

# Индивидуальный проект

## Этап 2

Люпп Софья Романовна

### Содержание

1	Цель работы .....	1
2	Задание .....	1
3	Теоретическое введение.....	1
4	Выполнение лабораторной работы.....	2
5	Выводы .....	13

## 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.

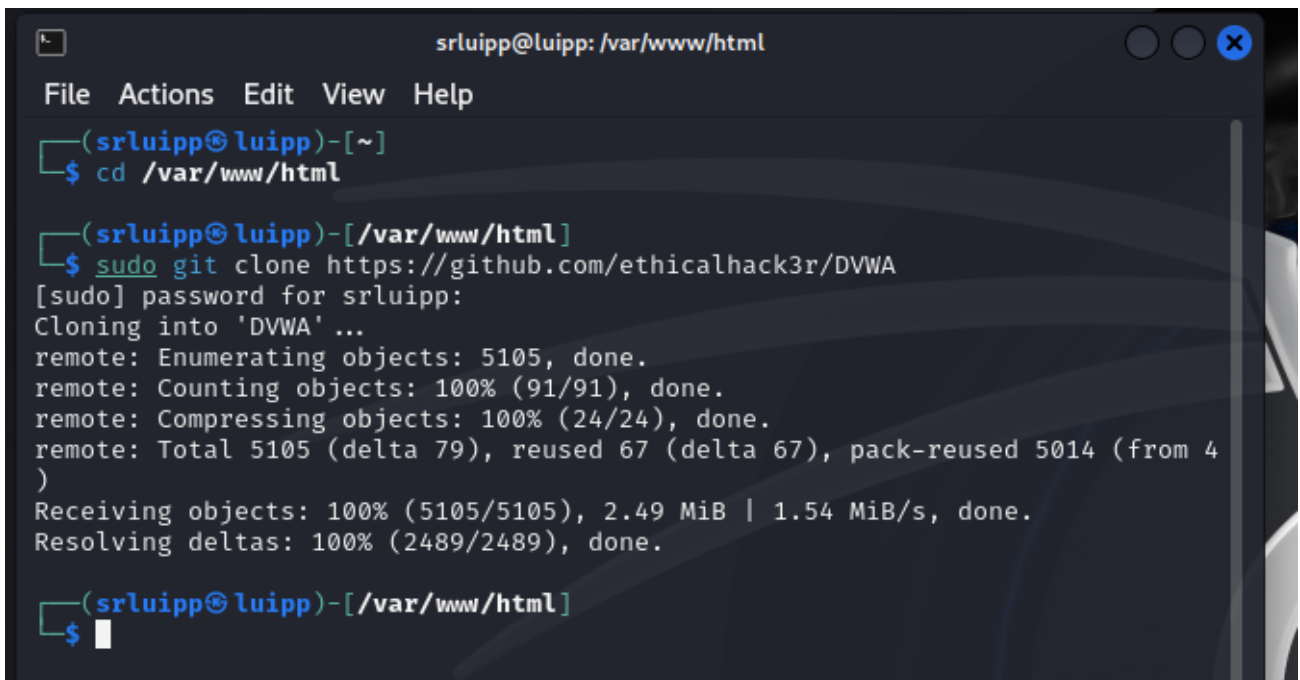
Некоторые из уязвимостей веб приложений, который содержит DVWA: - Брутфорс: Брутфорс HTTP формы страницы входа - используется для тестирования инструментов по атаке на пароль методом грубой силы и показывает небезопасность слабых паролей. - Исполнение (внедрение) команд: Выполнение команд уровня операционной системы. - Межсайтовая подделка запроса (CSRF): Позволяет «атакующему» изменить пароль администратора приложений. - Внедрение (инклюд) 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

