

Отчет по второму этапу индивидуального проекта

Основы информационной безопасности

Ищенко Ирина НПИбд-02-22

Содержание

1	Цель работы	5
2	Выполнение лабораторной работы	6
3	Выводы	13
	Список литературы	14

Список иллюстраций

2.1	Клонирование репозитория	6
2.2	Содержимое файла конфигурации	7
2.3	Обновление системы	7
2.4	Установка	8
2.5	Создание базы данных	9
2.6	Создание базы данных	9
2.7	Параметры сервера Apache	10
2.8	Запуск сервера	11
2.9	Страница настройка DVWA Kali Linux	11
2.10	Страница входа DVWA Kali Linux	12
2.11	Меню	12

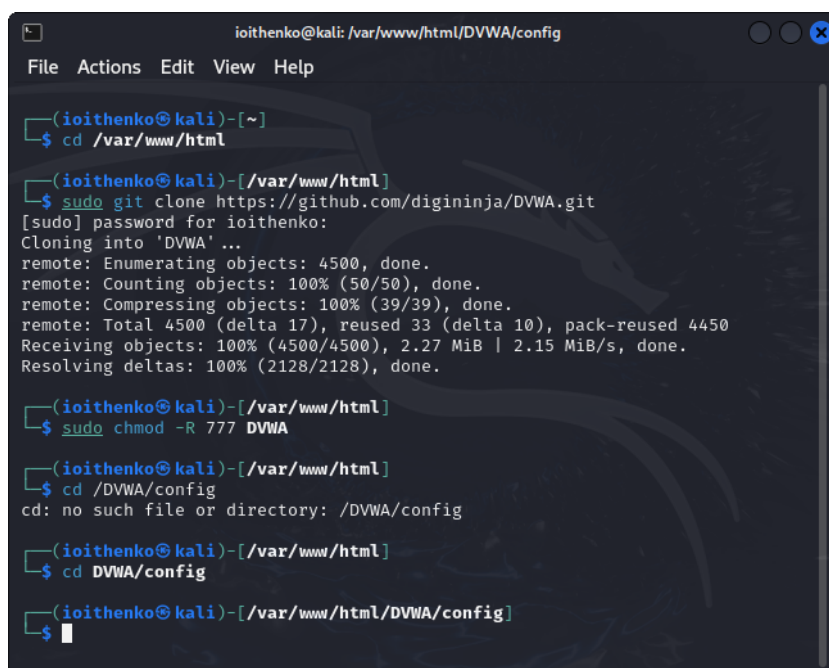
Список таблиц

1 Цель работы

Установка DVWA сервиса на Kali Linux [1].

2 Выполнение лабораторной работы

Перейдем в каталог html: `cd /var/www/html` Клонировать репозиторий git: `sudo git clone https://github.com/digininja/DVWA.git` Изменим права доступа к папке установки: `sudo chmod -R 777 DVWA` Перейдем к файлу конфигурации в каталоге установки (рис. 2.1): `cd DVWA/config`



```
ioithenko@kali: /var/www/html/DVWA/config
File Actions Edit View Help

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

(ioithenko@kali)-[/var/www/html]
$ sudo git clone https://github.com/digininja/DVWA.git
[sudo] password for ioithenko:
Cloning into 'DVWA' ...
remote: Enumerating objects: 4500, done.
remote: Counting objects: 100% (50/50), done.
remote: Compressing objects: 100% (39/39), done.
remote: Total 4500 (delta 17), reused 33 (delta 10), pack-reused 4450
Receiving objects: 100% (4500/4500), 2.27 MiB | 2.15 MiB/s, done.
Resolving deltas: 100% (2128/2128), done.

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

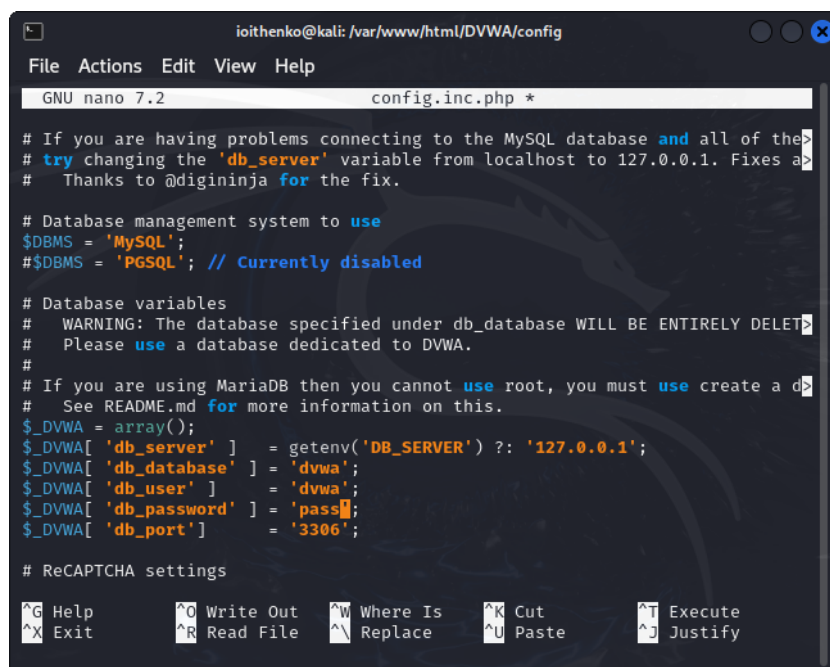
(ioithenko@kali)-[/var/www/html]
$ cd /DVWA/config
cd: no such file or directory: /DVWA/config

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

(ioithenko@kali)-[/var/www/html/DVWA/config]
$
```

