
Front matter

title: "Отчет по второму этапу индивидуального проекта"
subtitle: "Основы информационной безопасности"
author: "Бабенко Константин, НКАбд-01-23"

Generic options

lang: ru-RU
toc-title: "Содержание"

Bibliography

bibliography: bib/cite.bib
csl: pandoc/csl/gost-r-7-0-5-2008-numeric.csl

PDF output format

toc: true # Table of contents
toc-depth: 2
lof: true # List of figures
lot: true # List of tables
fontsize: 12pt
linestretch: 1.5
papersize: a4
documentclass: scrreprt

l18n polyglossia

polyglossia-lang:
name: russian
options:
- spelling=modern
- babelshorthands=true
polyglossia-otherlangs:
name: english

l18n babel

babel-lang: russian
babel-otherlangs: english

Fonts

mainfont: PT Serif
romanfont: PT Serif
sansfont: PT Sans
monofont: PT Mono
mainfontoptions: Ligatures=TeX
romanfontoptions: Ligatures=TeX
sansfontoptions: Ligatures=TeX,Scale=MatchLowercase
monofontoptions: Scale=MatchLowercase,Scale=0.9

Biblatex

biblatex: true
biblio-style: "gost-numeric"
biblatexoptions:

- parenttracker=true
- backend=biber
- hyperref=auto
- language=auto
- autolang=other*
- citestyle=gost-numeric

Pandoc-crossref LaTeX customization

figureTitle: "Рис."
tableTitle: "Таблица"
listingTitle: "Листинг"
lofTitle: "Список иллюстраций"
lotTitle: "Список таблиц"
lolTitle: "Листинги"

Misc options

indent: true
header-includes:

- \usepackage[indentfirst]
- \usepackage{float} # keep figures where there are in the text
- \floatplacement{figure}{H} # keep figures where there are in the text

Цель работы

Приобретение практических навыков по установке DVWA.

Задание

1. Установить DVWA на дистрибутив Kali Linux.

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.

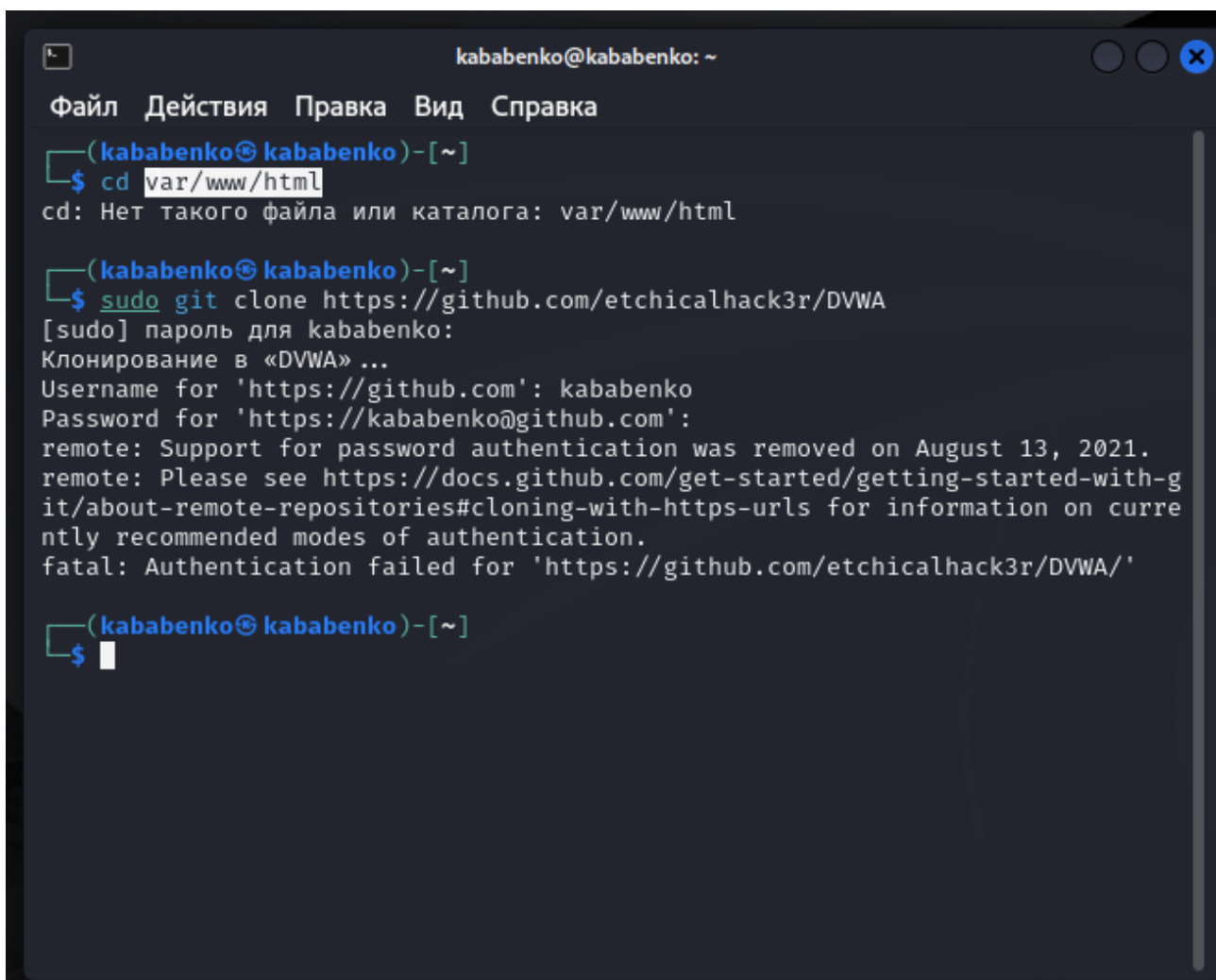
- Межсайтовая подделка запроса (CSRF): Позволяет «атакующему» изменить пароль администратора приложений.
- Внедрение (инклюд) файлов: Позволяет «атакующему» присоединить удалённые/локальные файлы в веб приложение.
- SQL внедрение: Позволяет «атакующему» внедрить SQL выражения в HTTP из поля ввода, DVWA 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.
[@guide, @parasram]