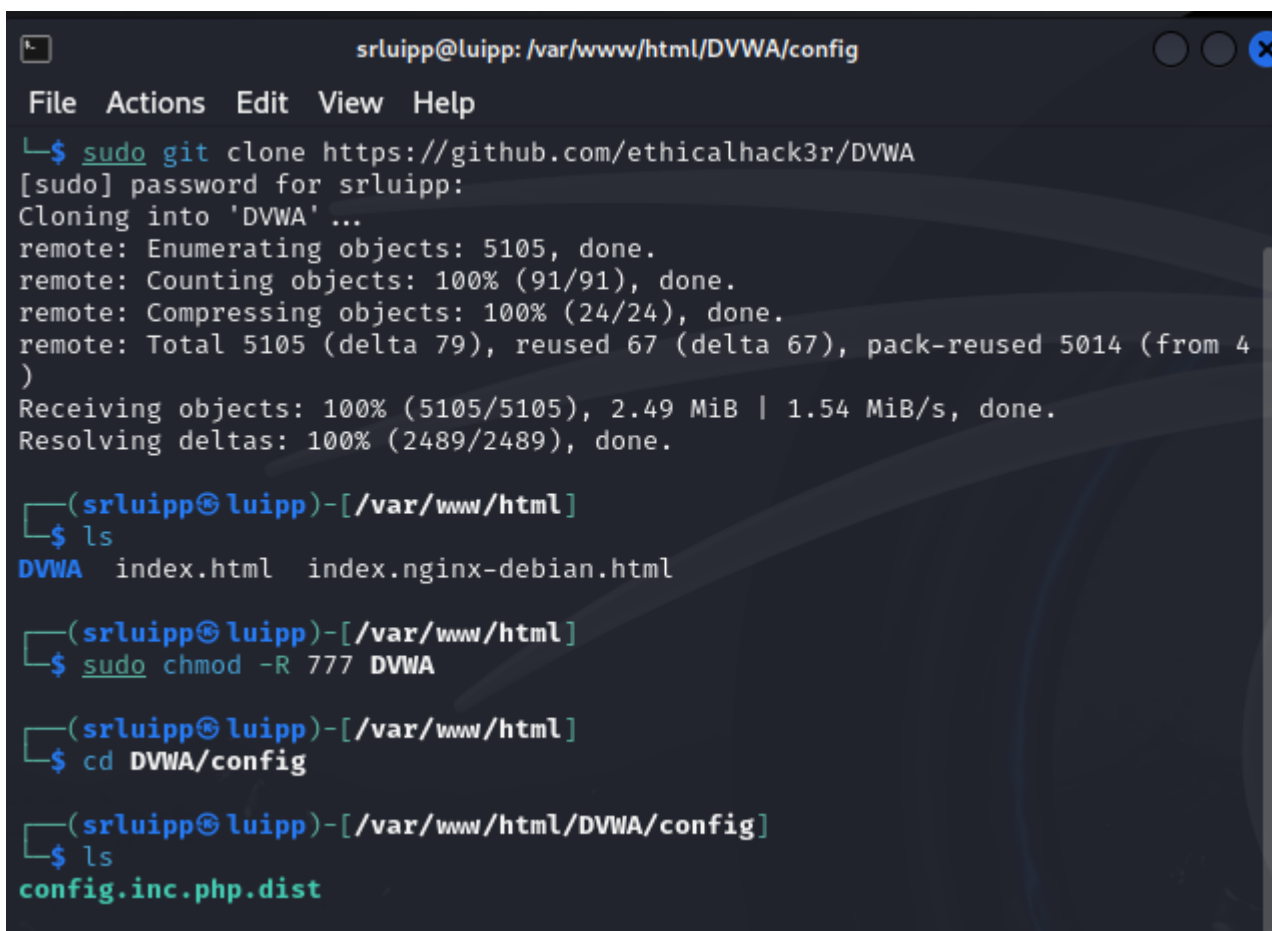
Настройка DVWA происходит на нашем локальном хосте, поэтому нужно перейти в директорию `/var/www/html`. Затем клонирую нужный репозиторий GitHub (рис. 1).

A screenshot of a terminal window titled 'srluipp@luipp: /var/www/html'. The window has a menu bar with 'File', 'Actions', 'Edit', 'View', and 'Help'. The terminal shows the following commands and output:

```
(srluipp@luipp)-[~]  
$ cd /var/www/html  
  
(srluipp@luipp)-[/var/www/html]  
$ sudo git clone https://github.com/ethicalhack3r/DVWA  
[sudo] password for srluipp:  
Cloning into 'DVWA' ...  
remote: Enumerating objects: 5105, done.  
remote: Counting objects: 100% (91/91), done.  
remote: Compressing objects: 100% (24/24), done.  
remote: Total 5105 (delta 79), reused 67 (delta 67), pack-reused 5014 (from 4)  
)  
Receiving objects: 100% (5105/5105), 2.49 MiB | 1.54 MiB/s, done.  
Resolving deltas: 100% (2489/2489), done.  
  
(srluipp@luipp)-[/var/www/html]  
$
```

*Клонирование репозитория*

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



```
srluipp@luipp: /var/www/html/DVWA/config
File Actions Edit View Help
└─$ sudo git clone https://github.com/ethicalhack3r/DVWA
[sudo] password for srluipp:
Cloning into 'DVWA' ...
remote: Enumerating objects: 5105, done.
remote: Counting objects: 100% (91/91), done.
remote: Compressing objects: 100% (24/24), done.
remote: Total 5105 (delta 79), reused 67 (delta 67), pack-reused 5014 (from 4)
Receiving objects: 100% (5105/5105), 2.49 MiB | 1.54 MiB/s, done.
Resolving deltas: 100% (2489/2489), done.

└─(srluipp@luipp)-[/var/www/html]
└─$ ls
DVWA  index.html  index.nginx-debian.html

└─(srluipp@luipp)-[/var/www/html]
└─$ sudo chmod -R 777 DVWA

└─(srluipp@luipp)-[/var/www/html]
└─$ cd DVWA/config

└─(srluipp@luipp)-[/var/www/html/DVWA/config]
└─$ ls
config.inc.php.dist
```

