

Информационная безопасность

Индивидуальный проект №2

Матюшкин Денис Владимирович (НПИбд-02-21)

Содержание

1	Цель работы	5
2	Теоретическое введение	6
3	Ход работы	7
4	Выводы	12
	Список литературы	13

Список иллюстраций

3.1	Клонирование репозитория dvwa	7
3.2	Копирование файла конфигурации	7
3.3	Новый пароль	8
3.4	Установка утилит	8
3.5	Новый пользователь БД	8
3.6	Редактирование файла php.ini	9
3.7	Запуск apache2	9
3.8	Запуск dvwa	10
3.9	Вход в dvwa	11

Список таблиц

1 Цель работы

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

2 Теоретическое введение

VirtualBox (Oracle VM VirtualBox) — программный продукт виртуализации для операционных систем Windows, Linux, FreeBSD, macOS, Solaris/OpenSolaris, ReactOS, DOS и других [1].

Kali Linux — возникший как результат слияния WHAX и Auditor Security Collection. Предназначен прежде всего для проведения тестов на безопасность. Наследник развивавшегося до 2013 года на базе Knoppix дистрибутива BackTrack [2].

Damn Vulnerable Web Application (DVWN) — это программный проект, который намеренно включает уязвимости безопасности и предназначен для образовательных целей [3].

3 Ход работы

1. Перейдите в каталог html и клонируйте репозиторий git (рис. 3.1).

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

(dvmatyushkin@dvmatyushkin)-[/var/www/html]
$ sudo git clone https://github.com/digininja/DVWA.git

[sudo] password for dvmatyushkin:
Cloning into 'DVWA' ...
remote: Enumerating objects: 4758, done.
remote: Counting objects: 100% (308/308), done.
remote: Compressing objects: 100% (180/180), done.
remote: Total 4758 (delta 167), reused 241 (delta 122), pack-reused 4450 (from 1)
Receiving objects: 100% (4758/4758), 2.39 MiB | 4.20 MiB/s, done.
Resolving deltas: 100% (2262/2262), done.
```

Рис. 3.1: Клонирование репозитория dvwa

2. Измените права доступа к папке установки. Перейдите к файлу конфигурации в каталоге установки, скопируйте файл конфигурации и переименуйте его (рис. 3.2).

```
(dvmatyushkin@dvmatyushkin)-[/var/www/html]
$ sudo chmod -R 777 DVWA

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

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

Рис. 3.2: Копирование файла конфигурации

3. Откройте файл настроек и измените пароль на что-то более простое для ввода (рис. 3.3).

```

$_DVWA = array();
$_DVWA[ 'db_server' ] = getenv( 'DB_SERVER' ) ?: '127.0.0.1';
$_DVWA[ 'db_database' ] = 'dvwa';
$_DVWA[ 'db_user' ] = 'dvwa';
$_DVWA[ 'db_password' ] = 'pass';
$_DVWA[ 'db_port' ] = '3306';

```

Рис. 3.3: Новый пароль

4. Установите mariadb (рис. 3.4).

```

(dvmatyushkin@dvmatyushkin)-[/var/www/html/DVWA/config]
$ sudo apt-get update
Hit:1 http://http.kali.org/kali kali-rolling InRelease
Reading package lists... Done

(dvmatyushkin@dvmatyushkin)-[/var/www/html/DVWA/config]
$ sudo apt-get -y install apache2 mariadb-server php php-mysqli php-gd libapache2-mod-php

Reading package lists... Done
Building dependency tree... Done

```

Рис. 3.4: Установка утилит

5. Создайте пользователя базы данных. Нужно использовать те же имя пользователя и пароль, которые использовались в файле конфигурации. Предоставьте пользователю все привилегии (рис. 3.5).

```

(dvmatyushkin@dvmatyushkin)-[/var/www/html/DVWA/config]
$ sudo service mysql start

(dvmatyushkin@dvmatyushkin)-[/var/www/html/DVWA/config]
$ sudo mysql -u root -p
Enter password:
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 user 'dvwa'@'127.0.0.1' identified by 'pass';
Query OK, 0 rows affected (0.005 sec)

MariaDB [(none)]> grant all privileges on dvwa.* to 'dvwa'@'127.0.0.1' identified by 'pass';
Query OK, 0 rows affected (0.005 sec)

```

Рис. 3.5: Новый пользователь БД

6. Откройте для редактирования файл php.ini в каталоге /etc/php/8.2/apache2,

чтобы включить следующие параметры: `allow_url_fopen` и `allow_url_include` (рис. 3.6).

```
; Whether to allow the treatment of URLs (like http:// or ftp://) as files.
; https://php.net/allow-url-fopen
allow_url_fopen = On

; Whether to allow include/require to open URLs (like https:// or ftp://) as files.
; https://php.net/allow-url-include
allow_url_include = On
```

Рис. 3.6: Редактирование файла `php.ini`

7. Запустите сервер Apache (рис. 3.7).

```
(dvmatyushkin@dvmatyushkin)-[/var/www/html/DVWA/config]
$ cd /etc/php/8.2/apache2

(dvmatyushkin@dvmatyushkin)-[/etc/php/8.2/apache2]
$ sudo mousepad php.ini

(dvmatyushkin@dvmatyushkin)-[/etc/php/8.2/apache2]
$ sudo service apache2 start

(dvmatyushkin@dvmatyushkin)-[/etc/php/8.2/apache2]
$
```

Рис. 3.7: Запуск `apache2`

8. Откройте DVWA в браузере, введя в адресной строке следующее: `127.0.0.1/DVWA/`. Прокрутите вниз и нажмите `Create / Reset Database` (Создать / сбросить базу данных). Это создаст базу данных, и через несколько секунд вы будете перенаправлены на страницу входа в DVWA (рис. 3.8).

