

# **отчёт по второму этапу индивидуального проекта**

**Установка DVWA**

Дарья Эдуардовна Ибатулина

# Содержание

<b>1</b>	<b>Цель работы</b>	<b>5</b>
<b>2</b>	<b>Задание</b>	<b>6</b>
<b>3</b>	<b>Теоретическое введение</b>	<b>7</b>
<b>4</b>	<b>Выполнение лабораторной работы</b>	<b>8</b>
<b>5</b>	<b>Выводы</b>	<b>15</b>
	<b>Список литературы</b>	<b>16</b>

## Список иллюстраций

4.1	Установка DVWA . . . . .	8
4.2	Перемещение утилиты DVWA в указанную директорию . . . . .	8
4.3	Проверка выполненных действий . . . . .	9
4.4	Запуск apache2 в терминале . . . . .	9
4.5	Запуск apache2 в браузере . . . . .	9
4.6	Копирование конфиг-файла в директорию . . . . .	10
4.7	Редактирование конфиг-файла . . . . .	10
4.8	Конфиг-файл . . . . .	11
4.9	Параметры DVWA в браузере . . . . .	11
4.10	Запуск сервиса mariadb . . . . .	12
4.11	Запуск mysql . . . . .	12
4.12	Создание базы данных . . . . .	12
4.13	Задание пароля от базы данных . . . . .	13
4.14	Переход в каталог . . . . .	13
4.15	Перезагрузка и установка нужного пакета . . . . .	13
4.16	Задание прав . . . . .	14
4.17	Задание прав #2 . . . . .	14
4.18	Проверка настроек . . . . .	14

## **Список таблиц**

# 1 Цель работы

Установить DVWA и произвести первичную настройку утилиты.

## 2 Задание

1. Произвести установку утилиты DVWA;
2. Настроить утилиту;
3. Проверить, всё ли установлено правильно.

## 3 Теоретическое введение

DVWA - это веб-приложение на PHP/MySQL, основная цель которого - стать помощником для профессионалов в области безопасности, чтобы проверить свои навыки и инструменты в легальной среде. Мы постарались сделать развертывание DVWA максимально простым и создали надстройку, которую можно легко применить к балансировщику нагрузки edgeNEXUS ALB-X.

## 4 Выполнение лабораторной работы

Клонирую репозиторий с DVWA на гитхабе (скачивается архив) (рис. [4.1]).

```
(deibatulina@deibatulina)-[~]
$ git clone https://github.com/digininja/DVWA.git
Cloning into 'DVWA' ...
remote: Enumerating objects: 4500, done.
remote: Counting objects: 100% (50/50), done.
remote: Compressing objects: 100% (39/39), done.
remote: Total 4500 (delta 17), reused 33 (delta 10), pack-reused 4450
Receiving objects: 100% (4500/4500), 2.30 MiB | 2.55 MiB/s, done.
Resolving deltas: 100% (2112/2112), done.

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

Рис. 4.1: Установка DVWA

Через учётную запись администратора перемещаю утилиту в указанную директорию (рис. [4.2]).

```
(deibatulina@deibatulina)-[~]
$ sudo mv DVWA /var/www/html
[sudo] password for deibatulina:
(deibatulina@deibatulina)-[~]
$
```

Рис. 4.2: Перемещение утилиты DVWA в указанную директорию

Произвожу проверку выполненных действий (рис. [4.3]).



```
(deibatulina@deibatulina)-[~]
$ cd /var/www/html

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

(deibatulina@deibatulina)-[/var/www/html]
$
```

Рис. 4.3: Проверка выполненных действий

Запускаю сервис *apache2* (рис. [4.4], [4.5]).