Выполнение лабораторной работы

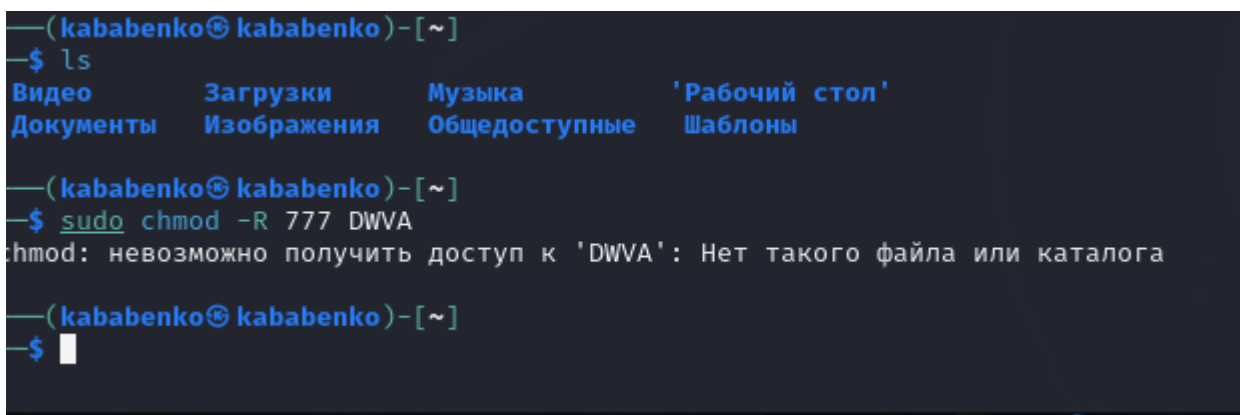
Настройка DVWA происходит на нашем локальном хосте, поэтому нужно перейти в директорию `/var/www/html`. Затем клонирую нужный репозиторий GitHub (рис. 1).



```
kababenko@kababenko: ~  
Файл Действия Правка Вид Справка  
(kababenko@kababenko)-[~]  
$ cd var/www/html  
cd: Нет такого файла или каталога: var/www/html  
  
(kababenko@kababenko)-[~]  
$ sudo git clone https://github.com/etichalhack3r/DVWA  
[sudo] пароль для kababenko:  
Клонирование в «DVWA» ...  
Username for 'https://github.com': kababenko  
Password for 'https://kababenko@github.com':  
remote: Support for password authentication was removed on August 13, 2021.  
remote: Please see https://docs.github.com/get-started/getting-started-with-git/about-remote-repositories#cloning-with-https-urls for information on currently recommended modes of authentication.  
fatal: Authentication failed for 'https://github.com/etichalhack3r/DVWA/'  
  
(kababenko@kababenko)-[~]  
$
```

{#fig:001 width=70%}

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



```
(kababenko@kababenko)-[~]  
$ ls  
Видео Загрузки Музыка 'Рабочий стол'  
Документы Изображения Общедоступные Шаблоны  
  
(kababenko@kababenko)-[~]  
$ sudo chmod -R 777 DVWA  
chmod: невозможно получить доступ к 'DVWA': Нет такого файла или каталога  
  
(kababenko@kababenko)-[~]  
$
```

{#fig:002 width=70%}

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

```
(kababenko@kababenko)-[~]
$ ls
Видео      Загрузки  Музыка    'Рабочий стол'
Документы  Изображения  Общедоступные  Шаблоны

(kababenko@kababenko)-[~]
$
```

{#fig:003 width=70%}

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)

