Индивидуальный проект 2

Информационная безопасность

Волчок Кристина Александровна НПМбд-02-21

Содержание

# 1 Цель работы

Установить Damn Vulnerable Web Application (DVWA) в гостевую систему Kali Linux для изучения и практики в области безопасности веб-приложений.

# 2 Задание

* Установить DVWA в гостевую систему Kali Linux.
* Использовать репозиторий: https://github.com/digininja/DVWA.
* Ознакомиться с основными уязвимостями, которые содержит DVWA.
* Понять различия между уровнями безопасности, предлагаемыми DVWA.

# 3 Теоретическое введение

**Теоретическое введение**

**DVWA (Damn Vulnerable Web Application)** — это уязвимое веб-приложение, специально созданное для обучения и практики в области веб-безопасности. Оно содержит преднамеренные уязвимости для отработки техник их обнаружения и эксплуатации.

**Основные уязвимости DVWA:**

* **Брутфорс**: атака методом перебора паролей через форму входа.
* **Исполнение команд**: возможность выполнять команды операционной системы через веб-интерфейс.
* **CSRF (Межсайтовая подделка запроса)**: позволяет изменить пароль администратора без его ведома.
* **Внедрение файлов**: подключение удаленных или локальных файлов в приложение.
* **SQL-инъекция**: внедрение SQL-запросов через поля ввода.
* **Небезопасная загрузка файлов**: загрузка вредоносных файлов на сервер.
* **XSS (Межсайтовый скриптинг)**: внедрение скриптов в приложение или базу данных.
* **Пасхальные яйца**: скрытые уязвимости, такие как раскрытие полных путей и обход аутентификации.

**Уровни безопасности DVWA:**

* **Низкий**: полностью уязвимый уровень без какой-либо защиты.
* **Средний**: попытки защитить приложение, которые оказались неэффективными.
* **Высокий**: уязвимости есть, но их эксплуатация затруднена.
* **Невозможный**: все уязвимости устранены; используется для сравнения с уязвимыми уровнями.

