

# Индивидуальный проект. Этап №2

## Установка DVWA

Камкина А. Л.

### Информация

#### Докладчик

- Камкина Арина Леонидовна
- студентка группы НКНбд-01-21
- Российский университет дружбы народов
- [1032216456@pfur.ru](mailto:1032216456@pfur.ru)
- <https://alkamkina.github.io/ru/>



## Вводная часть

### Цели и задачи

#### Цель работы:

Установить DVWA в гостевую систему к Kali Linux.

#### Задачи:

- Установить DVWA на Kali Linux
- Настроить DVWA

**Инструмент:** VirtualBox

## Выполнение лабораторной работы

### Переход в каталог

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

*Переход в каталог*

### Клонирование репозитория

```
(alkamkina@alkamkina)-[/var/www/html]  
$ sudo git clone https://github.com/digininja/DVWA.git  
[sudo] password for alkamkina:  
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 | 3.08 MiB/s, done.  
Resolving deltas: 100% (2296/2296), done.
```

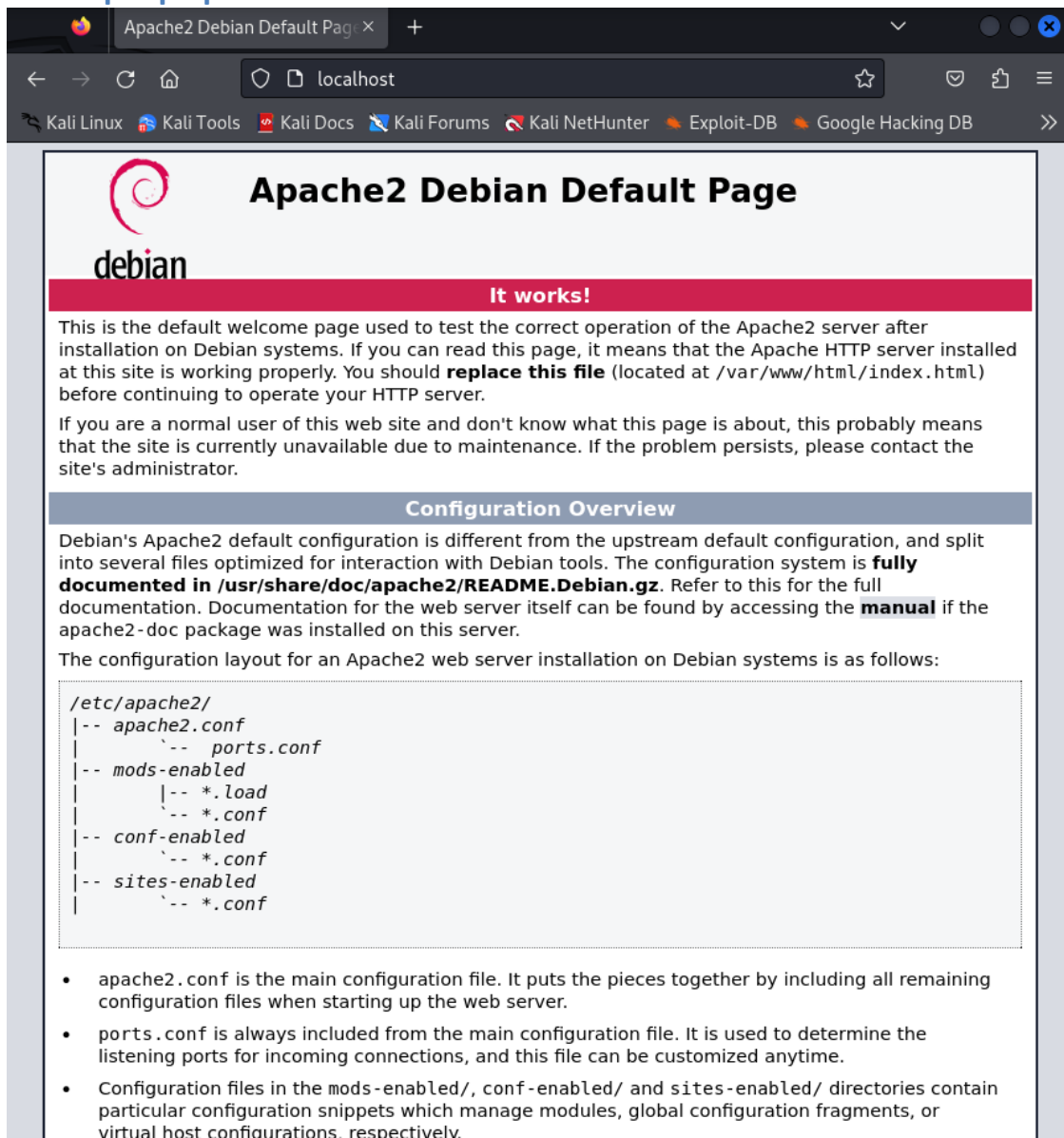
*Клонирование репозитория*

### Запуск веб сервера

```
(alkamkina@alkamkina)-[/var/www/html]  
$ ls  
DVWA index.html index.nginx-debian.html  
  
(alkamkina@alkamkina)-[/var/www/html]  
$ sudo service apache2 start
```

*Запуск веб сервера*

## Веб сервер apache2



**Apache2 Debian Default Page**

**It works!**

This is the default welcome page used to test the correct operation of the Apache2 server after installation on Debian systems. If you can read this page, it means that the Apache HTTP server installed at this site is working properly. You should **replace this file** (located at `/var/www/html/index.html`) before continuing to operate your HTTP server.