```
(deibatulina@deibatulina)-[/var/www/html]
$ sudo service apache2 start
```

Рис. 4.4: Запуск *apache2* в терминале

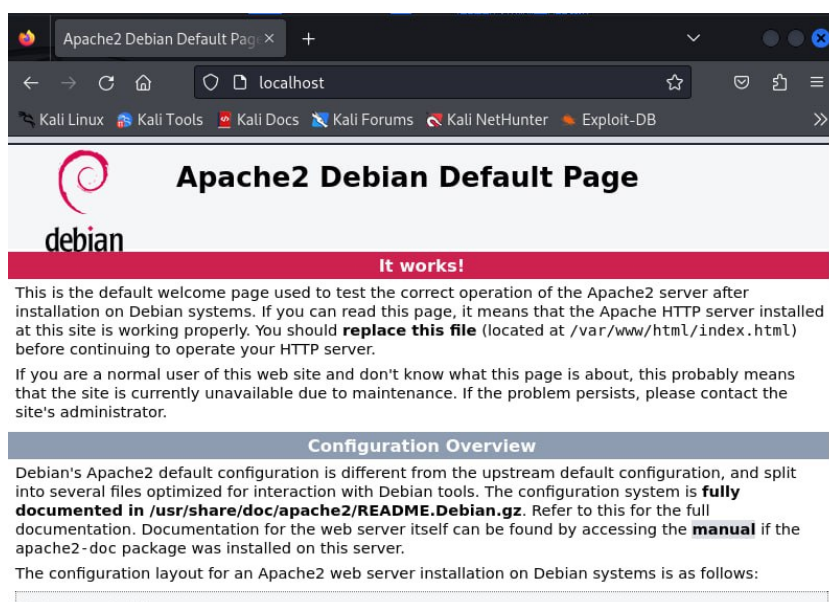


Рис. 4.5: Запуск *apache2* в браузере

Копирую конфигурационный файл в нужную директорию (рис. [4.6]).

```
(deibatulina@deibatulina)-[/var/www/html]
$ cd DVWA

(deibatulina@deibatulina)-[/var/www/html/DVWA]
$ ls
CHANGELOG.md  README.id.md  compose.yml  hackable  robots.txt
COPYING.txt   README.md     config       index.php  security.php
Dockerfile    README.pt.md  database     instructions.php  security.txt
README.ar.md  README.tr.md  docs        login.php  setup.php
README.es.md  README.zh.md  dvwa        logout.php tests
README.fa.md  SECURITY.md   external    php.ini   vulnerabilities
README.fr.md  about.php    favicon.ico  phpinfo.php

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

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

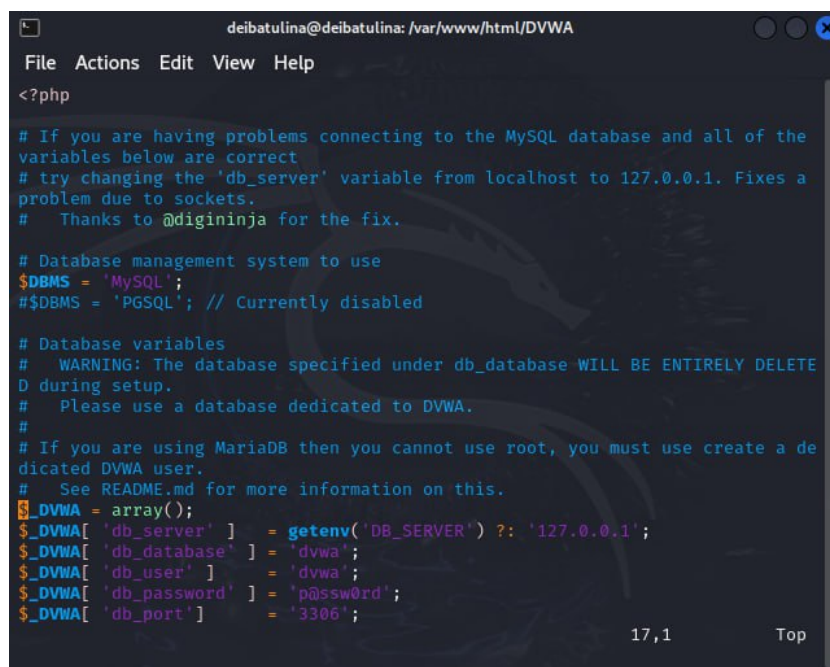
(deibatulina@deibatulina)-[/var/www/html/DVWA]
$
```

Рис. 4.6: Копирование конфиг-файла в директорию

Редактирую конфигурационный файл в текстовом редакторе *vim* (рис. [4.7], [4.8]).