Рис. 2.1: Клонирование репозитория

Скопируем файл конфигурации и переименуем его: `cp config.inc.php.dist config.inc.php` Откроем файл настроек и изменили пароль на `pass` (рис. 2.2): `sudo nano config.inc.php` На следующем снимке экрана показано содержимое файла конфигурации, включая всю информацию о базе данных:



```
ioithenko@kali: /var/www/html/DVWA/config
File Actions Edit View Help
GNU nano 7.2 config.inc.php *

# If you are having problems connecting to the MySQL database and all of the
# try changing the 'db_server' variable from localhost to 127.0.0.1. Fixes a
# Thanks to @digininja for the fix.

# Database management system to use
$DBMS = 'MySQL';
#$DBMS = 'PGSQL'; // Currently disabled

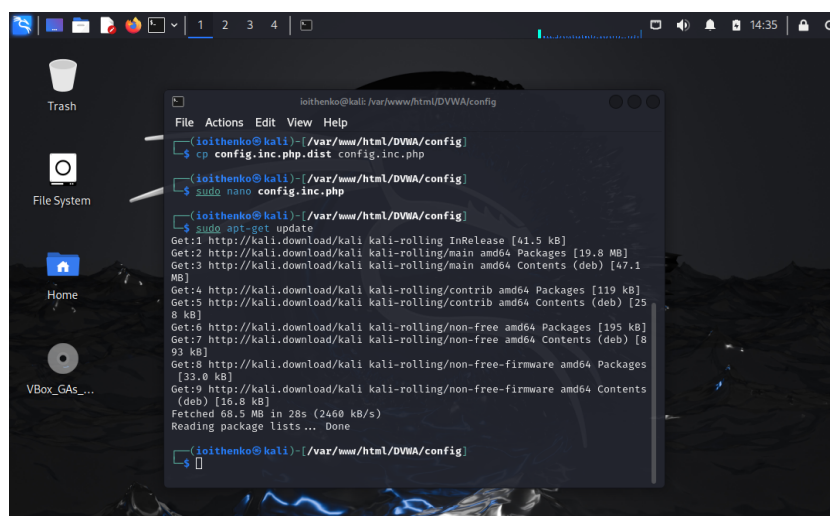
# Database variables
# WARNING: The database specified under db_database WILL BE ENTIRELY DELETED
# Please use a database dedicated to DVWA.
#
# If you are using MariaDB then you cannot use root, you must create a database
# See README.md for more information on this.
$_DVWA = array();
$_DVWA[ 'db_server' ] = getenv( 'DB_SERVER' ) ?: '127.0.0.1';
$_DVWA[ 'db_database' ] = 'dvwa';
$_DVWA[ 'db_user' ] = 'dvwa';
$_DVWA[ 'db_password' ] = 'passw0rd';
$_DVWA[ 'db_port' ] = '3306';

# ReCAPTCHA settings

^G Help      ^O Write Out  ^W Where Is   ^K Cut        ^T Execute
^X Exit      ^R Read File  ^N Replace    ^U Paste      ^J Justify
```

