

# Информационная безопасность

Индивидуальный проект №2

---

Матюшкин Д. В.

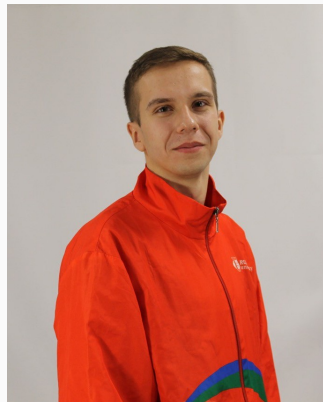
19 сентября 2024

Российский университет дружбы народов, Москва, Россия

## Информация

---

- Матюшкин Денис Владимирович
- студент 4-го курса
- группа НПИбд-02-21
- Российский университет дружбы народов
- 1032212279@pfur.ru
- <https://stifell.github.io/ru/>



## Цель работы

---

- Целью данной работы является установка DVWA в гостевую систему к Kali Linux.

## Выполнение лабораторной работы

---

# 1. Клонирование репозитория

```
(dvmatyushkin@dvmatyushkin)-[~]  
$ cd /var/www/html  
  
(dvmatyushkin@dvmatyushkin)-[/var/www/html]  
$ sudo git clone https://github.com/digininja/DVWA.git  
  
[sudo] password for dvmatyushkin:  
Cloning into 'DVWA' ...  
remote: Enumerating objects: 4758, done.  
remote: Counting objects: 100% (308/308), done.  
remote: Compressing objects: 100% (180/180), done.  
remote: Total 4758 (delta 167), reused 241 (delta 122), pack-reused 4450 (from 1)  
Receiving objects: 100% (4758/4758), 2.39 MiB | 4.20 MiB/s, done.  
Resolving deltas: 100% (2262/2262), done.
```

Рис. 1: Клонирование репозитория dvwa

## 2. Работа с правами доступа и клонирование файла

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

(dvmatyushkin@dvmatyushkin)-[/var/www/html]
$
cd DVWA/config

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

Рис. 2: Копирование файла конфигурации



### 3. Замена пароля

```
$_DVWA = array();  
$_DVWA[ 'db_server' ] = getenv( 'DB_SERVER' ) ?: '127.0.0.1';  
$_DVWA[ 'db_database' ] = 'dvwa';  
$_DVWA[ 'db_user' ] = 'dvwa';  
$_DVWA[ 'db_password' ] = 'pass';  
$_DVWA[ 'db_port' ] = '3306';
```

Рис. 3: Новый пароль

## 4. Установка mariadb

```
(dvmatyushkin@dvmatyushkin)-[/var/www/html/DVWA/config]
$ sudo apt-get update
Hit:1 http://http.kali.org/kali kali-rolling InRelease
Reading package lists ... Done

(dvmatyushkin@dvmatyushkin)-[/var/www/html/DVWA/config]
$ sudo apt-get -y install apache2 mariadb-server php php-mysqli php-gd libapache2-mod-php

Reading package lists ... Done
Building dependency tree ... Done
```

Рис. 4: Установка утилит

## 5. Создание нового пользователя mariadb

```
(dvmatyushkin@dvmatyushkin)-[/var/www/html/DVWA/config]
$ sudo service mysql start

(dvmatyushkin@dvmatyushkin)-[/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)]> create user 'dvwa'@'127.0.0.1' identified by 'pass';
Query OK, 0 rows affected (0.005 sec)

MariaDB [(none)]> grant all privileges on dvwa.* to 'dvwa'@'127.0.0.1' identified by 'pass';
Query OK, 0 rows affected (0.005 sec)
```

Рис. 5: Новый пользователь БД

## 6. Включение параметров

```
; 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. 6: Редактирование файла php.ini

## 7. Запуск утилиты

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

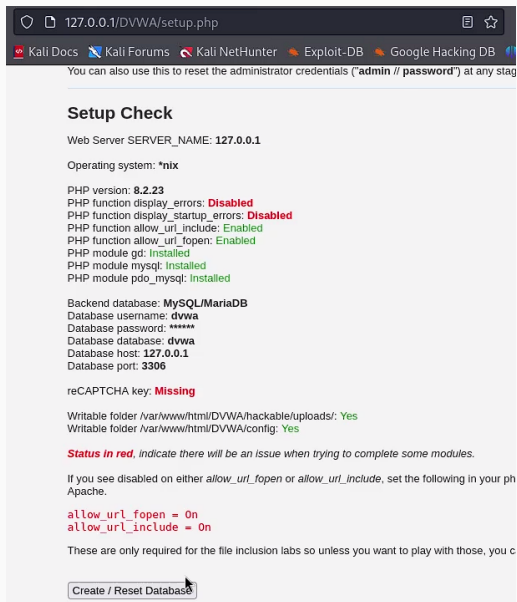
(dvmatyushkin@dvmatyushkin)-[/etc/php/8.2/apache2]
$ sudo mousepad php.ini

(dvmatyushkin@dvmatyushkin)-[/etc/php/8.2/apache2]
$ sudo service apache2 start

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

Рис. 7: Запуск apache2

## 8. Запуск dvwa и создание базы данных



The screenshot shows a web browser window with the address bar displaying "127.0.0.1/DVWA/setup.php". The browser's tab bar includes links to "Kali Docs", "Kali Forums", "Kali NetHunter", "Exploit-DB", and "Google Hacking DB". Below the address bar, a message states: "You can also use this to reset the administrator credentials ("admin // password") at any stag". The main content area is titled "Setup Check" and lists various system and configuration details. It includes the web server name (127.0.0.1), operating system (\*nix), PHP version (8.2.23), and the status of various PHP functions and modules. The backend database is identified as MySQL/MariaDB, with the username 'dvwa' and password '\*\*\*\*\*'. The database name is 'dvwa', the host is '127.0.0.1', and the port is '3306'. A reCAPTCHA key is listed as 'Missing'. Writable folders for uploads and config are both confirmed as 'Yes'. A note in red text explains that 'Status in red' indicates potential issues. Instructions are provided for disabling 'allow\_url\_fopen' or 'allow\_url\_include' in the php.ini file if needed. At the bottom, a button labeled "Create / Reset Database" is visible, with a mouse cursor hovering over it.

127.0.0.1/DVWA/setup.php

You can also use this to reset the administrator credentials ("admin // password") at any stag

### Setup Check

Web Server SERVER\_NAME: 127.0.0.1

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

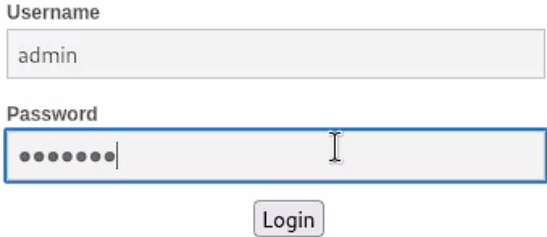
**Status in red**, indicate there will be an issue when trying to complete some modules.

If you see disabled on either `allow_url_fopen` or `allow_url_include`, set the following in your php 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 c

Create / Reset Database



A login form with two input fields and a button. The first field is labeled 'Username' and contains the text 'admin'. The second field is labeled 'Password' and contains ten dots, with a cursor at the end. Below the fields is a button labeled 'Login'.

Username

admin

Password

.....

Login

Рис. 9: Вход в dvwa

## Выводы

---



В ходе данной лабораторной работы мы установили DVWA в гостевую систему к Kali Linux.