### *Изменение прав доступа*

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

```
srluipp@luipp: /var/www/html/DVWA/config
File Actions Edit View Help
)
Receiving objects: 100% (5105/5105), 2.49 MiB | 1.54 MiB/s, done.
Resolving deltas: 100% (2489/2489), done.

(srluipp@luipp)-[/var/www/html]
$ ls
DVWA index.html index.nginx-debian.html

(srluipp@luipp)-[/var/www/html]
$ sudo chmod -R 777 DVWA

(srluipp@luipp)-[/var/www/html]
$ cd DVWA/config

(srluipp@luipp)-[/var/www/html/DVWA/config]
$ ls
config.inc.php.dist

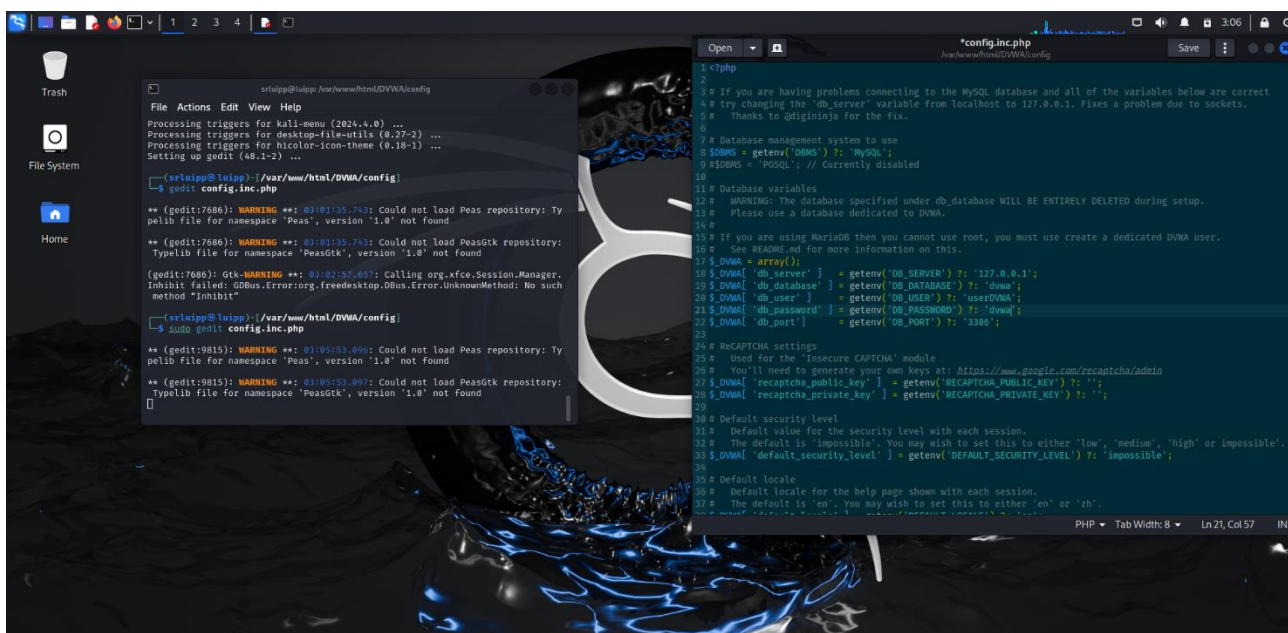
(srluipp@luipp)-[/var/www/html/DVWA/config]
$ sudo cp config.inc.php.dist config.inc.php

(srluipp@luipp)-[/var/www/html/DVWA/config]
$ ls
config.inc.php config.inc.php.dist

(srluipp@luipp)-[/var/www/html/DVWA/config]
$
```

