Отчёт о выполнении. Индивидуальный проект. Этап 2

Установка DVWA

Щербак Маргарита Романовна, НПИбд-02-21

2024

Содержание

Список иллюстраций

Цель работы

Установить DVWA в гостевую систему к Kali Linux.

Теоретическое введение

Виртуализация является одним из ключевых инструментов в современной информационной безопасности и IT-инфраструктуре. Использование виртуальных машин (VM) позволяет создавать изолированные среды для работы, тестирования и изучения различных операционных систем и программного обеспечения без риска воздействия на основную систему. Одним из наиболее популярных дистрибутивов, используемых для задач информационной безопасности, является Kali Linux [1].

Kali Linux — это специализированный дистрибутив Linux, разработанный для проведения тестирования на проникновение и анализа информационной безопасности. Он содержит множество инструментов для проведения аудитов безопасности, обнаружения уязвимостей и эксплуатации различных системных слабостей [2].

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 фай-

лы 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.

Выполнение проекта

1. Запустила виртуальную машину и ввела пароль и логин для входа в систему (рис.1).

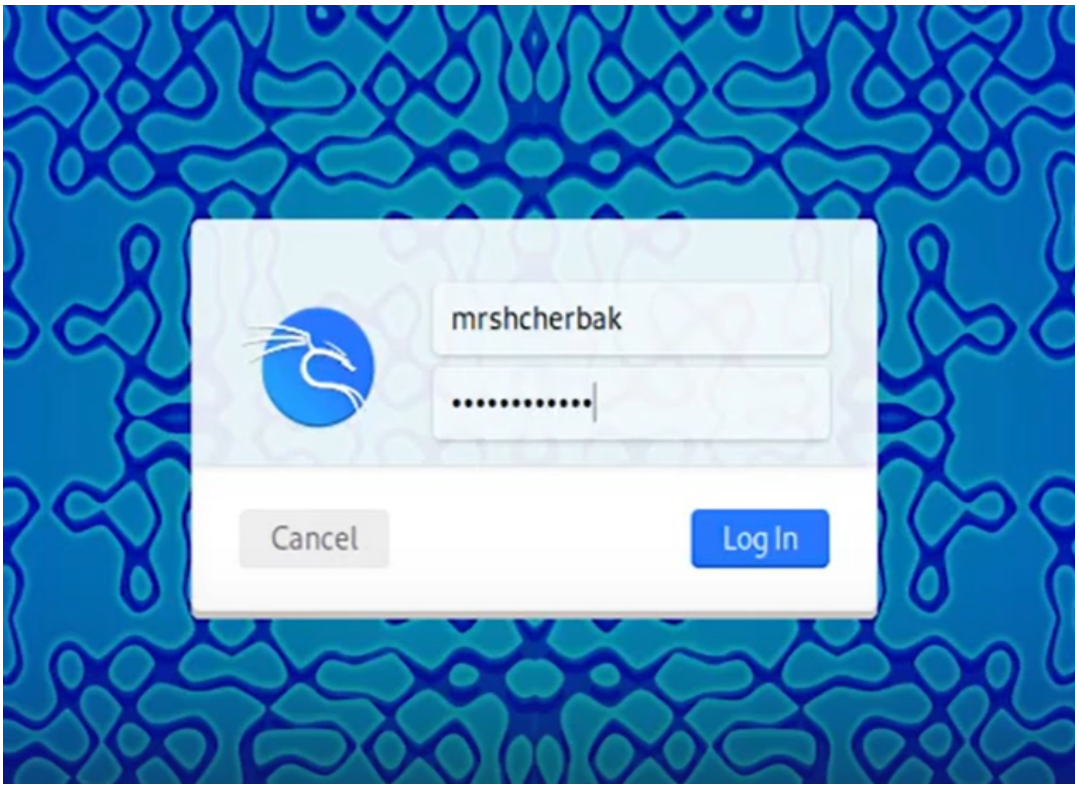

Рис. 1: Вход в Kali Linux

2. Открыла терминал (рис.2).

