

Отчёт о выполнении индивидуальный проект Этап 2

Установка DVWA

Акондзо Жордани Лади Гаэл

Содержание

1	Цель работы	5
2	Задание	6
3	Выполнение лабораторной работы	7
3.1	Установка необходимых зависимостей	7
3.2	Запуск служб Apache и MariaDB	8
3.3	Настройка MariaDB	8
3.4	Загрузка и настройка DVWA	9
3.5	Завершение установки DVWA	11
3.6	Окончательная настройка	12
4	Выводы	16

Список иллюстраций

3.1	Установка необходимых зависимостей	7
3.2	Запуск служб Apache и MariaDB	8
3.3	Запуск служб Apache и MariaDB	8
3.4	Настройка MariaDB	9
3.5	Загрузка и настройка DVWA	9
3.6	Загрузка и настройка DVWA	10
3.7	Загрузка и настройка DVWA	10
3.8	Загрузка и настройка DVWA	11
3.9	Завершение установки DVWA	12
3.10	Проверка настроек базы данных (Setup Check)	12
3.11	Уровень безопасности DVWA	13
3.12	Уровень безопасности DVWA	13
3.13	Изменения в файле php.ini	14
3.14	Изменения в файле php.ini	14
3.15	Изменения в файле php.ini	15

List of Tables

1 Цель работы

Научиться основным способам тестирования веб приложений

2 Задание

- Найти максимальное количество уязвимостей различных типов.
- Реализовать успешную эксплуатацию каждой уязвимости.

3 Выполнение лабораторной работы

3.1 Установка необходимых зависимостей

- DVWA требует наличия некоторых зависимостей для работы, таких как Apache, MariaDB (или MySQL), PHP и несколько модулей PHP (рис. 3.1).

```
(jordan@kali)~$ sudo apt install apache2 mariadb-server php php-mysql php-gd libapache2-mod-php -y
[sudo] password for jordan:
Note, selecting 'php8.2-mysql' instead of 'php-mysqli'
apache2 is already the newest version (2.4.62-1).
apache2 set to manually installed.
mariadb-server is already the newest version (1:11.4.3-1).
mariadb-server set to manually installed.
php is already the newest version (2:8.2+93+nm1).
php set to manually installed.
php8.2-mysql is already the newest version (8.2.23-1).
php8.2-mysql set to manually installed.
libapache2-mod-php is already the newest version (2:8.2+93+nm1).
libapache2-mod-php set to manually installed.
The following packages were automatically installed and are no longer required:
 fonts-liberation2      libpostproc57
 ibverbs-providers      libproxy1-plugin-gsettings
 libassuan0             libproxy1-plugin-networkmanager
 libavfilter9           libproxy1-plugin-webkit
 libboost-iostreams1.83.0 libpython3.11-dev
 libboost-thread1.83.0  librados2
 libcephfs2             librdmacm1t64
 libdisplay-info1       libusbmuxd6
 libgeos3.12.2          openjdk-17-jre
 libgfpapi0             openjdk-17-jre-headless
 libgfrpc0              python3-lib2to3
 libgfxdr0              python3.11
 libglusterfs0          python3.11-dev
 libibverbs1            python3.11-minimal
 libmobiledevice6       rwho
 libjsoncpp25           rwho
 libplacebo338          samba-vfs-modules
 libplist3
Use 'sudo apt autoremove' to remove them.
Installing:
 php-gd
Installing dependencies:
 php8.2-gd
Summary:
  Upgrading: 0, Installing: 2, Removing: 0, Not Upgrading: 156
  Download size: 33.0 kB
  Space needed: 154 kB / 62.9 GB available
Get:1 http://kali.download/kali kali-rolling/main amd64 php8.2-gd amd64 8.2.23-1 [29.2 kB]
Get:2 http://kali.download/kali kali-rolling/main amd64 php-gd all 2:8.2+93+nm1 [2776 B]
```

Рис. 3.1: Установка необходимых зависимостей

3.2 Запуск служб Apache и MariaDB

- Убедился, что службы Apache и MariaDB запущены (рис. 3.2).

```
(jordani@kali)-[~]
$ sudo systemctl start apache2

(jordani@kali)-[~]
$ sudo systemctl start mariadb

(jordani@kali)-[~]
$
```