### *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)



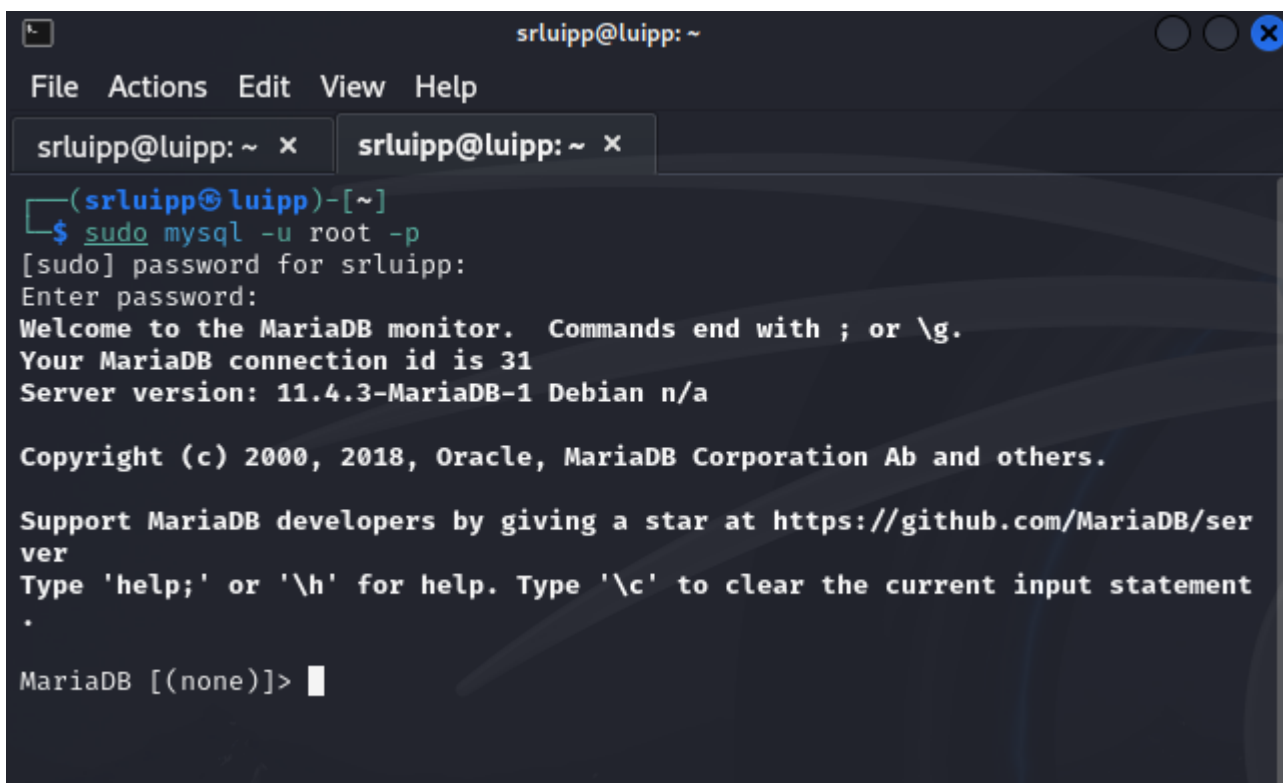
Создание копии файла

Далее открываю файл в текстовом редакторе (рис. 5)

```
srluipp@luipp: ~  
File Actions Edit View Help  
(srluipp@luipp)-[~]  
$ systemctl status mysql  
● mariadb.service - MariaDB 11.4.3 database server  
   Loaded: loaded (/usr/lib/systemd/system/mariadb.service; disabled; pres>  
   Active: active (running) since Sat 2025-03-22 03:11:35 CDT; 26s ago  
 Invocation: 74c2a3edbf8d49e3b9cd2f773f741e22  
    Docs: man:mariadb(8)  
          https://mariadb.com/kb/en/library/systemd/  
 Process: 12564 ExecStartPre=/usr/bin/install -m 755 -o mysql -g root -d >  
 Process: 12566 ExecStartPre=/bin/sh -c systemctl unset-environment _WSRE>  
 Process: 12568 ExecStartPre=/bin/sh -c [ ! -e /usr/bin/galera_recovery ]>  
 Process: 12668 ExecStartPost=/bin/sh -c systemctl unset-environment _WSR>  
 Process: 12670 ExecStartPost=/etc/mysql/debian-start (code=exited, statu>  
 Main PID: 12629 (mariadb)  
   Status: "Taking your SQL requests now ..."  
    Tasks: 15 (limit: 14286)  
  Memory: 241.4M (peak: 246.1M)  
     CPU: 3.221s  
   CGroup: /system.slice/mariadb.service  
           └─12629 /usr/sbin/mariadb  
  
Mar 22 03:11:34 luipp mariadb[12629]: 2025-03-22 3:11:34 0 [Note] InnoDB: >  
Mar 22 03:11:34 luipp mariadb[12629]: 2025-03-22 3:11:34 0 [Note] Plugin '>  
Mar 22 03:11:34 luipp mariadb[12629]: 2025-03-22 3:11:34 0 [Note] Plugin '>  
Mar 22 03:11:34 luipp mariadb[12629]: 2025-03-22 3:11:34 0 [Note] InnoDB: >  
Mar 22 03:11:35 luipp mariadb[12629]: 2025-03-22 3:11:35 0 [Note] Server s>  
Mar 22 03:11:35 luipp mariadb[12629]: 2025-03-22 3:11:35 0 [Note] mariadb>
```

