

Установка DVWA

Этап 2

Абу Сувейлим Мухаммед Мунифович

Содержание

1	Цель работы	5
2	Задание	6
3	Теоретическое введение	7
4	Выполнение лабораторной работы	8
5	Выводы	14
	Список литературы	15

Список иллюстраций

4.1	Git Clone	8
4.2	Директория html	8
4.3	Ошибка Unable to connect to localhost	9
4.4	Сервер apache2	9
4.5	Главная страница Apache2	9
4.6	Ошибка config file not found	10
4.7	Директория DVWA и файл Config	10
4.8	Страница нвстройки	11
4.9	Настройка базы данных	11
4.10	База данных dvwa	12
4.11	folder writable 1	12
4.12	Все дополнительные опции	13

Список таблиц

1 Цель работы

Научиться как загрузить и установить DVWA на Kali Linux [1].

2 Задание

Установить DVWA в гостевую систему к Kali Linux.

3 Теоретическое введение

Damn Vulnerable Web Application (DVWA) – это веб-приложение PHP / MySQL, которое чертовски уязвимо.

Его основная цель – помочь специалистам по безопасности проверить свои навыки и инструменты в правовой среде, помочь веб-разработчикам лучше понять процессы обеспечения безопасности веб-приложений и помочь студентам и преподавателям узнать о безопасности веб-приложений в контролируемой среде. [2]

4 Выполнение лабораторной работы

Для начала скачаем последнюю версию из репозитория командой (рис. 4.1):

```
(smabu@smabu)-[~]  
$ 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 (from 1)  
Receiving objects: 100% (4784/4784), 2.36 MiB | 7.68 MiB/s, done.  
Resolving deltas: 100% (2296/2296), done.
```

Рис. 4.1: Git Clone

Далее переместимся в директорию /var/www/html (рис. 4.2):

```
(smabu@smabu)-[~]  
$ sudo mv DVWA /var/www/html  
  
(smabu@smabu)-[~]  
$ cd /var/www/html  
  
(smabu@smabu)-[/var/www/html]  
$ ls  
DVWA index.html index.nginx-debian.html
```

Рис. 4.2: Директория html

Если попробовть войти в localhost, получаем ошибку, так как не устанновлен сервер (рис. 4.3):

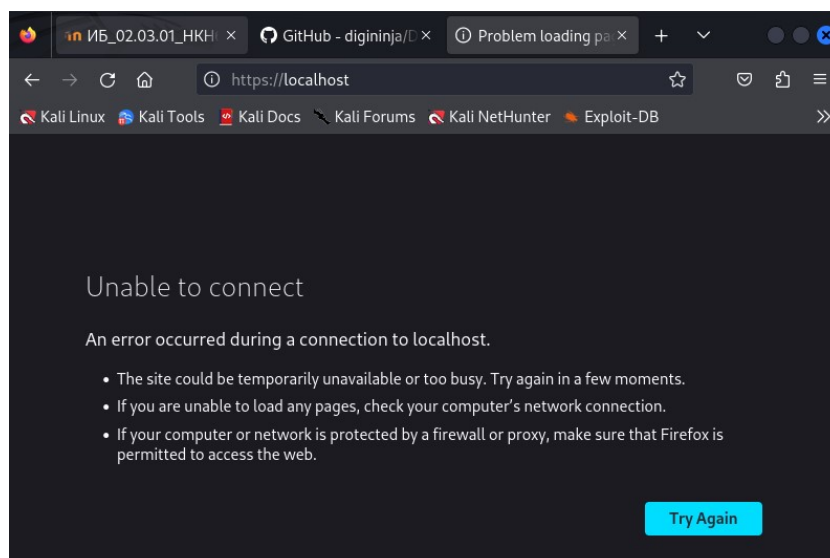


Рис. 4.3: Ошибка Unable to connect to localhost

Чтобы решить эту проблему нужно запустить сервер apache2 (рис. 4.4; 4.5):

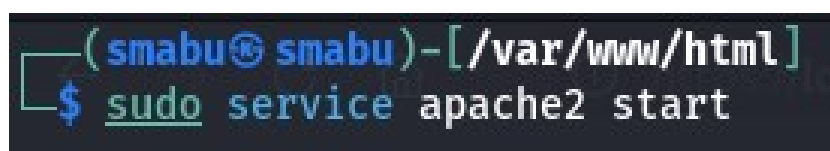


Рис. 4.4: Сервер apache2



Рис. 4.5: Главная страница Apache2

Также если попробовать войти в localhost/DVWA не получится (рис. 4.6):

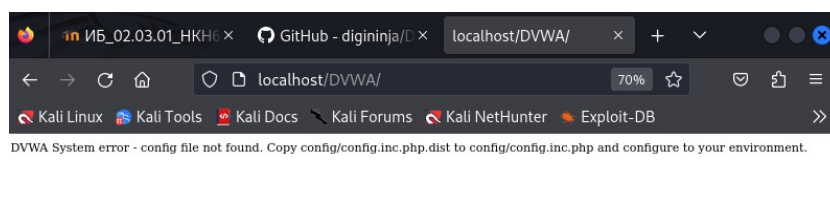


Рис. 4.6: Ошибка config file not found

Аналогично, чтобы решить эту проблему мы переместимся в директорию DVWA (рис. 4.7)

