

Второй этап индивидуального проекта

Установка DVWA

Вакутайпа М.

16 марта 2025

Российский университет дружбы народов, Москва, Россия

Информация

- Вакутайпа Милдред
- НКАбд 02-23
- Факультет Физико-математических и естественных наук
- Российский университет дружбы народов
- 1032239009@rudn.ru
- <https://wakutaipa.github.io/ru/>

Цель работы

Получить практические навыки по установке DVWA.

Задание

1. Установить DVWA.

Выполнение лабораторной работы

Открою github и захожу в репозиторий dvwa и копирую ссылку.

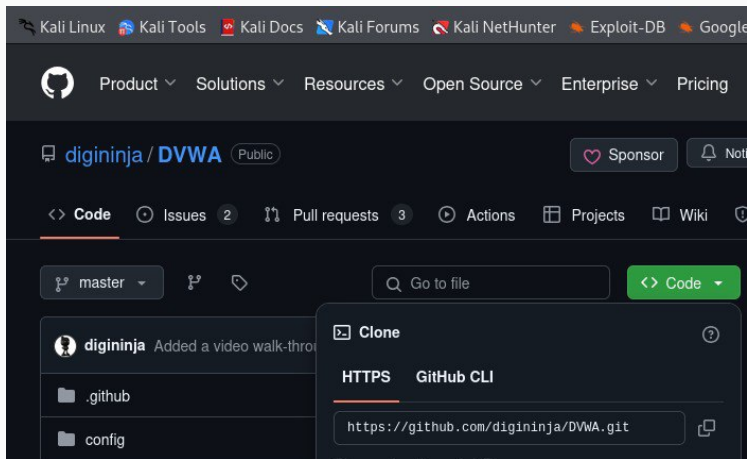
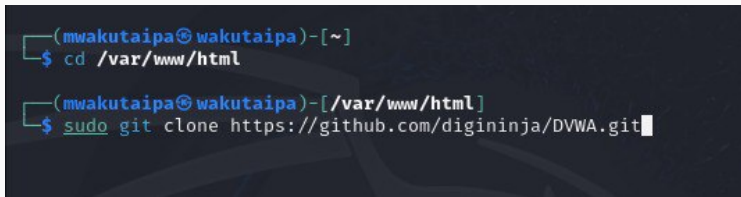


Рис. 1: репозиторий DVWA

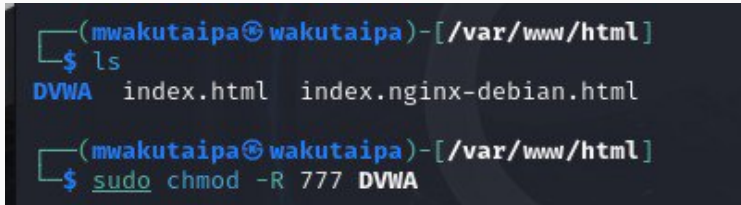
Открою терминал, и с помощью `cd`, вхожу в директорию `html`, где сохраняются файлы локального хоста. В этой же директории клонирую репозиторий.

A terminal window with a dark background and light-colored text. The prompt is `(mwakutaipa@wakutaipa)-[~]`. The first command entered is `$ cd /var/www/html`. The second prompt is `(mwakutaipa@wakutaipa)-[/var/www/html]`. The second command entered is `$ sudo git clone https://github.com/digininja/DVWA.git`, followed by a cursor.

```
(mwakutaipa@wakutaipa)-[~]  
$ cd /var/www/html  
  
(mwakutaipa@wakutaipa)-[/var/www/html]  
$ sudo git clone https://github.com/digininja/DVWA.git
```

Рис. 2: Клонирование DVWA в /html

С помощью ls проверю, что клонирование было успешно и потом разрешаю все права на все файлы в DVWA используя chmod -R 777

A terminal window with a dark background. The prompt is (mwakutaipa@wakutaipa)-[/var/www/html]. The user enters 'ls' and the output is 'DVWA index.html index.nginx-debian.html'. Then the user enters 'sudo chmod -R 777 DVWA'.

```
(mwakutaipa@wakutaipa)-[/var/www/html]  
$ ls  
DVWA index.html index.nginx-debian.html  
  
(mwakutaipa@wakutaipa)-[/var/www/html]  
$ sudo chmod -R 777 DVWA
```

Рис. 3: chmod -R 777

Проверяю работу и захожу в dvwa/config, чтобы настроить веб-приложение.