*Открытие файла в редакторе*

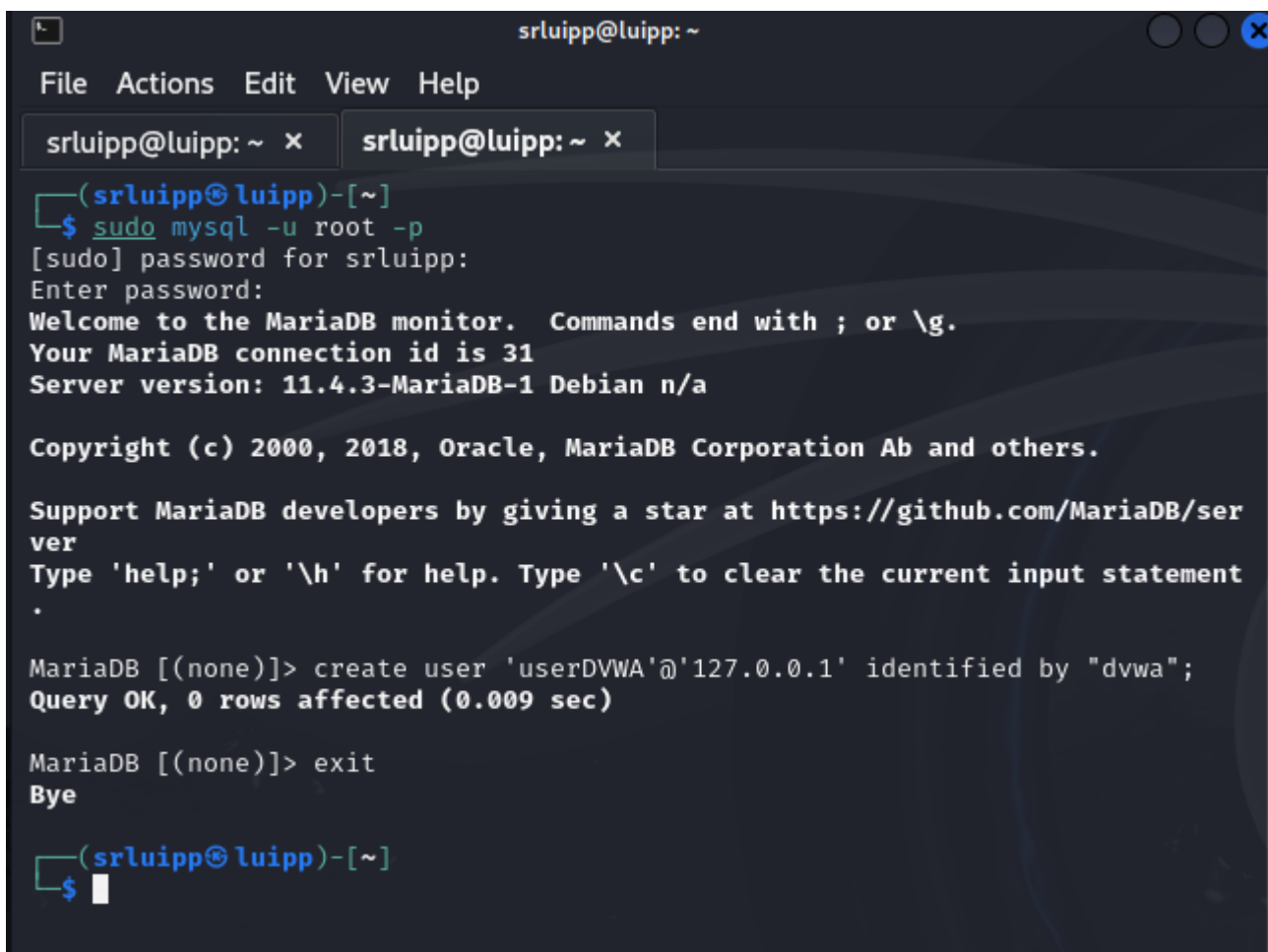
Изменяю данные об имени пользователя и пароле (рис. 6)



```
srluipp@luipp: ~  
File Actions Edit View Help  
srluipp@luipp: ~ x srluipp@luipp: ~ x  
(srluipp@luipp)-[~]  
$ sudo mysql -u root -p  
[sudo] password for srluipp:  
Enter password:  
Welcome to the MariaDB monitor.  Commands end with ; or \g.  
Your MariaDB connection id is 31  
Server version: 11.4.3-MariaDB-1 Debian n/a  
  
Copyright (c) 2000, 2018, Oracle, MariaDB Corporation Ab and others.  
  
Support MariaDB developers by giving a star at https://github.com/MariaDB/server  
Type 'help;' or '\h' for help. Type '\c' to clear the current input statement  
.  
MariaDB [(none)]>
```