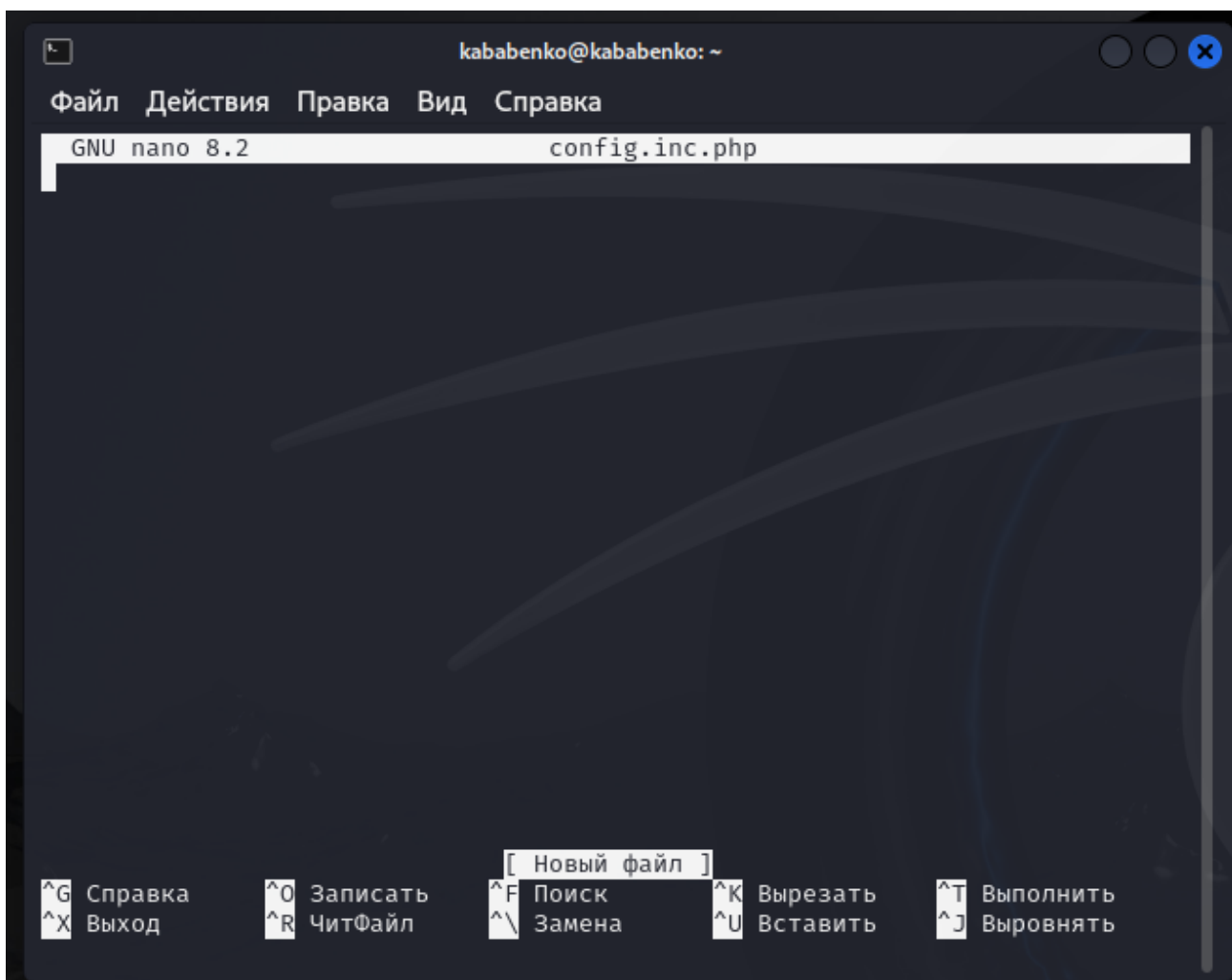
```
(kababenko@kababenko)-[~]
$ sudo cp config.inc.php.dist config.inc.php
cp: не удалось выполнить stat для 'config.inc.php.dist': Нет такого файла или каталога

(kababenko@kababenko)-[~]
$ ls
Видео      Загрузки  Музыка    'Рабочий стол'
Документы  Изображения  Общедоступные  Шаблоны

(kababenko@kababenko)-[~]
$
```

