

Отчёт по индивидуальному проекту. Этап 2

Дисциплина: Основы информационной безопасности

Разанацуа Сара Естэлл НКАбд-02-23

Содержание

1	Цель работы	5
2	Выполнение лабораторной работы	6
3	Выводы	11
	Список литературы	12

Список иллюстраций

2.1	Клонируем репозиторий	6
2.2	конфигурации	7
2.3	редактировать файл	7
2.4	Установка mariadb	8
2.5	Запустим базу	8
2.6	создадим нового пользователя	9
2.7	Запустим базу	9
2.8	Запустим базу	10
2.9	Запустим базу	10

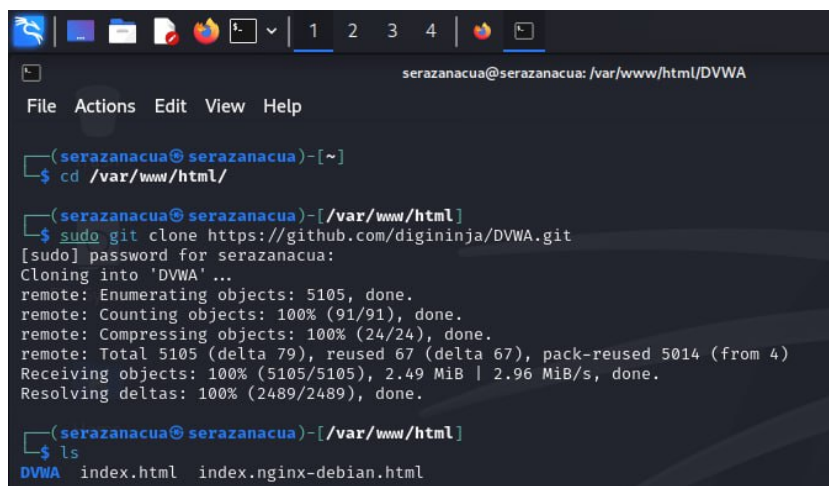
Список таблиц

1 Цель работы

- Установка DVWA в гостевой системе Kali Linux.

2 Выполнение лабораторной работы

- Перейдем в каталог html: `cd /var/www/html` Клонировать репозиторий git: `sudo git clone https://github.com/digininja/DVWA.git`. Перейдем к файлу конфигурации в каталоге установки (рис. 2.1): `cd DVWA`. затем давайте проверим список на наличие содержимого каталога



```
serazanacua@serazanacua: /var/www/html/DVWA
File Actions Edit View Help

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

(serazanacua@serazanacua)-[/var/www/html]
$ sudo git clone https://github.com/digininja/DVWA.git
[sudo] password for serazanacua:
Cloning into 'DVWA' ...
remote: Enumerating objects: 5105, done.
remote: Counting objects: 100% (91/91), done.
remote: Compressing objects: 100% (24/24), done.
remote: Total 5105 (delta 79), reused 67 (delta 67), pack-reused 5014 (from 4)
Receiving objects: 100% (5105/5105), 2.49 MiB | 2.96 MiB/s, done.
Resolving deltas: 100% (2489/2489), done.

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

Рис. 2.1: Клонировать репозиторий

- Скопируем файл конфигурации и переименуем его: `cp config.inc.php.dist config.inc.php` (рис. 2.2).

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

(serazanacua@serazanacua)~/var/www/html/DVWA$ ls config
config.inc.php.dist
(serazanacua@serazanacua)~/var/www/html/DVWA$ sudo cp config/config.inc.php.dist config/config.inc.php
(serazanacua@serazanacua)~/var/www/html/DVWA$
```

Рис. 2.2: конфигурации

- Откроем файл настроек vim config/config.inc.php (рис. 2.3).

```
serazanacua@serazanacua: /var/www/html/DVWA
File Actions Edit View Help
#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 = getenv('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 dedicated 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'] = getenv('DB_DATABASE') ?: 'dvwa';
$DVWA['db_user'] = getenv('DB_USER') ?: 'dvwa';
$DVWA['db_password'] = getenv('DB_PASSWORD') ?: 'p@ssw0rd';
$DVWA['db_port'] = getenv('DB_PORT') ?: '3306';

# RECAPTCHA settings
# Used for the 'Insecure CAPTCHA' module
# You'll need to generate your own keys at: https://www.google.com/recaptcha/admin
$DVWA['recaptcha_public_key'] = getenv('RECAPTCHA_PUBLIC_KEY') ?: '';
$DVWA['recaptcha_private_key'] = getenv('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', 'medium', 'high' or 'impossible'.
$DVWA['default_security_level'] = getenv('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'] = getenv('DEFAULT_LOCALE') ?: 'en';

# Disable authentication
# Some tools don't like working with authentication and passing cookies around
# so this setting lets you turn off authentication.
$DVWA['disable_authentication'] = getenv('DISABLE_AUTHENTICATION') ?: false;

define('MYSQL', 'mysql');
define('SQLITE', 'sqlite');

# SQLi DB Backend
# Use this to switch the backend database used in the SQLi and Blind SQLi labs.
# This does not affect the backend for any other services, just these two labs.
# If you do not understand what this means, do not change it.
"config/config.inc.php" [readonly][dos] 56L, 2494B      1,1      Top
```

