Индивидуальный проект

Этап 2

Люпп Софья Романовна

Содержание

[1 Цель работы 1](#_Toc193537839)

[2 Задание 1](#_Toc193537840)

[3 Теоретическое введение 1](#_Toc193537841)

[4 Выполнение лабораторной работы 2](#_Toc193537842)

[5 Выводы 7](#_Toc193537843)

[Список литературы 7](#_Toc193537844)

# 1 Цель работы

Приобретение практических навыков по установке DVWA.

# 2 Задание

1. Установить DVWA на дистрибутив Kali Linux.

# 3 Теоретическое введение

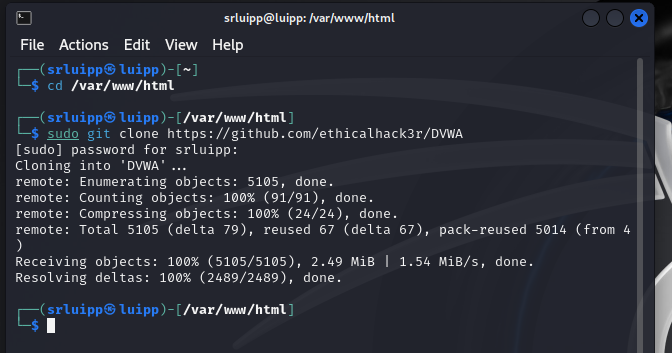
DVWA - это уязвимое веб-приложение, разработанное на PHP и MYSQL.

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 четыре 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]

# 4 Выполнение лабораторной работы

Настройка DVWA происходит на нашем локальном хосте, поэтому нужно перейти в директорию /var/www/html. Затем клонирую нужный репозиторий GitHub (рис. 1).



Клонирование репозитория

Проверяю, что файлы склонировались правильно, далее повышаю права доступа к этой папке до 777 (рис. 2.)

Изображение выглядит как текст, снимок экрана, программное обеспечение, Шрифт

Контент, сгенерированный ИИ, может содержать ошибки.

Изменение прав доступа

Чтобы настроить DVWA, нужно перейти в каталог /dvwa/config, затем проверяю содержимое каталога (рис. 3)

Изображение выглядит как текст, электроника, снимок экрана, программное обеспечение

Контент, сгенерированный ИИ, может содержать ошибки.

Перемещение по директориям

Создаем копию файла, используемого для настройки DVWA config.inc.php.dist с именем config.inc.php. Копируем файл, а не изменяем его, чтобы у нас был запасной вариант, если что-то пойдет не так (рис. 4)

Изображение выглядит как текст, снимок экрана, компьютер, Мультимедийное программное обеспечение

Контент, сгенерированный ИИ, может содержать ошибки.

Создание копии файла

Далее открываю файл в текстовом редакторе (рис. 5)

Изображение выглядит как текст, снимок экрана, программное обеспечение, компьютер

Контент, сгенерированный ИИ, может содержать ошибки.

Открытие файла в редакторе

Изменяю данные об имени пользователя и пароле (рис. 6)

Изображение выглядит как текст, снимок экрана, Шрифт, программное обеспечение

Контент, сгенерированный ИИ, может содержать ошибки.

Редактирование файл

По умолчанию в Kali Linux установлен mysql, поэтому можно его запустить без предварительного скачивания, далее выполняю проверку, запущен ли процесс (рис. 7)

Изображение выглядит как текст, снимок экрана, программное обеспечение, Шрифт

Контент, сгенерированный ИИ, может содержать ошибки.

Запуск mysql

Авторизируюсь в базе данных от имени пользователя root. Появляется командная строка с приглашением “MariaDB”, далее создаем в ней нового пользователя, используя учетные данные из файла config.inc.php (рис. 8)

Изображение выглядит как текст, снимок экрана, программное обеспечение, мультимедиа

Контент, сгенерированный ИИ, может содержать ошибки.

Авторизация в базе данных

Теперь нужно пользователю предоставить привилегии для работы с этой базой данных (рис. 9)

Изображение выглядит как текст, снимок экрана, компьютер, Мультимедийное программное обеспечение

Контент, сгенерированный ИИ, может содержать ошибки.

Изменение прав

Необходимо настроить сервер apache2, перехожу в соответствующую директорию (рис. 10)

Изображение выглядит как текст, снимок экрана, программное обеспечение, Мультимедийное программное обеспечение

Контент, сгенерированный ИИ, может содержать ошибки.