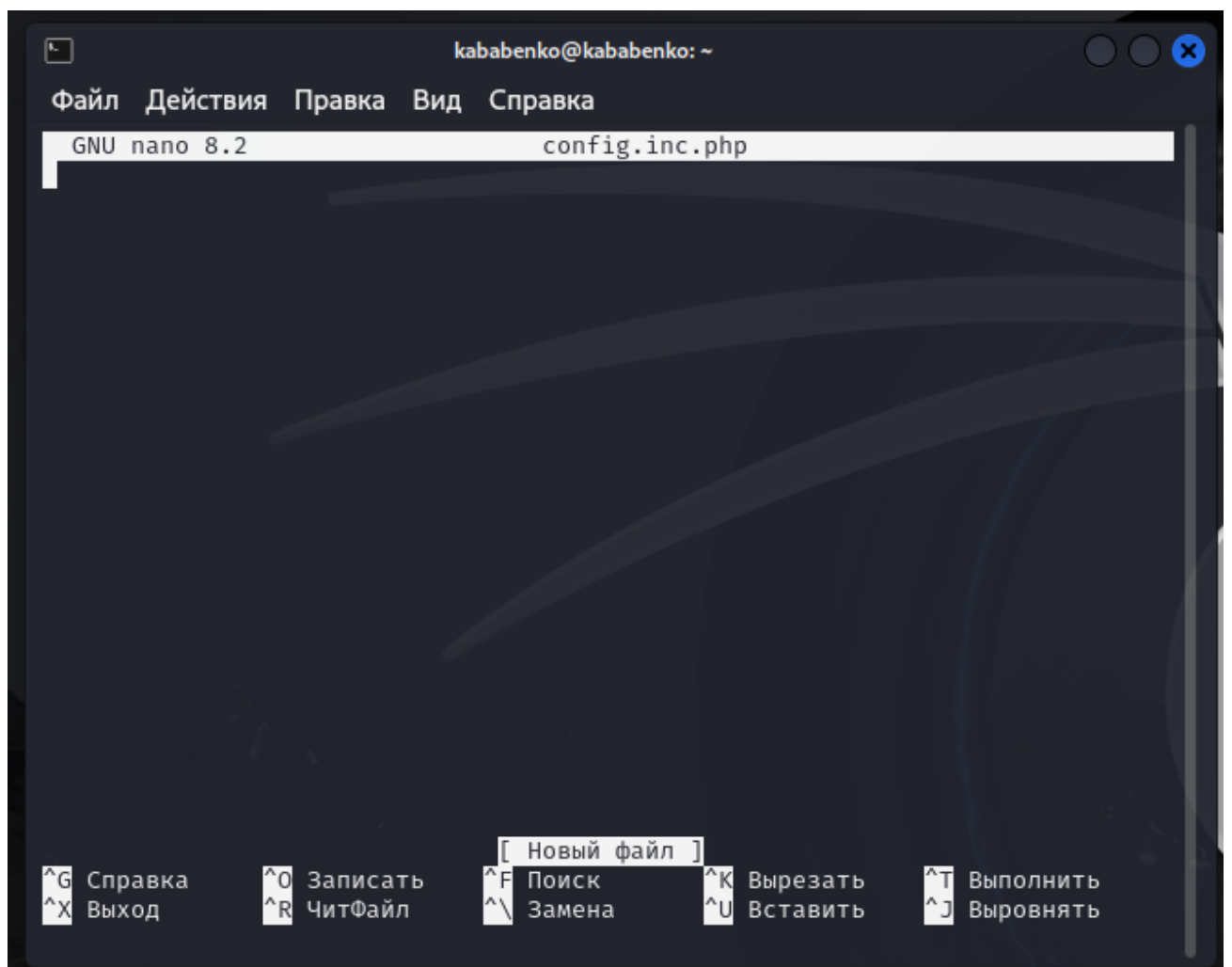
{#fig:004 width=70%}

Далее открываю файл в текстовом редакторе (рис. 5)



{#fig:005 width=70%}

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



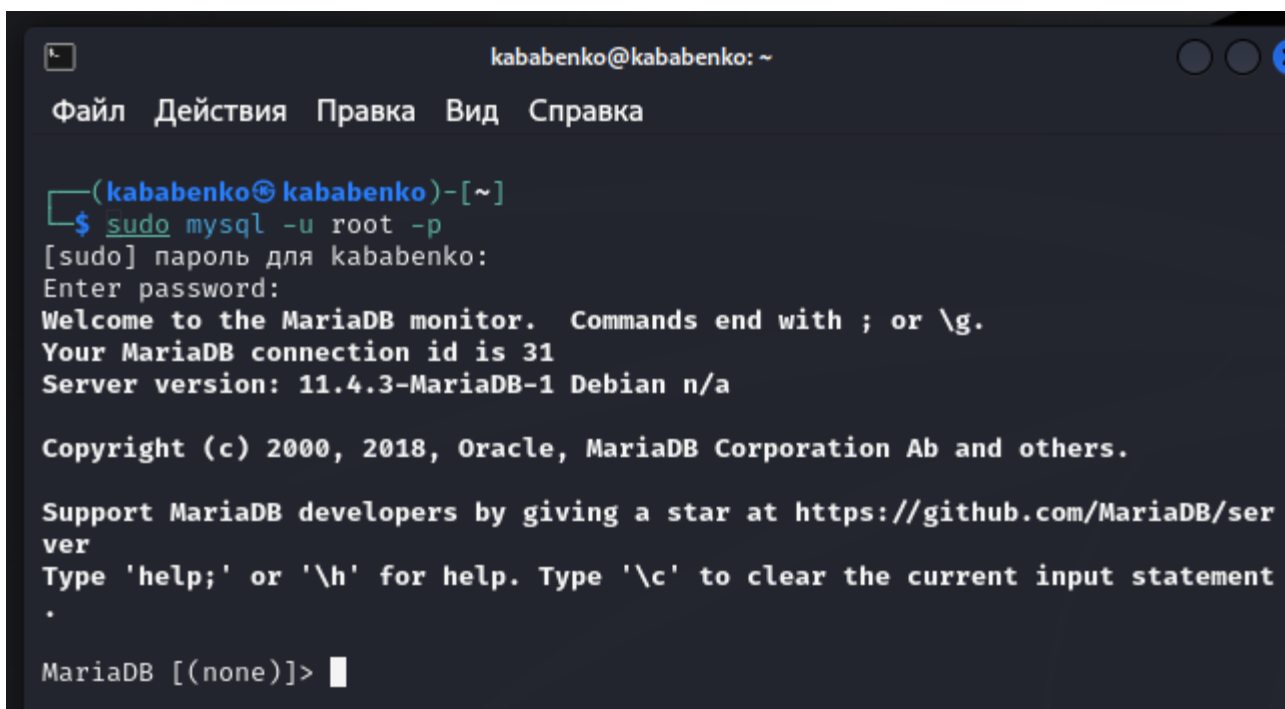
{#fig:006 width=70%}

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

```
kababenko@kababenko: ~  
Файл Действия Правка Вид Справка  
● mariadb.service - MariaDB 11.4.3 database server  
  Loaded: loaded (/usr/lib/systemd/system/mariadb.service; disabled; pres>  
  Active: active (running) since Tue 2025-03-18 21:58:26 MSK; 35s ago  
  Invocation: ffbfe27f468847a2b18a1c7ef2619f80  
  Docs: man:mariadb(8)  
        https://mariadb.com/kb/en/library/systemd/  
  Process: 2732 ExecStartPre=/usr/bin/install -m 755 -o mysql -g root -d />  
  Process: 2734 ExecStartPre=/bin/sh -c systemctl unset-environment _WSREP>  
  Process: 2736 ExecStartPre=/bin/sh -c [ ! -e /usr/bin/galera_recovery ] >  
  Process: 2826 ExecStartPost=/bin/sh -c systemctl unset-environment _WSRE>  
  Process: 2828 ExecStartPost=/etc/mysql/debian-start (code=exited, status>  
  Main PID: 2797 (mariadb)  
  Status: "Taking your SQL requests now ..."  
  Tasks: 14 (limit: 30078)  
  Memory: 242.6M (peak: 247M)  
  CPU: 1.849s  
  CGroup: /system.slice/mariadb.service  
          └─2797 /usr/sbin/mariadb  
  
мар 18 21:58:25 kababenko mariadb[2797]: 2025-03-18 21:58:25 0 [Note] InnoD>  
мар 18 21:58:25 kababenko mariadb[2797]: 2025-03-18 21:58:25 0 [Note] InnoD>  
мар 18 21:58:25 kababenko mariadb[2797]: 2025-03-18 21:58:25 0 [Note] Plugi>  
мар 18 21:58:25 kababenko mariadb[2797]: 2025-03-18 21:58:25 0 [Note] Plugi>  
мар 18 21:58:25 kababenko mariadb[2797]: 2025-03-18 21:58:25 0 [Note] InnoD>  
мар 18 21:58:25 kababenko mariadb[2797]: 2025-03-18 21:58:25 0 [Note] Serve>  
мар 18 21:58:26 kababenko mariadb[2797]: 2025-03-18 21:58:26 0 [Note] maria>  
lines 1-26
```