Рис. 2.2: Содержимое файла конфигурации

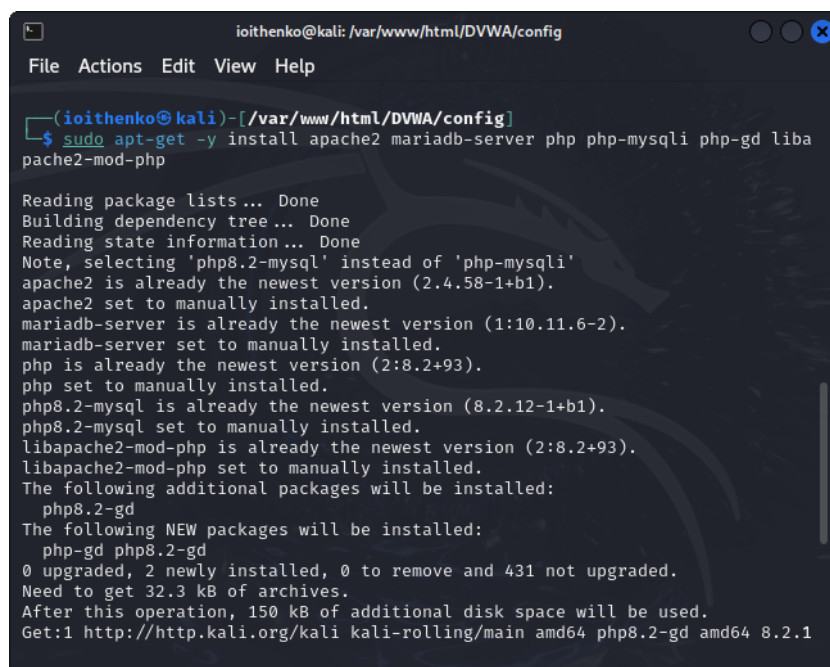
Установим mariadb, предварительно обновив систему (рис. 2.3) и (рис. 2.4): `sudo apt-get update`



```
ioithenko@kali: /var/www/html/DVWA/config
File Actions Edit View Help
(ioithenko@kali)-[ /var/www/html/DVWA/config ]
$ cp config.inc.php.dist config.inc.php
(ioithenko@kali)-[ /var/www/html/DVWA/config ]
$ sudo nano config.inc.php
(ioithenko@kali)-[ /var/www/html/DVWA/config ]
$ sudo apt-get update
Get:1 http://kali.download/kali kali-rolling InRelease [41.5 kB]
Get:2 http://kali.download/kali kali-rolling/main amd64 Packages [19.8 MB]
Get:3 http://kali.download/kali kali-rolling/main amd64 Contents (deb) [47.1 MB]
Get:4 http://kali.download/kali kali-rolling/contrib amd64 Packages [119 kB]
Get:5 http://kali.download/kali kali-rolling/contrib amd64 Contents (deb) [25 8 kB]
Get:6 http://kali.download/kali kali-rolling/non-free amd64 Packages [195 kB]
Get:7 http://kali.download/kali kali-rolling/non-free amd64 Contents (deb) [8 93 kB]
Get:8 http://kali.download/kali kali-rolling/non-free-firmware amd64 Packages [33.0 kB]
Get:9 http://kali.download/kali kali-rolling/non-free-firmware amd64 Contents (deb) [16.8 kB]
Fetched 68.5 MB in 28s (2460 kB/s)
Reading package lists... Done
(ioithenko@kali)-[ /var/www/html/DVWA/config ]
$
```