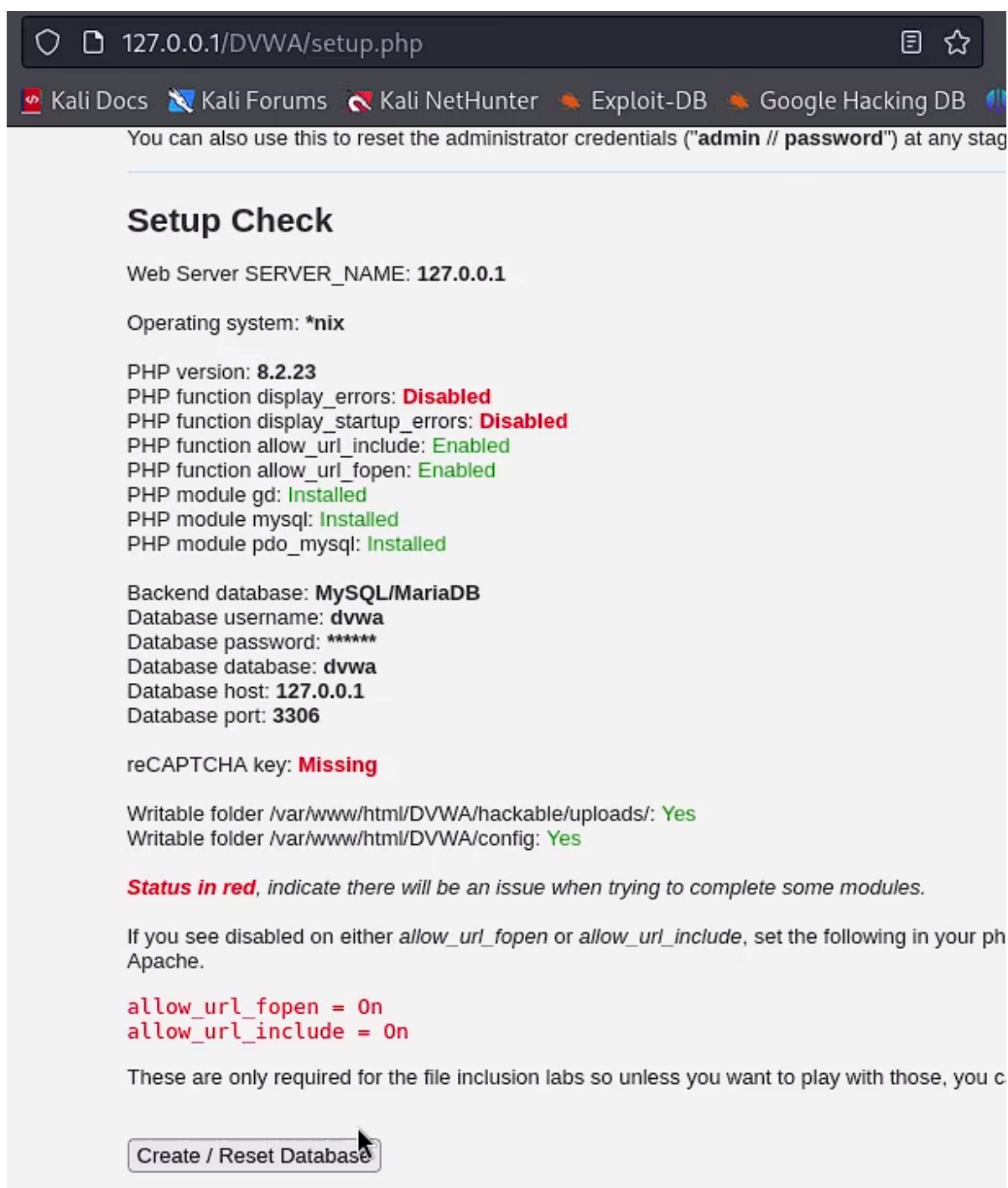


Рис. 3.8: Запуск dvwa

9. Войдите в учетную запись (рис. 3.9).

Username

Password

Рис. 3.9: Вход в dvwa

4 Выводы

В ходе данной лабораторной работы мы установили DVWA в гостевую систему к Kali Linux.

Список литературы

1. VirtualBox Documentation [Электронный ресурс]. Oracle, 2024. URL: <https://www.virtualbox.org/wiki/Documentation>.
2. Kali Official Documentation [Электронный ресурс]. Offensive Security, 2024. URL: <https://www.kali.org/docs/>.
3. Damn Vulnerable Web Application (DVWA) [Электронный ресурс]. DVWA team, 2023. URL: <https://github.com/digininja/DVWA>.