{#fig:007 width=70%}

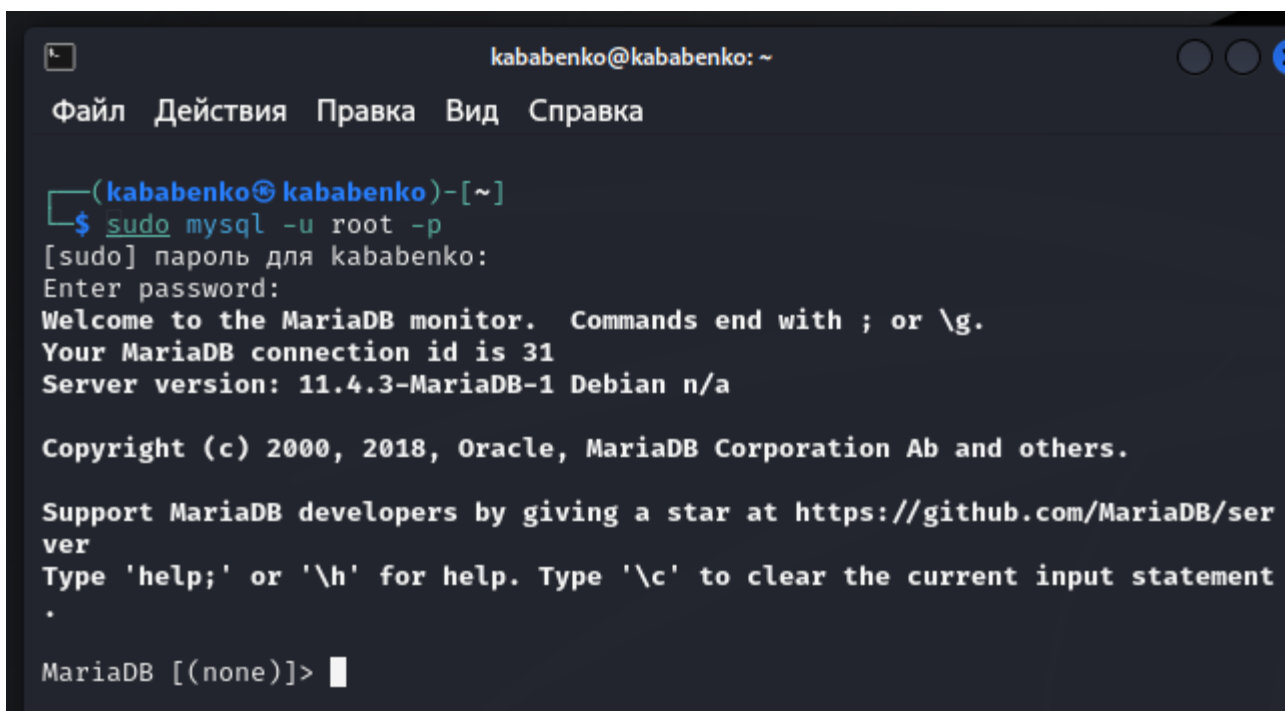
Авторизируюсь в базе данных от имени пользователя root. Появляется командная строка с приглашением "MariaDB", далее создаем в ней нового пользователя, используя учетные данные из файла config.inc.php (рис. 8)



```
kababenko@kababenko: ~  
Файл Действия Правка Вид Справка  
  
(kababenko@kababenko)-[~]  
$ sudo mysql -u root -p  
[sudo] пароль для kababenko:  
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)]> █
```