Перемещение между директориями

В файле php.ini нужно будет изменить один параметр, поэтому открываю файл в текстовом редакторе.

Открытие файла в текстовом редакторе

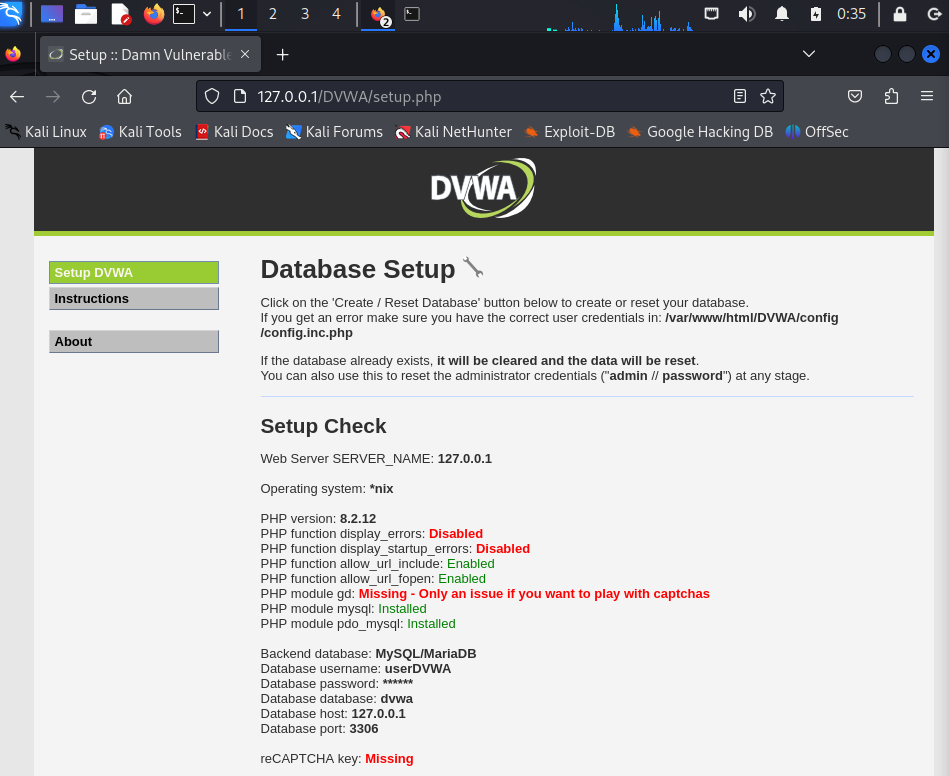
В файле параметры allow\_url\_fopen и allow\_url\_include должны быть поставлены как On.

Редактирование файла

Запускаем службу веб-сервера apache и проверяем, запущена ли служба.

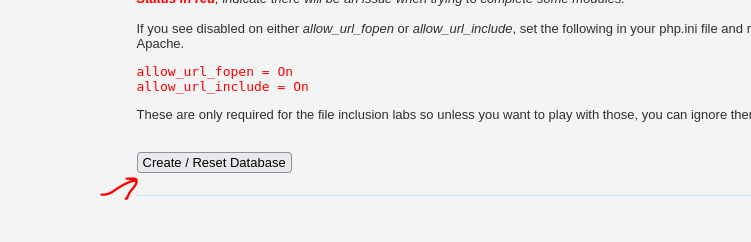
Запуск apche

Мы настроили DVWA, Apache и базу данных, поэтому открываем браузер и запускаем веб-приложение, введя 127.0.0/DVWA.



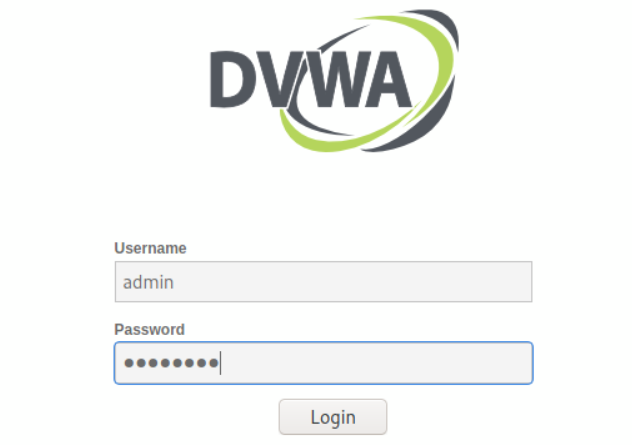
Запуск веб-приложения

Прокручиваем страницу вниз и нажимем на кнопку create\reset database (рис. 11)