```
(deibatulina@deibatulina)-[/var/www/html/DVWA]
$ vim config/config.inc.php
```

Рис. 4.7: Редактирование конфиг-файла



```
deibatulina@deibatulina: /var/www/html/DVWA
File Actions Edit View Help
<?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' ] = 'dvwa';
$_DVWA[ 'db_password' ] = 'p@ssw0rd';
$_DVWA[ 'db_port' ] = '3306';

17,1 Top
```

Рис. 4.8: Конфиг-файл

Проверяю выставленные параметры в браузере, логируюсь через учётную запись *admin* с паролем *password* (рис. [4.9]).

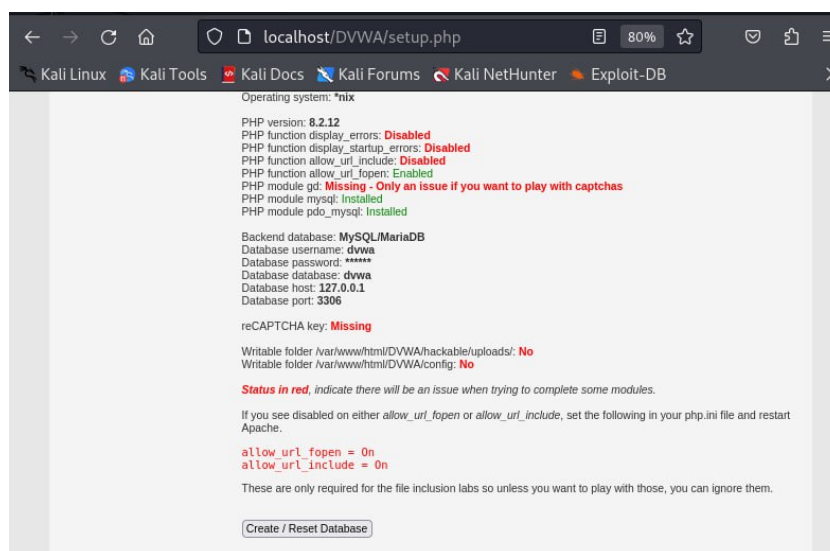


Рис. 4.9: Параметры DVWA в браузере

Запускаю сервис *mariadb* (рис. [4.10]).

```
(deibatulina@deibatulina)-[/var/www/html/DVWA]
$ service mariadb start

(deibatulina@deibatulina)-[/var/www/html/DVWA]
$
```

Рис. 4.10: Запуск сервиса mariadb

Переключившись на учетную запись администратора, запускаю mysql (рис. [4.11]).

```
(root@deibatulina)-[~]
# mysql
Welcome to the MariaDB monitor.  Commands end with ; or \g.
Your MariaDB connection id is 31
Server version: 10.11.6-MariaDB-2 Debian n/a

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

Type 'help;' or '\h' for help. Type '\c' to clear the current input statement
.

MariaDB [(none)]>
```

Рис. 4.11: Запуск mysql

Создаю базу данных (рис. [4.12]).

```
MariaDB [(none)]> create database dvwa;
Query OK, 1 row affected (0.000 sec)

MariaDB [(none)]> create user dvwa@localhost identified by 'p@ssw0rd';
ERROR 1396 (HY000): Operation CREATE USER failed for 'dvwa'@'localhost'
MariaDB [(none)]> drop user 'dvwa';
ERROR 1396 (HY000): Operation DROP USER failed for 'dvwa'@'%'
MariaDB [(none)]> drop user 'dvwa'@'localhost';
Query OK, 0 rows affected (0.009 sec)

MariaDB [(none)]> create user dvwa@localhost identified by 'p@ssw0rd';
Query OK, 0 rows affected (0.046 sec)

MariaDB [(none)]> grant all on dvwa.* to dvwa@localhost;
Query OK, 0 rows affected (0.007 sec)

MariaDB [(none)]> flush privileges;
Query OK, 0 rows affected (0.001 sec)

MariaDB [(none)]>
```

Рис. 4.12: Создание базы данных

Ввожу пароль от базы данных (рис. [4.13]).

