Отчет по первому этапу индивидуального проекта

Информационная безопасность

Кармацкий Никита Сергеевич

Содержание

# 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.

# 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).

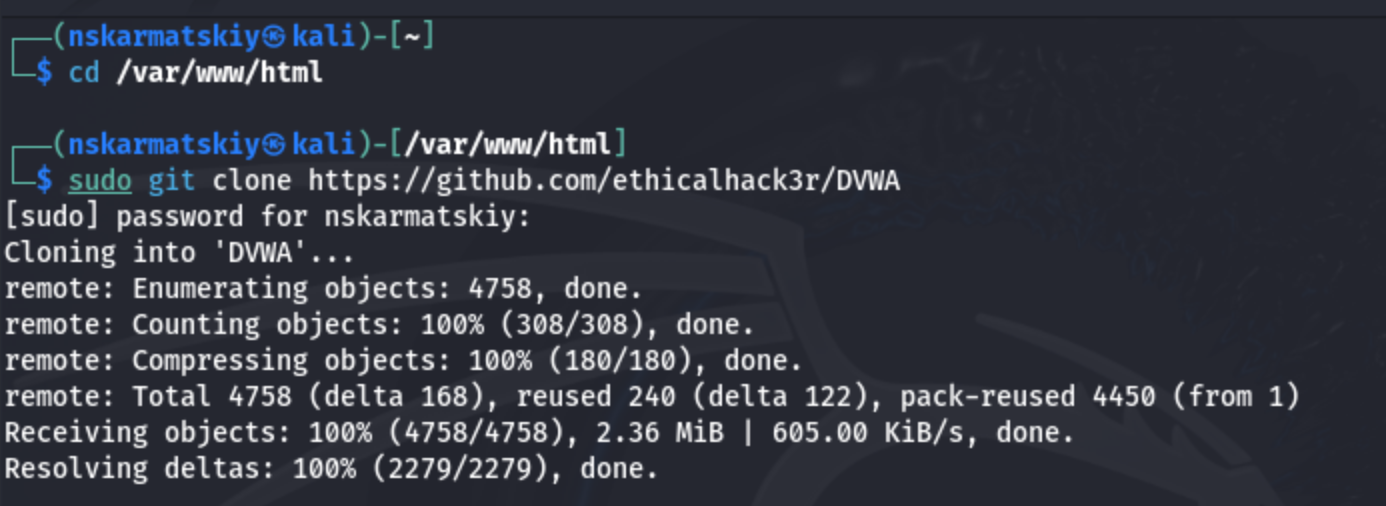


Рис. 1: Клонирования репозитория

Проверяем, что файлы скопировалтсб правильно, далее повышаем права доступа к этому каталогу до 777 (рис. 2).

