

Основы информационной безопасности. Индивидуальный проект

Этап №2. Установка DVWA на Kali Linux

Нзита Диатезилуа Катенди

21 сентября 2024 г.

Российский университет дружбы народов, Москва, Россия

Информация

- Нзита Диатезилуа Катенди
- студент
- Российский университет дружбы народов
- 1032215220@pfur.ru
- <https://github.com/NzitaKatendi>

Вводная часть

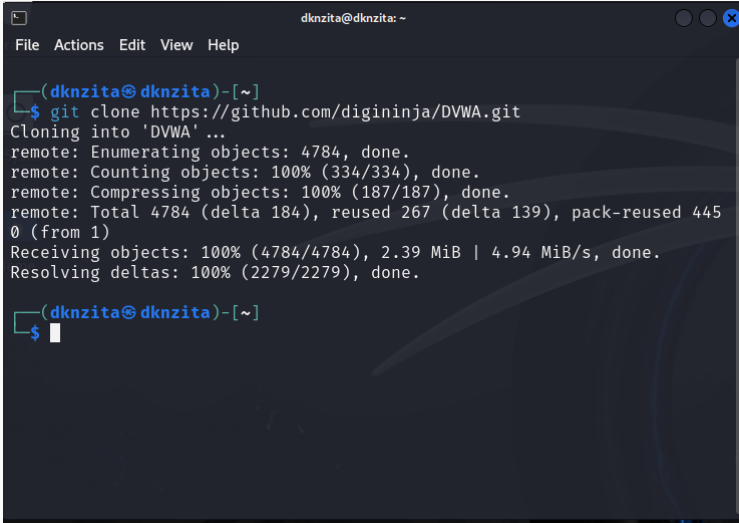
Целью данной работы является установка DVWA на Kali Linux.

Задачи:

- Установить DVWA.

Инструмент: VirtualBox

Выполнение лабораторной работы



```
dknzita@dknzita: ~  
File Actions Edit View Help  
  
(dknzita@dknzita)-[~]  
$ 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 184), reused 267 (delta 139), pack-reused 445  
0 (from 1)  
Receiving objects: 100% (4784/4784), 2.39 MiB | 4.94 MiB/s, done.  
Resolving deltas: 100% (2279/2279), done.  
  
(dknzita@dknzita)-[~]  
$
```

Рис. 1: Клонирование репозитория с DVWA

```
(dknzita@dknzita)-[~]
$ sudo mv DVWA /var/www/html
[sudo] password for dknzita:

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

(dknzita@dknzita)-[/var/www/html]
$ ls
DVWA  index.html  index.nginx-debian.html

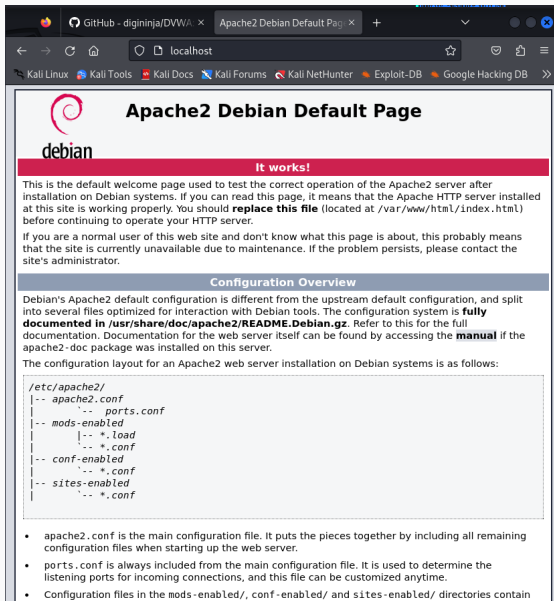
(dknzita@dknzita)-[/var/www/html]
$ cd DVWA

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

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

(dknzita@dknzita)-[/var/www/html]
$ sudo service apache2 start

(dknzita@dknzita)-[/var/www/html]
$
```