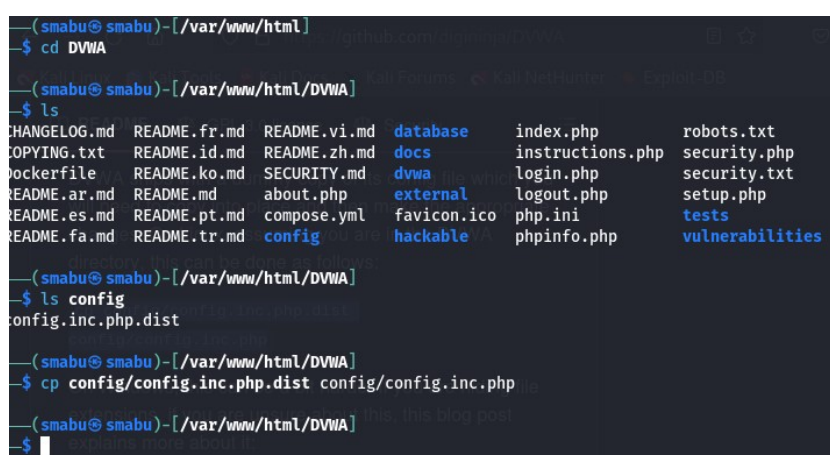


Рис. 4.7: Директория DVWA и файл Config

DVWA поставляется с фиктивной копией своего конфигурационного (config) файла, который нам нужно будет скопировать в директорию, а затем внести соответствующие изменения. В Linux это можно сделать как показано на (рис. 4.7).

Теперь можно открыть страницу настройки localhost/DVWA/setup.php (рис. 4.8):

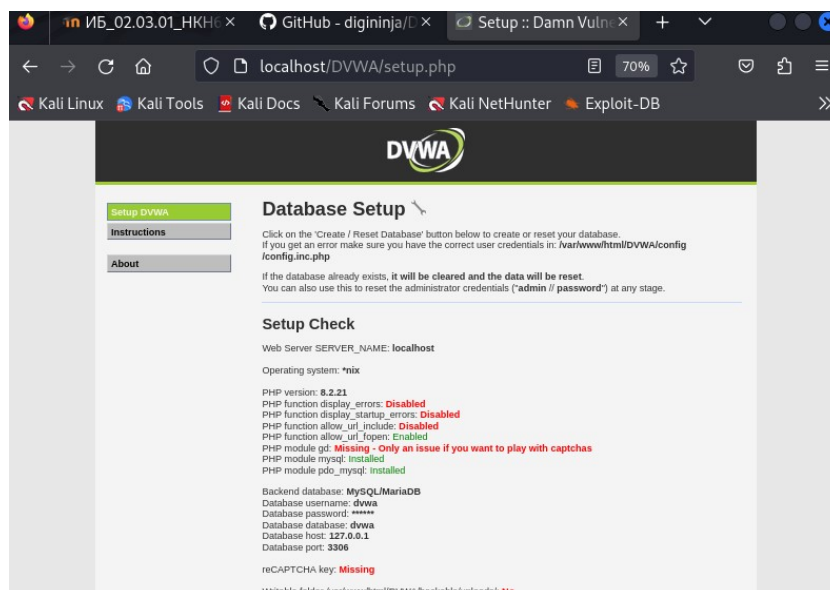


Рис. 4.8: Страница нвстройки

Осталось настроить базу данных (рис. 4.9):

```
MariaDB [(none)]> create database dvwa;
Query OK, 1 row affected (0.000 sec)

MariaDB [(none)]> create user dvwa@localhost identified by 'p@ssw0rd';
Query OK, 0 rows affected (0.001 sec)

MariaDB [(none)]> grant all on dvwa.* to dvwa@localhost;
Query OK, 0 rows affected (0.001 sec)

MariaDB [(none)]> flush privileges;
Query OK, 0 rows affected (0.000 sec)

MariaDB [(none)]>
```

Рис. 4.9: Настройка базы данных

В качестве проверки, можно войти в базу данных как пользователь dvwa (рис. 4.10):

```
(smabu@smabu)-[~]
$ mysql -u dvwa -pp@ssw0rd
Welcome to the MariaDB monitor.  Commands end with ; or \g.
Your MariaDB connection id is 44
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. 4.10: База данных dvwa

Выполнив следующие действия мы можем открыть доступ к некоторым функциям (рис. 4.11, 4.12):

```
(root@smabu)-[/etc/php/8.2/apache2]
# ls -al /var/www/html/DVWA/config
total 28
drwxrwxr-x  2 smabu smabu  4096 Sep 20 18:30 .
drwxrwxr-x 12 smabu smabu  4096 Sep 20 18:21 ..
-rw-r--r--  1 smabu smabu 12288 Sep 20 18:33 .config.inc.php.swp
-rw-rw-r--  1 smabu smabu  2194 Sep 20 18:30 config.inc.php
-rw-rw-r--  1 smabu smabu  2194 Sep 20 18:21 config.inc.php.dist

(root@smabu)-[/etc/php/8.2/apache2]
# chown www-data /var/www/html/DVWA/config

(root@smabu)-[/etc/php/8.2/apache2]
# ls -al /var/www/html/DVWA/config
total 28
drwxrwxr-x  2 www-data smabu  4096 Sep 20 18:30 .
drwxrwxr-x 12 smabu      smabu  4096 Sep 20 18:21 ..
-rw-r--r--  1 smabu      smabu 12288 Sep 20 18:33 .config.inc.php.swp
-rw-rw-r--  1 smabu      smabu  2194 Sep 20 18:30 config.inc.php
-rw-rw-r--  1 smabu      smabu  2194 Sep 20 18:21 config.inc.php.dist

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

Рис. 4.11: folder writable 1

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

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: 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: dwwa
 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.ini` file and restart Apache.

Рис. 4.12: Все дополнительные опции

5 Выводы

Успешно смогли установить DVWA в гостевую систему к Kali Linux.

Список литературы

1. Парасрам Шива Х.Т. Замм Алекс. Kali Linux. Тестирование на проникновение и безопасность. СПб, 2020. 448 с.
2. cryptoparty. DVWA – Уязвимое веб-приложение. 2018.