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

(mwakutaipa@wakutaipa)-[/var/www/html/DVWA]
$ cd config
```

Рис. 4: директория config

Далее копирую config.int.php который содержит конфигурацию приложения.

A terminal window with a dark background and light-colored text. The prompt is (mwakutaipa@wakutaipa)-[/var/www/html/DVWA/config]. The first command is \$ cp config.inc.php.dist config.inc.php. The second command is \$ ls, followed by the output config.inc.php config.inc.php.dist.

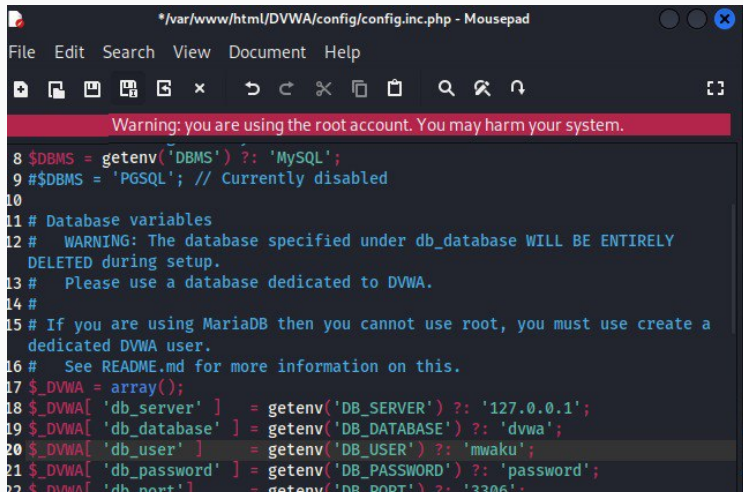
```
(mwakutaipa@wakutaipa)-[/var/www/html/DVWA/config]
$ cp config.inc.php.dist config.inc.php

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

Рис. 5: копирование config.int.php

редактирование файла конфигурации

В этом файле изменяю пароль, имя пользователя на mwaku и создаю базу данных waku и сохраняю изменения.



```
8 $DBMS = getenv('DBMS') ?: 'MySQL';
9 # $DBMS = 'PGSQL'; // Currently disabled
10
11 # Database variables
12 # WARNING: The database specified under db_database WILL BE ENTIRELY
13 # DELETED during setup.
14 # Please use a database dedicated to DVWA.
15 # If you are using MariaDB then you cannot use root, you must use create a
16 # dedicated DVWA user.
17 # See README.md for more information on this.
18 $DVWA = array();
19 $DVWA['db_server'] = getenv('DB_SERVER') ?: '127.0.0.1';
20 $DVWA['db_database'] = getenv('DB_DATABASE') ?: 'dvwa';
21 $DVWA['db_user'] = getenv('DB_USER') ?: 'mwaku';
22 $DVWA['db_password'] = getenv('DB_PASSWORD') ?: 'password';
23 $DVWA['db_port'] = getenv('DB_PORT') ?: '3306';
```

Запускаю mysql с помощью `start mysql` и проверяю используя `status mysql`.



```
(mwakutaipa@wakutaipa)-[/var/www/html/DVWA/config]
$ sudo systemctl start mysql

(mwakutaipa@wakutaipa)-[/var/www/html/DVWA/config]
$ sudo systemctl status mysql
```

Рис. 7: Запуск mysql

```
● mariadb.service - MariaDB 11.4.3 database server
   Loaded: loaded (/usr/lib/systemd/system/mariadb.service; disabled; pres>
   Active: active (running) since Thu 2025-03-06 21:17:59 MSK; 39s ago
   Invocation: 040abb6c83334f3f82b8c46746dd36fe
   Docs: man:mariadbd(8)
```

Рис. 8: проверка работы mysql

Далее я захожу в mysql используя `mysql -u root -p`

```
(mwakutaipa@wakutaipa) - [/var/www/html/DVWA/config]
$ sudo su
(root@wakutaipa) - [/var/www/html/DVWA/config]
# 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

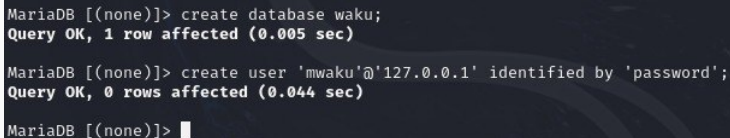
Copyright (c) 2000, 2018, Oracle, MariaDB Corporation Ab and others.

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)]> █
```