Рис. 2.3: редактировать файл

- Установим mariadb (рис. 2.4).

```
(root@serazanacua)-[/etc/php/8.2/apache2]
# vim php.ini

(root@serazanacua)-[/etc/php/8.2/apache2]
# apt update
Get:1 http://kali.download/kali kali-rolling InRelease [41.5 kB]
Get:2 http://kali.download/kali kali-rolling/main amd64 Packages [20.7 MB]
Get:3 http://kali.download/kali kali-rolling/main amd64 Contents (deb) [49.3 MB]
Get:4 http://kali.download/kali kali-rolling/contrib amd64 Packages [115 kB]
Get:5 http://kali.download/kali kali-rolling/contrib amd64 Contents (deb) [26 7 kB]
Get:6 http://kali.download/kali kali-rolling/non-free amd64 Packages [203 kB]
Get:7 http://kali.download/kali kali-rolling/non-free amd64 Contents (deb) [8 84 kB]
Get:8 http://kali.download/kali kali-rolling/non-free-firmware amd64 Packages [10.8 kB]
Get:9 http://kali.download/kali kali-rolling/non-free-firmware amd64 Contents (deb) [24.3 kB]
Fetched 71.5 MB in 37s (1,915 kB/s)
1529 packages can be upgraded. Run 'apt list --upgradable' to see them.

(root@serazanacua)-[/etc/php/8.2/apache2]
# apt install php-gd
```

Рис. 2.4: Установка mariadb

- Запустим базу данных: `sudo su-`, затем `mysql` (рис. 2.5).

```
root@serazanacua: ~
File Actions Edit View Help

(serazanacua@serazanacua)-[~]
$ sudo su -
[sudo] password for serazanacua:
(root@serazanacua)-[~]
# mysql
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 database dvwa;
Query OK, 1 row affected (0.001 sec)
```

Рис. 2.5: Запустим базу

- создадим нового пользователя базы данных. Для этого давайте подключимся к базе данных как пользователь `root`, а затем воспользуемся следующими командами:(рис. 2.6).


```
File Actions Edit View Help
/var/www/html/DVWA
/var/www/html/DVWA
root@serazanacua: ~
(serazanacua@serazanacua)-[~]
$ sudo su -
[sudo] password for serazanacua:
(root@serazanacua)-[~]
# mysql
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 database dvwa;
Query OK, 1 row affected (0.001 sec)

MariaDB [(none)]> create user dvwa@localhost identified by 'p@ssw0rd';
Query OK, 0 rows affected (0.008 sec)

MariaDB [(none)]> grant all on dvwa.* to dvwa@localhost;
Query OK, 0 rows affected (0.005 sec)

MariaDB [(none)]> flush privileges;
```

Рис. 2.6: создадим нового пользователя

- Запустив сервер Apache (рис. 2.7): `sudo service apache2 start`

```
(serazanacua@serazanacua)-[/var/www/html/DVWA]
$ sudo service apache2 start
```

Рис. 2.7: Запустим базу

- Открываем DVWA в браузере: `localhost/DVWA/setup.php` (рис. 2.8).

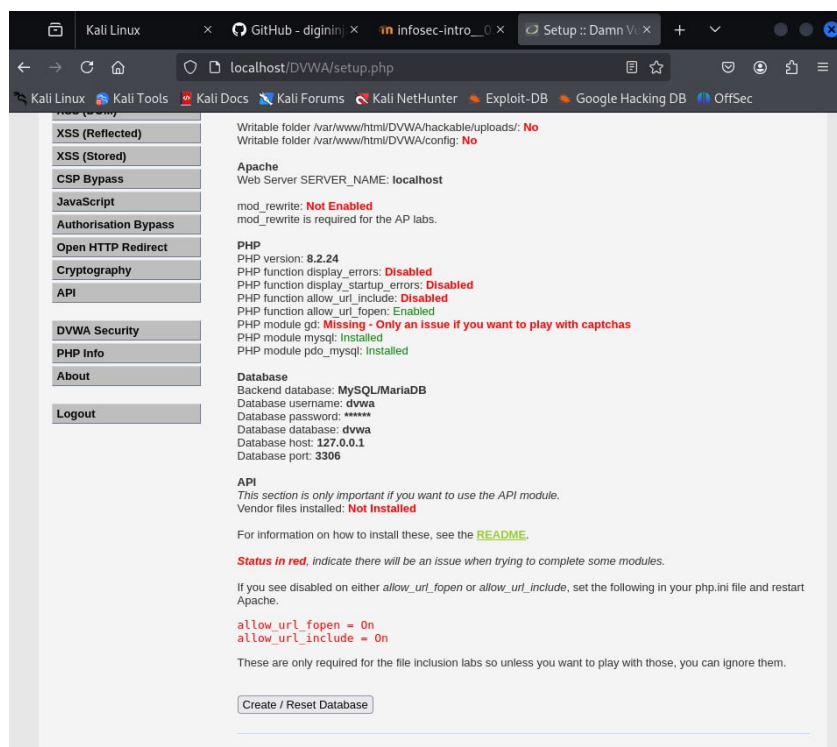


Рис. 2.8: Запустим базу

- Давайте нажмем Create / Reset Database. Давайте нажмем create, чтобы создать базу данных. Затем введите имя пользователя и пароль



Username

admin

Password

Login

Login failed

Рис. 2.9: Запустим базу

3 Выводы

- В ходе выполнения данной лабораторной работы, я установил DVWA в гостевой системе Kali Linux.

Список литературы

1. Парасрам, Ш. Kali Linux: Тестирование на проникновение и безопасность : Для профессионалов. Kali Linux / Ш. Парасрам, А. Замм, Т. Хериянто, и др. – Санкт-Петербург : Питер, 2022. – 448 сс.