{#fig:008 width=70%}

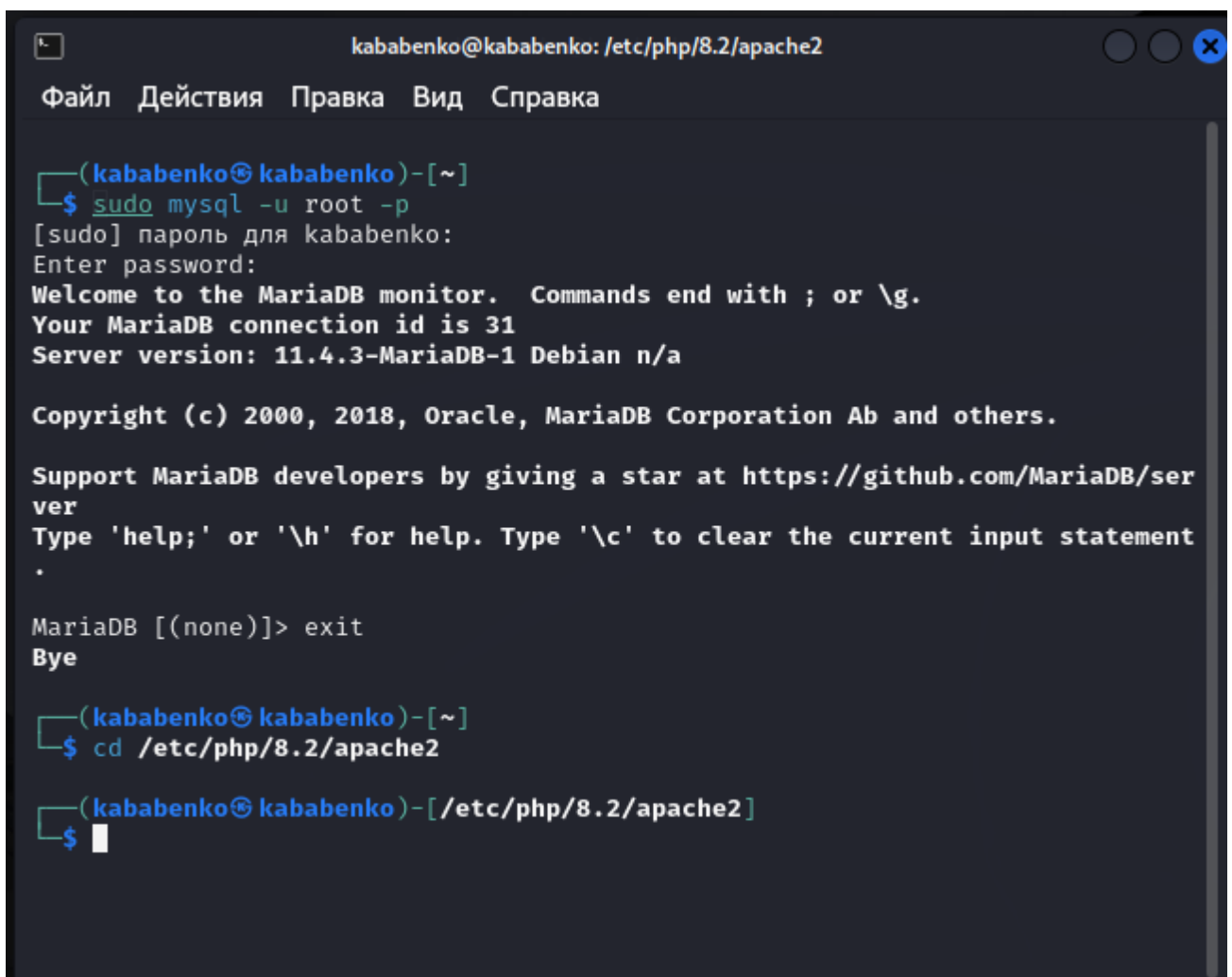
Теперь нужно пользователю предоставить привилегии для работы с этой базой данных (рис. 9)



```
kababenko@kababenko: ~  
Файл Действия Правка Вид Справка  
  
(kababenko@kababenko)-[~]  
$ sudo mysql -u root -p  
[sudo] пароль для kababenko:  
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)]> █
```

{#fig:009 width=70%}

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



```
kababenko@kababenko: /etc/php/8.2/apache2
Файл Действия Правка Вид Справка

(kababenko@kababenko)-[~]
$ sudo mysql -u root -p
[sudo] пароль для kababenko:
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)]> exit
Bye

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

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

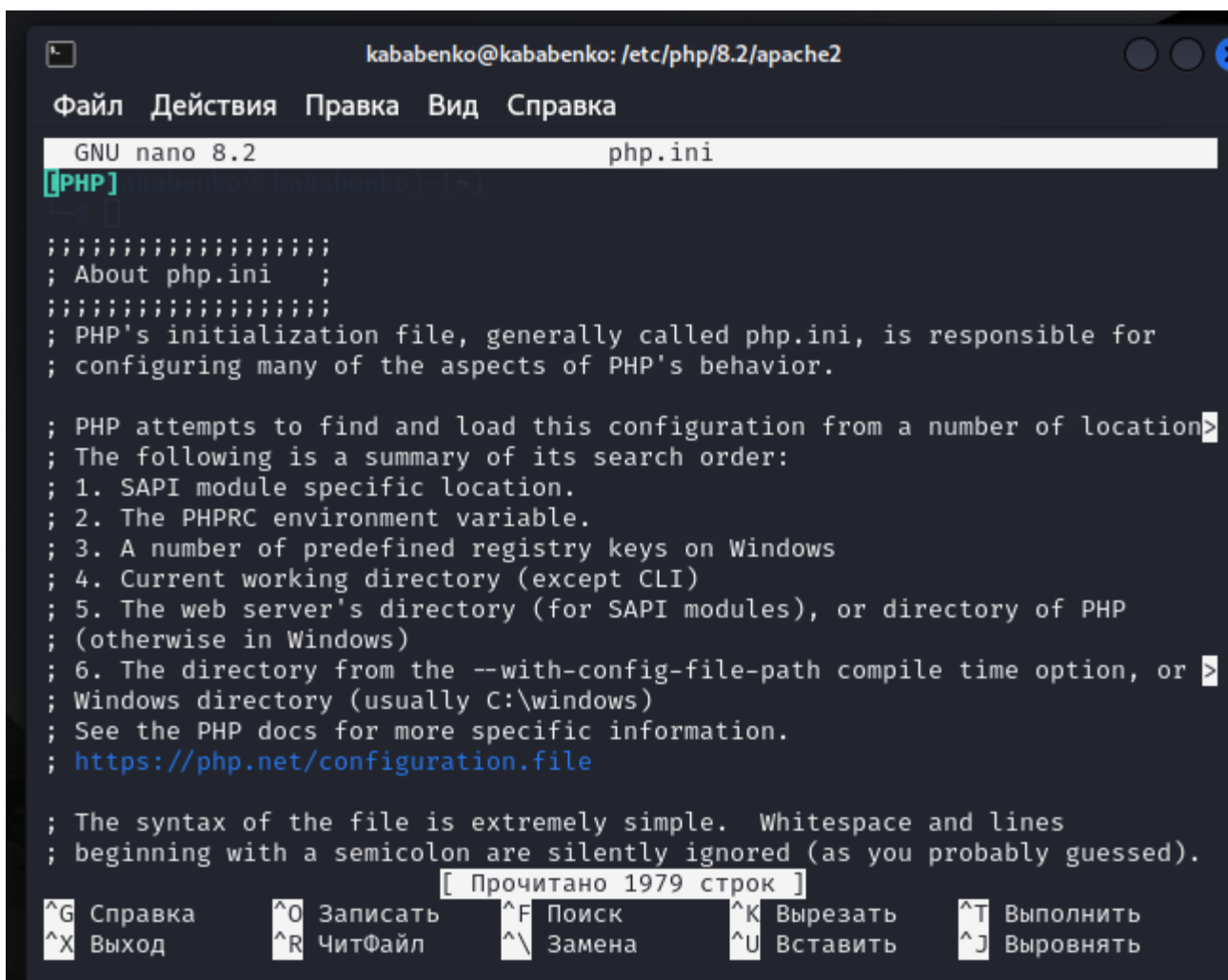
{#fig:010 width=70%}

В файле `php.ini` нужно будет изменить один параметр, поэтому открываю файл в текстовом редакторе (рис. 11)