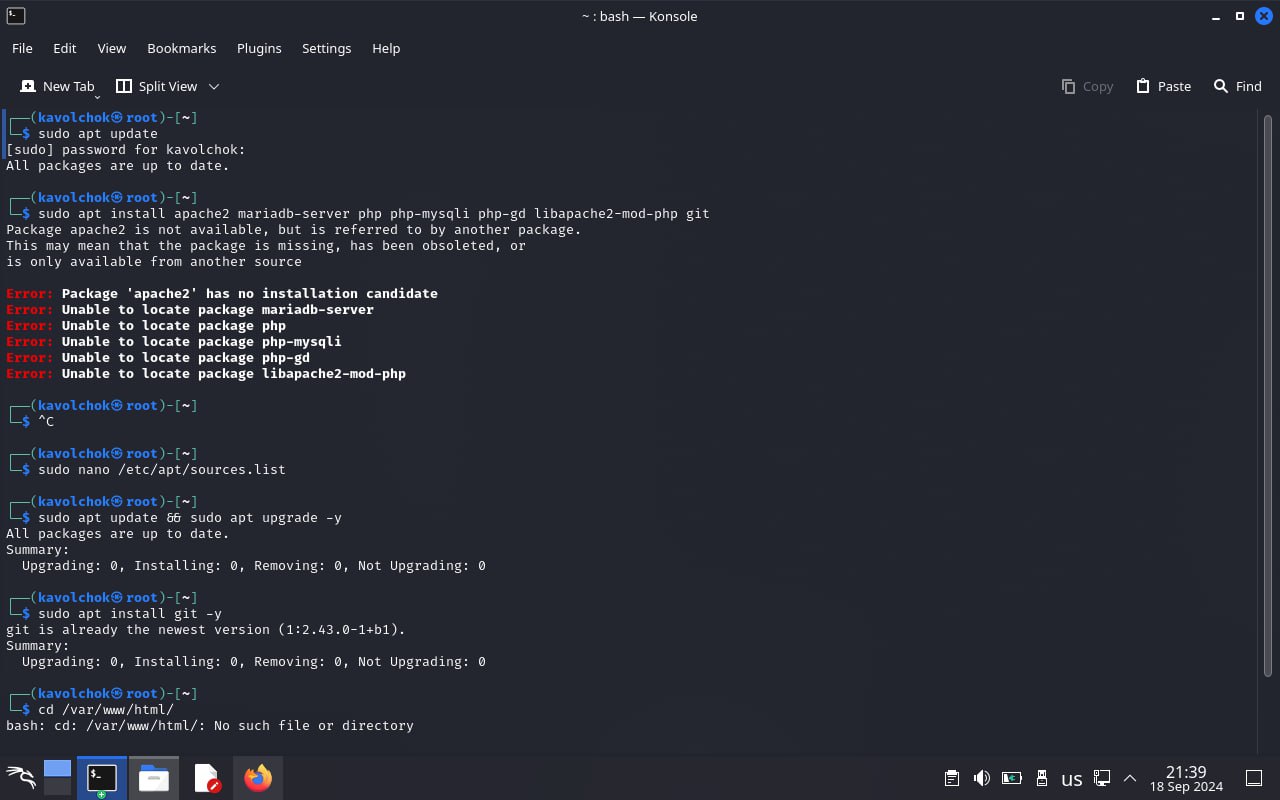
# 4 Выполнение лабораторной работы

**Процесс установки DVWA**

**Обновление системы:**

Для начала я обновляю систему с помощью следующей команды:

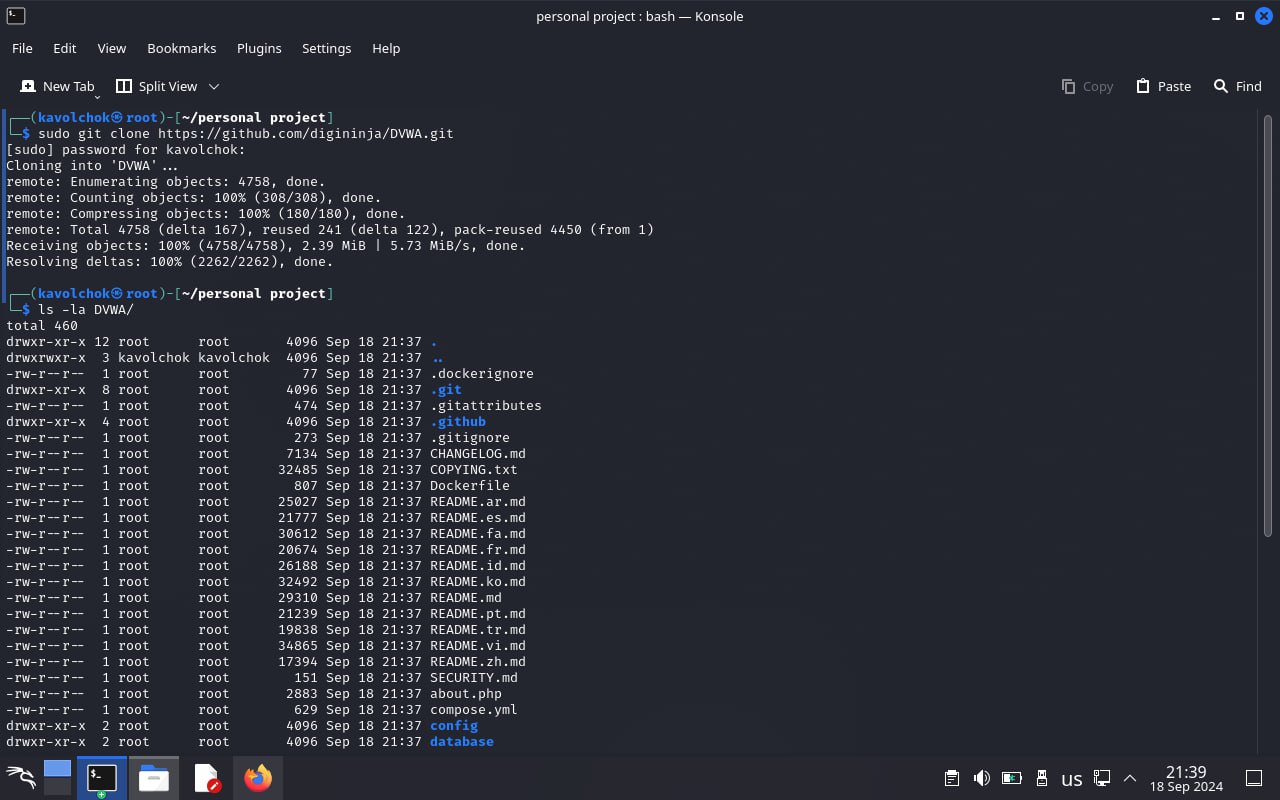
(sudo apt update && sudo apt upgrade -y)



