Индивидуальный проект

Этап 2

Прокопьева Марина Евгеньевна

Содержание

Список иллюстраций

Список таблиц

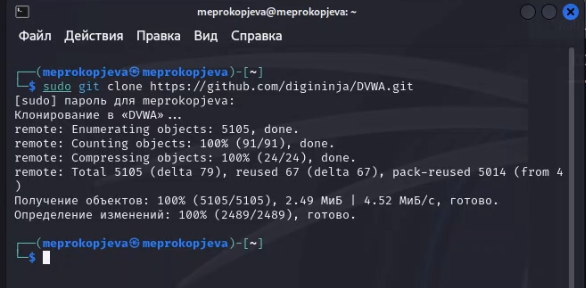
# 1 2 Этап

Этап 2. Установка DVWA

Установите DVWA в гостевую систему к Kali Linux.  
Репозиторий: https://github.com/digininja/DVWA.  
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 Выполнение этапы

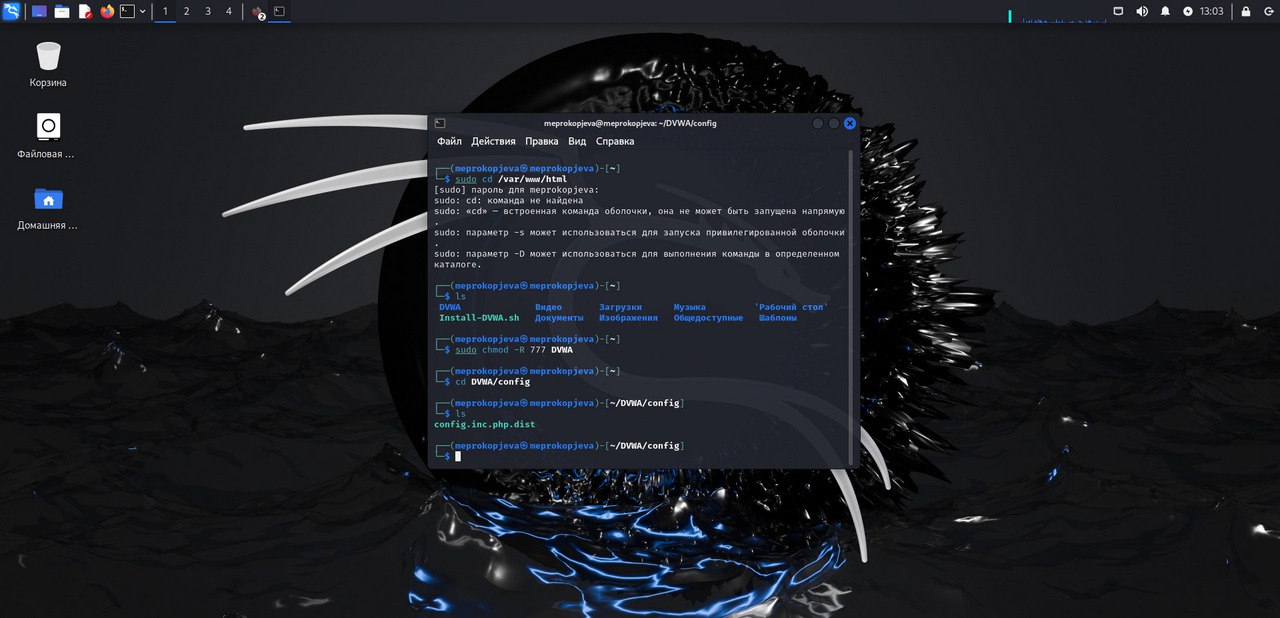
Настройка DVWA происходит на нашем локальном хосте, поэтому нужно перейти в директорию /var/www/html. Затем клонирую нужный репозиторий GitHub (рис. 1).