Рис. 2.3: Обновление системы

`sudo apt-get -y install apache2 mariadb-server php php-mysql php-gd libapache2-mod-php`



```
ioithenko@kali: /var/www/html/DVWA/config
File Actions Edit View Help

(ioithenko@kali)-[/var/www/html/DVWA/config]
$ sudo apt-get -y install apache2 mariadb-server php php-mysqli php-gd liba
pache2-mod-php

Reading package lists ... Done
Building dependency tree ... Done
Reading state information ... Done
Note, selecting 'php8.2-mysql' instead of 'php-mysqli'
apache2 is already the newest version (2.4.58-1+b1).
apache2 set to manually installed.
mariadb-server is already the newest version (1:10.11.6-2).
mariadb-server set to manually installed.
php is already the newest version (2:8.2+93).
php set to manually installed.
php8.2-mysql is already the newest version (8.2.12-1+b1).
php8.2-mysql set to manually installed.
libapache2-mod-php is already the newest version (2:8.2+93).
libapache2-mod-php set to manually installed.
The following additional packages will be installed:
  php8.2-gd
The following NEW packages will be installed:
  php-gd php8.2-gd
0 upgraded, 2 newly installed, 0 to remove and 431 not upgraded.
Need to get 32.3 kB of archives.
After this operation, 150 kB of additional disk space will be used.
Get:1 http://http.kali.org/kali kali-rolling/main amd64 php8.2-gd amd64 8.2.1
```

Рис. 2.4: Установка

Запустим базу данных: `sudo service mysql start` Войдем в базу данных (пароля нет, поэтому просто нажмем Enter при появлении запроса): `sudo mysql -u root -p` Создадим пользователя базы данных. Нужно использовать те же имя пользователя и пароль, которые использовались в файле конфигурации (см. скрин выше) (рис. 2.5): `create user 'dvwa'@'127.0.0.1' identified by 'pass';`


```
ioithenko@kali: /var/www/html/DVWA/config
File Actions Edit View Help

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

(ioithenko@kali)-[/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: 10.11.6-MariaDB-2 Debian n/a

Copyright (c) 2000, 2018, Oracle, MariaDB Corporation Ab and others.

Type 'help;' or '\h' for help. Type '\c' to clear the current input statement
.

MariaDB [(none)]>
MariaDB [(none)]> 1
→ create user 'user'@'127.0.0.1' identified by 'pass';
ERROR 1064 (42000): You have an error in your SQL syntax; check the manual that corresponds to your MariaDB server version for the right syntax to use near '1'
MariaDB [(none)]> create user 'user'@'127.0.0.1' identified by 'pass';
Query OK, 0 rows affected (0.005 sec)

MariaDB [(none)]> 
```

Рис. 2.5: Создание базы данных

Предоставим пользователю все привилегии (рис. 2.6): `grant all privileges on dvwa.* to 'dvwa'@'127.0.0.1' identified by 'pass';`; Результат этих операций с базой данных должен выглядеть так

```
ioithenko@kali: /var/www/html/DVWA/config
File Actions Edit View Help

zsh: suspended sudo mysql -u root -p

(ioithenko@kali)-[/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 48
Server version: 10.11.6-MariaDB-2 Debian n/a

Copyright (c) 2000, 2018, Oracle, MariaDB Corporation Ab and others.

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 (0.054 sec)

MariaDB [(none)]> grant all privileges on dvwa.* to 'dvwa'@'127.0.0.1' identified by 'pass';
Query OK, 0 rows affected (0.052 sec)

MariaDB [(none)]> exit
Bye

(ioithenko@kali)-[/var/www/html/DVWA/config]
$ 
```

Рис. 2.6: Создание базы данных

Пришло время перейти в каталог apache2 для настройки сервера Apache: `cd /etc/php/8.2/apache2` Откроем для редактирования файл `php.ini`, чтобы включить следующие параметры: `allow_url_fopen` и `allow_url_include` (рис. 2.7): `sudo mousepad php.ini`