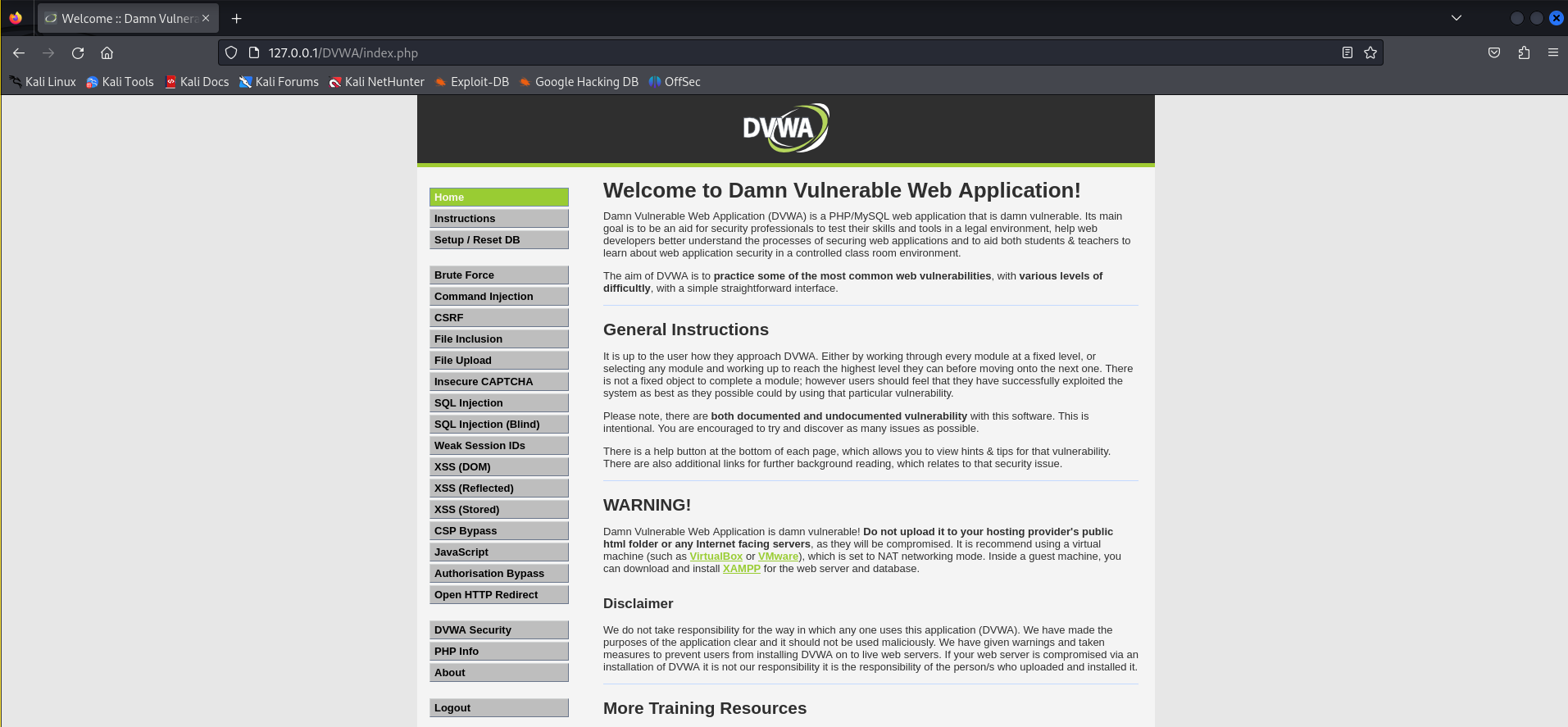
“Создание базы данных”

Авторизуюсь с помощью предложенных по умолчанию данных (рис. 12)



Авторизация

Оказываюсь на домшней странице веб-приложения, на этом установка окончена (рис. 13)



Домашняя страница DVWA

# 5 Выводы

Приобрела практические навыки по установке уязвимого веб-приложения DVWA.