### *Редактирование файла*

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

A screenshot of a terminal window titled 'srluipp@luipp: ~'. The window has a menu bar with 'File', 'Actions', 'Edit', 'View', and 'Help'. Below the menu bar are two tabs, both labeled 'srluipp@luipp: ~'. The terminal content shows a user running 'sudo mysql -u root -p', entering a password, and being prompted to 'Welcome to the MariaDB monitor'. The user then enters 'create user 'userDVWA'@'127.0.0.1' identified by "dvwa";', which is successful. Finally, the user enters 'exit' and the terminal returns to the shell prompt.

```
(srluipp@luipp)-[~]
$ sudo mysql -u root -p
[sudo] password for srluipp:
Enter password:
Welcome to the MariaDB monitor.  Commands end with ; or \g.
Your MariaDB connection id is 31
Server version: 11.4.3-MariaDB-1 Debian n/a

Copyright (c) 2000, 2018, Oracle, MariaDB Corporation Ab and others.

Support MariaDB developers by giving a star at https://github.com/MariaDB/server
Type 'help;' or '\h' for help. Type '\c' to clear the current input statement
.

MariaDB [(none)]> create user 'userDVWA'@'127.0.0.1' identified by "dvwa";
Query OK, 0 rows affected (0.009 sec)

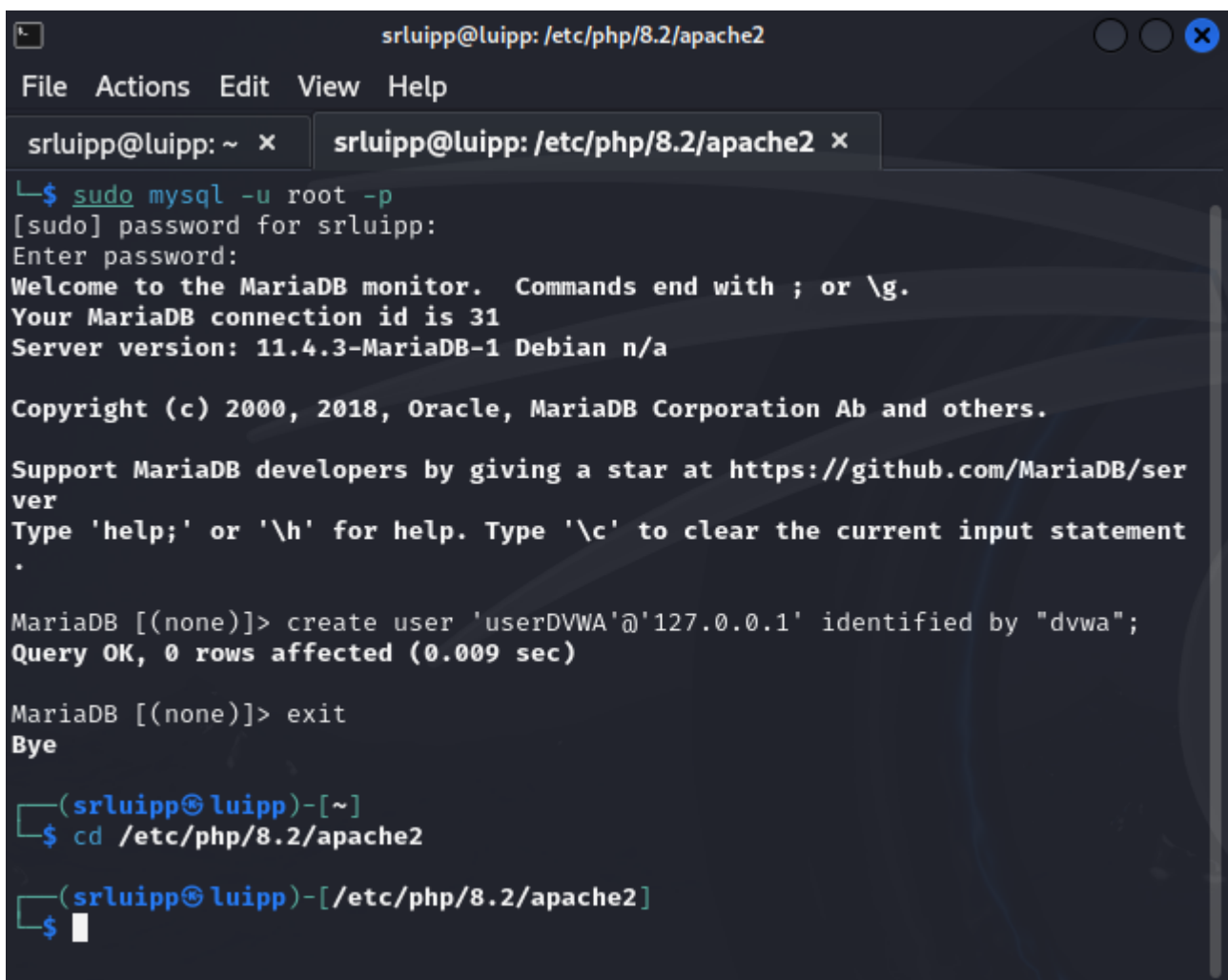
MariaDB [(none)]> exit
Bye

(srluipp@luipp)-[~]
$
```