```
kababenko@kababenko: /etc/php/8.2/apache2
Файл Действия Правка Вид Справка
GNU nano 8.2 php.ini
[PHP]
;
; ;
; About php.ini ;
; ;
; PHP's initialization file, generally called php.ini, is responsible for
; configuring many of the aspects of PHP's behavior.
;
; PHP attempts to find and load this configuration from a number of locations
; The following is a summary of its search order:
; 1. SAPI module specific location.
; 2. The PHPRC environment variable.
; 3. A number of predefined registry keys on Windows
; 4. Current working directory (except CLI)
; 5. The web server's directory (for SAPI modules), or directory of PHP
; (otherwise in Windows)
; 6. The directory from the --with-config-file-path compile time option, or
; Windows directory (usually C:\windows)
; See the PHP docs for more specific information.
; https://php.net/configuration.file
;
; The syntax of the file is extremely simple. Whitespace and lines
; beginning with a semicolon are silently ignored (as you probably guessed).
[ Прочитано 1979 строк ]
^G Справка ^O Записать ^F Поиск ^K Вырезать ^T Выполнить
^X Выход ^R ЧитФайл ^\ Замена ^U Вставить ^J Выровнять
```

{#fig:011 width=70%}

В файле параметры `allow_url_fopen` и `allow_url_include` должны быть поставлены как **On** (рис. 12)



```
kababenko@kababenko: /etc/php/8.2/apache2
Файл Действия Правка Вид Справка
GNU nano 8.2 php.ini
[PHP]
;
; ;
; About php.ini ;
;
; ;
; PHP's initialization file, generally called php.ini, is responsible for
; configuring many of the aspects of PHP's behavior.
;
; PHP attempts to find and load this configuration from a number of locations
; The following is a summary of its search order:
; 1. SAPI module specific location.
; 2. The PHPRC environment variable.
; 3. A number of predefined registry keys on Windows
; 4. Current working directory (except CLI)
; 5. The web server's directory (for SAPI modules), or directory of PHP
; (otherwise in Windows)
; 6. The directory from the --with-config-file-path compile time option, or
; Windows directory (usually C:\windows)
; See the PHP docs for more specific information.
; https://php.net/configuration.file
;
; The syntax of the file is extremely simple. Whitespace and lines
; beginning with a semicolon are silently ignored (as you probably guessed).
[ Прочитано 1979 строк ]
^G Справка ^O Записать ^F Поиск ^K Вырезать ^T Выполнить
^X Выход ^R ЧитФайл ^\ Замена ^U Вставить ^J Выровнять
```

{#fig:012 width=70%}

Запускаем службу веб-сервера apache и проверяем, запущена ли служба (рис. 13)

```

(kababenko@kababenko)-[/etc/php/8.2/apache2]
$ sudo systemctl start apache2

(kababenko@kababenko)-[/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; preset: disabled)
   Active: active (running) since Tue 2025-03-18 22:08:55 MSK; 39s ago
 Invocation: e9eefa74a7cb4d81bfed733f43c64e56
    Docs: https://httpd.apache.org/docs/2.4/
  Process: 8055 ExecStart=/usr/sbin/apachectl start (code=exited, status=0/SUCCESS)
 Main PID: 8071 (apache2)
    Tasks: 6 (limit: 4557)
  Memory: 24.7M (peak: 25M)
     CPU: 121ms
    CGroup: /system.slice/apache2.service
            └─8071 /usr/sbin/apache2 -k start
              └─8074 /usr/sbin/apache2 -k start
                └─8075 /usr/sbin/apache2 -k start
                  └─8076 /usr/sbin/apache2 -k start
                    └─8077 /usr/sbin/apache2 -k start
                      └─8078 /usr/sbin/apache2 -k start

map 18 22:08:55 kababenko systemd[1]: Starting apache2.service - The Apache HTTP Server ...
map 18 22:08:55 kababenko systemd[1]: Started apache2.service - The Apache HTTP Server.

```

{#fig:013 width=70%}

Мы настроили DVWA, Apache и базу данных, поэтому открываем браузер и запускаем веб-приложение, введя 127.0.0/DVWA (рис. 14)



Apache2 Debian Default Page

It works!

This is the default welcome page used to test the correct operation of the Apache2 server after installation on Debian systems. If you can read this page, it means that the Apache HTTP server installed at this site is working properly. You should **replace this file** (located at `/var/www/html/index.html`) before continuing to operate your HTTP server.

If you are a normal user of this web site and don't know what this page is about, this probably means that the site is currently unavailable due to maintenance. If the problem persists, please contact the site's administrator.

Configuration Overview

Debian's Apache2 default configuration is different from the upstream default configuration, and split into several files optimized for interaction with Debian tools. The configuration system is **fully documented in `/usr/share/doc/apache2/README.Debian.gz`**. Refer to this for the full documentation. Documentation for the web server itself can be found by accessing the **manual** if the `apache2-doc` package was installed on this server.

The configuration layout for an Apache2 web server installation on Debian systems is as follows:

