

# Индивидуальный проект, 2 этап

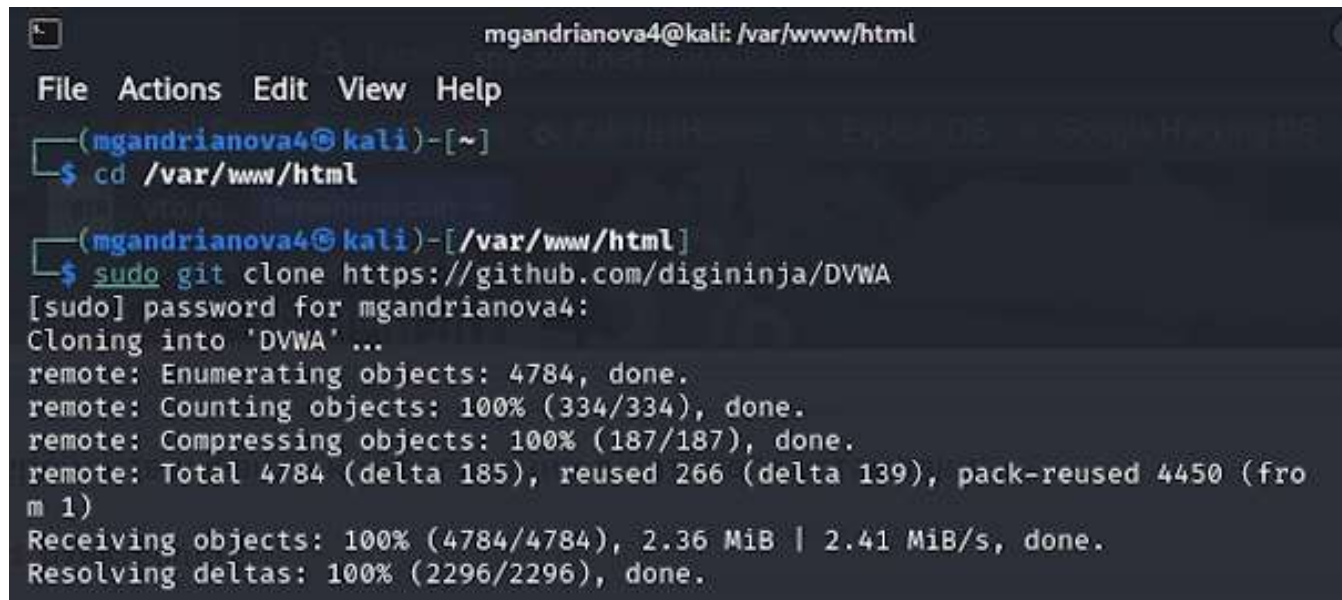
Андрианова Марина Георгиевна  
RUDN University, Moscow,  
Russian Federation  
2024, 21 September

# Цель работы

Целью данной работы является установка DVWA на дистрибутив Kali Linux.

# Выполнение 2-го этапа индивидуального проекта

Переходим в каталог html. Клонировем репозиторий git(рис.1).

A screenshot of a terminal window with a dark background. The window title is 'mgandrianova4@kali: /var/www/html'. The terminal shows a menu bar with 'File', 'Actions', 'Edit', 'View', and 'Help'. The user is in the directory '~' and runs 'cd /var/www/html'. Then, they run 'sudo git clone https://github.com/digininja/DVWA'. The terminal shows the password prompt '[sudo] password for mgandrianova4:' and the cloning progress: 'Cloning into 'DVWA' ...', 'remote: Enumerating objects: 4784, done.', 'remote: Counting objects: 100% (334/334), done.', 'remote: Compressing objects: 100% (187/187), done.', 'remote: Total 4784 (delta 185), reused 266 (delta 139), pack-reused 4450 (from 1)', 'Receiving objects: 100% (4784/4784), 2.36 MiB | 2.41 MiB/s, done.', and 'Resolving deltas: 100% (2296/2296), done.'

```
mgandrianova4@kali: /var/www/html
File Actions Edit View Help
(mgandrianova4@kali)-[~]
$ cd /var/www/html
(mgandrianova4@kali)-[/var/www/html]
$ sudo git clone https://github.com/digininja/DVWA
[sudo] password for mgandrianova4:
Cloning into 'DVWA' ...
remote: Enumerating objects: 4784, done.
remote: Counting objects: 100% (334/334), done.
remote: Compressing objects: 100% (187/187), done.
remote: Total 4784 (delta 185), reused 266 (delta 139), pack-reused 4450 (from 1)
Receiving objects: 100% (4784/4784), 2.36 MiB | 2.41 MiB/s, done.
Resolving deltas: 100% (2296/2296), done.
```