Установка DVWA

**Установка необходимых пакетов:**

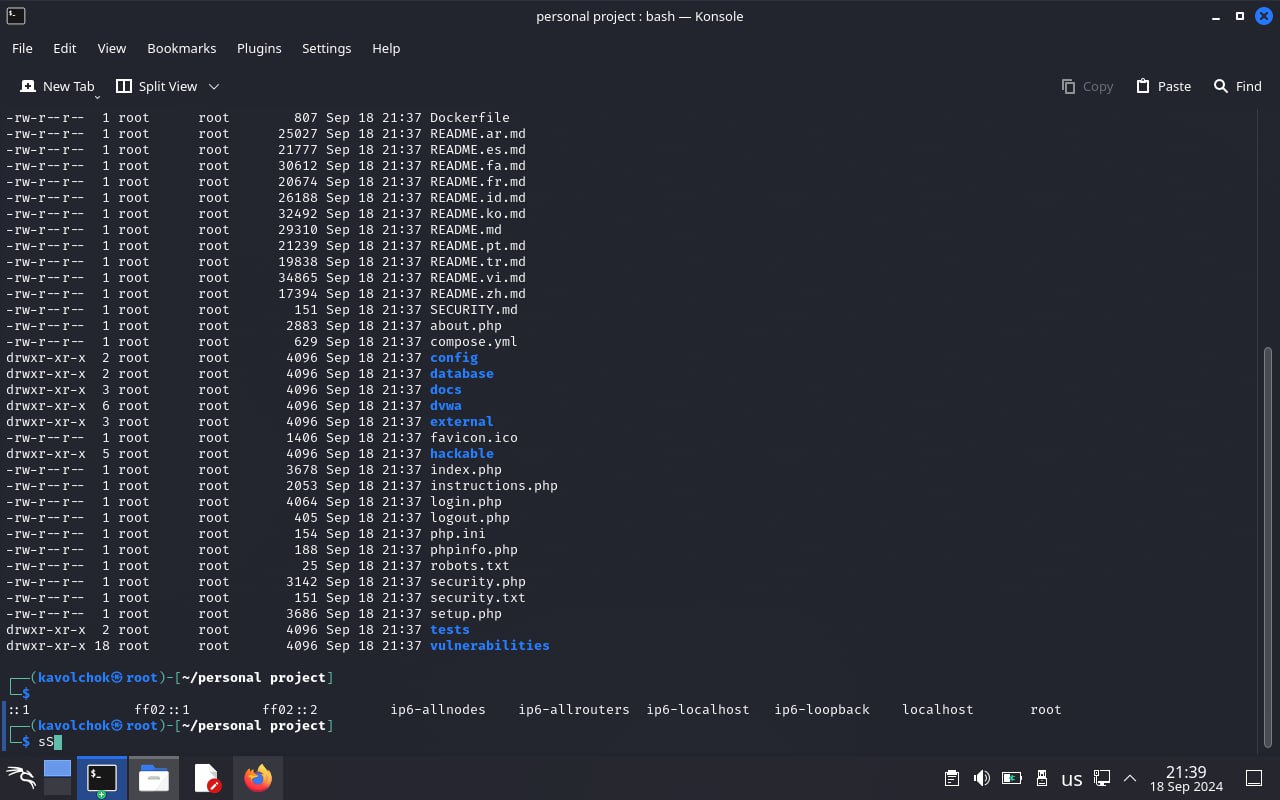
После обновления системы я устанавливаю необходимые пакеты:



Установка необходимых пакетов

**Запуск и настройка служб:**

Затем я запускаю и настраиваю службы Apache и MariaDB для их автоматического запуска при старте системы:



Запуск и настройка служб

**Настройка базы данных:**

После того как службы запущены, я перехожу к настройке базы данных:

(sudo mysql\_secure\_installation)  
(sudo mysql -u root -p)