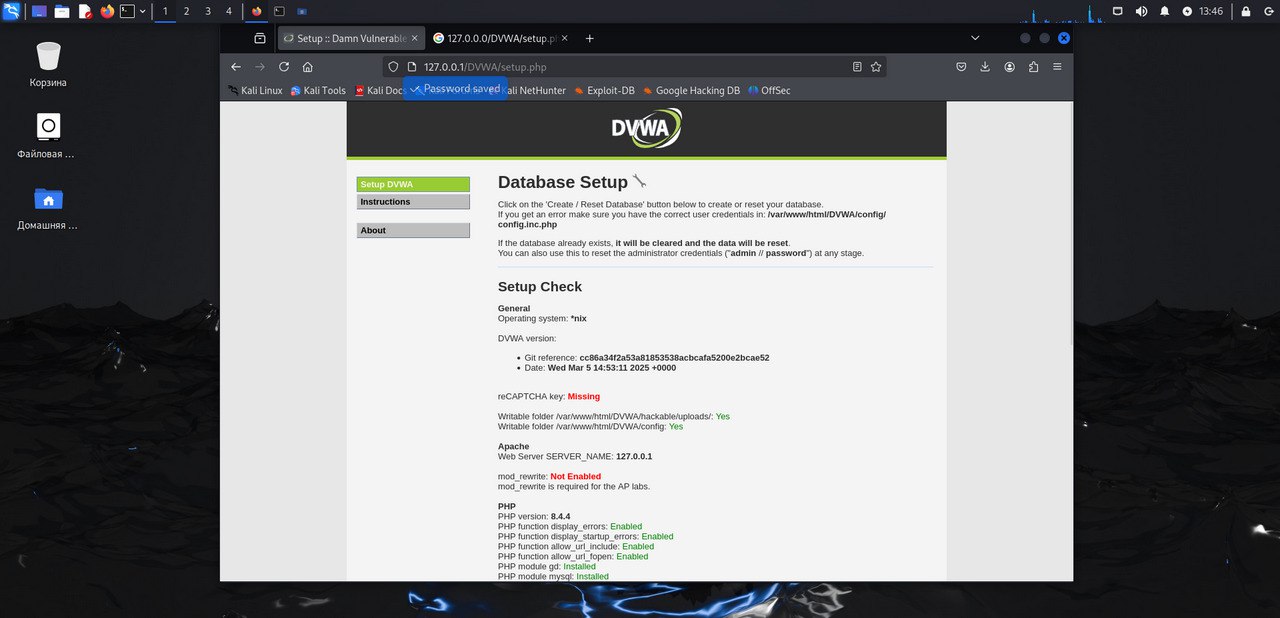
Проверяю, что файлы склонировались правильно, далее повышаю права доступа к этой папке до 777

Чтобы настроить DVWA, нужно перейти в каталог /dvwa/config, затем проверяю содержимое каталога

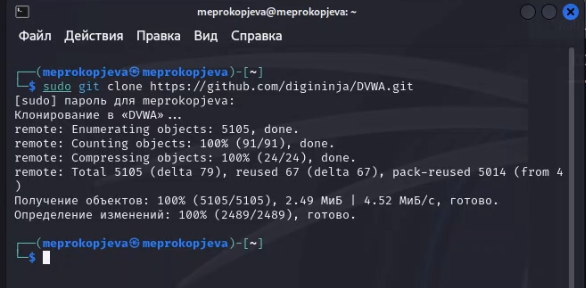
Создаем копию файла, используемого для настройки DVWA config.inc.php.dist с именем config.inc.php. Копируем файл, а не изменяем его, чтобы у нас был запасной вариант, если что-то пойдет не так



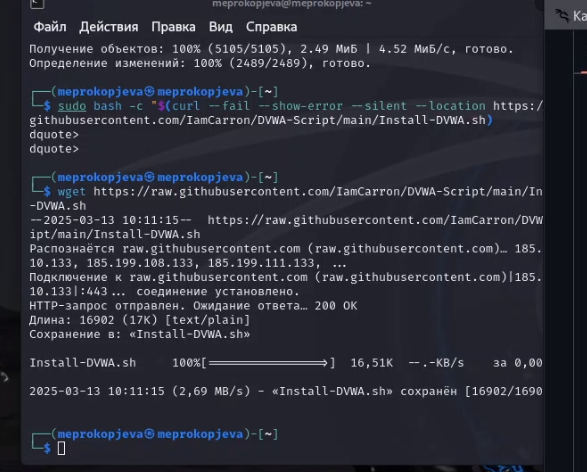
Далее открываю файл в текстовом редакторе



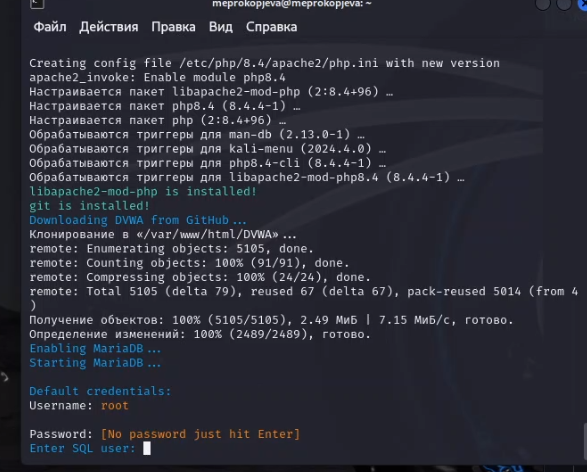
Изменяю данные об имени пользователя и пароле

