

Отчёт по 2-му этапу индивидуального проекта

Дисциплина: Информационная безопасность

Выполнил: Танрибергенов Эльдар

Содержание

1	Цель работы	4
2	Задания	5
3	Ход работы	6
4	Выводы	13

Список иллюстраций

3.1	Загрузка DVWA	6
3.2	Установка необходимых пакетов	6
3.3	Клонирование репозитория DVWA	6
3.4	Изменение имени и прав директории	6
3.5	Редактирование конфиг. файла	7
3.6	Редактирование конфиг. файла: задание имени и пароля пользователя	7
3.7	Конфигурирование apache2	7
3.8	Конфигурирование apache2	8
3.9	Запуск apache2	8
3.10	Проверка запуска apache2	8
3.11	Создание пользователя в базе данных	9
3.12	Предоставление пользователю всех привелегий	9
3.13	Открытие DVWA в браузере, создание/сброс базы данных	10
3.14	Вход от имени admin	11
3.15	Проверка brute force	11
3.16	Проверка brute force: результат	12
3.17	Проверка командной вставки	12

1 Цель работы

Установить DVWA в гостевую систему к Kali Linux и ознакомиться.

2 Задания

- Установить DVWA в гостевую систему к Kali Linux и ознакомиться.

3 Ход работы

```
[sudo] password for etanribergenov:
(root@etanribergenov)-[/home/etanribergenov]
# apt-get install dvwa
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following additional packages will be installed:
  libapache2-mod-php8.2 php8.2 php8.2-cli php8.2-common p
  php8.2-readline
Suggested packages:
```

Рис. 3.1: Загрузка DVWA

```
(root@etanribergenov)-[/home/etanribergenov]
# apt-get install -y apache2 mariadb-server mariadb-client php php-mysql php-gd libapache2-mod-php
Reading package lists... Done
Building dependency tree... Done
```

Рис. 3.2: Установка необходимых пакетов

```
(root@etanribergenov)-[/var/www/html]
# git clone https://github.com/digininja/DVWA.git
Cloning into 'DVWA' ...
remote: Enumerating objects: 4857, done.
remote: Counting objects: 100% (17/17), done.
remote: Compressing objects: 100% (13/13), done.
remote: Total 4857 (delta 5), reused 11 (delta 4), pack-reused 4840 (from 1)
Receiving objects: 100% (4857/4857), 2.43 MiB | 1.10 MiB/s, done.
Resolving deltas: 100% (2342/2342), done.
```

Рис. 3.3: Клонирование репозитория DVWA

```
(root@etanribergenov)-[/var/www/html/DVWA/config]
# cd /var/www/html
(root@etanribergenov)-[/var/www/html]
# mv DVWA dvwa
(root@etanribergenov)-[/var/www/html]
# chmod -R 777 dvwa
```

Рис. 3.4: Изменение имени и прав директории

```

(root@etanribergenov)-[/var/www/html]
# cd DVWA/config

(root@etanribergenov)-[/var/www/html/DVWA/config]
# cp config.inc.php.dist config.inc.php

(root@etanribergenov)-[/var/www/html/DVWA/config]
# nano config.inc.php

```

Рис. 3.5: Редактирование конфиг. файла

```

root@etanribergenov: /var/www/html/dvwa/config
File Actions Edit View Help
GNU nano 8.1 config.inc.php *
<?php

# If you are having problems connecting to the MySQL database and all of the variables
# try changing the 'db_server' variable from localhost to 127.0.0.1. Fixes a problem d
# Thanks to @diginiinja 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
# Please use a database dedicated to DVWA.
#
# If you are using MariaDB then you cannot use root, you must use create a dedicated D
# 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') ?: 'etanribergenov';
$_DVWA['db_password'] = getenv('DB_PASSWORD') ?: 'pass';
$_DVWA['db_port'] = getenv('DB_PORT') ?: '3306';

# ReCAPTCHA settings

```

Рис. 3.6: Редактирование конфиг. файла: задание имени и пароля пользователя

```

(root@etanribergenov)-[/var/www/html/DVWA/config]
# cd /etc/php/8.2/apache2

(root@etanribergenov)-[/etc/php/8.2/apache2]
# mousepad php.ini