### *Заняск 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)



A terminal window with a dark background and light text. The title bar shows 'srluipp@luipp: /etc/php/8.2/apache2'. The menu bar includes 'File', 'Actions', 'Edit', 'View', and 'Help'. There are two tabs: 'srluipp@luipp: ~' and 'srluipp@luipp: /etc/php/8.2/apache2'. The terminal content shows a user running 'sudo mysql -u root -p', entering a password, and being prompted to create a user. The user 'userDVWA' is created with host '127.0.0.1' and password 'dvwa'. After exiting the MySQL prompt, the user runs 'cd /etc/php/8.2/apache2' in the shell prompt.

```
srluipp@luipp: /etc/php/8.2/apache2
File Actions Edit View Help
srluipp@luipp: ~ x srluipp@luipp: /etc/php/8.2/apache2 x
└─$ sudo mysql -u root -p
[sudo] password for srluipp:
Enter password:
Welcome to the MariaDB monitor.  Commands end with ; or \g.
Your MariaDB connection id is 31
Server version: 11.4.3-MariaDB-1 Debian n/a

Copyright (c) 2000, 2018, Oracle, MariaDB Corporation Ab and others.

Support MariaDB developers by giving a star at https://github.com/MariaDB/server
Type 'help;' or '\h' for help. Type '\c' to clear the current input statement
.

MariaDB [(none)]> create user 'userDVWA'@'127.0.0.1' identified by "dvwa";
Query OK, 0 rows affected (0.009 sec)

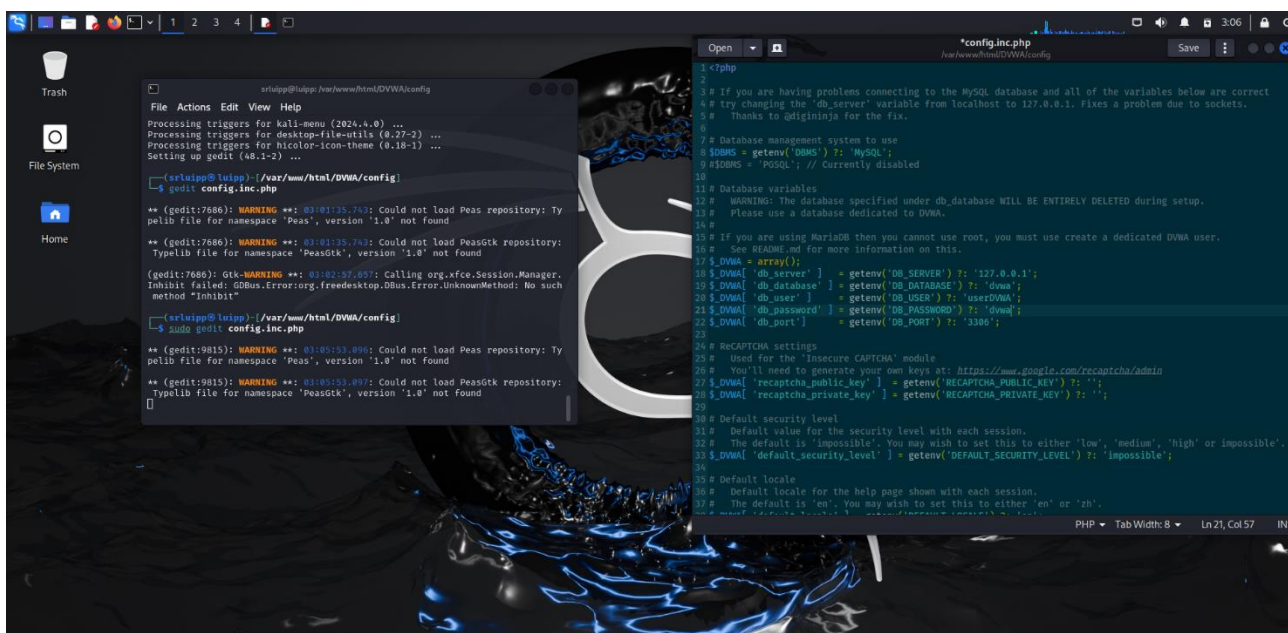
MariaDB [(none)]> exit
Bye

(srluipp@luipp)-[~]
$ cd /etc/php/8.2/apache2

(srluipp@luipp)-[/etc/php/8.2/apache2]
$
```