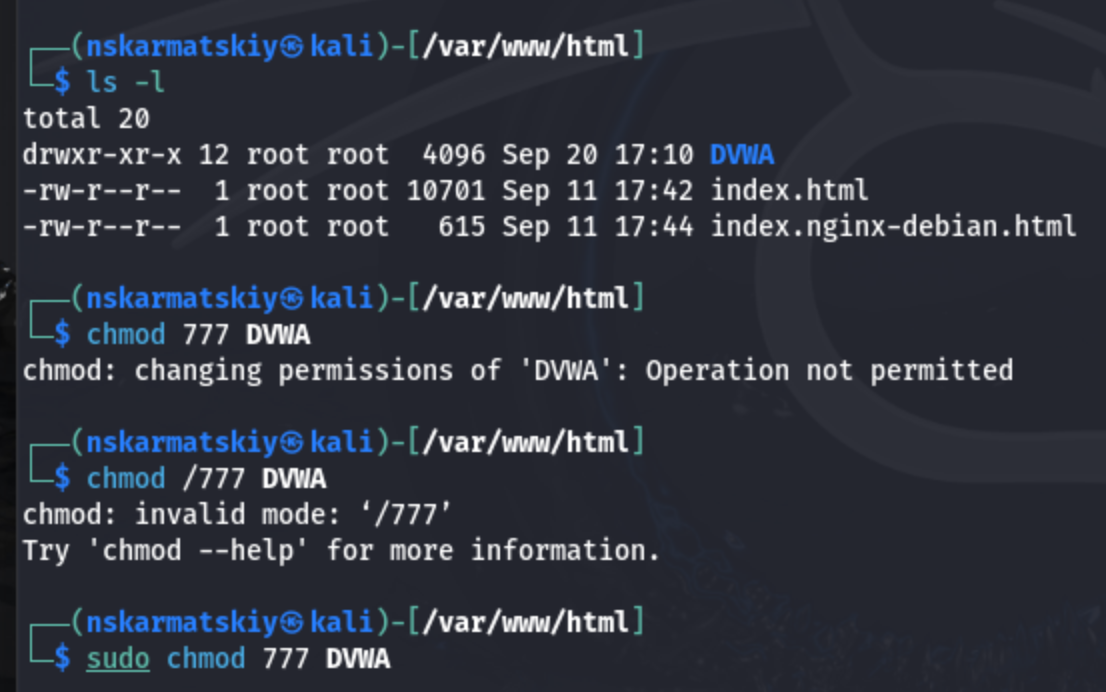


Рис. 2: Изменение прав доступа

Чтобы настроить DVWA, нужно перейти в каталог /dvwa/config, затем нужно отредактировать файл config/config.inc.php, который мы получаем копируя шаблон (рис. 3).

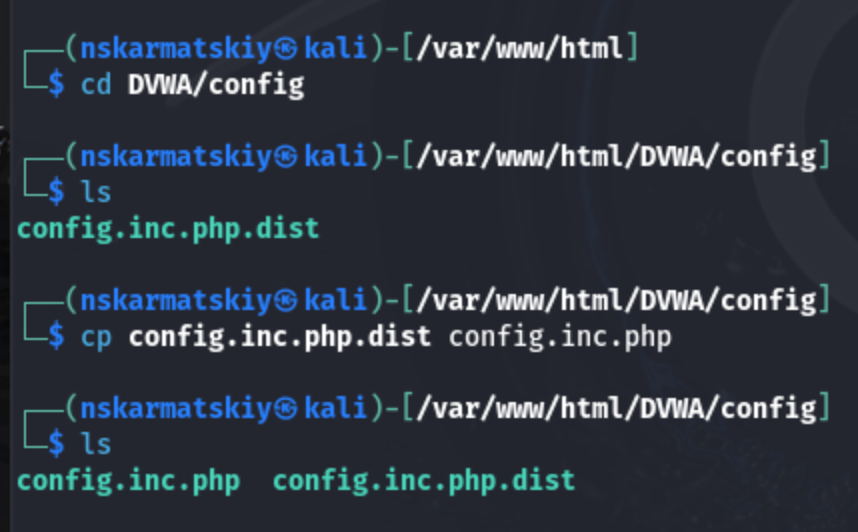


Рис. 3: Создание копии файла

Открываем файл на редактирование и меняем имя пользователя и пароль (рис. 4).

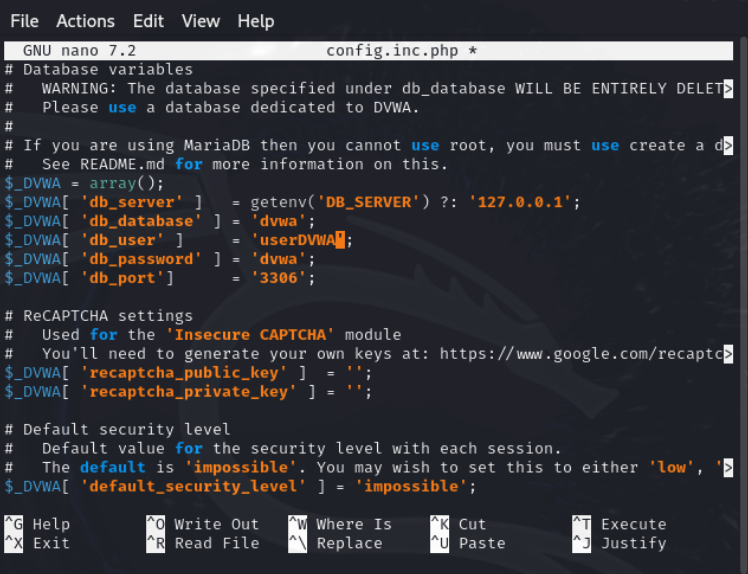


Рис. 4: Редактирование файла

Запускаем сервис sql и проверяем, что он запущен. (рис. 5).