```

Рис. 3.7: Конфигурирование apache2

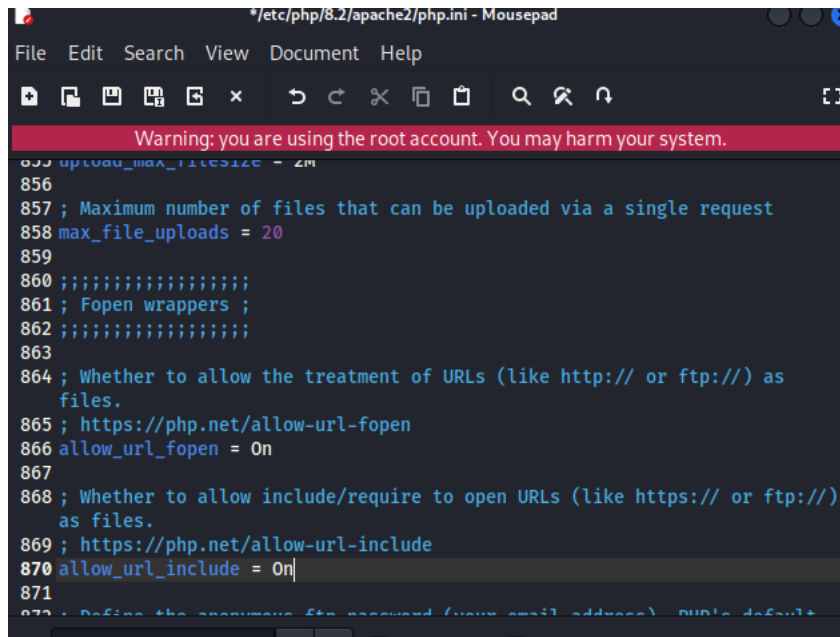


Рис. 3.8: Конфигурирование apache2

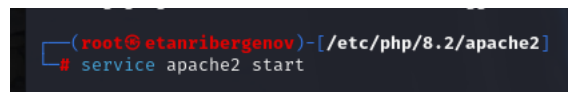


Рис. 3.9: Запуск apache2

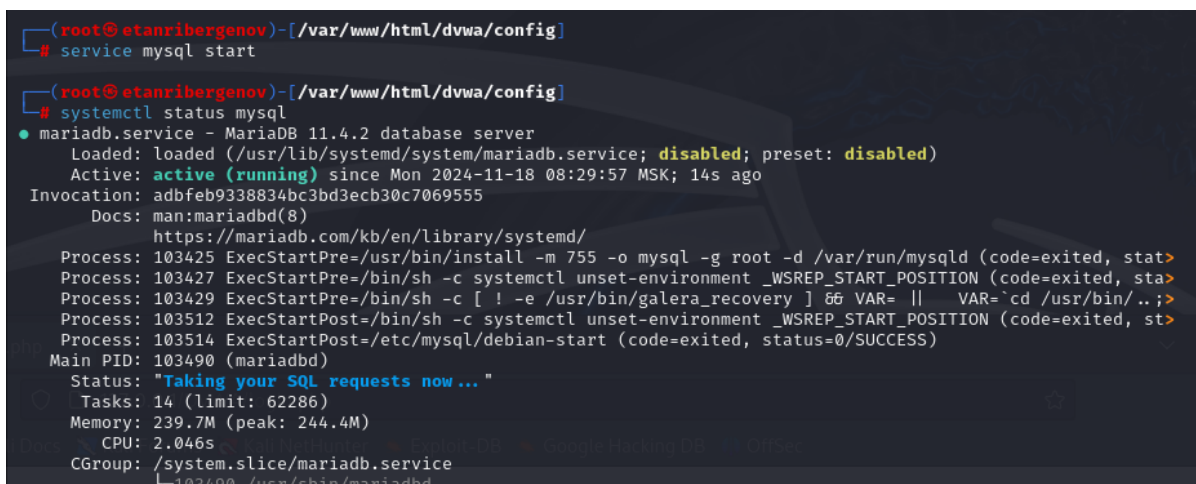


Рис. 3.10: Проверка запуска apache2


```
root@etanribergenov: ~/var/www/html/dvwa/config
# mysql -u root -p
Enter password:
Welcome to the MariaDB monitor.  Commands end with ; or \g.
Your MariaDB connection id is 31
Server version: 11.4.2-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 user 'etanribergenov'@'127.0.0.1' identified by 'pass';
Query OK, 0 rows affected (0.008 sec)

MariaDB [(none)]> █
```

Рис. 3.11: Создание пользователя в базе данных

```
MariaDB [(none)]> grant all privileges on dvwa.* to 'etanribergenov'@'127.0.0.1' identified by 'pass';
Query OK, 0 rows affected (0.007 sec)

MariaDB [(none)]> █
```