Рис.1. Переход в каталог и клонирование репозитория

Проверяем, что файлы скопировались правильно и изменяем права доступа к папке установки(рис.2).

```
(mgandrianova4@kali)-[/var/www/html]
$ ls
DVWA index.html index.nginx-debian.html

(mgandrianova4@kali)-[/var/www/html]
$ sudo chmod -R 777 DVWA
```

Рис.2. Изменение прав доступа

Переходим к файлу конфигурации в каталоге установки: /dvwa/config. Проверяем содержимое каталога (рис.3).

```
(mgandrianova4@kali)-[/var/www/html]
$ cd DVWA/config

(mgandrianova4@kali)-[/var/www/html/DVWA/config]
$ ls
config.inc.php.dist
```

Рис.3. Переход к файлу конфигурации

Копируем файл конфигурации (config.inc.php.dist) и переименовываем его на config.inc.php (рис.4).

```
(mgandrianova4@kali)-[/var/www/html/DVWA/config]
$ sudo cp config.inc.php.dist config.inc.php

(mgandrianova4@kali)-[/var/www/html/DVWA/config]
$ ls
config.inc.php  config.inc.php.dist
```

Рис.4. Копирование и переименование файла

Открываем файл настроек (рис.5) и изменяем пароль (рис.6).

```
(mgandrianova4@kali)-[/var/www/html/DVWA/config]
$ sudo nano config.inc.php
```

Рис.5. Открытие файла настроек

```
mgandrianova4@kali: /var/www/html/DVWA/config
File Actions Edit View Help
GNU nano 8.1 config.inc.php *
<?php

# If you are having problems connecting to the MySQL database and all of the variables below are correct
# try changing the 'db_server' variable from localhost to 127.0.0.1. Fixes a problem due to sockets.
# Thanks to @digininja for the fix.

# Database management system to use
$DBMS = 'MySQL';
# $DBMS = 'PGSQL'; // Currently disabled

# Database variables
# WARNING: The database specified under db_database WILL BE ENTIRELY DELETED during setup.
# Please use a database dedicated to DVWA.
#
# If you are using MariaDB then you cannot use root, you must use create a dedicated DVWA user.
# See README.md for more information on this.
$_DVWA = array();
$_DVWA[ 'db_server' ] = getenv( 'DB_SERVER' ) ?: '127.0.0.1';
$_DVWA[ 'db_database' ] = 'dvwa';
$_DVWA[ 'db_user' ] = 'mgdvwa';
$_DVWA[ 'db_password' ] = 'toor20';
$_DVWA[ 'db_port' ] = '3306';
```

Рис.6. Редактирование файла

Запускаем базу данных mysql и проверяем, запущен ли процесс (рис.7).

```
(mgandrianova4@kali)-[/var/www/html/DVWA/config]
$ cd /etc/php/8.2/apache2
(mgandrianova4@kali)-[/etc/php/8.2/apache2]
$ ls
conf.d  php.ini
(mgandrianova4@kali)-[/etc/php/8.2/apache2]
$ cd ~/
(mgandrianova4@kali)-[~]
$ sudo systemctl start mysql
(mgandrianova4@kali)-[~]
$ systemctl status mysql
● mariadb.service - MariaDB 11.4.3 database server
   Loaded: loaded (/usr/lib/systemd/system/mariadb.service; disabled; preset: disabled)
   Active: active (running) since Fri 2024-09-20 22:14:30 MSK; 19s ago
 Invocation: 5e947e3b7c9a405dab9d31ddd69c9321
    Docs: man:mariadb(8)
          https://mariadb.com/kb/en/library/systemd/
   Process: 9470 ExecStartPre=/usr/bin/install -m 755 -o mysql -g root -d /var/run/mysqld (code=exited, status=0/SUCCESS)
   Process: 9479 ExecStartPre=/bin/sh -c systemctl unset-environment _WSREP_START_POSITION (code=exited, status=0/SUCCESS)
   Process: 9481 ExecStartPre=/bin/sh -c [ ! -e /usr/bin/galera_recovery ] && VAR= || VAR="/usr/bin/galera_recovery"; [ $? -eq 0 ]   && systemctl set-environment _>
   Process: 9612 ExecStartPost=/bin/sh -c systemctl unset-environment _WSREP_START_POSITION (code=exited, status=0/SUCCESS)
   Process: 9614 ExecStartPost=/etc/mysql/debian-start (code=exited, status=0/SUCCESS)
  Main PID: 9541 (mariabdd)
```