*Авторизация в базе данных*

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



## Изменение прав

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

```
srluipp@luipp: /etc/php/8.2/apache2
File Actions Edit View Help
srluipp@luipp: ~ x srluipp@luipp: /etc/php/8.2/apache2 x

(srluipp@luipp)-[/etc/php/8.2/apache2]
$ systemctl status start apache2
Unit start.service could not be found.
● apache2.service - The Apache HTTP Server
   Loaded: loaded (/usr/lib/systemd/system/apache2.service; disabled; pres>
   Active: active (running) since Sat 2025-03-22 03:20:19 CDT; 17s ago
  Invocation: 305fae0624aa48c1bcbab9b933cf94bd
     Docs: https://httpd.apache.org/docs/2.4/
   Process: 17178 ExecStart=/usr/sbin/apachectl start (code=exited, status=>
  Main PID: 17194 (apache2)
     Tasks: 6 (limit: 2164)
    Memory: 20.5M (peak: 20.7M)
       CPU: 183ms
    CGroup: /system.slice/apache2.service
            └─17194 /usr/sbin/apache2 -k start
              └─17197 /usr/sbin/apache2 -k start
                └─17198 /usr/sbin/apache2 -k start
                  └─17199 /usr/sbin/apache2 -k start
                    └─17200 /usr/sbin/apache2 -k start
                      └─17201 /usr/sbin/apache2 -k start

Mar 22 03:20:19 luipp systemd[1]: Starting apache2.service - The Apache HTTP>
Mar 22 03:20:19 luipp systemd[1]: Started apache2.service - The Apache HTTP >
lines 1-21/21 (END)
```

*Перемещение между директориями*

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

*Открытие файла в текстовом редакторе*

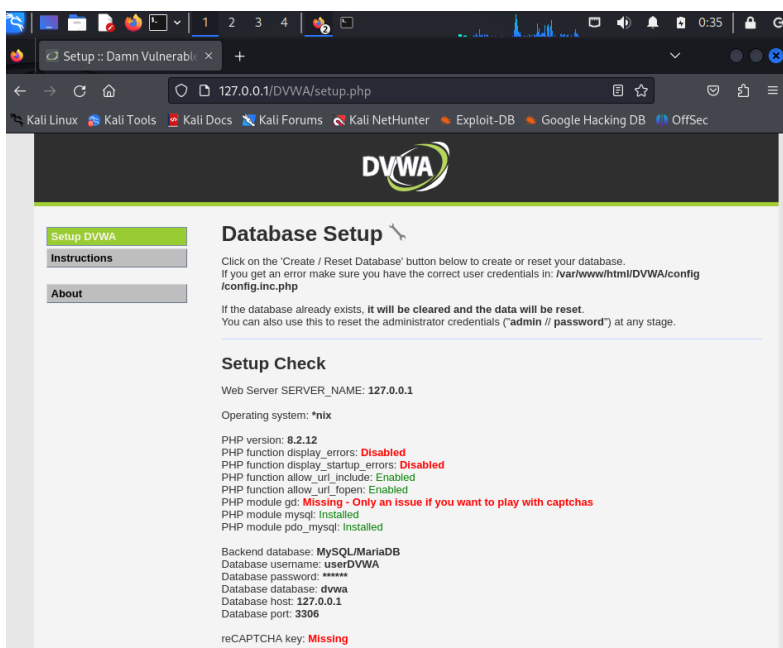
В файле параметры `allow_url_fopen` и `allow_url_include` должны быть поставлены как `On`.

*Редактирование файла*

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

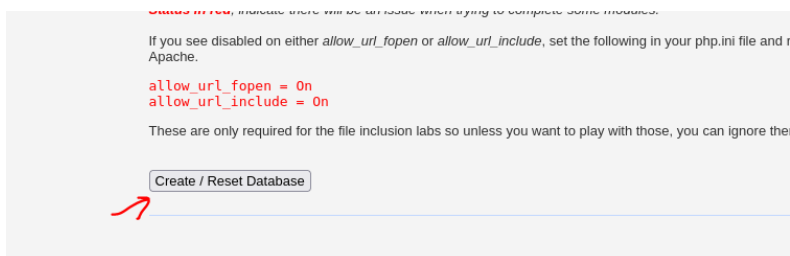
*Запуск `apche`*

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 нажмем на кнопку create\reset database (рис. 11)



## “Создание базы данных”

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



Username

admin

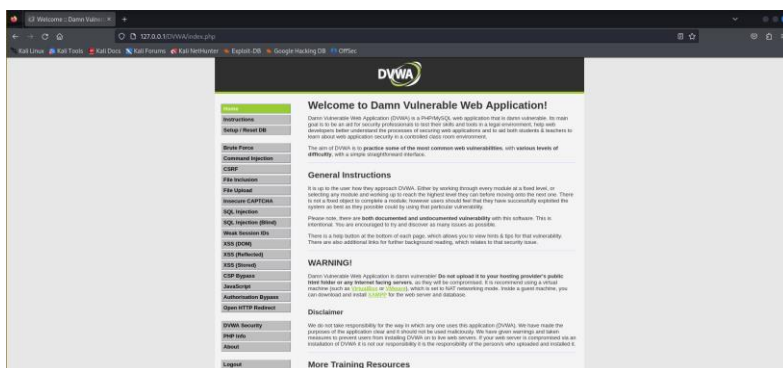
Password

••••••••

Login

## Авторизация

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



Домашняя страница DVWA

## 5 Выводы

Приобрела практические навыки по установке уязвимого веб-приложения DVWA.