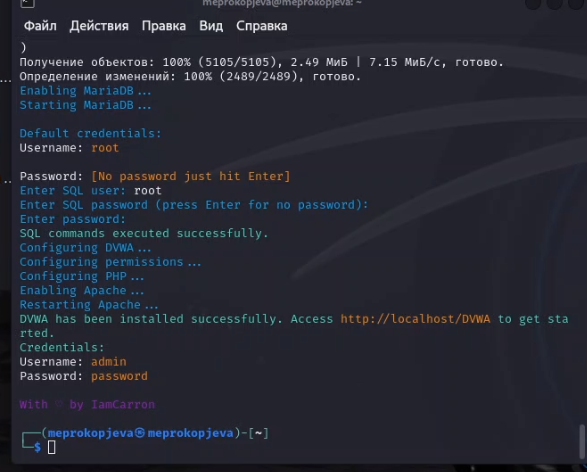


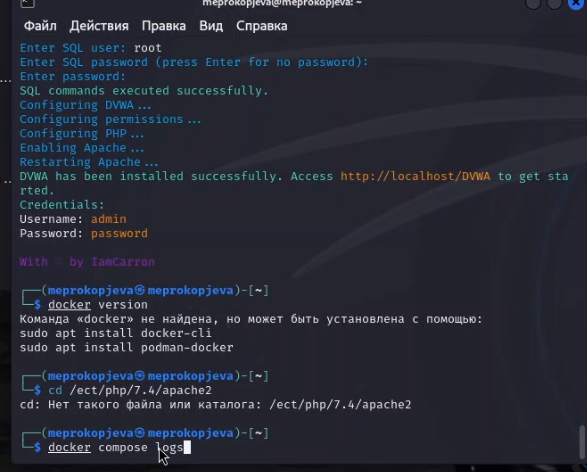
По умолчанию в Kali Linux установлен mysql, поэтому можно его запустить без предварительного скачивания, далее выполняю проверку, запущен ли процесс



