# Индивидуальный проект

## Этап 2. Установка DVWA

Крутова Е. Д.

07 сентября 2024

Российский университет дружбы народов, Москва, Россия

# Информация

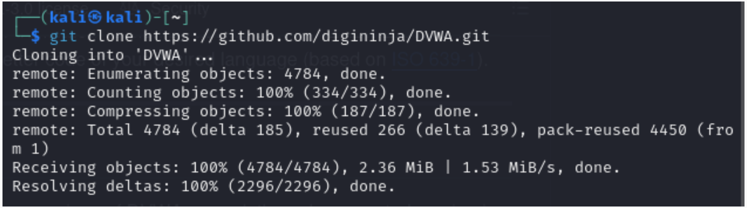
## Докладчик

- Крутова Екатерина Дмитриевна
- студентка группы НПИбд-01-21
- Российский университет дружбы народов
- 1032216536@pfur.ru
- https://edkrutova.github.io/ru/

# Цель работы

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

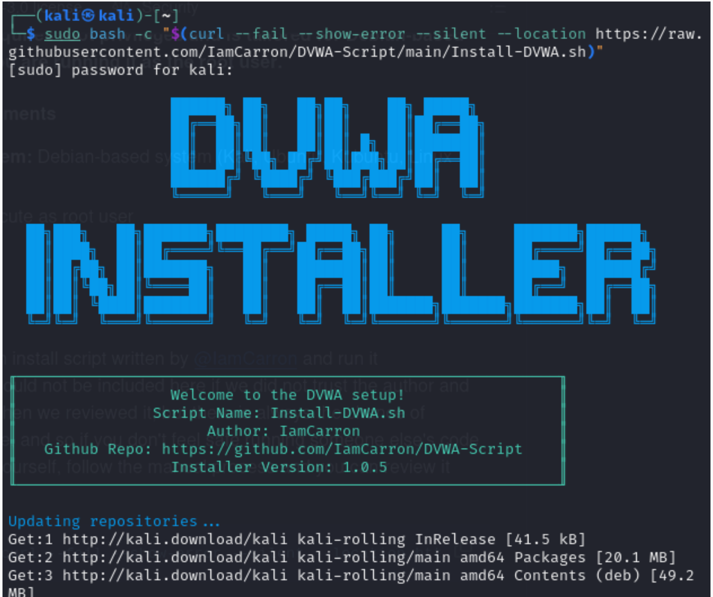
# Шаг 1



```
┌──(kali㉿kali)-[~]
└─$ 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 (fro
m 1)
Receiving objects: 100% (4784/4784), 2.36 MiB | 1.53 MiB/s, done.
Resolving deltas: 100% (2296/2296), done.
```

**Рис. 1:** Скачивание DVWA из репозитория

# Шаг 2

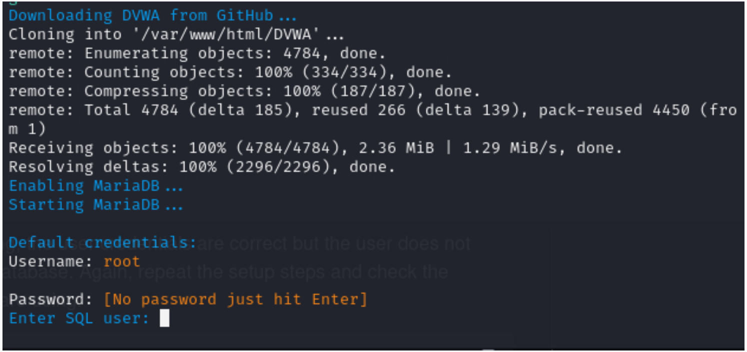


```
┌──(kali㉿kali)-[~]
└─$ sudo bash -c "$(curl --fail --show-error --silent --location https://raw.
githubusercontent.com/IamCarron/DVWA-Script/main/Install-DVWA.sh)"
[sudo] password for kali:
```

```
          Welcome to the DVWA setup!
        Script Name: Install-DVWA.sh
              Author: IamCarron
  Github Repo: https://github.com/IamCarron/DVWA-Script
          Installer Version: 1.0.5


Updating repositories ...
Get:1 http://kali.download/kali kali-rolling InRelease [41.5 kB]
Get:2 http://kali.download/kali kali-rolling/main amd64 Packages [20.1 MB]
Get:3 http://kali.download/kali kali-rolling/main amd64 Contents (deb) [49.2
MB]
```