If you are a normal user of this web site and don't know what this page is about, this probably means that the site is currently unavailable due to maintenance. If the problem persists, please contact the site's administrator.

### Configuration Overview

Debian's Apache2 default configuration is different from the upstream default configuration, and split into several files optimized for interaction with Debian tools. The configuration system is **fully documented in `/usr/share/doc/apache2/README.Debian.gz`**. Refer to this for the full documentation. Documentation for the web server itself can be found by accessing the **manual** if the `apache2-doc` package was installed on this server.

The configuration layout for an Apache2 web server installation on Debian systems is as follows:

```
/etc/apache2/
|-- apache2.conf
|   |-- ports.conf
|-- mods-enabled
|   |-- *.load
|   |-- *.conf
|-- conf-enabled
|   |-- *.conf
|-- sites-enabled
|   |-- *.conf
```

- `apache2.conf` is the main configuration file. It puts the pieces together by including all remaining configuration files when starting up the web server.
- `ports.conf` is always included from the main configuration file. It is used to determine the listening ports for incoming connections, and this file can be customized anytime.
- Configuration files in the `mods-enabled/`, `conf-enabled/` and `sites-enabled/` directories contain particular configuration snippets which manage modules, global configuration fragments, or virtual host configurations, respectively.

## Веб сервер apache2

## Копирование фала

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

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

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

(alkamkina@alkamkina)-[/var/www/html/DVWA]
$ cp config/config.inc.php.dist config/config.inc.php
cp: cannot create regular file 'config/config.inc.php': Permission denied

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

*Копирование фала*

## Просмотр файла

```
(alkamkina@alkamkina)-[/var/www/html/DVWA]
$ cat config/config.inc.php
<?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 de
dicated 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';

# ReCAPTCHA settings
# Used for the 'Insecure CAPTCHA' module
# You'll need to generate your own keys at: https://www.google.com/recaptch
a/admin
$_DVWA[ 'recaptcha_public_key' ] = '';
$_DVWA[ 'recaptcha_private_key' ] = '';

# Default security level
# Default value for the security level with each session.
# The default is 'impossible'. You may wish to set this to either 'low', 'm
edium', 'high' or impossible'.
$_DVWA[ 'default_security_level' ] = 'impossible';

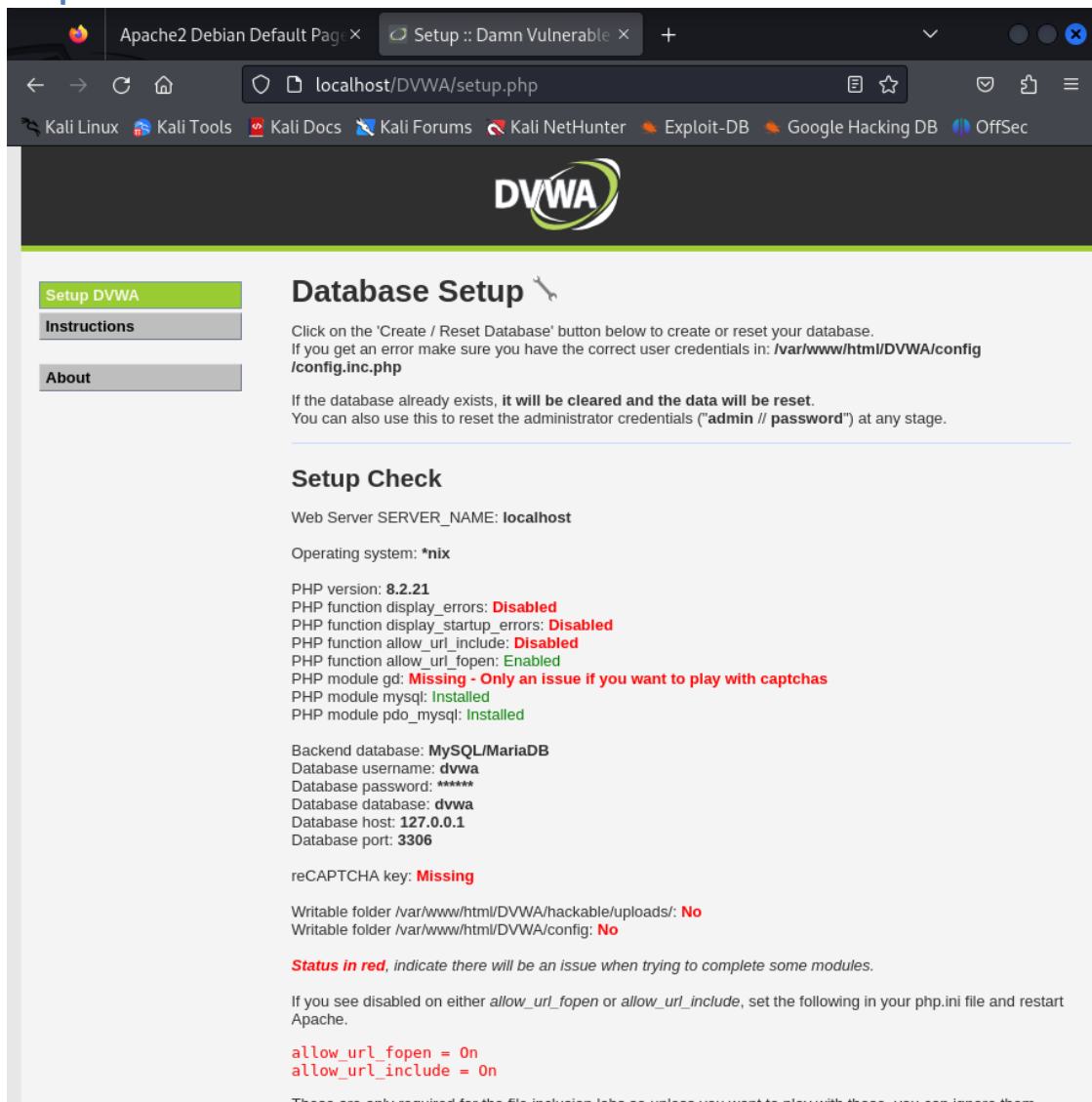
# Default locale
# Default locale for the help page shown with each session.
# The default is 'en'. You may wish to set this to either 'en' or 'zh'.
$_DVWA[ 'default_locale' ] = 'en';

# Disable authentication
# Some tools don't like working with authentication and passing cookies aro
```