Рис. 9: вход в mysql

Создаю базу данных waku и нового пользователя используя create user 'mwaku'@'127.0.0.1' identified by 'password'. Используя эту команду, создала пользователя mwaku, работающего на сервер локального хоста (127.0.0.1) и пароль password.



```
MariaDB [(none)]> create database waku;  
Query OK, 1 row affected (0.005 sec)  
  
MariaDB [(none)]> create user 'mwaku'@'127.0.0.1' identified by 'password';  
Query OK, 0 rows affected (0.044 sec)  
  
MariaDB [(none)]> █
```

Рис. 10: создание пользоателя

Разрешаю все права доступа этому пользователю к базе данных и завершаю работы.

```
MariaDB [(none)]> grant all privileges on waku.* to 'mwaku'@'127.0.0.1';  
Query OK, 0 rows affected (0.012 sec)  
  
MariaDB [(none)]> exit
```

Рис. 11: Разрешение права

Запускаю сервер apache2.

A terminal window with a dark background. The prompt is '(root@wakutaipa)-[/var/www/html/DVWA/config]'. The command '# systemctl start apache2' has been entered. The prompt is repeated on the next line, followed by a red hash symbol and a white cursor block.

```
(root@wakutaipa)-[/var/www/html/DVWA/config]
# systemctl start apache2

(root@wakutaipa)-[/var/www/html/DVWA/config]
# █
```

Рис. 12: Запуск apache2

Далее вхожу в /etc/php/8.2.

```
(root@wakutaipa)-[/var/www/html/DVWA/config]
# cd /etc/php

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

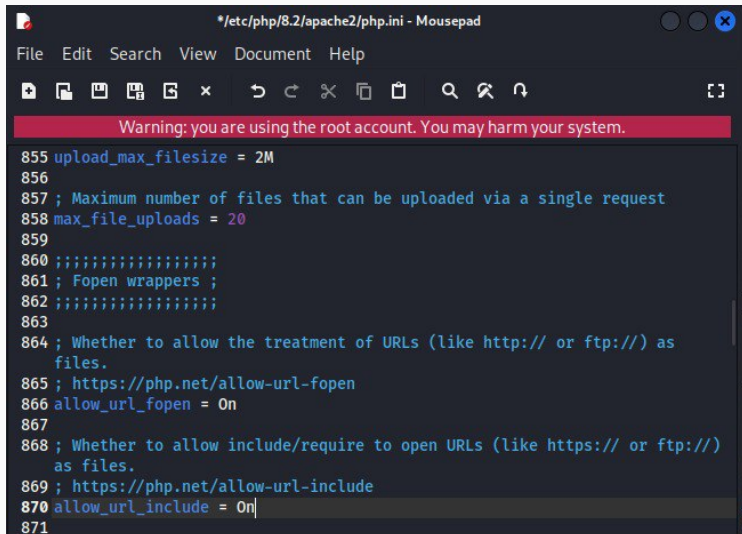
(root@wakutaipa)-[/etc/php]
# cd 8.2

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

Рис. 13: вход в /etc/php/8.2

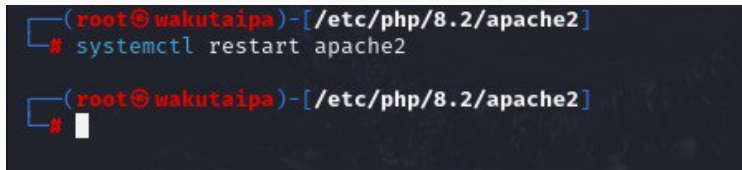
Включение allow_url

Включаю значения allow_url_fopen и allow_url_include в файле apache2/php.ini.



```
855 upload_max_filesize = 2M
856
857 ; Maximum number of files that can be uploaded via a single request
858 max_file_uploads = 20
859
860 ;;;;;;;;;;;;;;;;;
861 ; Fopen wrappers ;
862 ;;;;;;;;;;;;;;;;;
863
864 ; Whether to allow the treatment of URLs (like http:// or ftp://) as
   files.
865 ; https://php.net/allow-url-fopen
866 allow_url_fopen = On
867
868 ; Whether to allow include/require to open URLs (like https:// or ftp://)
   as files.
869 ; https://php.net/allow-url-include
870 allow_url_include = On
871
```

Перезапускаю сервер apache2 используя `systemctl restart apache2`.

A terminal window with a dark background. The prompt is `(root@wakutaipa) - [/etc/php/8.2/apache2]`. The command `# systemctl restart apache2` has been entered. Below it, the prompt is repeated, and a white cursor is visible at the end of the line.

```
(root@wakutaipa) - [/etc/php/8.2/apache2]
# systemctl restart apache2

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

Рис. 15: Перезапуск apache2

Открою 127.0.0.1./dvwa/setup.php в браузере.