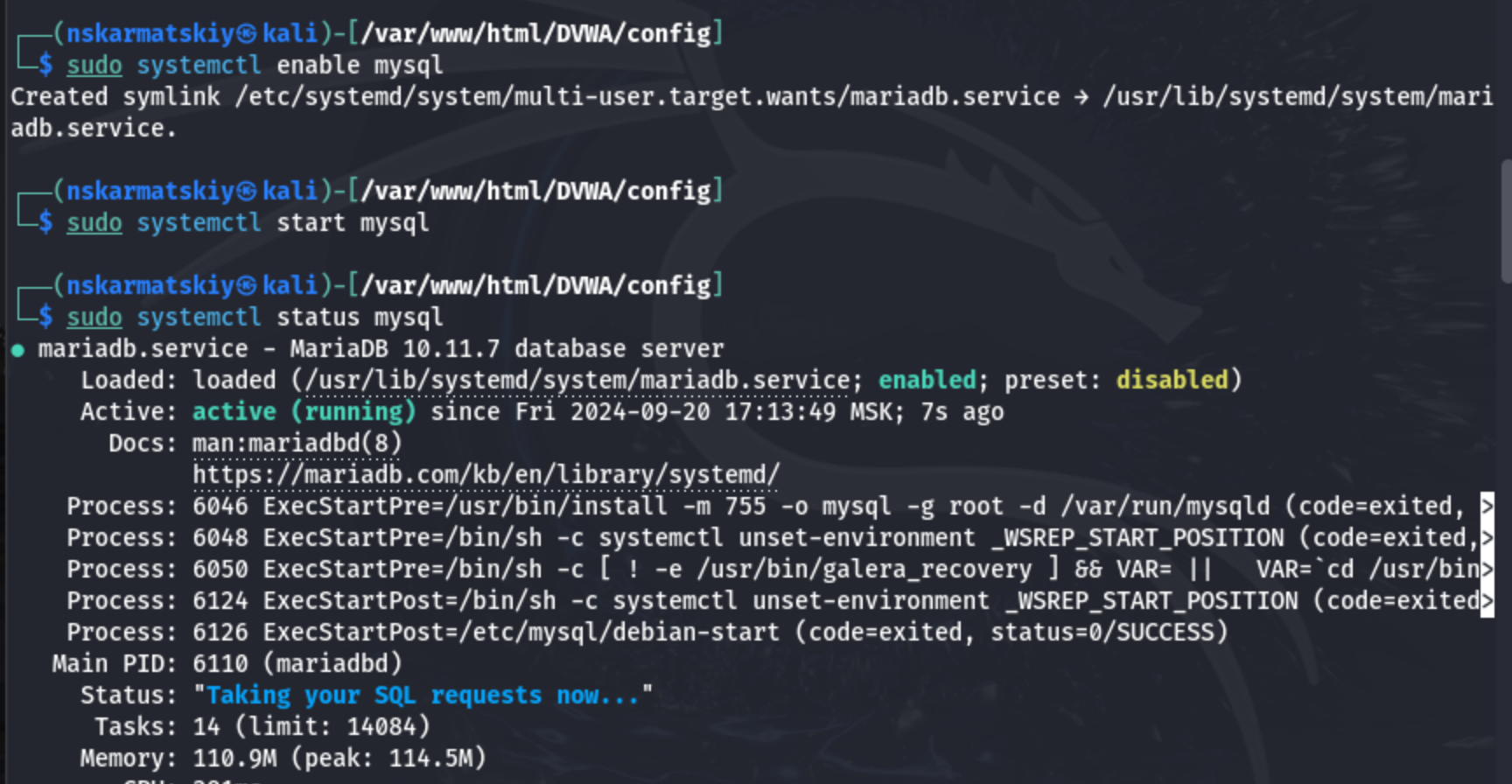


Рис. 5: Редактирование файла

Авторизируемся в базе данных MariaDB под именем пользователя, которого мы задали в файле config.inc.php, а так же представляем привелегии для работы с этой базой данных (рис. 6).