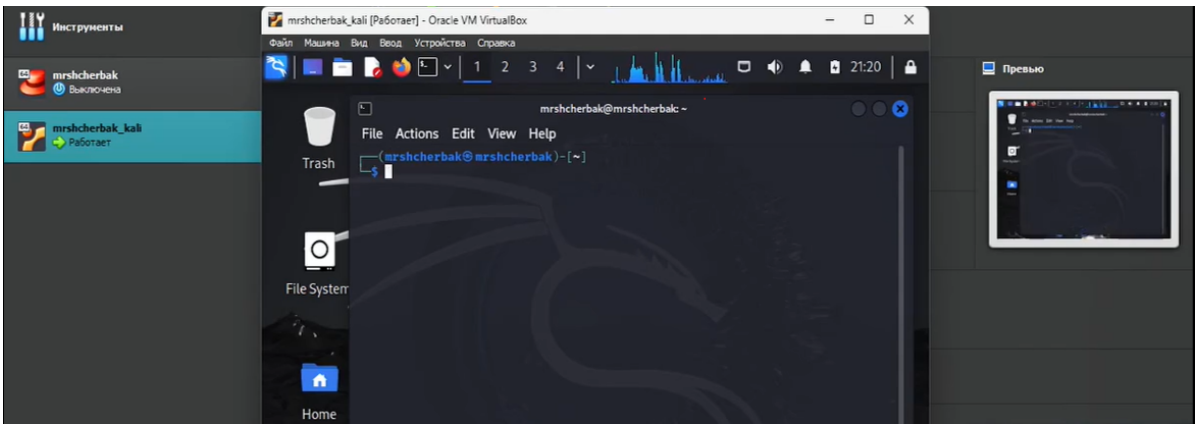

Рис. 2: Работа в терминале

3. Перешла в папку /var/www/html и от имени администратора клонировала репозиторий git hub. Изменила права доступа к папке установки (рис.3).