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

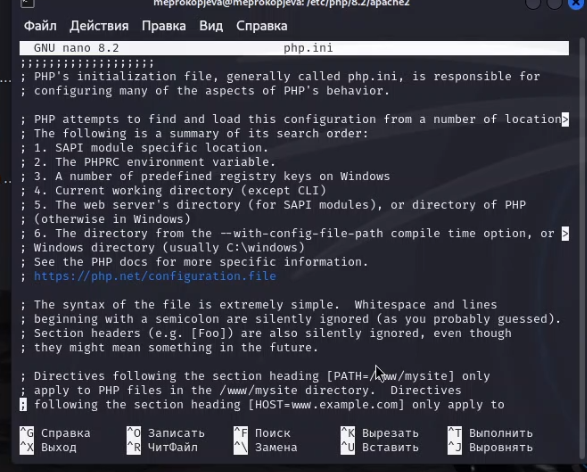


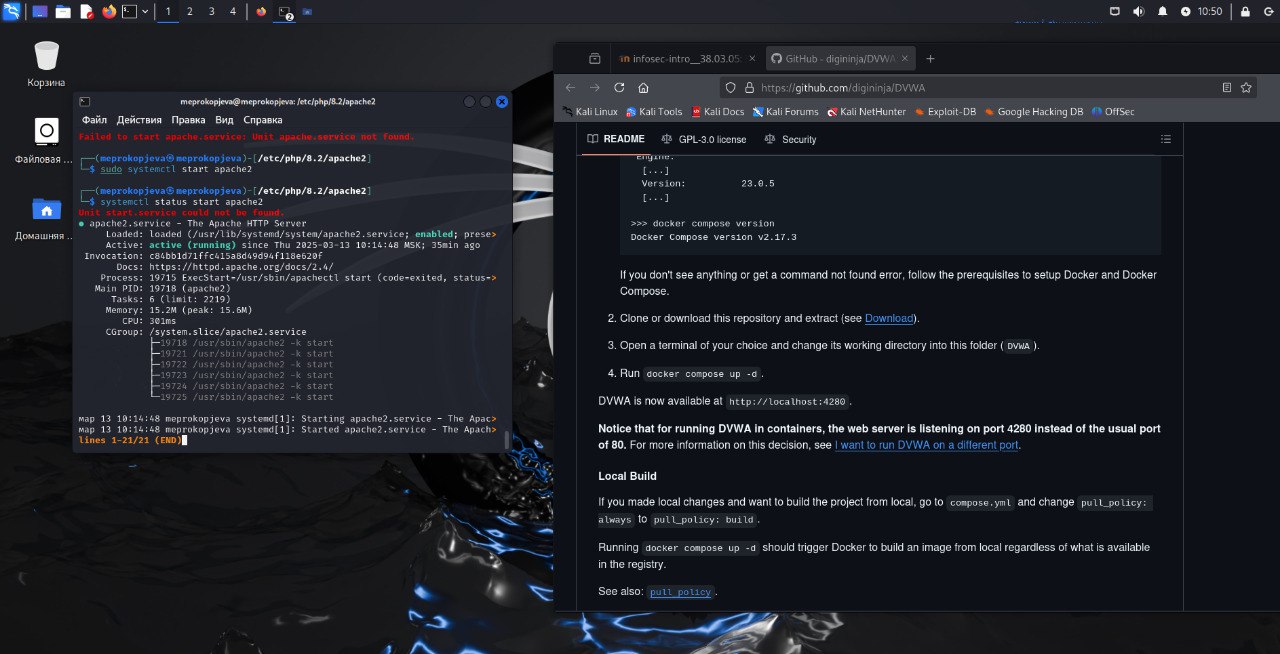




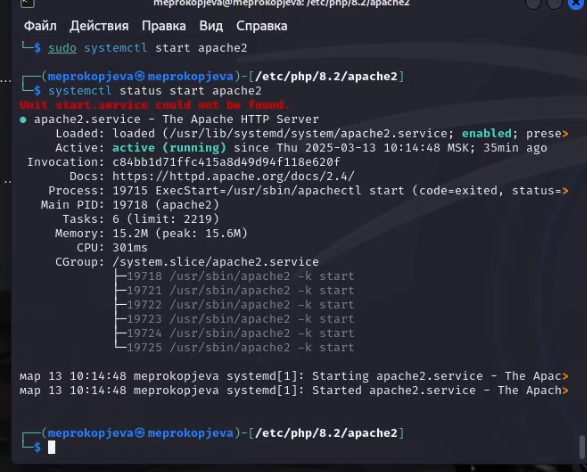
Теперь нужно пользователю предоставить привилегии для работы с этой базой данных

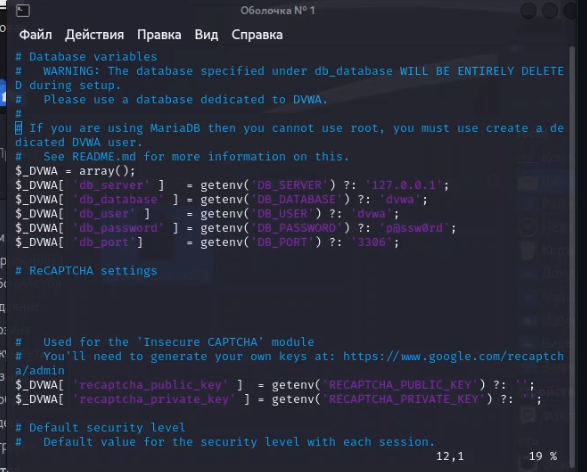
Необходимо настроить сервер apache2, перехожу в соответствующую директорию