Рис.7. Запуск mysql



Входим в базу данных от имени пользователя root. Появляется командная строка с приглашением "MariaDB"(рис.8).

```
(mgandrianova4@kali)~$ cd /var/www/html/DVWA/config
(mgandrianova4@kali)~/var/www/html/DVWA/config$ sudo mysql -u root -p
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)]> \h

General information about MariaDB can be found at
http://mariadb.org

List of all client commands:
Note that all text commands must be first on line and end with ';'
?          (\?) Synonym for 'help'.
charset    (\C) Switch to another charset. Might be needed for processing binlog with multi-byte charsets.
clear      (\c) Clear the current input statement.
connect    (\r) Reconnect to the server. Optional arguments are db and host.
delimiter  (\d) Set statement delimiter.
edit       (\e) Edit command with $EDITOR.
ego        (\G) Send command to MariaDB server, display result vertically.
exit       (\q) Exit mysql. Same as quit.
```

Рис.8. Вход в базу данных

Далее создаём в ней нового пользователя, используя учётные данные из файла config.inc.php. Также предоставляем пользователю привилегии для работы с этой базой данных (рис.9).

```
MariaDB [(none)]> create user 'mgdvwa'@'127.0.0.1' identified by 'toor20';  
Query OK, 0 rows affected (0.012 sec)  
  
MariaDB [(none)]> grant all privileges on dvwa.* to 'mgdvwa'@'127.0.0.1' identified by 'toor20';  
Query OK, 0 rows affected (0.006 sec)  
  
MariaDB [(none)]> exit  
Bye
```

Рис.9. MariaDB

Для настройки сервера apache2 переходим в соответствующую директорию (рис.10).

A terminal window with a dark background. The prompt is '(mgandrianova4@kali) - [/var/www/html/DVWA/config]'. The command '\$ cd /etc/php/8.2/apache2' is entered and highlighted in blue.

```
(mgandrianova4@kali) - [/var/www/html/DVWA/config]  
$ cd /etc/php/8.2/apache2
```

Рис.10. Переход в каталог apache2

Открываем для редактирования файл `php.ini` (рис.11), чтобы включить следующие параметры: `allow_url_fopen` и `allow_url_include`.

A terminal window with a dark background. The prompt is `(mgandrianova4@kali) - [/etc/php/8.2/apache2]`. The user has entered the command `$ sudo nano php.ini`.

```
(mgandrianova4@kali) - [/etc/php/8.2/apache2]  
$ sudo nano php.ini
```

Рис.11. Редактирование файла

Файл большой, поэтому нам потребовалось прокрутить до середины файла, чтобы добраться до `foren` и изменить значения "off" на 'on'(рис.12).

```
;;;;;;;;;;;;;;
; Fopen wrappers ;
;;;;;;;;;;;;;;

; Whether to allow the treatment of URLs (like http:// or ftp://) as files.
; https://php.net/allow-url-fopen
allow_url_fopen = On

; Whether to allow include/require to open URLs (like https:// or ftp://) as files.
; https://php.net/allow-url-include
allow_url_include = On
```

Рис.12. Fopen wrappers

Запускаем сервер Apache и проверяем, запущена ли служба(рис.13).

```
(mgandrianova4@kali)-[/etc/php/8.2/apache2]
$ sudo systemctl start apache2

(mgandrianova4@kali)-[/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 Fri 2024-09-20 22:26:01 MSK; 21s ago
 Invocation: 613646354449468c8b179a0e2cc08736
    Docs: https://httpd.apache.org/docs/2.4/
  Process: 15347 ExecStart=/usr/sbin/apachectl start (code=exited, status=0/SUCCESS)
 Main PID: 15371 (apache2)
   Tasks: 6 (limit: 4549)
  Memory: 21.7M (peak: 22.1M)
     CPU: 497ms
    CGroup: /system.slice/apache2.service
            └─15371 /usr/sbin/apache2 -k start
              └─15374 /usr/sbin/apache2 -k start
                └─15375 /usr/sbin/apache2 -k start
                  └─15376 /usr/sbin/apache2 -k start
                    └─15377 /usr/sbin/apache2 -k start
                      └─15378 /usr/sbin/apache2 -k start

Sep 20 22:26:00 kali systemd[1]: Starting apache2.service - The Apache HTTP Server ...
```