Рис. 3.2: Запуск служб Apache и MariaDB

- Чтобы эти службы запускались автоматически при старте системы, выполнил следующие команды (рис. 3.3).

```
jordani@kali: ~
(jordani@kali)-[~]
$ sudo systemctl enable mariadb
Synchronizing state of mariadb.service with SysV service script with /usr/lib/systemd/systemd-sysv-install.
Executing: /usr/lib/systemd/systemd-sysv-install enable mariadb
Created symlink '/etc/systemd/system/multi-user.target.wants/mariadb.service' → '/usr/lib/systemd/system/mariadb.service'.

(jordani@kali)-[~]
$ sudo systemctl enable apache2
Synchronizing state of apache2.service with SysV service script with /usr/lib/systemd/systemd-sysv-install.
Executing: /usr/lib/systemd/systemd-sysv-install enable apache2
Created symlink '/etc/systemd/system/multi-user.target.wants/apache2.service' → '/usr/lib/systemd/system/apache2.service'.

(jordani@kali)-[~]
$
```

Рис. 3.3: Запуск служб Apache и MariaDB

3.3 Настройка MariaDB

- Подключусь к MariaDB для создания базы данных и пользователя для DVWA. Потом в командной строке MariaDB выполнил следующие команды (рис. 3.4).


```
jordani@kali: ~  
(jordani@kali)-[~]  
$ 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)]> create database dvwa;  
Query OK, 1 row affected (0.001 sec)  
  
MariaDB [(none)]> create user dvwa@localhost identified by 'Jordanigael7';  
Query OK, 0 rows affected (0.315 sec)  
  
MariaDB [(none)]> grant all on dvwa.* to dvwa@localhost;  
Query OK, 0 rows affected (0.004 sec)  
  
MariaDB [(none)]> flush privileges;  
Query OK, 0 rows affected (0.002 sec)  
  
MariaDB [(none)]>
```

Рис. 3.4: Настройка MariaDB


3.4 Загрузка и настройка DVWA

- Скачайл последнюю версию DVWA из репозитория GitHub (рис. 3.5).

```
(jordani@kali)-[~]  
$ cd /var/www/html  
  
(jordani@kali)-[/var/www/html]  
$ sudo git clone https://github.com/digininja/DVWA.git  
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 | 602.00 KiB/s, done.  
Resolving deltas: 100% (2296/2296), done.  
  
(jordani@kali)-[/var/www/html]  
$
```

Рис. 3.5: Загрузка и настройка DVWA


- Потом создал файл конфигурации для DVWA (рис. 3.6).



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

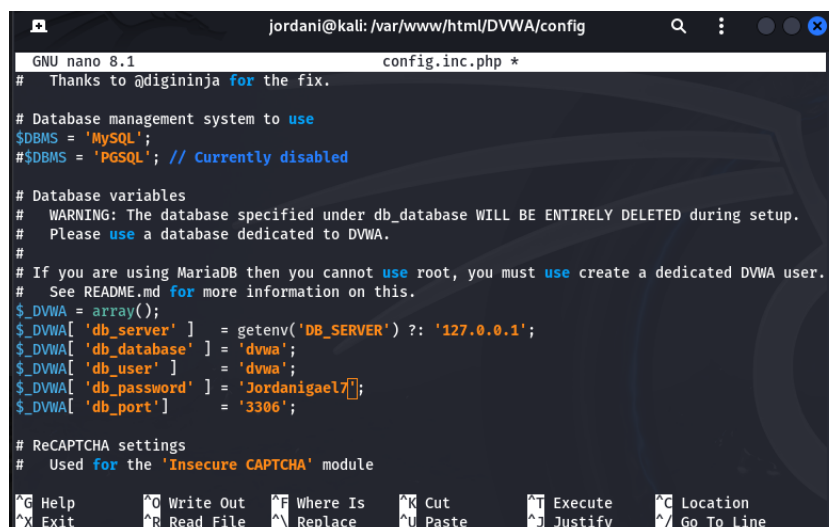
Рис. 3.6: Загрузка и настройка DVWA

- Открыл этот файл для редактирования и внёс изменения в информацию о базе данных (рис. 3.8) и (рис. 3.7).



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

Рис. 3.7: Загрузка и настройка DVWA



```
GNU nano 8.1 config.inc.php *
# 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'] = 'Jordanigael7';
$_DVWA['db_port'] = '3306';

# ReCAPTCHA settings
# Used for the 'Insecure CAPTCHA' module

^G Help      ^O Write Out  ^F Where Is   ^K Cut        ^I Execute    ^C Location
^X Exit      ^R Read File  ^\ Replace    ^U Paste      ^J Justify    ^_ Go To Line
```

Рис. 3.8: Загрузка и настройка DVWA

3.5 Завершение установки DVWA

- Потос открыл браузер и перешёл по адресу: <http://localhost/DVWA/setup.php>. Следовал инструкциям на странице для завершения установки. По окончании установки, вошёл в DVWA, используя следующие данные для входа (рис. 3.9):

