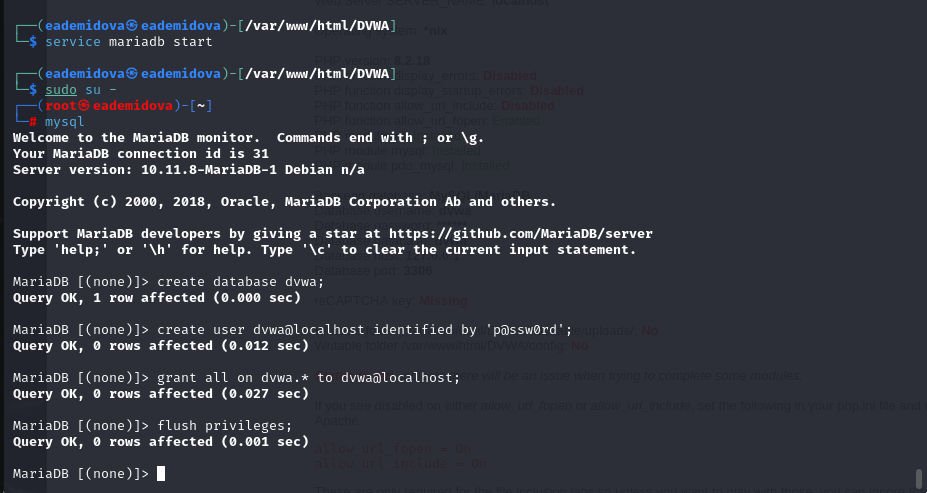


Просмтр файла конфигураций

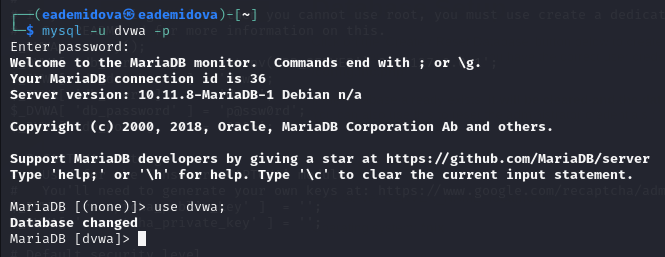


Просмотр стартового окна DVWA

Запустим сервер mariadb и создадим на нем пользователя(имя и пароль совпадают с данными в файле конфигураций dvwa)(рис. ??, ??).

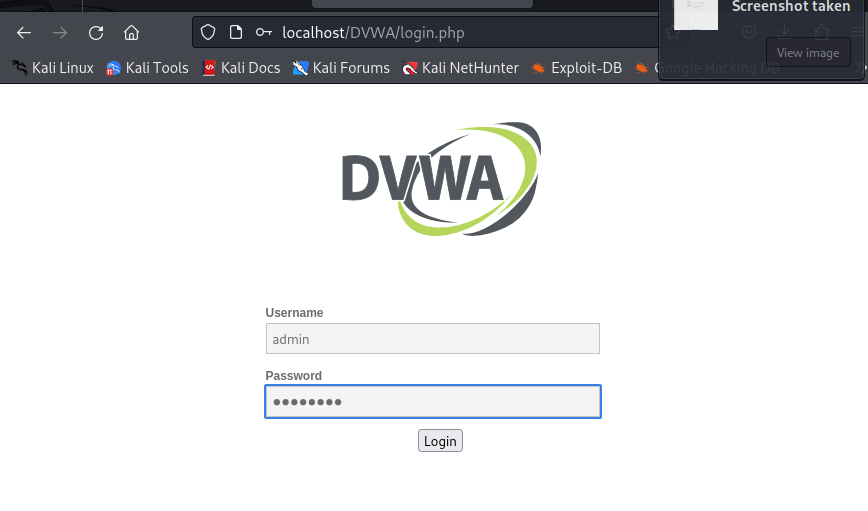


Создание пользователя mariadb и базы данных

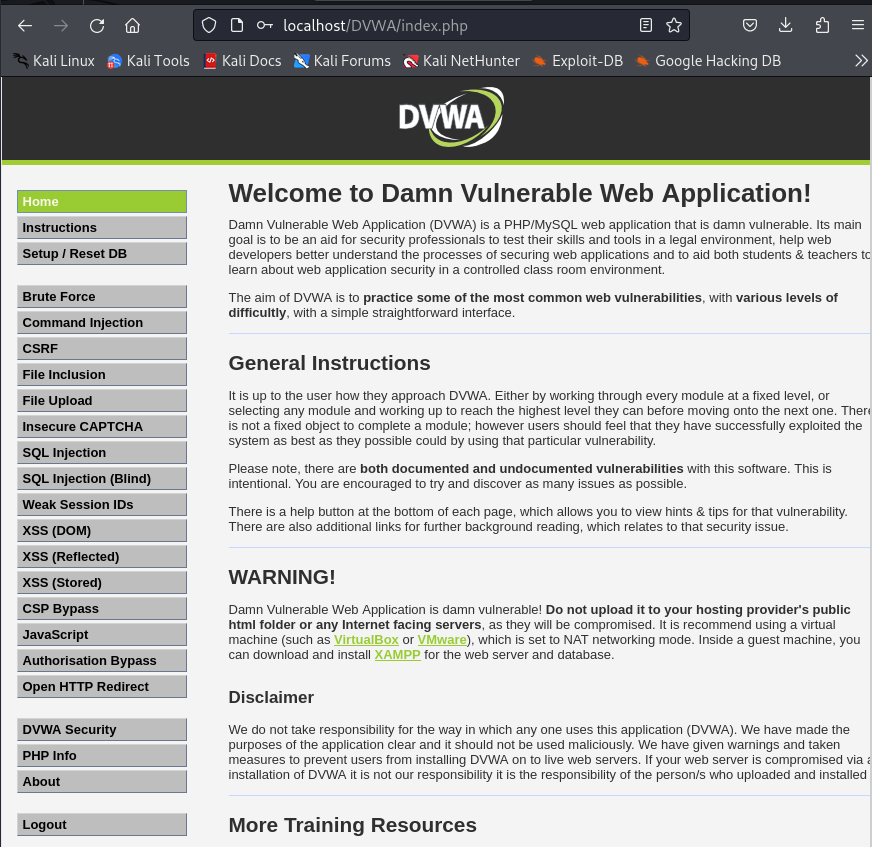


Проверка пользователя mariadb

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. ??, ??).



Аутентификация



Запуск DVWA

# 4 Выводы

В результате выполнения работы был уавстановлен DVWA на Kali Linux.

# Список литературы

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