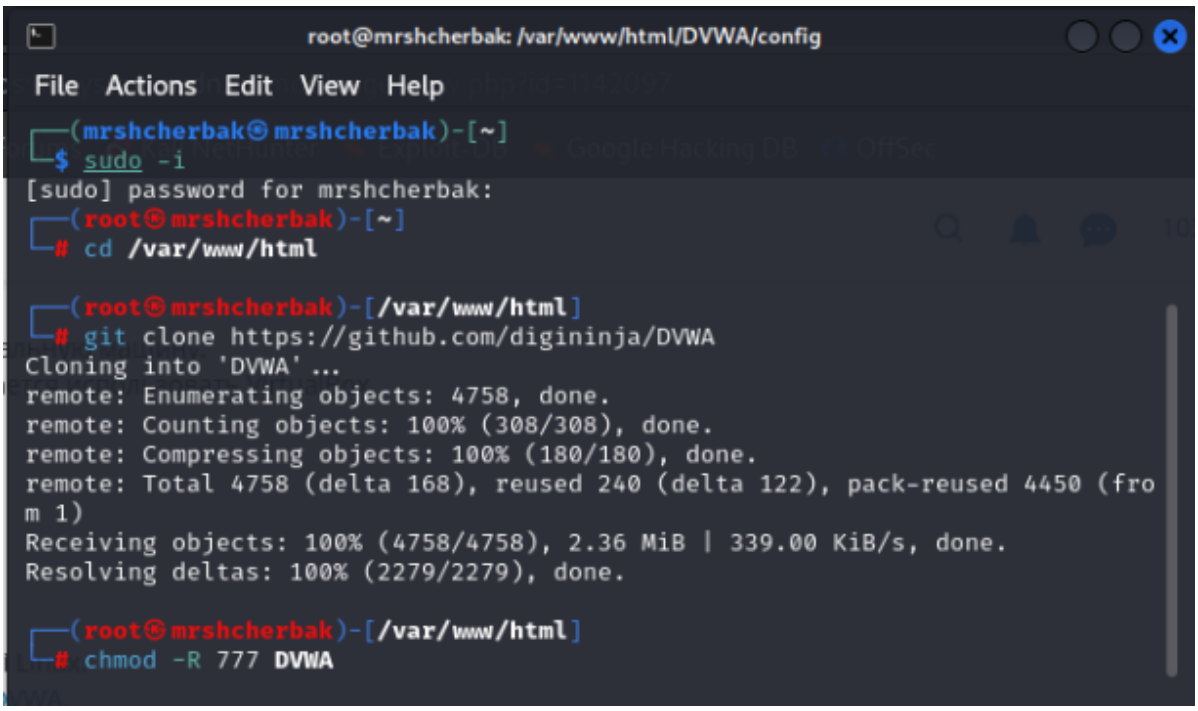

Рис. 3: Клонирование необходимого репозитория git hub

4. Перешла к файлу конфигурации в каталоге установки, скопировала файл конфигурации и переименовала его. Установила mariadb (рис.4). Содержимое файла

config.inc.php представлено на рис.5.

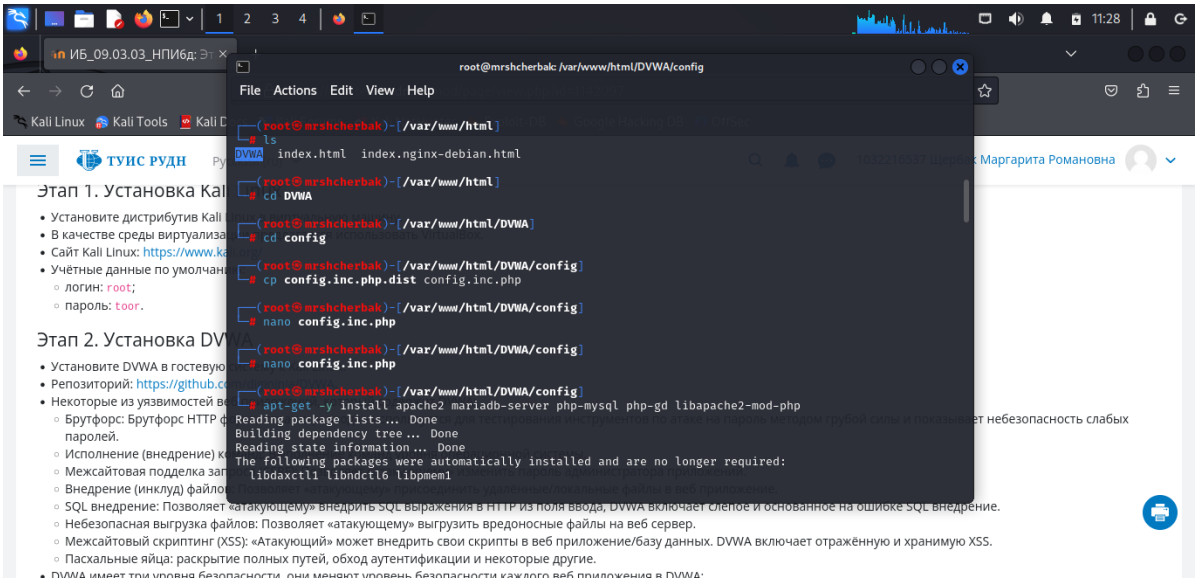

Рис. 4: Необходимая настройка и установка mariadb

Рис. 5: Файл config.inc.php

5. Запустила базу данных и вошла в нее (рис.6).