Рис. 3.12: Предоставление пользователю всех привелегий

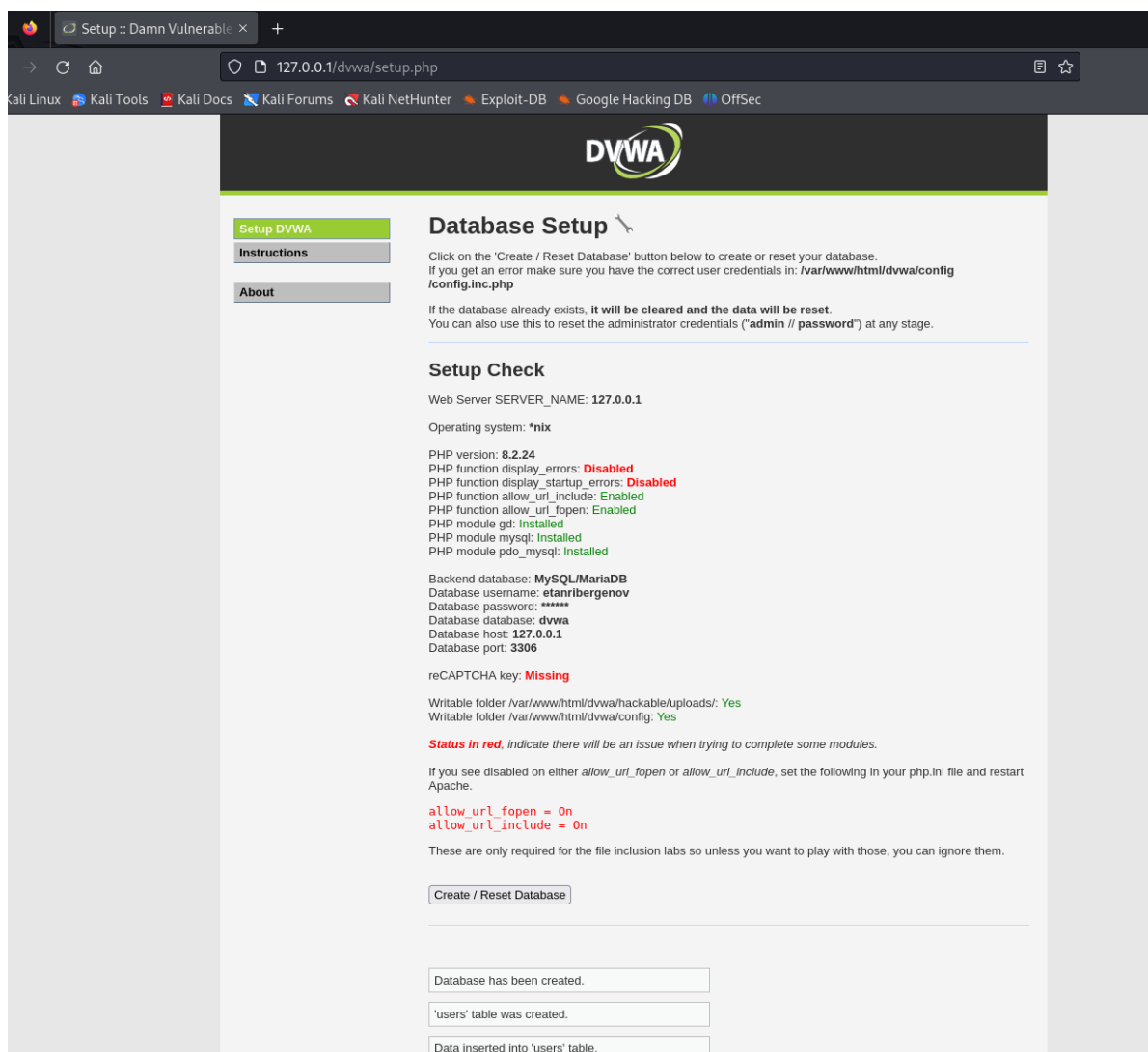


Рис. 3.13: Открытие DVWA в браузере, создание/сброс базы данных

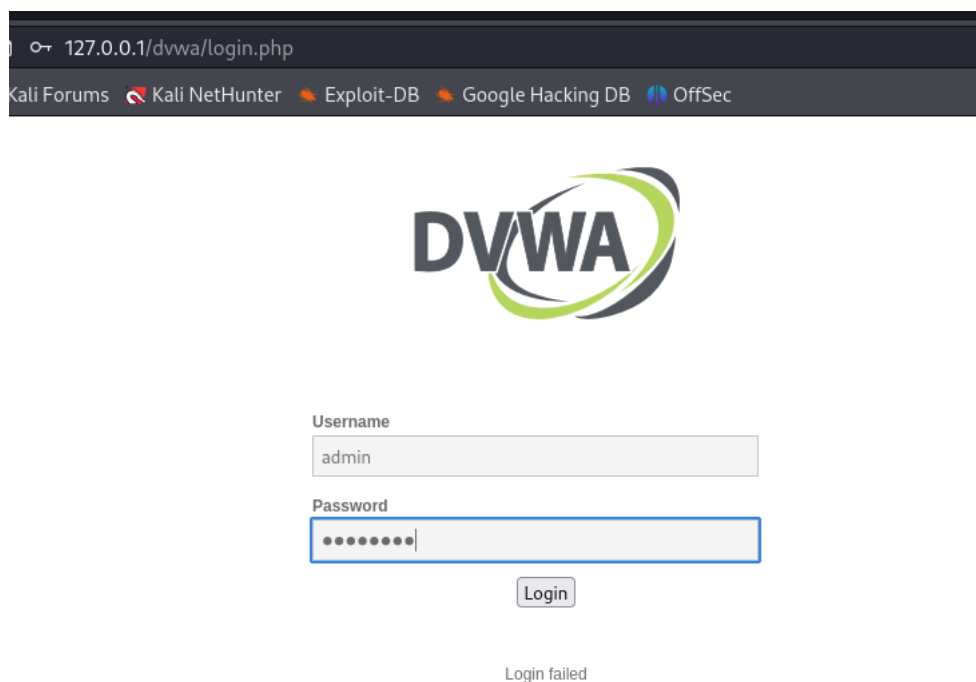


Рис. 3.14: Вход от имени admin

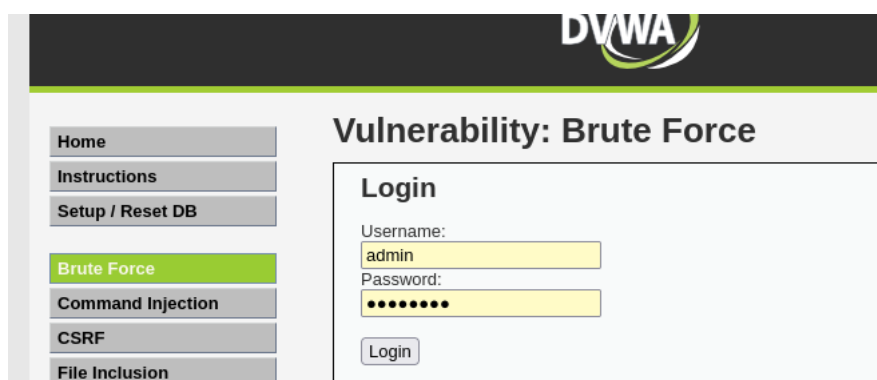