Рис.13. Запуск сервера Apache

Пробуем открыть DVWA в браузере. Перед нами открылась страница настройки, это означает, что мы успешно установили DVWA на Kali Linux(рис.14).

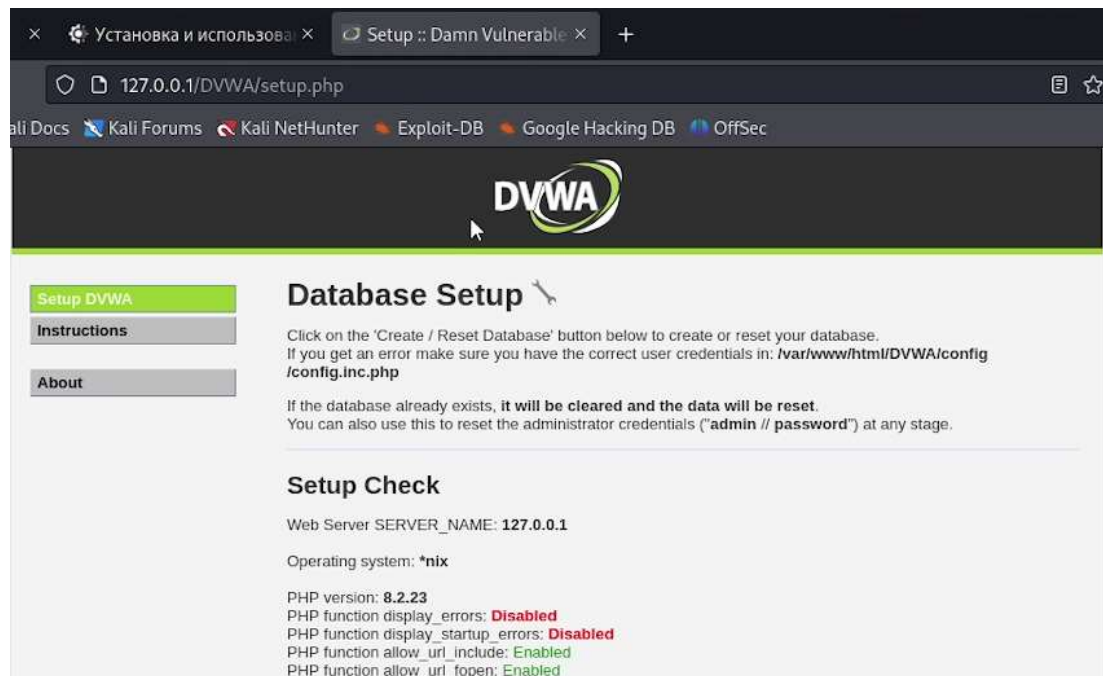


Рис.14. Запуск DVWA в браузере


Прокручиваем вниз и нажимаем "Create / Reset Database" (Создать / сбросить базу данных) (рис.15).



Рис.15. Создание базы данных



И через несколько секунд нас перенаправили на страницу входа в DVWA. Авторизуемся с помощью предложенных по умолчанию данных (рис.16).



The DVWA logo is centered at the top of the form. It consists of the letters 'DVWA' in a bold, dark grey sans-serif font. To the right of the text is a stylized circular graphic composed of two curved, overlapping lines, one in a light green color and the other in a dark grey color, creating a sense of motion or a sphere.

Username

Password

Login

Рис.16. Авторизация

Оказываемся на домашней странице веб-приложения. Можем заметить, что существует множество интересных уязвимостей, которые мы можем протестировать, например, брутфорс, SQL-инъекция и другие (рис.17). На этом установка окончена.



Рис.17. Домашняя страница DVWA

# Выводы

Установила веб-приложение DVWA на дистрибутив Kali Linux.