Логин: admin

Пароль: password

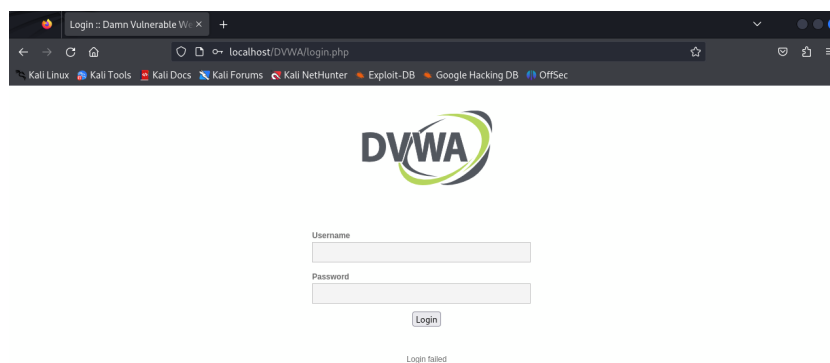


Рис. 3.9: Завершение установки DVWA

3.6 Окончательная настройка

- Проверка настроек базы данных (Setup Check) (рис. 3.10).

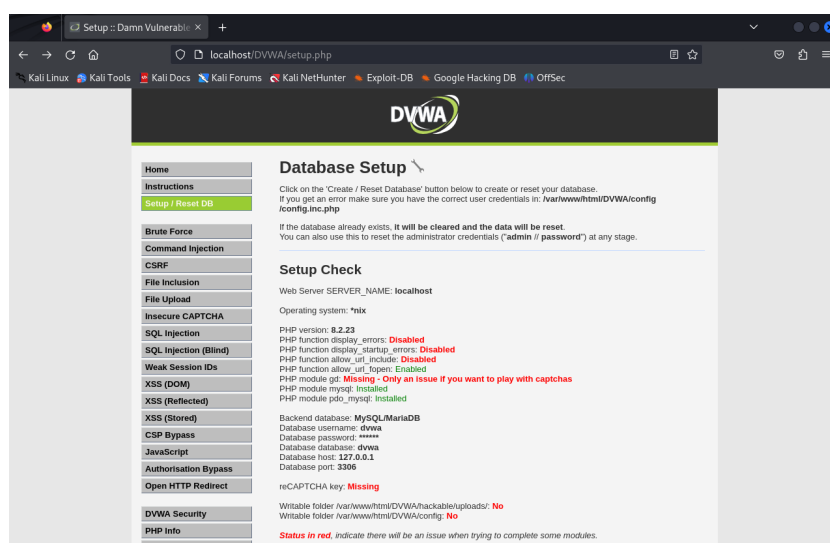


Рис. 3.10: Проверка настроек базы данных (Setup Check)

- **Уровень безопасности DVWA:** Протестировал несколько уровней безопасности, начиная с Impossible, где все уязвимости заблокированы, и продол-

жив с Low, который позволяет изучать наиболее распространенные уязвимости без каких-либо мер безопасности (рис. 3.11) и (рис. 3.12).