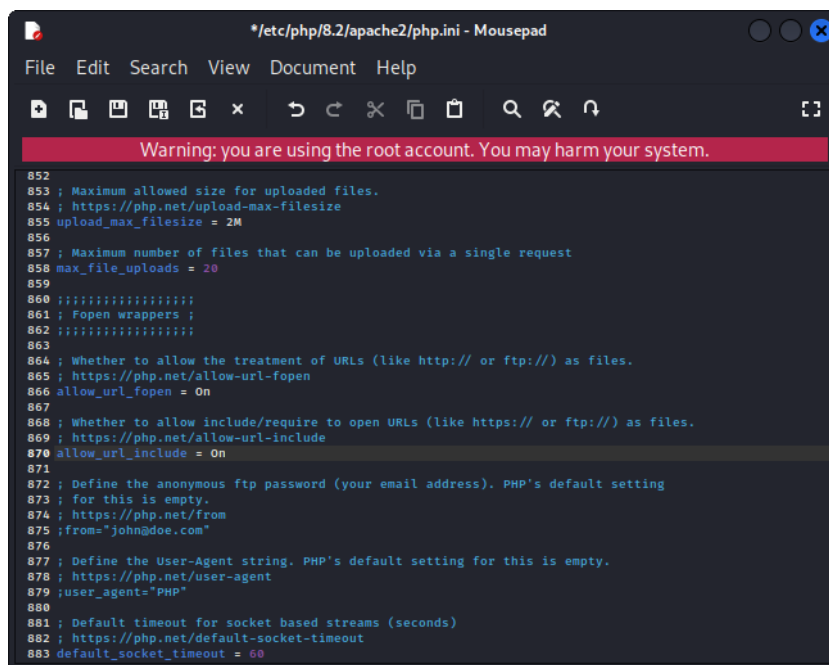
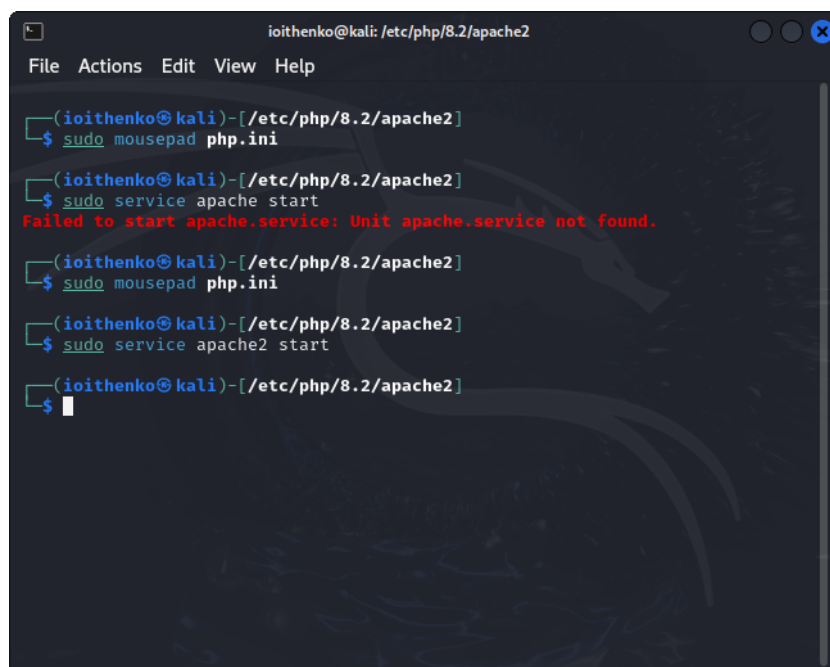