# Шаг 3



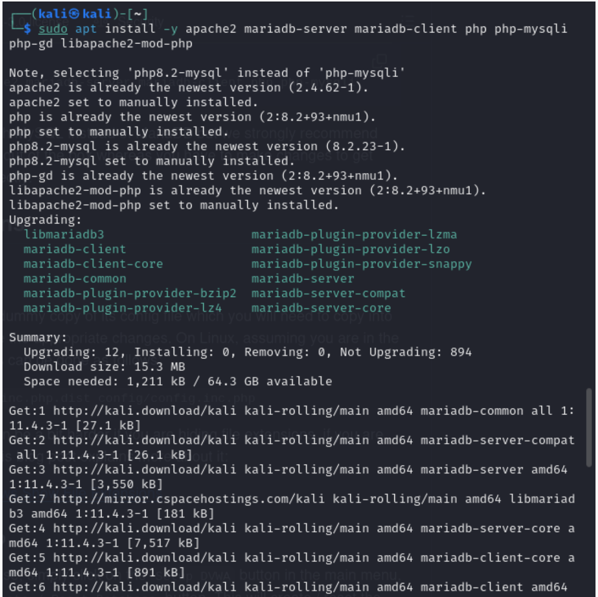
```
Downloading DVWA from GitHub ...
Cloning into '/var/www/html/DVWA' ...
remote: Enumerating objects: 4784, done.
remote: Counting objects: 100% (334/334), done.
remote: Compressing objects: 100% (187/187), done.
remote: Total 4784 (delta 185), reused 266 (delta 139), pack-reused 4450 (fro
m 1)
Receiving objects: 100% (4784/4784), 2.36 MiB | 1.29 MiB/s, done.
Resolving deltas: 100% (2296/2296), done.
Enabling MariaDB ...
Starting MariaDB ...

Default credentials:
Username: root

Password: [No password just hit Enter]
Enter SQL user: 
```

**Рис. 3:** Завершение установки

# Шаг 4



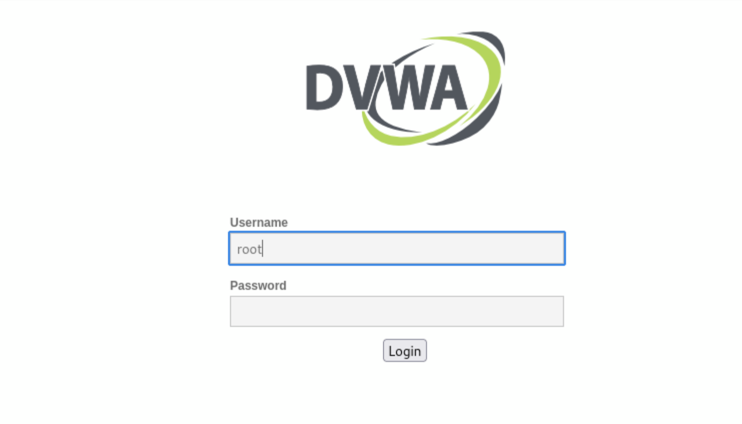
```
┌──(kali㉿kali)-[~]
└─$ sudo apt install -y apache2 mariadb-server mariadb-client php php-mysqli
php-gd libapache2-mod-php

Note, selecting 'php8.2-mysql' instead of 'php-mysqli'
apache2 is already the newest version (2.4.62-1).
apache2 set to manually installed.
php is already the newest version (2:8.2+93+nmu1).
php set to manually installed.
php8.2-mysql is already the newest version (8.2.23-1).
php8.2-mysql set to manually installed.
php-gd is already the newest version (2:8.2+93+nmu1).
libapache2-mod-php is already the newest version (2:8.2+93+nmu1).
libapache2-mod-php set to manually installed.
Upgrading:
  libmariadb3                      mariadb-plugin-provider-lzma
  mariadb-client                   mariadb-plugin-provider-lzo
  mariadb-client-core              mariadb-plugin-provider-snappy
  mariadb-common                   mariadb-server
  mariadb-plugin-provider-bzip2    mariadb-server-compat
  mariadb-plugin-provider-lz4      mariadb-server-core

Summary:
  Upgrading: 12, Installing: 0, Removing: 0, Not Upgrading: 894
  Download size: 15.3 MB
  Space needed: 1,211 kB / 64.3 GB available

Get:1 http://kali.download/kali kali-rolling/main amd64 mariadb-common all 1:
11.4.3-1 [27.1 kB]
Get:2 http://kali.download/kali kali-rolling/main amd64 mariadb-server-compat
 all 1:11.4.3-1 [26.1 kB]
Get:3 http://kali.download/kali kali-rolling/main amd64 mariadb-server amd64
1:11.4.3-1 [3,550 kB]
Get:7 http://mirror.cspacehostings.com/kali kali-rolling/main amd64 libmariad
b3 amd64 1:11.4.3-1 [181 kB]
Get:4 http://kali.download/kali kali-rolling/main amd64 mariadb-server-core a
md64 1:11.4.3-1 [7,517 kB]
Get:5 http://kali.download/kali kali-rolling/main amd64 mariadb-client-core a
md64 1:11.4.3-1 [891 kB]
Get:6 http://kali.download/kali kali-rolling/main amd64 mariadb-client amd64
```