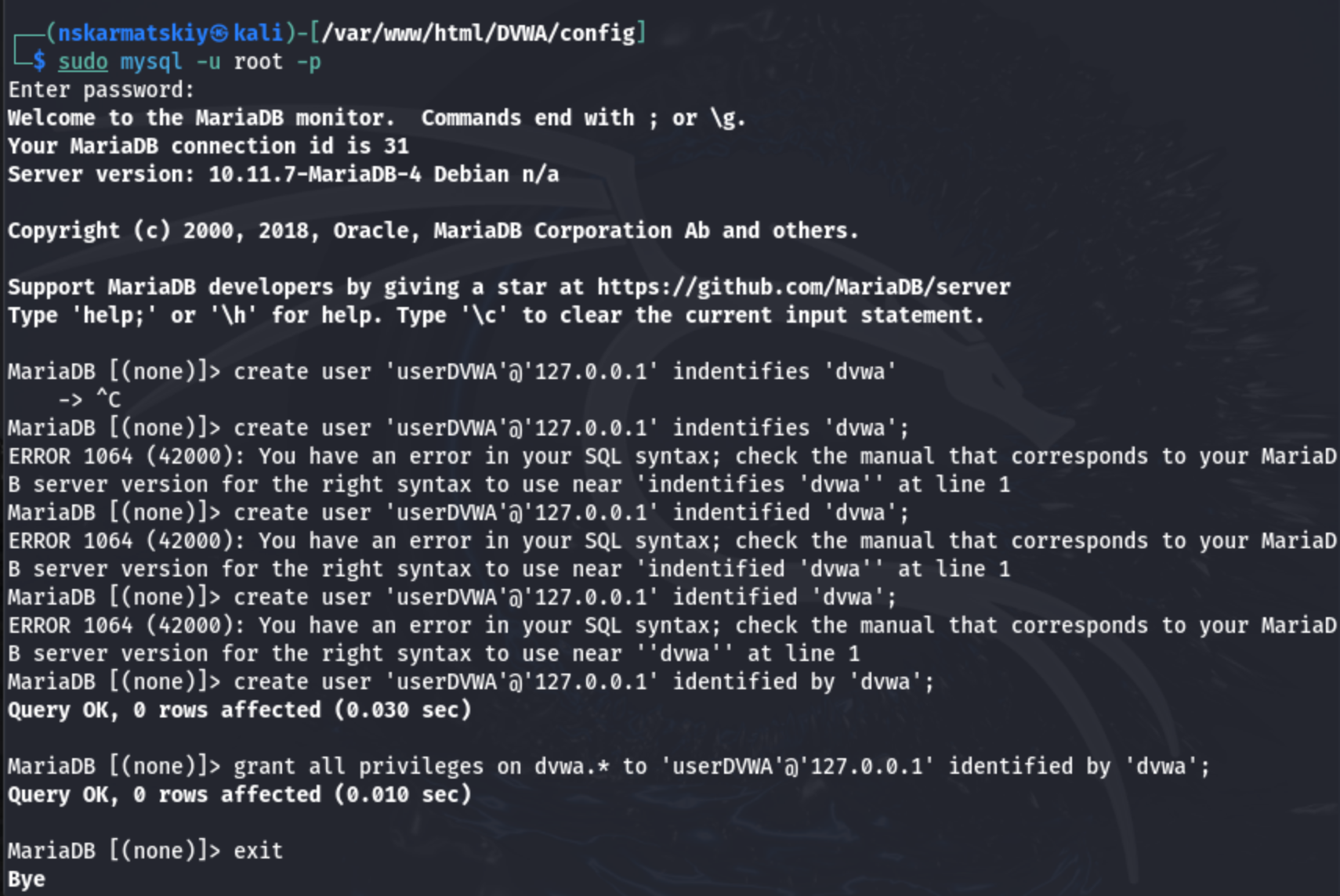


Рис. 6: Настройка в базе данных

Далее настраиваем серев apache2, для этого переходим в каталог с настройками(рис. 7).

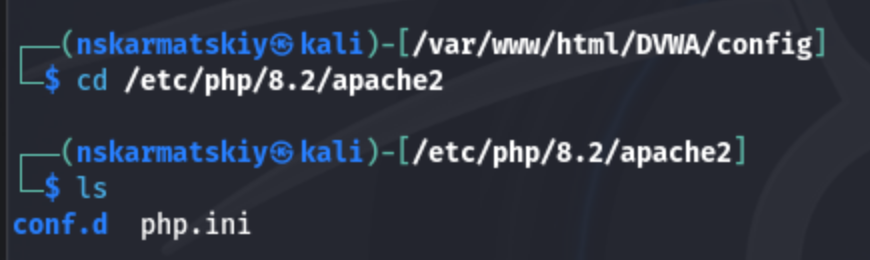


Рис. 7: Переход в директорию с apache2

Открываем файл apache2.conf. В файле параметры allow\_url\_fopen и allow\_url\_include должны быть поставлены как On (рис. 8)