```

(deibatulina@deibatulina)-[/home/deibatulina]
PS> mysql -u dvwa -p
Enter password:
Welcome to the MariaDB monitor.  Commands end with ; or \g.
Your MariaDB connection id is 38
Server version: 10.11.6-MariaDB-2 Debian n/a

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

Type 'help;' or '\h' for help. Type '\c' to clear the current input statement
.
MariaDB [(none)]> use dvwa;
Database changed
MariaDB [dvwa]>

```

Рис. 4.13: Задание пароля от базы данных

Настраиваю нужные параметры (рис. [4.14], [4.15], [4.16], [4.17]).

```

(deibatulina@deibatulina)-[/home/deibatulina]
PS> sudo su -
[sudo] password for deibatulina:
(root@deibatulina)-[~]
# cd /etc/php
(root@deibatulina)-[/etc/php]
# ls
8.2
(root@deibatulina)-[/etc/php]
# cd 8.2
(root@deibatulina)-[/etc/php/8.2]
# ls
apache2 cli mods-available
(root@deibatulina)-[/etc/php/8.2]
# cd apache2
(root@deibatulina)-[/etc/php/8.2/apache2]
# ls
conf.d php.ini
(root@deibatulina)-[/etc/php/8.2/apache2]
# vim php.ini

```

Рис. 4.14: Переход в каталог

```

(root@deibatulina)-[/etc/php/8.2/apache2]
# apachectl restart
(root@deibatulina)-[/etc/php/8.2/apache2]
# apt install php-gd

```

Рис. 4.15: Перезагрузка и установка нужного пакета

```

(root@deibatulina)-[/etc/php/8.2/apache2]
$ chown www-data /var/www/html/DVWA/hackable/uploads/

(root@deibatulina)-[/etc/php/8.2/apache2]
$ chmod 777 /var/www/html/DVWA/hackable/uploads/

(root@deibatulina)-[/etc/php/8.2/apache2]
$

```

Рис. 4.16: Задание прав

```

(root@deibatulina)-[/etc/php/8.2/apache2]
$ chown www-data /var/www/html/DVWA/config

(root@deibatulina)-[/etc/php/8.2/apache2]
$

```

Рис. 4.17: Задание прав #2

Проверяю выставленные настройки (рис. [4.18]).

[Home](#)
[Instructions](#)
[Setup / Reset DB](#)
[Brute Force](#)
[Command Injection](#)
[CSRF](#)
[File Inclusion](#)
[File Upload](#)
[Insecure CAPTCHA](#)
[SQL Injection](#)
[SQL Injection \(Blind\)](#)
[Weak Session IDs](#)
[XSS \(DOM\)](#)
[XSS \(Reflected\)](#)
[XSS \(Stored\)](#)
[CSP Bypass](#)
[JavaScript](#)
[Authorisation Bypass](#)
[Open HTTP Redirect](#)

## Database Setup

Click on the 'Create / Reset Database' button below to create or reset your database. If you get an error make sure you have the correct user credentials in: `/var/www/html/DVWA/config/config.inc.php`

If the database already exists, it will be cleared and the data will be reset. You can also use this to reset the administrator credentials ("admin // password") at any stage.

### Setup Check

Web Server SERVER\_NAME: localhost

Operating system: \*nix

PHP version: 8.2.12  
 PHP function display\_errors: Disabled  
 PHP function display\_startup\_errors: Disabled  
 PHP function allow\_url\_include: Enabled  
 PHP function allow\_url\_fopen: Enabled  
 PHP module gd: Installed  
 PHP module mysql: Installed  
 PHP module pdo\_mysql: Installed

Backend database: MySQL/MariaDB  
 Database username: dvwa  
 Database password: \*\*\*\*\*  
 Database database: dvwa  
 Database host: 127.0.0.1  
 Database port: 3306

reCAPTCHA key: Missing

Writable folder /var/www/html/DVWA/hackable/uploads/: Yes  
 Writable folder /var/www/html/DVWA/config: Yes

**Status in red**, indicate there will be an issue when trying to complete some modules.

If you see disabled on either `allow_url_fopen` or `allow_url_include`, set the following in your php.ini file and restart Apache.

`allow_url_fopen = On`  
`allow_url_include = On`

Рис. 4.18: Проверка настроек

## 5 Выводы

Установила DVWA и произвела её первичную настройку.

## **Список литературы**