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

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

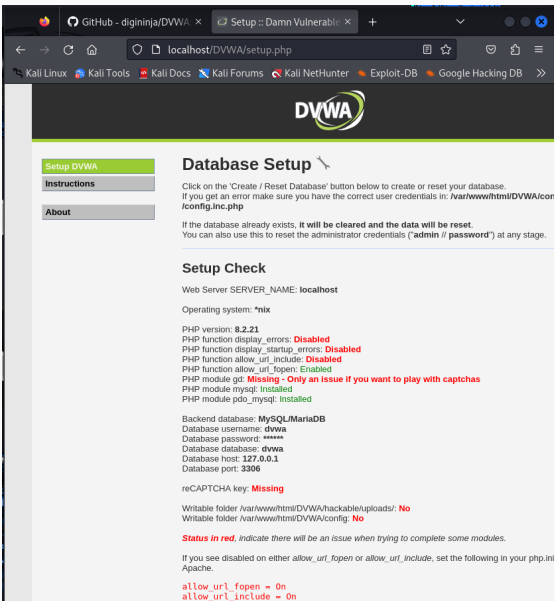
(dknzita@dknzita)-[/var/www/html/DVWA]
$ ls
CHANGELOG.md  README.md      database      logout.php
COPYING.txt   README.pt.md   docs          php.ini
Dockerfile    README.tr.md   dvwa          phpinfo.php
README.ar.md  README.vi.md   external      robots.txt
README.es.md  README.zh.md   favicon.ico  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

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

(dknzita@dknzita)-[/var/www/html/DVWA]
$ cp config/config.inc.php config/config.inc.php
cp: cannot stat 'config/config.inc.php': No such file or directory

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

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



The screenshot shows a web browser window with the URL `localhost/DVWA/setup.php`. The page has a dark header with the DVWA logo. On the left, there is a sidebar with three tabs: "Setup DVWA" (highlighted in green), "Instructions", and "About". The main content area is titled "Database Setup" and contains the following text:

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.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**

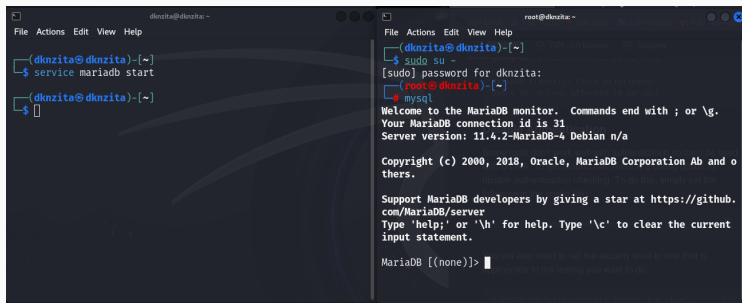
reCAPTCHA key: **Missing**

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` Apache.

```
allow_url_fopen = On
allow_url_include = On
```



```
dknzita@dknzita: ~  
File Actions Edit View Help  
(dknzita@dknzita)-[~]  
$ service mariadb start  
(dknzita@dknzita)-[~]  
$  
  
root@dknzita: ~  
File Actions Edit View Help  
(dknzita@dknzita)-[~]  
$ sudo su -  
[sudo] password for dknzita:  
(root@dknzita)-[~]  
# 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)]>
```

Рис. 6: Проверка пользователя mariadb

```
(dknzita@dknzita)-[~]  
$ mysql -u dvwa -pDia123  
Welcome to the MariaDB monitor.  Commands end with ; or \g.  
Your MariaDB connection id is 35  
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]> █
```

Рис. 7: Аутентификация

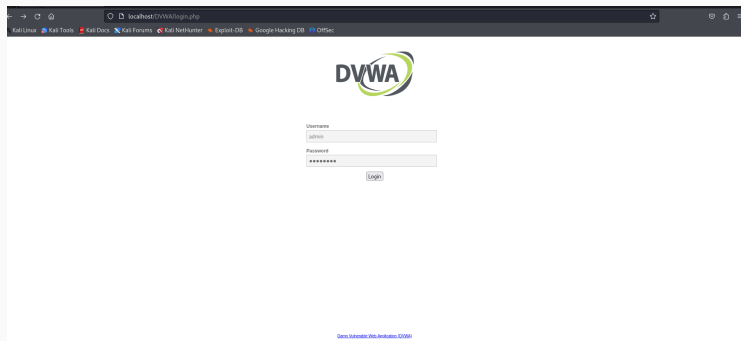


Рис. 8: Запуск DVWA

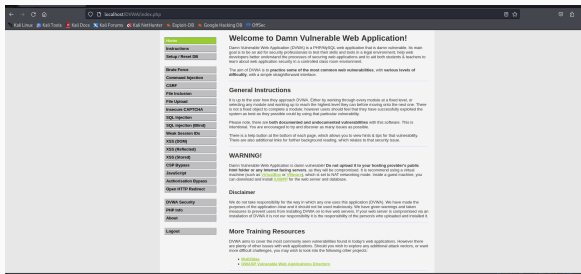


Рис. 9: DVWA

Заключение

В результате выполнения работы был установлен DVWA на Kali Linux.

1. DVWA [Электронный ресурс]. GitHub, Inc, 2024. URL: <https://github.com/digininja/DVWA>.