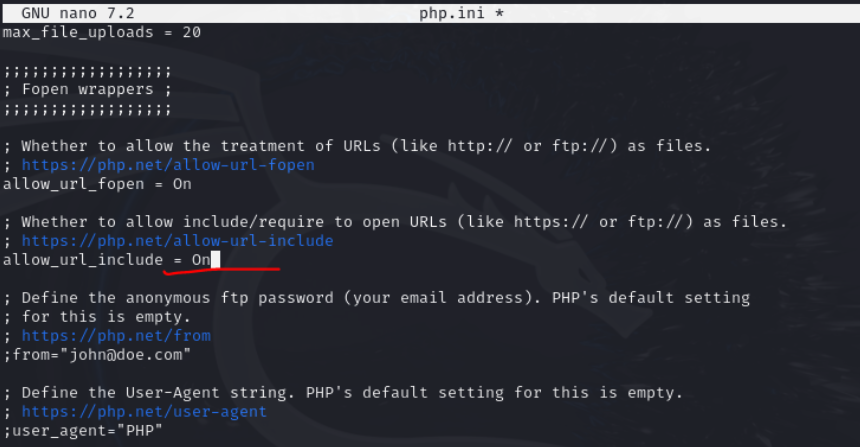


Рис. 8: Настройка apache2

Запускаем сервис apache2 и проверяем, что он запущен (рис. 9).



Рис. 9: Запуск apache2

Мы настроили DVWA, Apache и базу данных, поэтому открываем браузер и запускаем веб-приложение, введя 127.0.0.1/DVWA (рис. 10)