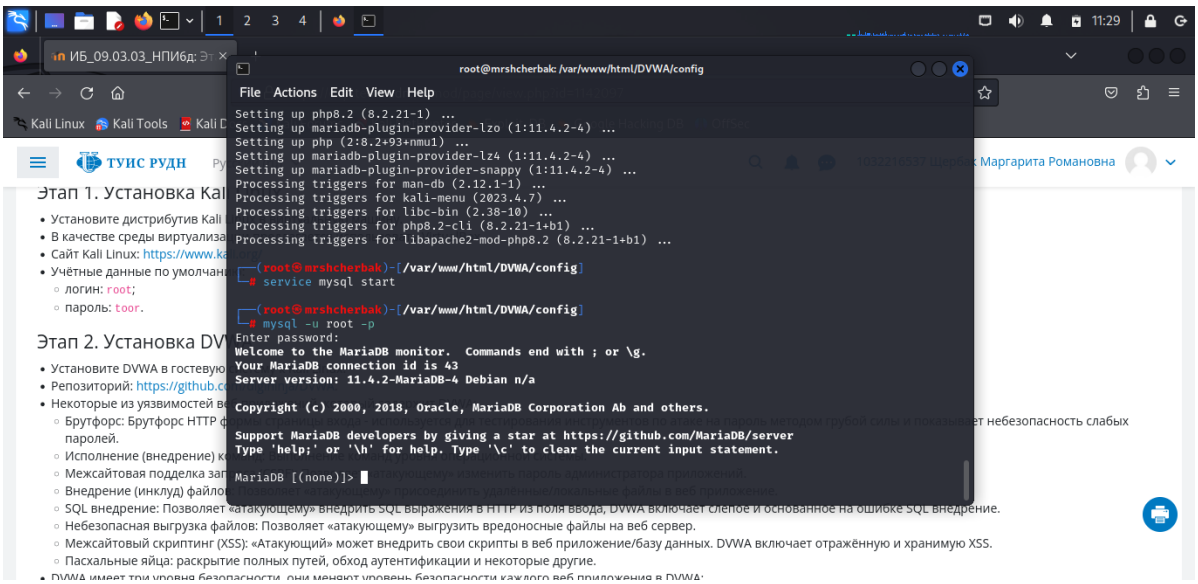

Рис. 6: Запуск mariadb и вход в базу данных

6. Создала пользователя базы данных. Нужно использовать те же имя пользователя и пароль, которые использовались в файле конфигурации (рис.7).

Рис. 7: Создание пользоателя

7. Открыла для редактирования файл php.ini, чтобы включить следующие параметры: allow_url_fopen и allow_url_include (рис.8).