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



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



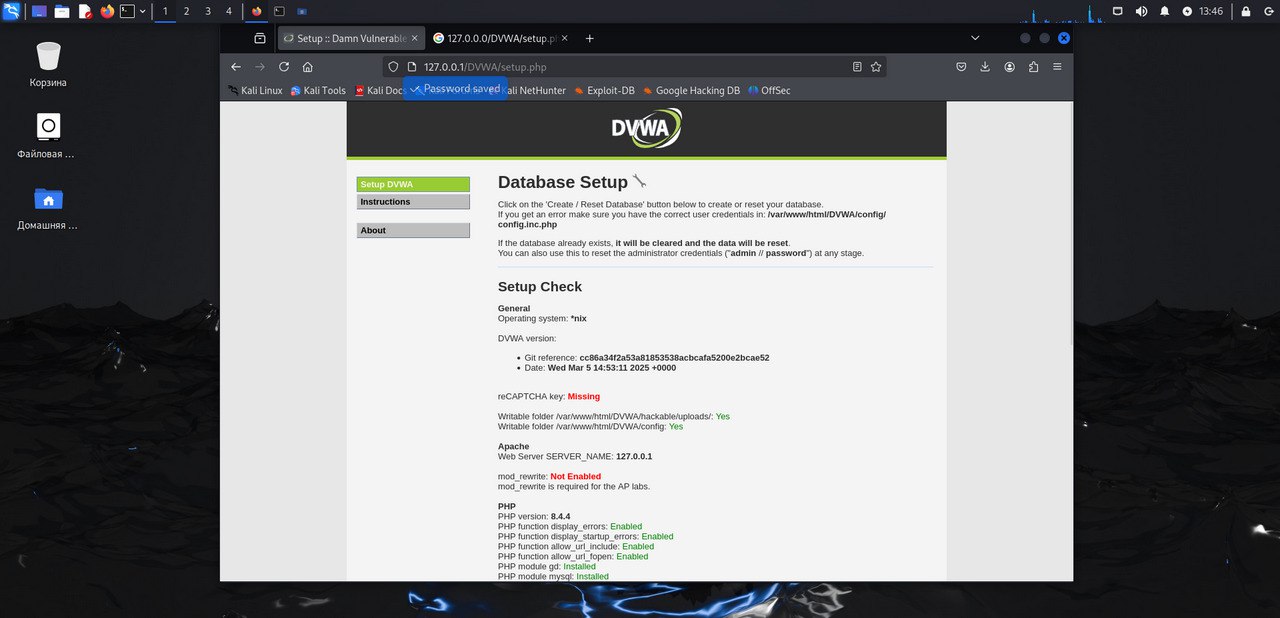


Запускаем службу веб-сервера apache и проверяем, запущена ли служба

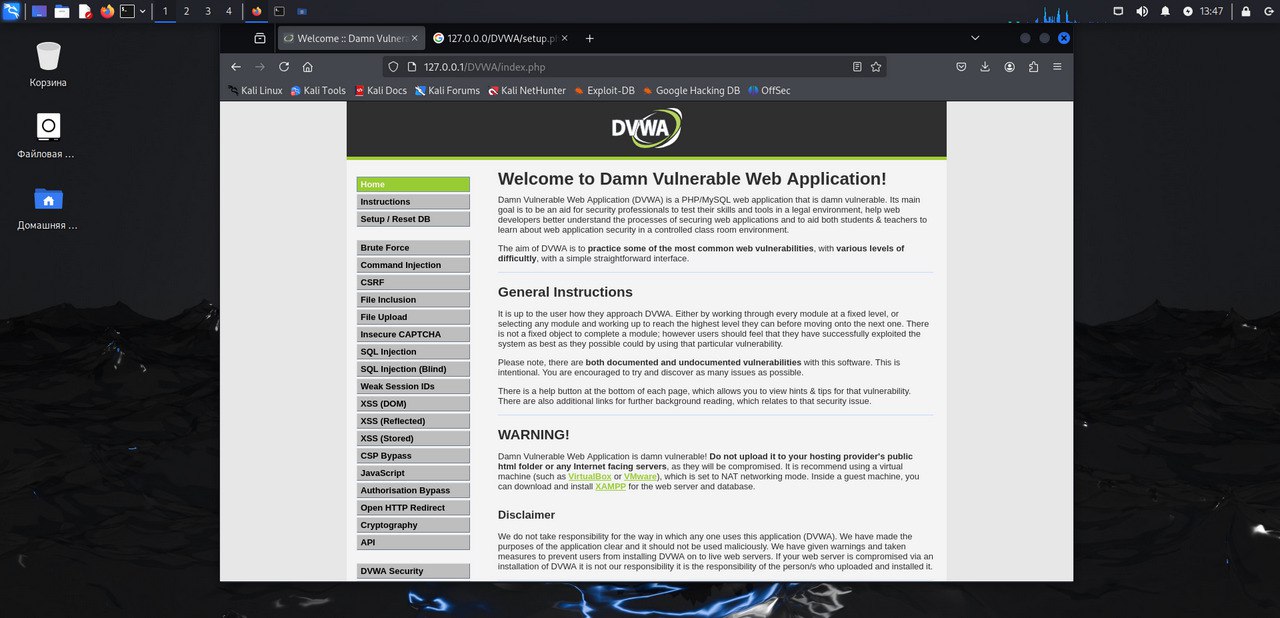
Мы настроили DVWA, Apache и базу данных, поэтому открываем браузер и запускаем веб-приложение, введя 127.0.0/DVWA

Прокручиваем страницу вниз и нажимем на кнопку create\reset database

Авторизуюсь с помощью предложенных по умолчанию данных



Оказываюсь на домшней странице веб-приложения, на этом установка окончена



# 3 Выводы

Приобрела практические навыки по установке уязвимого веб-приложения DVWA.