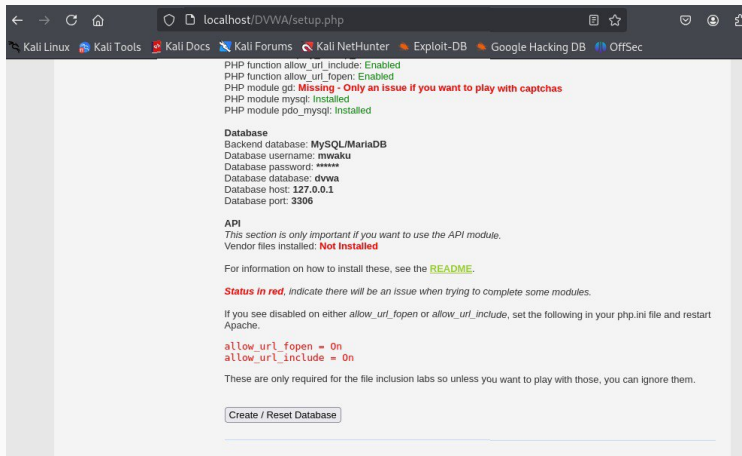



Рис. 16: страница веб-приложения

Нажимаю кнопку create/Reset database. Создается базу данных и мне перенаправляют на страницу входа. Вхожу используя логин admin и пароль p@ssword.



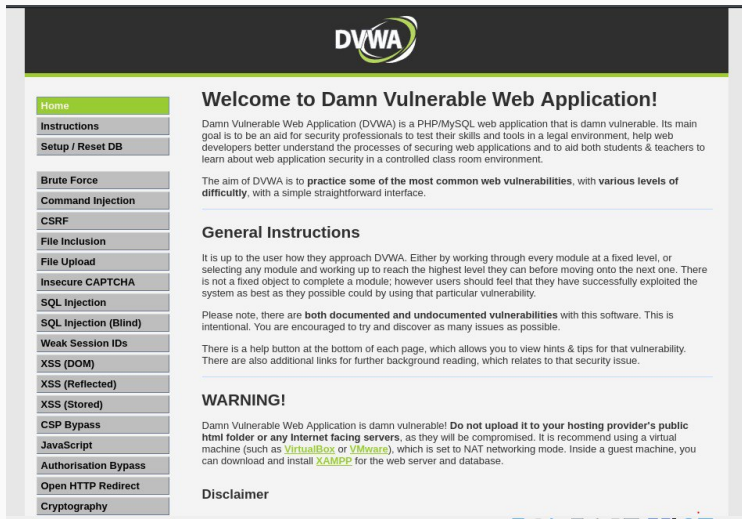
The DVWA logo features the text "DVWA" in a bold, dark grey sans-serif font. To the right of the text is a stylized graphic consisting of two curved, overlapping shapes: a light green one in the foreground and a dark grey one behind it, resembling a swoosh or a stylized 'D'.

Username

Password

Login

После входа попадаем на домашнюю страницу dvwa.



DVWA

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

Cryptography

Welcome to Damn Vulnerable Web Application!

Damn Vulnerable Web Application (DVWA) is a PHP/MySQL web application that is damn vulnerable. Its main goal is to be an aid for security professionals to test their skills and tools in a legal environment, help web developers better understand the processes of securing web applications and to aid both students & teachers to learn about web application security in a controlled class room environment.

The aim of DVWA is to **practice some of the most common web vulnerabilities**, with **various levels of difficulty**, with a simple straightforward interface.

General Instructions

It is up to the user how they approach DVWA. Either by working through every module at a fixed level, or selecting any module and working up to reach the highest level they can before moving onto the next one. There is not a fixed object to complete a module; however users should feel that they have successfully exploited the system as best as they possible could by using that particular vulnerability.

Please note, there are **both documented and undocumented vulnerabilities** with this software. This is intentional. You are encouraged to try and discover as many issues as possible.

There is a help button at the bottom of each page, which allows you to view hints & tips for that vulnerability. There are also additional links for further background reading, which relates to that security issue.

WARNING!

Damn Vulnerable Web Application is damn vulnerable! **Do not upload it to your hosting provider's public html folder or any internet facing servers**, as they will be compromised. It is recommend using a virtual machine (such as [VirtualBox](#) or [VMware](#)), which is set to NAT networking mode. Inside a guest machine, you can download and install [XAMPP](#) for the web server and database.

Disclaimer

Выводы

Получила навыки по установке DVWA.

Список литературы

Set up DVWA in Kali

Linux][<https://akshaygupta21.medium.com/how-to-setup-dvwa-in-kali-linux-e7c0dc272bba>]