В MySQL я ввожу следующие команды для создания базы данных и пользователя:

```sql CREATE DATABASE dvwa; CREATE USER ‘dvwauser’@‘localhost’ IDENTIFIED BY ‘password’; GRANT ALL PRIVILEGES ON dvwa.\* TO ‘dvwauser’@‘localhost’; FLUSH PRIVILEGES; EXIT;

\*\* Клонирование репозитория DVWA:\*\*

Теперь я клонирую репозиторий DVWA в директорию веб-сервера:

(cd /var/www/html/)  
(sudo git clone https://github.com/digininja/DVWA.git)

**Настройка прав доступа:**

Я убеждаюсь, что права доступа к директории настроены корректно:

(sudo chown -R www-data:www-data /var/www/html/DVWA/)  
(sudo chmod -R 755 /var/www/html/DVWA/)

После этого я перехожу в папку конфигурации и настраиваю файл:

(cd /var/www/html/DVWA/config/)  
(sudo cp config.inc.php.dist config.inc.php)  
(sudo nano config.inc.php)

**Завершение установки через браузер:**

Я открываю браузер и перехожу по адресу:

http://localhost/DVWA/setup.php

Нажимаю кнопку “Create / Reset Database”.

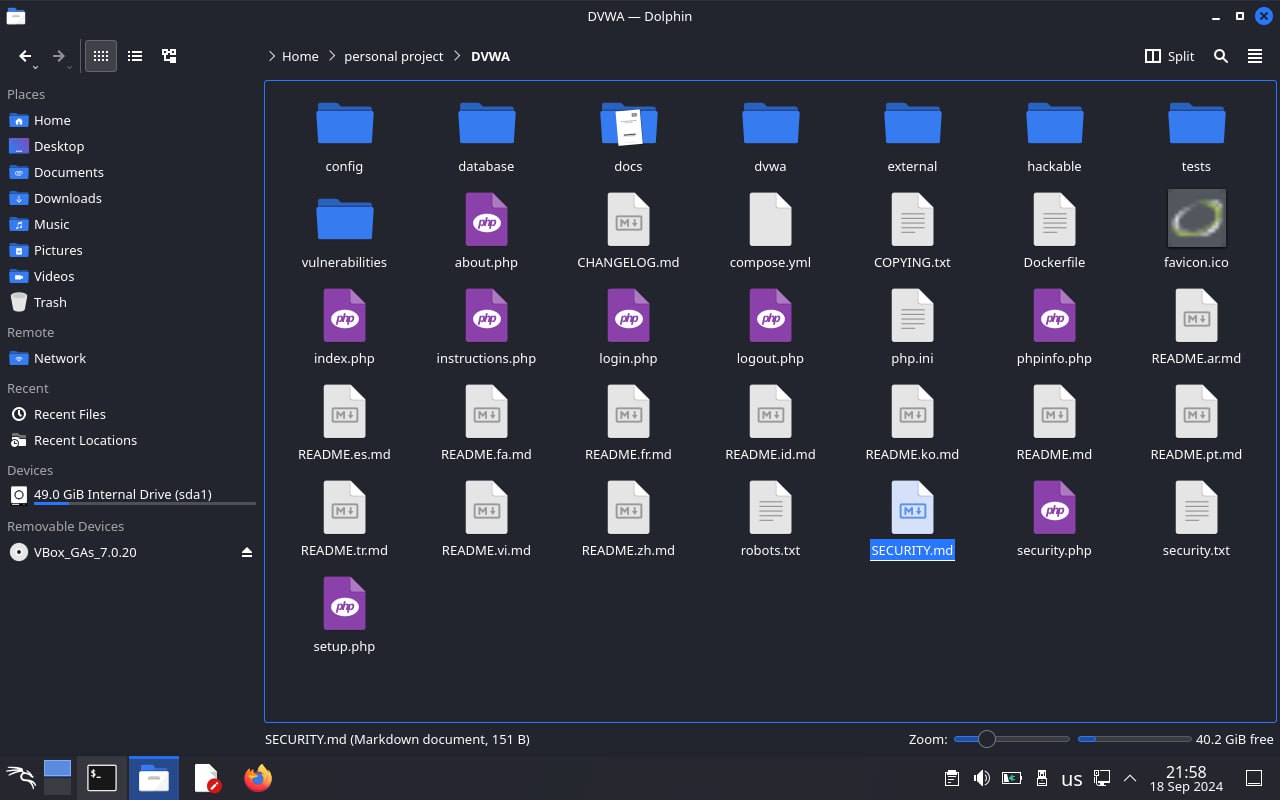
**Вход в DVWA:**

Перехожу на страницу входа:

http://localhost/DVWA/login.php

Ввожу следующие данные для входа:

* Имя пользователя: admin
* Пароль: password



Настроенная DVWA

# 5 Выводы

В результате выполнения задания была успешно установлена DVWA в гостевую систему Kali Linux. Это позволяет получить практический опыт в области веб-безопасности, изучая и эксплуатируя различные уязвимости. Работа с DVWA способствует повышению квалификации и пониманию методов защиты веб-приложений.