Рис. 2.7: Параметры сервера Apache

Настройка DVWA Kali Linux. Параметры сервера Apache

Запустив сервер Apache (рис. 2.8): `sudo service apache2 start`



```
ioithenko@kali: /etc/php/8.2/apache2
File Actions Edit View Help

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

(ioithenko@kali)-[/etc/php/8.2/apache2]
$ sudo service apache start
Failed to start apache.service: Unit apache.service not found.

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

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

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

Рис. 2.8: Запуск сервера

Открываем DVWA в браузере, введя в адресной строке следующее: 127.0.0.1/DVWA/ Если открылась страница настройки, это означает, что вы успешно установили DVWA на Kali Linux (рис. 2.9):

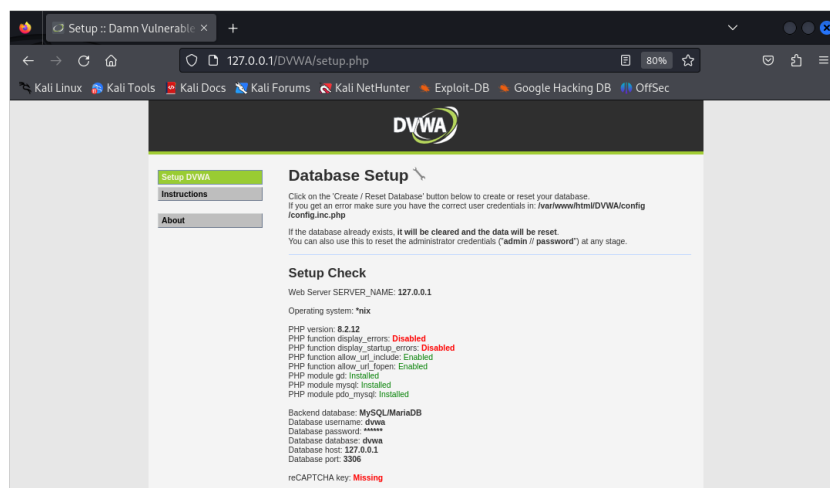


Рис. 2.9: Страница настройка DVWA Kali Linux

Прокрутив вниз и нажав Create / Reset Database (Создать / сбросить базу данных). Это создаст базу данных, и через несколько секунд вы будете перенаправ-

лены на страницу входа в DVWA (рис. 2.10):

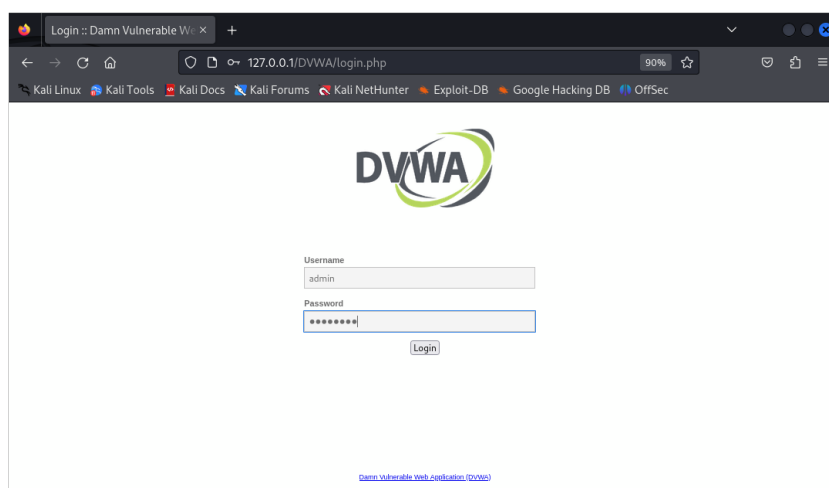


Рис. 2.10: Страница входа DVWA Kali Linux

Введем следующие учетные данные:

admin password

Как видно на следующем снимке экрана, существует множество интересных уязвимостей, которые можно протестировать, например, брутфорс, SQL-инъекция и другие (рис. 2.11) [2]:

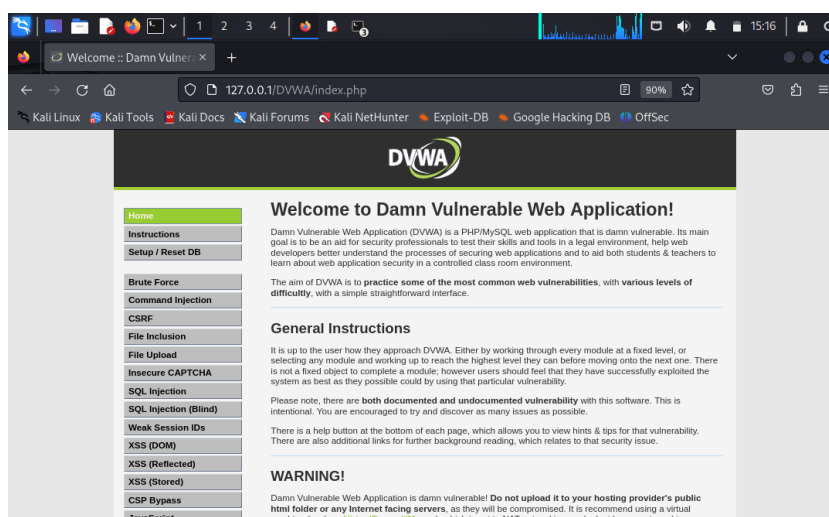


Рис. 2.11: Меню

3 Выводы

В ходе данного этапа проекта я установила DVWA сервер на Kali Linux.

Список литературы

1. Ш. Парасрам Т.Х. А. Замм. Kali Linux: Тестирование на проникновение и безопасность. 4-е изд. Санкт-Петербург: Питер, 2022. 448 с.
2. Установка и использование DVWA на Kali Linux.