Рис. 3.15: Проверка brute force

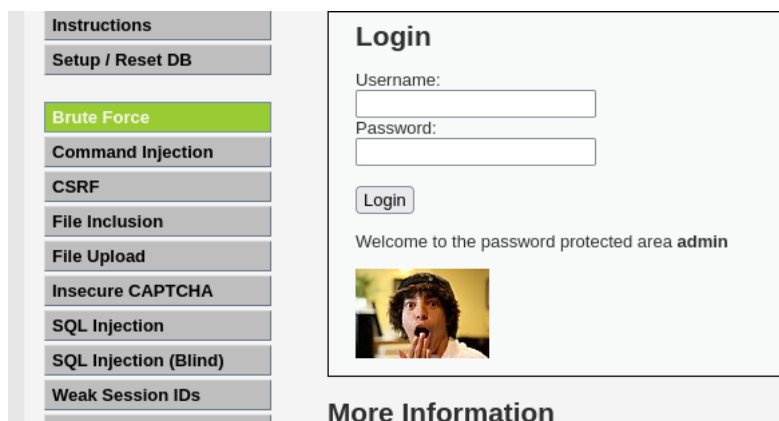


Рис. 3.16: Проверка brute force: результат

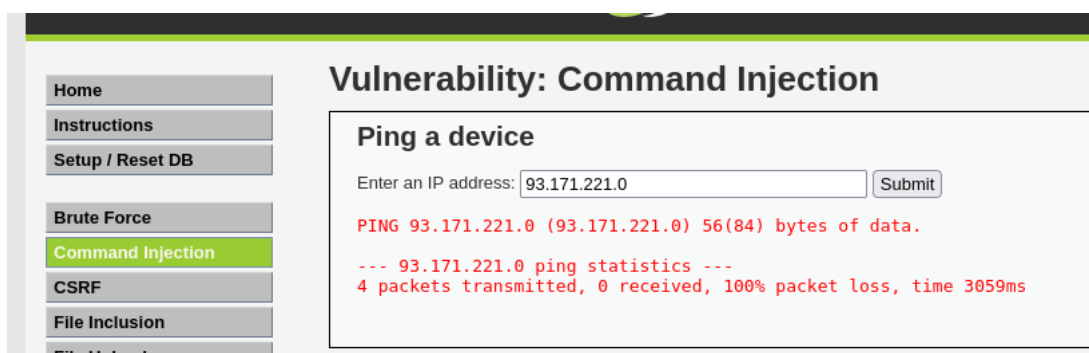


Рис. 3.17: Проверка командной вставки

4 Выводы

В результате выполнения работы я ознакомился с DVWA, установив в гостевую систему к Kali Linux.