```
/etc/apache2/
|-- apache2.conf
|   |-- ports.conf
|-- mods-enabled
|   |-- *.load
|   |-- *.conf
|-- conf-enabled
|   |-- *.conf
|-- sites-enabled
|   |-- *.conf
```

- `apache2.conf` is the main configuration file. It puts the pieces together by including all remaining configuration files when starting up the web server.
- `ports.conf` is always included from the main configuration file. It is used to determine the listening ports for incoming connections, and this file can be customized anytime.
- Configuration files in the `mods-enabled/`, `conf-enabled/` and `sites-enabled/` directories contain

{#fig:014 width=70%}

Прокручиваем страницу вниз и нажимаем на кнопку `create\reset database` (рис. 15)



Apache2 Debian Default Page

It works!

This is the default welcome page used to test the correct operation of the Apache2 server after installation on Debian systems. If you can read this page, it means that the Apache HTTP server installed at this site is working properly. You should **replace this file** (located at `/var/www/html/index.html`) before continuing to operate your HTTP server.

If you are a normal user of this web site and don't know what this page is about, this probably means that the site is currently unavailable due to maintenance. If the problem persists, please contact the site's administrator.

Configuration Overview

Debian's Apache2 default configuration is different from the upstream default configuration, and split into several files optimized for interaction with Debian tools. The configuration system is **fully documented in `/usr/share/doc/apache2/README.Debian.gz`**. Refer to this for the full documentation. Documentation for the web server itself can be found by accessing the **manual** if the `apache2-doc` package was installed on this server.

The configuration layout for an Apache2 web server installation on Debian systems is as follows:

```
/etc/apache2/
|-- apache2.conf
|   |-- ports.conf
|-- mods-enabled
|   |-- *.load
|   |-- *.conf
|-- conf-enabled
|   |-- *.conf
|-- sites-enabled
|   |-- *.conf
```

- `apache2.conf` is the main configuration file. It puts the pieces together by including all remaining configuration files when starting up the web server.
- `ports.conf` is always included from the main configuration file. It is used to determine the listening ports for incoming connections, and this file can be customized anytime.
- Configuration files in the `mods-enabled/`, `conf-enabled/` and `sites-enabled/` directories contain

{#fig:015 width=70%}

Авторизуюсь с помощью предложенных по умолчанию данных (рис. 16)



Username

admin

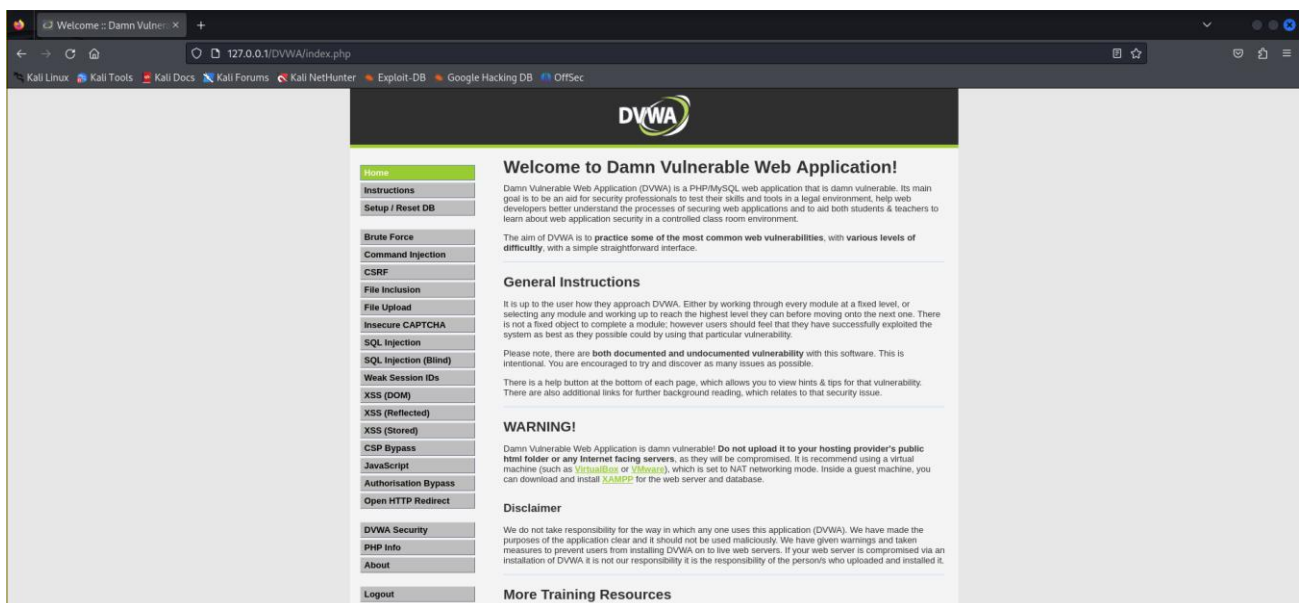
Password

••••••••

Login

{#fig:016 width=70%}

Оказываюсь на домашней странице веб-приложения, на этом установка окончена (рис. 17)



{#fig:017 width=70%}Выводы

Приобрела практические навыки по установке уязвимого веб-приложения DVWA.

Список литературы{.unnumbered}

::: {#refs}

:::