## Просмотр файла



## Стартовое окно DVWA



The screenshot shows a web browser window with the address bar displaying `localhost/DVWA/setup.php`. The browser's tab bar shows two tabs: "Apache2 Debian Default Page" and "Setup :: Damn Vulnerable". The browser's address bar also shows a search bar with the text "Kali Linux", "Kali Tools", "Kali Docs", "Kali Forums", "Kali NetHunter", "Exploit-DB", "Google Hacking DB", and "OffSec".

The DVWA logo is displayed at the top of the page. On the left side, there is a sidebar with three links: "Setup DVWA" (highlighted in green), "Instructions", and "About".

### 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: **8.2.21**  
PHP function display\_errors: **Disabled**  
PHP function display\_startup\_errors: **Disabled**  
PHP function allow\_url\_include: **Disabled**  
PHP function allow\_url\_fopen: **Enabled**  
PHP module gd: **Missing - Only an issue if you want to play with captchas**  
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/`: **No**  
Writable folder `/var/www/html/DVWA/config/`: **No**

**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.

## Стартовое окно DVWA

## Создание пользователя

```
root@alkamkina: ~  
File Actions Edit View Help  
(root@alkamkina)-[~]  
# mysql  
Welcome to the MariaDB monitor.  Commands end with ; or \g.  
Your MariaDB connection id is 31  
Server version: 11.4.2-MariaDB-4 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 (0.007 sec)  
  
MariaDB [(none)]> create user dvwa@localhost identified by 'p@ssw0rd';  
Query OK, 0 rows affected (0.026 sec)  
  
MariaDB [(none)]> grant all on dvwa.* to dvwa@localhost;  
ERROR 1064 (42000): You have an error in your SQL syntax; check the manual that  
corresponds to your MariaDB server version for the right syntax to use near  
'grant all on dvwa.* to dvwa@localhost' at line 1  
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 (0.001 sec)  
  
MariaDB [(none)]> █
```

Создание пользователя

## Создание пользователя

```
(alkamkina@alkamkina)-[/var/www/html/DVWA]  
$ service mariadb start  
  
(alkamkina@alkamkina)-[/var/www/html/DVWA]  
$ mysql -u dvwa -p  
Enter password:  
Welcome to the MariaDB monitor.  Commands end with ; or \g.  
Your MariaDB connection id is 32  
Server version: 11.4.2-MariaDB-4 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)]> use dvwa;  
Database changed  
MariaDB [dvwa]> █
```

Создание пользователя



[Вход](#)

---



**Username**

admin


**Password**

••••••••

Login

*Вход*

## Стартовая страница 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

DVWA Security

PHP Info

About

Logout

### 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

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

Стартовая страница DVWA

## Заключение

### Вывод

В ходе выполнения работы был установлен DVWA на Kali Linux.