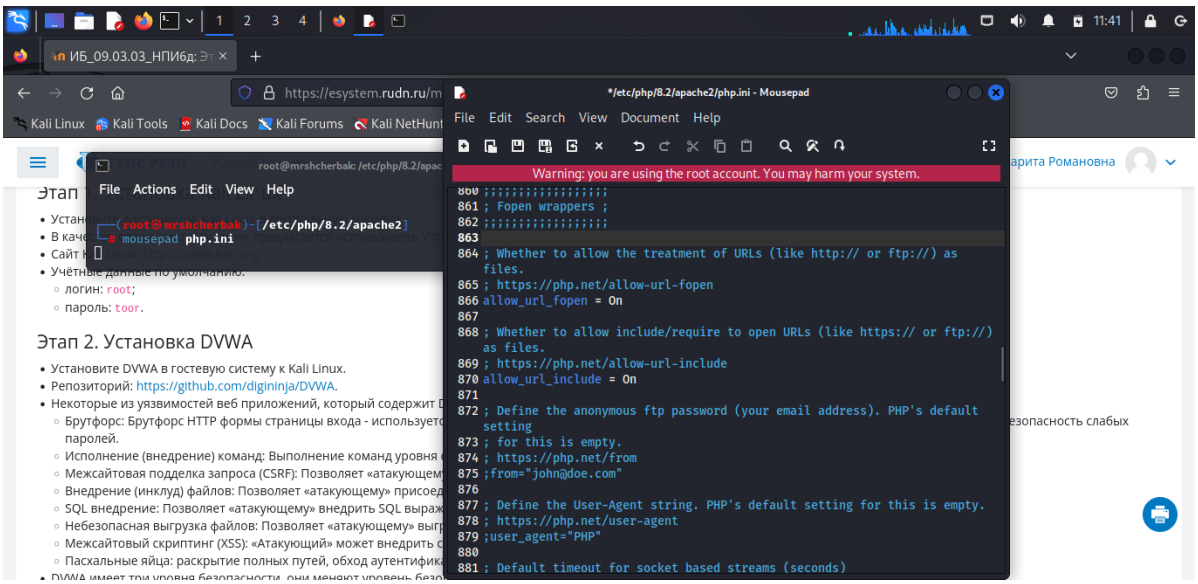

Рис. 8: Настройка сервера Apache

8. Запустила сервер Apache и открыла DVWA в браузере для проверки работы сервера (рис.9).

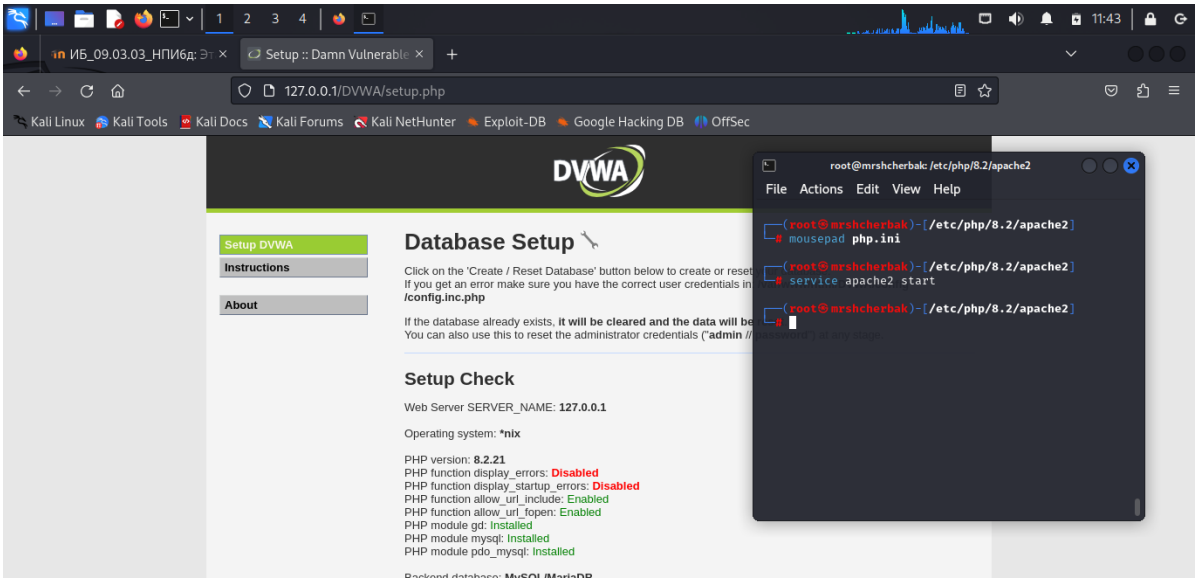

Рис. 9: Запуск сервера Apache и проверка работы

Вывод

Таким образом, в ходе 2 этапа индивидуального проекта я установила DVWA в гостевую систему к Kali Linux.

Библиография

1. Документация по Virtual Box: https://www.virtualbox.org/wiki/Documentation
2. Документация по этапам индивидульного проекта: Парасрам Шива, Замм Алекс, Хериянто Теди, Али Шакил, Буду Дамиан, Йохансен Джерард, Аллен Ли П18 Kali Linux. Тестирование на проникновение и безопасность. — СПб.: Питер, 2020. — 448 с.: ил. — (Серия «Для профессионалов»). ISBN 978-5-4461-1252-4