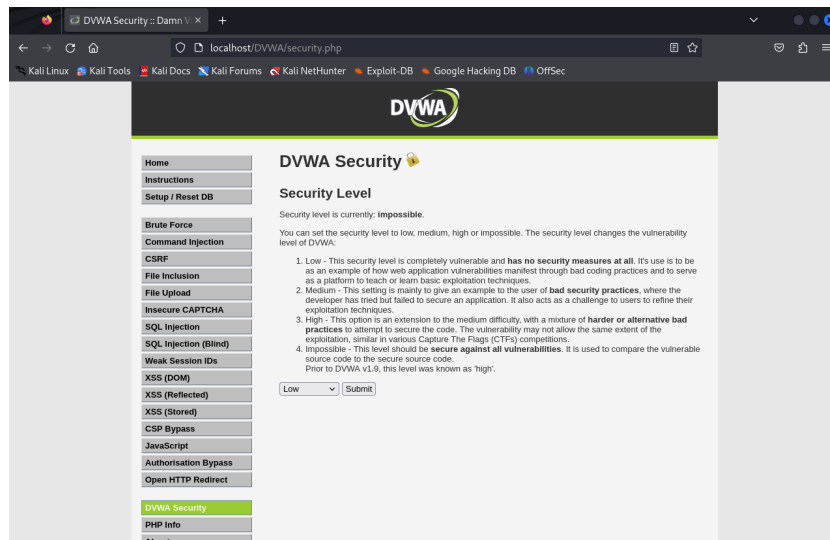


Рис. 3.11: Уровень безопасности DVWA

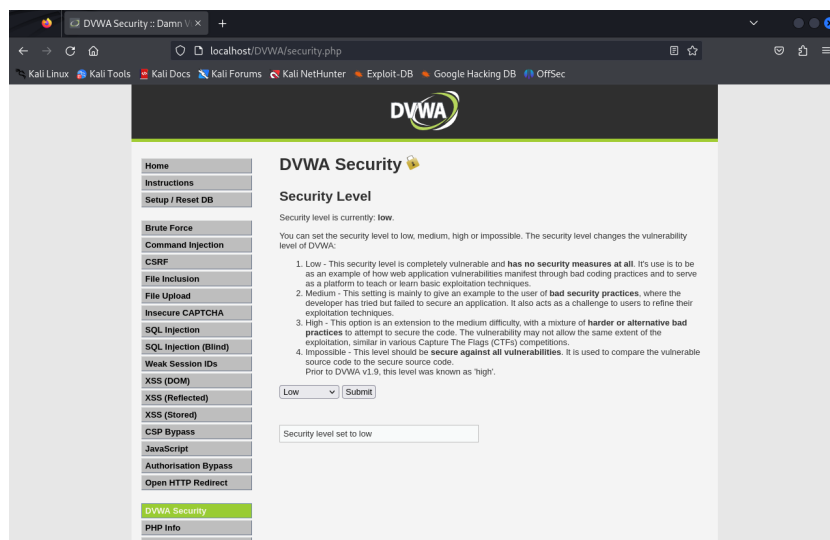


Рис. 3.12: Уровень безопасности DVWA

- **Изменения в файле `php.ini`:** Параметры `allow_url_fopen = On` и `allow_url_include = On` были включены, что важно для тестирования уязвимостей, связанных с включением локальных или удалённых файлов (LFI/RFI) (рис. 3.13), (рис. 3.14) и (рис. 3.15).

```
root@kali: /etc/php/8.2/apache2

$ sudo su -
[sudo] password for jordani:
(root@kali)~]
# cd /etc/php

(root@kali)-[/etc/php]
# ls
8.2

(root@kali)-[/etc/php]
# cd 8.2

(root@kali)-[/etc/php/8.2]
# ls
apache2 cli mods-available

(root@kali)-[/etc/php/8.2]
# cd apache2

(root@kali)-[/etc/php/8.2/apache2]
# ls
conf.d php.ini

(root@kali)-[/etc/php/8.2/apache2]
#
```

Рис. 3.13: Изменения в файле php.ini

```
root@kali: /etc/php/8.2/apache2

(root@kali)-[/etc/php/8.2/apache2]
# apachectl restart
AH00558: apache2: Could not reliably determine the server's fully qualified domain name, using 127.0.1.1. Set the 'ServerName' directive globally to suppress this message

(root@kali)-[/etc/php/8.2/apache2]
# id www-data
uid=33(www-data) gid=33(www-data) groups=33(www-data)

(root@kali)-[/etc/php/8.2/apache2]
# ls -al /var/www/html/DVWA/hackable/uploads/
total 12
drwxr-xr-x 2 root root 4096 Sep 21 19:46 .
drwxr-xr-x 5 root root 4096 Sep 21 19:46 ..
-rw-r--r-- 1 root root 667 Sep 21 19:46 dvwa_email.png

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

(root@kali)-[/etc/php/8.2/apache2]
# ls -al /var/www/html/DVWA/hackable/uploads/
total 12
drwxr-xr-x 2 www-data root 4096 Sep 21 19:46 .
drwxr-xr-x 5 root root 4096 Sep 21 19:46 ..
-rw-r--r-- 1 root root 667 Sep 21 19:46 dvwa_email.png

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

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

(root@kali)-[/etc/php/8.2/apache2]
#
```

Рис. 3.14: Изменения в файле php.ini

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

DVWA Security

PHP Info

About

Logout

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: 8.2.23
 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`

These are only required for the file inclusion labs so unless you want to play with those, you can ignore them.

Рис. 3.15: Изменения в файле php.ini

4 Выводы

На этом этапе я научился устанавливать и настраивать DVWA на Kali Linux. Я освоил конфигурацию баз данных, работу с Apache и MariaDB, а также внес необходимые изменения в настройки PHP для тестирования уязвимостей. Изучение разных уровней безопасности в DVWA позволило понять, как плохие практики разработки делают приложения уязвимыми для атак.