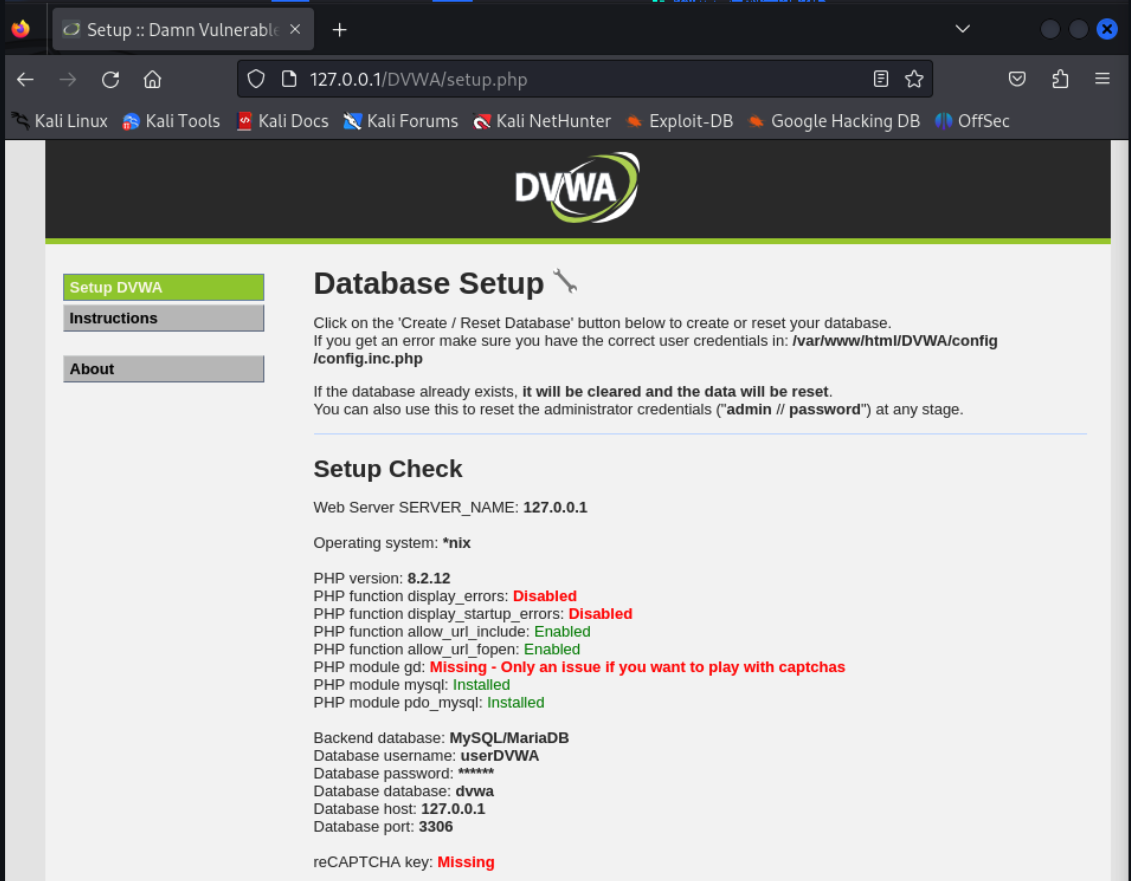


Рис. 10: Запуск веб-приложения

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

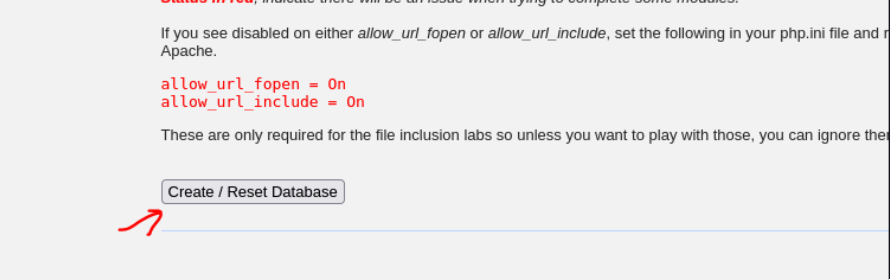


Рис. 11: “Создание базы данных”

Авторизуюемся с помощью предложенных по умолчанию данных(admin:password) (рис. 12)

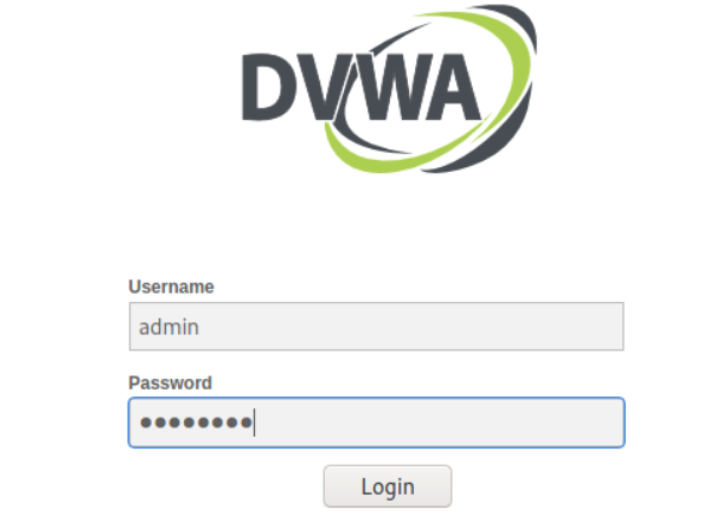


Рис. 12: Авторизация

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

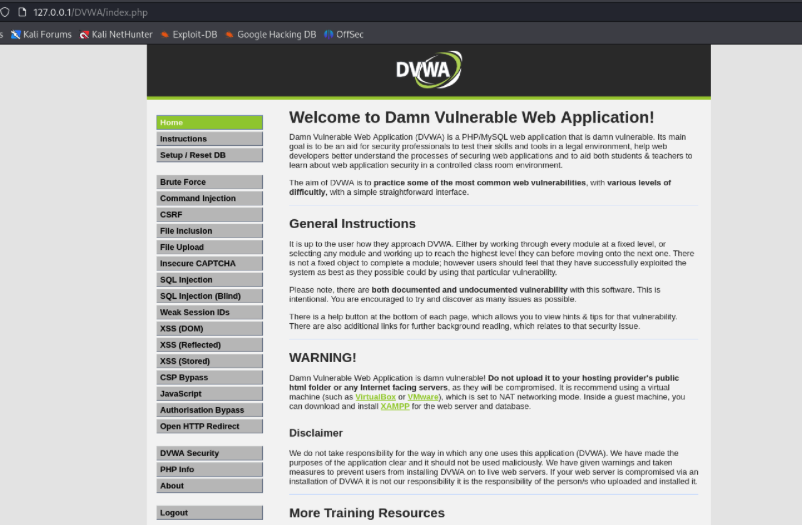


Рис. 13: Домашняя страница DVWA

# 5 Выводы

Приобрели практические навыки по установке уязвимого веб-приложения DVWA.