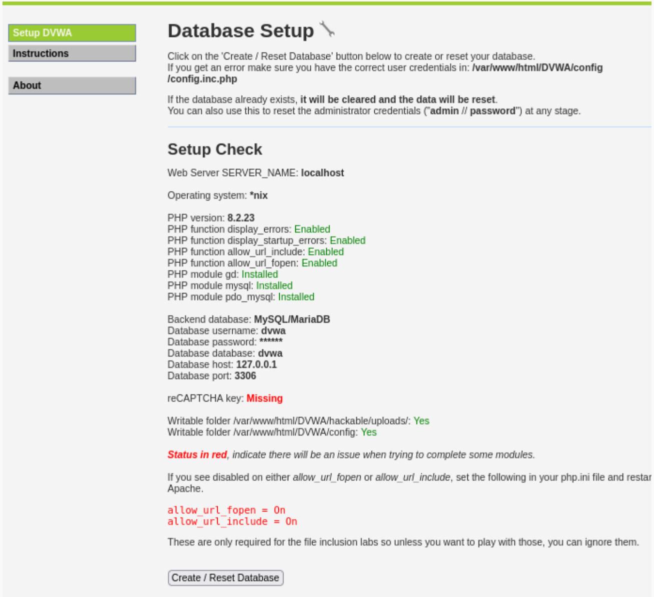
# Шаг 5



root

**Рис. 5:** Вход в DVWA

# Шаг 6



## 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: Enabled
PHP function display_startup_errors: Enabled
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: **&#42;&#42;&#42;&#42;&#42;&#42;**
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

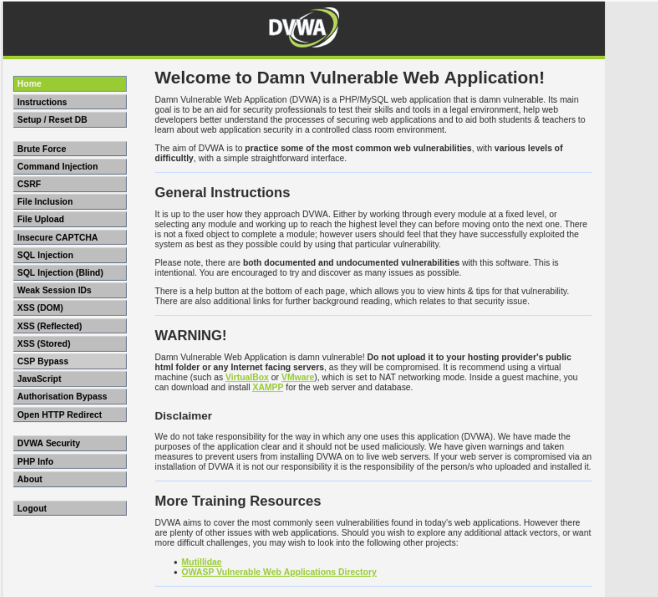
***Status in red**, indicate there will be an issue when trying to complete some modules.*

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

# Итог



## 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 difficultly**, 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

We do not take responsibility for the way in which any one uses this application (DVWA). We have made the purposes of the application clear and it should not be used maliciously. We have given warnings and taken measures to prevent users from installing DVWA on to live web servers. If your web server is compromised via an installation of DVWA it is not our responsibility it is the responsibility of the person/s who uploaded and installed it.

## More Training Resources

DVWA aims to cover the most commonly seen vulnerabilities found in today's web applications. However there are plenty of other issues with web applications. Should you wish to explore any additional attack vectors, or want more difficult challenges, you may wish to look into the following other projects:

- Mutillidae
- OWASP Vulnerable Web Applications Directory

# Выводы

Я установила DVWA в гостевую систему к Kali Linux.